2012

A method for securing online community service: A study of selected Western Australian councils

Sunsern Limwiriyakul
Edith Cowan University

Edith Cowan University

Copyright Warning

Edith Cowan University

A Method for Securing Online Community Service : A Study of Selected Western Australian Councils

A thesis submitted in partial fulfillment of the requirements

for the degree of

Doctor of Information Technology

By

Sunsern Limwiriyakul

Principal Supervisor: Professor Craig Valli
Associate Supervisor: Dr. Andrew Woodward

2012

School of Computer and Security Science
Faculty of Computing, Health and Science
Edith Cowan University, Western Australia

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

ABSTRACT

Since the Internet was made publicly accessible, it has become increasingly popular and its deployment has been broad and global thereby facilitating a range of available online services such as Electronic Mail (email), news or bulletins, Internet Relay Chat (IRC) and World Wide Web (WWW). Progressively, other online services such as telephony, video conference, video on demand, Interactive Television (ITV) and Geographic Information System (GIS) have been integrated with the Internet and become publicly available.

Presently, Internet broadband communication services incorporating both wired and wireless network technologies has seen the emergence of the concept of a digital community which has been growing and expanding rapidly around the world. Internet and the ever expanding online services to the wider digital community has raised the issue of security of these services during usage. Most local councils throughout Western Australia have resorted to delivering online services such as library, online payments and email accessibility. The provision and usage of these services have inherent security risks. Consequently, this study investigated the concept of a secure digital community in the secure provision and usage of these online services in selected local councils in Western Australia (WA).

After an extensive review of existing literature, information security frameworks were derived from the adaptation of various resources, such as the OSSTMM 2.2 Section C: Internet Technology Security benchmark which was used as the main template. In addition, this template was enhanced into a framework model by incorporating other benchmarks such as NIST, CIS, ISSAF as well as other sources of information. These included information security related books, related ICT network and security websites such as CERT, CheckPoint, Cisco, GFI, Juniper, MS, NESSUS and NMAP together with journals and personal interviews. The proposed information security frameworks were developed to enhance the level of security strength of the email and online web systems as well as to increase the level of confidence in the system security within the selected local councils in WA. All the investigative studies were based upon the available selected local councils' data and the associated analyses of the results as obtained from the testing software. In addition, the interpretive multiple-case study

principles were used during the investigation to achieve or fulfil the purpose of this study. The findings from this study were then abstracted for use in a framework and made available for use as a model for possible adaptation and implementation to other similarly structured councils or organisations.

As a result, the study confirmed that the proposed information security frameworks have the capability and potential to improve the level of security strength. In addition, the level of satisfaction and confidence of council staff of the selected local councils in WA in the system security would also be increased due to the application of these frameworks.

Although these information security frameworks may be recommended as practical and supporting tools for local councils, the findings from this study were specific only to the selected local councils used in this study. Further research using other councils, may be necessary in order for the information security frameworks to be adopted within a wider range of councils or organisations in WA or elsewhere.

DECLARATION

I certify that the thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;

(ii) contain any material previously published or written by another person except where due reference is made in the text of this thesis;

(iii) contain any defamatory material;. or

(iv) contain any data that has not been collected in a manner consistent with ethics approval.

I also grant permission for the Library at Edith Cowan University to make duplicate copies of my thesis as required.

Student signature
Date ..... 3/2/12 .....

Principal supervisor signature
Date ..... 3/2/12 .....

Associate supervisor signature
Date ..... 3/2/12 .....

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to all those involved in providing me with tremendous support, guidance and encouragement during my DIT study. My sincere appreciation is extended to all those who dedicated their time to help bring this undertaking to a conclusion. Their efforts far surpassed my every expectation. My admiration has grown for all those who devoted their time, efforts, knowledge, generosity and patience to assist me to accomplish this very arduous DIT study.

I would like to express my special thanks first to my principal, associate supervisor and internal reviewer, Professor. Craig Valli, Dr. Andrew Woodward and Associate Professor Ken Fowle respectively. I am heartily grateful to them for their encouragement, supervision and continuous support from the initial to the final stages that enabled me to complete this DIT degree.

In addition, I would like to offer my sincere gratitude and appreciation to Dr. Panida Subsorn and Mr. Yunous Vagh for their support, valuable advice, time and innumerable useful guidance sessions and discussions, which have significantly enhanced the achievement of my DIT study. Furthermore, I would like to extend my sincere thanks to Edith Cowan University and my family for financial support while working on my DIT study. In addition, I would like to thank the selected local councils in Western Australia for their kind assistance in data gathering and for their acceptance of being involved as case studies.

Finally, I am also immensely grateful to have a fabulous family. I greatly thank them for their tireless encouragements, enduring love and wholehearted support throughout my DIT study. My sincerest thankfulness to my beloved father, mother and sister for continually being supportive and for providing the essential occasional distraction from my DIT study, during the time this thesis has taken to bring to completion.

LIST OF PUBLICATIONS

Limwiriyakul, S. (2009). Method for Securing Online Community Service: A Study of Selected Western Australian Councils. *Proceedings of the Seventh Australian Information Security Management Conference (SECAU 2009)*. Perth: Western Australia.

Limwiriyakul, S. & Valli, C. (2011). An IT security investigation into the email systems of selected local government councils in WA. *Proceedings of the 2011 International Conference on Information and Electronics Engineering (ICIEE 2011)*. Bangkok, Thailand.

Limwiriyakul, S. & Valli, C. (2011). Results from the deployment of a targeted security testing framework for the testing of email systems in local government in Western Australia. *International Journal of Information and Electronics Engineering (IJIEE)*, 1 (1), 16-22.

Limwiriyakul, S. & Valli, C. (2011). An IT security investigation into the online payment systems of selected local government councils in WA. *Proceedings of the 2011 International Conference on Security and Management* (*SAM'11)*. Las Vegas, Nevada, USA.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

LIST OF ACRONYMS

AAA	Authentication, Authorization and Accounting
ABS	Australian Bureau of Statistics
ACL	Access Control List
AD	Active Directory
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AS/NZ	Australia/New Zealand
ASAP	As Soon As Possible
ASP	Active Server Page
BPDU	Bridge Protocol Data Unit
CAS	Client Access Server
CERT	Computer Emergency Response Team
CIS	Center for Internet Security
CMS	Content Management System
CPU	Central Processing Unit
DDE	Dynamic Data Exchange
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DESX	Data Encryption Standard XORed
DHCP	Dynamic Host Configuration Protocol
DI	Deep Inspection
DMZ	Demilitarised Zone
DNS	Domain Name Server
DoS	Denial of Service
DSL	Digital Subscriber Line
DSN	Database Source Name or Delivery Status Notification???
DSProxy	Directory Service Proxy
DTP	Data Tools Platform
Email	Electronic Mail
ESMTP	Extended SMTP
EWS	Exchange Web Services
FTP	File Transfer Protocol
GB	Gigabyte
GDR	Grant, Deny and Revoke
GIS	Geographic Information System
GPS	Global Positioning System
GUI	Graphical User Interface
GW	Gateway
HDD	Hard Disk Drive
HSRP	Hot Standby Router Protocol
HTML	Hypertext Markup Language

HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
ID	Identity
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IEC	The International Electrotechnical Commission
IIS	Internet Information Services
IMAP	Internet Message Access Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion Prevention System
IS	Information Systems
ISA	Internet Security and Acceleration
ISO	The International Organization for Standardization
ISP	Internet Service Provider
ISSAF	The Information Systems Security Assessment Framework
IT	Information Technology
KB	Kilobyte
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
MD5	Message-Digest Algorithm 5
MIP	Mapped Internet Protocol
MP3	MPEG-1 or MPEG-2 Audio Layer III
MS	Microsoft
MS ESMTP	Microsoft ESMTP
MS-DS	Microsoft-DS
MSRPC	Microsoft Remote Procedure Call
N/A	Not Applicable
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NIST	The National Institute of Standards and Technology
NMAP	Network Mapper
NSPI	Name Service Provider Interface
NTFS	New Technology File System
NTLM	NT LAN Manager
NTP	Network Time Protocol
OAB	Offline Address Book
OS	Operating System
OSI	Open Systems Interconnection
OSSTMM	The Open Source Security Testing Methodology Manual
OWA	Outlook Web App/Outlook Web Access
OWASP	The Open Web Application Security Project

PAT	Port Address Translation
PDF	Portable Document Format
PHP	Hypertext Preprocessor
PIM	Physical Interface Module
PoE	Power over Ethernet
POP	Post Office Protocol
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RC	Rivest Cipher
RDP	Remote Desktop Protocol
RPC	Remote Procedure Call
RSA	Rivest Shamir Adleman
SATA	Serial Advanced Technology Attachment
SBS	Small Business Server
SCSI	Small Computer System Interface
SDK	Software Development Kit
SFP	Small Form-Factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNMPTRAP	Simple Network Management Protocol Trap
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSG	Secure Services Gateway
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDDI	Universal Description, Discovery, and Integration
UDP	The User Datagram Protocol
UM	Unified Messaging
UNC	Universal Naming Convention
UPS	Uninterruptible Power Supply/Uninterruptible Power Source
URL	Uniform Resource Locator
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMware	Simple Standard Virtual Server
VoIP	Voice over Internet Protocol
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VTP	VLAN Trunking Protocol
WA	Western Australia

WALGA	The Western Australian Local Government Association
WAN	Wide Area Network
WCMS	Web Content Management System
WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation
WSDL	Web Services Description Language
WSS	Windows SharePoint Services
WWW	World Wide Web
XML	Extensible Markup Language
XSS	Cross-Site Scripting

CHAPTER 1. INTRODUCTION

1.1 Background to the research

In the preceding decades, a number of nations worldwide have increasingly availed themselves of advances in Information and Communication Technologies (ICT), particularly in Internet technologies as a key business component in various organisations (Al-Mashari, 2007; Steyaert, 2000). This is mainly due to the pervasiveness, popularity and usage diversity of the Internet. These factors have prompted various public and private organisations to adjust their business strategies in the achievement of their goals (Teece, 2010). The advent of Internet technologies, as a component of ICT tools, has enabled most government and commercial organisations to adjust to the change of making a worldwide business presence through its powerful capabilities (Reddick, 2005; Shan & Wang, 2009).

Additionally, ICT has been considered as an information competence tool as it provides information and related services, and supports interaction and cooperation among the users (Pazalos et al., 2010). The increasing availability of high speed Internet broadband communications infrastructure is an enabler of communication. Distribution of information and knowledge for both government and non-government sectors have become highly interactive and dynamic as a characteristic of the global digital community (Gillett et al., 2004; Ishida, 2003; Limwiriyakul, 2009; Limwiriyakul & Valli, 2011a, b, c; Ortiz & Tapia, 2008a, b; Pazalos et al., 2010; Tanabe et al., 2002; Tapia et al., 2006).

According to Intel Corporation (2005a, b, c), a “digital community” is a connected community or social networking entity which uses the Internet communication and computing infrastructure to provide flexible and innovative services to respond to users’ demands (Limwiriyakul, 2009; Limwiriyakul & Valli, 2011a, b, c). Therefore, most significant cities around the world have made large investments of money for the development of large network infrastructures to facilitate high-speed connections for the online service of their local public and private organisations (Gillett et al., 2004; Ishida, 2003; Ortiz & Tapia, 2008a, b; Pazalos et al., 2010; Tanabe et al., 2002; Tapia et al., 2006).

Specifically, government organisations have engaged the above mentioned technologies in providing additional Information Technology (IT)-based development facilitators to commence and supply online information and services to their residences (in the case of local government councils) and partnerships (Al-Mashari, 2007; Shan & Wang, 2009; Torres et al., 2005). This facilitation may enhance a level of service satisfaction, ease of access, correctness, confidentiality, effectiveness within governments and partnerships, provide rapid and better services delivery, promote their recent products and services, and diminish service costs (Abie et al., 2004; Al-Mashari, 2007; Hirwade, 2010). As a result, their residences and partnerships may have increased and better electronic communication with their local and national governments and increase the knowledge of the general populace (Shan & Wang, 2009).

The values aforementioned produce a suitable background to this research as they present the potential benefits to engage in research that may be useful for broader implementation scope or practitioners in similar or dissimilar circumstances and societies. These benefits include the developed approaches and methods as recommendations for future revisions or improvements for successfully operating their correlated initiatives in an efficient manner. This research therefore commenced with the intention of analysing three reported case studies of electronic systems in government organisations for cyber security. The particular emphasis was on email and online web systems in order to investigate and reveal the factors which have impacted upon these systems and their security. An additional aim of the research was to search for solutions to provide performance efficiency for these systems.

1.2 Background to the statement of the problem

The amount of users employing online services via Internet technologies have been increasing recently (Australian Communications and Media Auhtority, 2008; Phiri & Agbinya, 2006). Most countries have been utilising online services in recent decades and attempting to find an effective method to deal with the security and privacy of their users (Economic Commission for Africa, 2003; Paul et al., 2011; Phiri & Agbinya, 2006). Nevertheless, Internet users are continually at risk, as they may have a credible chance of being attacked and are easily vulnerable to outside attackers or hackers (Farahmand et al., 2003; Farahmand et al., 2005).

Consequently, this may impact directly or indirectly on the current unsecured network communications for the security and privacy of the users or service providers. This may result in increased prevention and protection costs in terms of maintenance, upgrades and performance issues for the providers.

With the continual development of new technology in ICT, the Internet has currently become one of the quickest growing global network technologies (Al-Ahmad & Al-Kaabi, 2008). However, its usage comes with major concerns in security, trust and privacy for public and private organisations, as it relates directly to the online exchange of personal, organisational or financial data or information (Kim et al., 2006; Limwiriyakul, 2009; Limwiriyakul & Valli, 2011a, b, c). Therefore, a well-secured network system is considered a good solution for preventing and protecting unexpected attacks, and to enhance privacy and security for the assurance of a degree of confidentiality in Internet usage (Hwang et al., 2004; Kim et al., 2006).

Particularly, the World Wide Web (WWW) and email are the most well-known Internet technologies that are being used in most councils in Western Australia (WA) (Limwiriyakul, 2009; Limwiriyakul & Valli, 2011a, b, c; WALGA, 2010a). Nevertheless, there are other Internet related or convergence technologies that have been employed in several councils in WA such as Voice over Internet Protocol (VoIP), Voice over Wireless Local Area Network (VoWLAN), wireless LAN, Geographic Information System (GIS), Global Positioning System (GPS) and digital radio (Limwiriyakul, 2009; Limwiriyakul & Valli, 2011a, b, c; personal communications with the local councils in WA, 2005, 2006, 2007, 2008, 2009).

These technologies provide services such as online payment, online library services, security patrol, digital surveillance, telephony (VoIP), online GIS and Internet café to local government employees, residents and community groups. As the digital community concept starts to develop, Internet related services will be more widely available to the public. Electronic voting, electronic polling, electronic health and Internet radio are all examples of services to the digital community.

In addition, security is one of the most important factors for the digital community as it must ensure confidentiality and privacy of users' information over the Internet (Intel Corporation, 2005a, b, c; Limwiriyakul, 2009; Limwiriyakul & Valli, 2011a, b, c).

Therefore, this research is aimed to analyse and test the security of common Internet technologies which are currently in use at the selected local councils in WA. In this research, the email and online web systems were tested in the selected councils. Furthermore, this research provided recommendations to the selected councils. These included the creation of the developed information security frameworks and analyses of security weaknesses for the email and online web systems, as well as recommendations related to the security weaknesses and steps required to reduce risks to all users.

There were several known ICT security risks related to incidents that had occurred to the various councils' systems. These risks were indentified based on work done by the network administrators over the past seven years at the local councils in WA. Elicitation of these threats was centered on several private discussions with other IT managerial and IT operational staff from various local councils in WA (personal communications with the local councils in WA, 2005, 2006, 2007, 2008, 2009). Email spamming, online web hacking and wireless hijacking were some of the examples of the incidents that were encountered and communicated during those exchanges.

Additionally, one of the common key issues that emerged from the discussions with the IT managerial and IT operational staff was that the security breaches occurred as a result of the general lack of security awareness and apathy by the IT managerial and IT operational staff.

Thus, three research questions were addressed in order to investigate possible solutions to the problems that were uncovered. These research questions were enumerated as:

i. has the current system been implemented securely in a way that meets the national and international security standards?;
ii. how the developed information security frameworks can potentially improve a level of security strength for the use of the email and online web systems in the three selected councils in WA?; and
iii. how the developed information security frameworks can be employed to incorporate functionalities of the current systems at the selected WA local councils?

The research examined the level of security in the deployment of the email and online web systems in the selected local councils in WA by adapting the Open Source Security Testing Methodology Manual (OSSTMM) 2.2 Section C: Internet technology security as a security testing benchmark and model (Herzog, 2006). According to personal communications with Professor Dr. Craig Valli (2007), the OSSTMM is a solid information security framework and moreover, it is freely avalible on the Internet unlike the proprietary International Standard Organization (ISO) standard. Consequently, the OSSTMM 2.2 Section C was chosen as a security testing benchmark for this research.

In addition, other open source information security standards including The National Institute of Standards and Technology (NIST), Center for Internet Security (CIS) and The Information Systems Security Assessment Framework (ISSAF) were also utilised in conjunction with the OSSTMM methodology.

Other resources included information security related books, journals, personal interviews as well as information bulletins from Computer Emergency Response Team (CERT), CheckPoint, Cisco, GFI Software, Juniper, Microsoft (MS), NESSUS, Network Mapper (NMAP) and related ICT network and security websites.

1.3 Contributions of the research

The developed information security frameworks for the security of the email and online web systems were generated for the selected councils by examining, and expanding upon preliminary research into the WA councils' ICT services (personal communications with the local councils in WA, 2005, 2006, 2007). This earlier research contributed to identification of potential risks in the email and online web systems.

Security approaches were employed to data handling and information particularly in the areas of email, network, web and database security techniques in order to deal with the councils' complex data sets with a view to enhancing administration.

The IT operational staff at the selected councils had limited usage and awareness of cyber security software commonly used in the industry by system administrators, in particular NMAP version 5.0 and GFI LANguard version 9.0. This research served to

extend awareness of the usage nuances for these tools through advanced techniques, thereby extending the knowledge base for the IT operational staff in this area.

The innovation in this research lies in the realistic application of the applied security techniques. The implementation of these techniques also served to generate confidence in the selected councils' IT managerial and IT operational staff in developing and maintaining systems in unsecured environments especially in relation to the email and online web systems.

Several investigations were conducted to verify the feasibility of the developed information security frameworks. Real-time data was used to generate the email and online web systems testing results (see Chapters 4, 5 and 6 for details of the way in which data was allocated to the developed information security frameworks and for testing of each of the selected councils respectively).

All the security testing and analysis for both these systems were carried out using actual and real-time data. Consequently, the developed information security frameworks may readily be applied in the actual email and online web systems.

The developed information security frameworks provided an alternative security pathway for possible adoption by the selected councils. The research provided a means of enhancing the planning and operations of the councils' ICT systems and its compliance with the current ICT policies. Results from this research were considered to be good examples of security based implementations of the email and online web systems within the selected councils according to the councils own IT operational staff.

In addition, the IT operational staff in the selected councils considered the security recommendations from the developed information security frameworks for future audits and tests within the existing councils as well as for other councils and/or organisations for external validity.

1.4 Thesis structure

The remainder of this thesis is organised into six chapters. Each chapter begins with an introduction and ends with a summary and conclusions.

Chapter 2, which contains the discussion of the existing literature, is organised into six subsections: studies on the demand and use of Internet technologies related services in WA, studies on general risks analysis associated with the online services deployment, studies on the standard online services systems testing, studies on the email system, studies on the online web system and finally the conclusion of the chapter. Each of the six aspects presents an overview and discussion of current literature and integrates the conclusions drawn from previous research.

Chapter 3 presents the research methodology and the developed information security frameworks. The research methods are presented within seven subsections: the background to the research method, the interpretive multiple-case study principles, research design and procedures, research materials, the theoretical frameworks and conceptual adaptations, the limitations to the research and a brief summary of the chapter. The materials used in the research described are the architecture, configuration codes and vulnerability of internal border routers, firewalls, switches, Intrusion Detection System/Intrusion Prevention System (IDS/IPS), email, database and online web servers datasets. The software packages used, namely NMAP version 5.0 and GFI LANguard version 9.0 are also detailed here.

Additionally, details of the data analysis procedures, materials, components and working processes of the developed information security frameworks are provided in this chapter.

Chapter 4 is the beginning of discussion of the data selections and collections. It also provides detailed testing procedures as carried out at the first selected council. This is followed by some background information, recordings of the pre-interview consultation, document review, interview investigation, existing architecture discovery, email system testing analysis, online web system testing analysis and recommendations. The last part of the chapter contains the related discussions on the research topic.

Chapter 5 focuses exclusively on the second selected council. It describes a similar process to that of Chapter 4, in terms of considering the available data, conducting testings and presenting, analysing and evaluating the email and online systems testing results.

Chapter 6 contains the investigation and discussion of the third selected council. It follows along the lines of enquiry as Chapters 4 and 5, in terms of examining the available data, performing testings and demonstrating, analysing and assessing the email and online systems testing results.

Chapter 7 includes a discussion on the findings from this research, together with a section on the seven common issues discovered from Chapters 4, 5 and 6 as well as another section on the identification of the limitations of this research.

Chapter 8 contains a summary of the key issues and conclusions of this research, with reference to the findings presented in Chapters 4, 5 and 6. It also includes recommendations borne out from this research and offers suggestions for future research directions.

CHAPTER 2. REVIEW OF LITERATURE

This literature review is based around the examination of the security issues of the common Internet related technologies currently deployed at the selected local councils in WA. In this chapter, the literature reviewed relates to: (1) studies on the demand and use of Internet technology related services in WA; (2) studies on general risks analyses associated with the online services deployment; (3) studies on the standard online services systems testing; (4) studies on the email system; (5) studies on the online web system; and (6) the conclusion of the chapter.

Overall, the selection of the literature reviewed was based on the relevance to the first five points as enunciated and all the reviews were therefore from the associated panel of experts in these specified areas. The selection method could therefore be considered a semblance of the Delphi technique (McDonald et al., 2009).

2.1 The demand and use of Internet technologies related services in WA

There are 141 local councils in WA which make up approximately 23 percent of the total of all local councils in Australia. Some local councils voluntarily share resources in order to provide better services to their residents and users through a collaborative initiative (Limwiriyakul, 2009; Stanton, 2004).

Findings released by the Australian Bureau of Statistics (ABS) show that the number of WA households with access to a home computer has increased correspondingly since 1998 from 44 percent, to 81 percent in 2009 (ABS, 2009). Apparently, the number of WA households with Internet access has also grown from 15 percent in 1998 to 75 percent in 2009 (ABS, 2009).

Furthermore, at the end of 2009, the number of WA households with broadband Internet access has risen to 64 percent while the number of WA households with dial-up Internet access has dropped to only 10 percent (ABS, 2009).

According to other research released by the ABS between 2004 and 2005, approximately 48 percent of businesses employ electronic lodgements with government organisations via the Internet or online services. Approximately 30 percent of businesses utilise online payment systems as the most common online activity to make payments via the Internet to government organisations (ABS, 2006; Limwiriyakul, 2009).

These studies indicate that Internet availability and usage have been increasing, and the demand for government agencies to provide electronic lodgements or online payment services such as fees, rates, licence renewals and infringements payments has been growing as well.

In 2007, according to the Western Australian Local Government Association WALGA (2007), 132 of the 141 total local councils in WA have their own website in WA (Limwiriyakul, 2009). Currently, all local councils in WA have developed their own websites for the public to gain online access to the available online information and services (WALGA, 2010b). Online library services via a third-party service provider such as the State Library in WA make up the largest portion of the most common online services being used. These services are followed by, Internet access services for general purpose usage and online payment services via a third-party service provider such as Australia Post, which make up the second and the third largest portions of the most common online services accessed respectively.

Figure 2.1 summarises the available online services and Internet related technologies provided by the local councils in WA (Limwiriyakul, 2009).

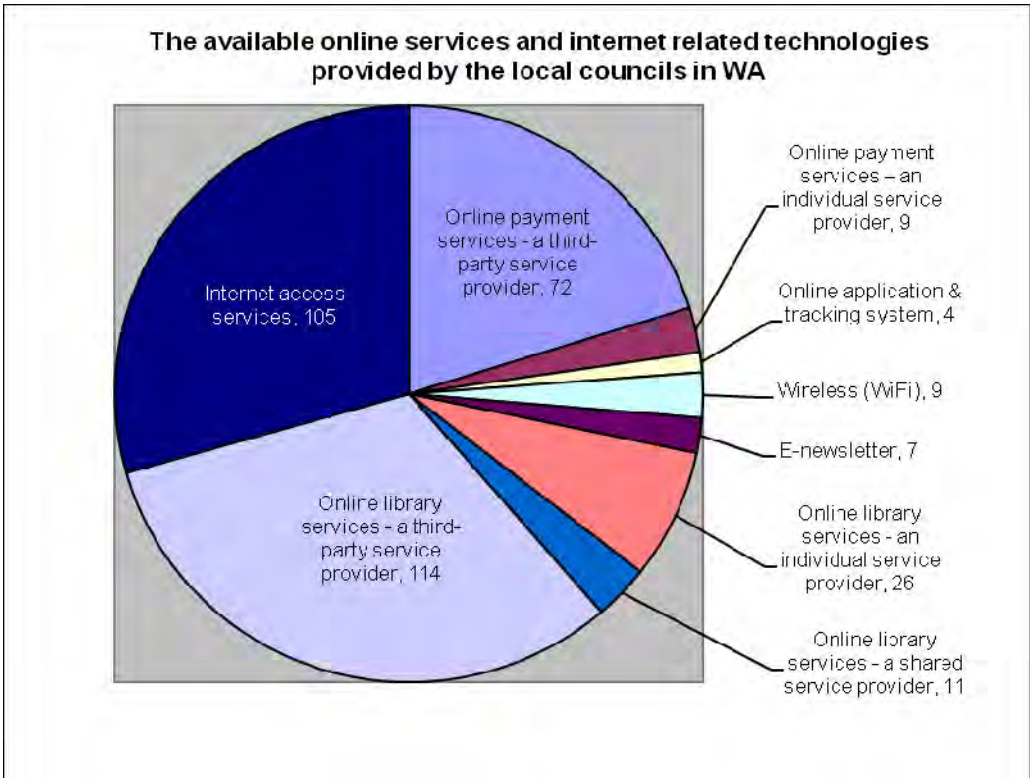

Figure 2.1. The available online services and Internet related technologies provided by the 132 local councils in WA

The use of email, online web, online library, online GIS and online GPS systems are the five major online services systems provided by the local councils in WA (personal communications with the local councils in WA, 2005, 2006, 2007, 2008, 2009). Details of these services are described below.

2.1.1 The email system

Since its inception, email usage has become one of the most common methods of electronic communication in the world as well as in Australia today (Australian Communications and Media Auhtority, 2008; Fadia, 2006). This is due to the fact that it is easier to use, is faster, inexpensive, reliable and easier to manage or filter as compared to traditional mail. It increasingly has become part of all businesses means for exchange of information.

All WA councils have their own email address available to its residents or anyone for inter-staff communication. Many of the councils also have their own email service available to their staff for intra-staff communication (Limwiriyakul, 2009).

2.1.2 The online web system

The online web system covers online information and online payment services. There are 105 WA councils who provide Internet and online access to their residents and others. The online access provides for the councils' general and specific information, often replacing and extending paper based information. There are 72 councils out of these 105 which provide online payment systems that fully rely on third-party payment services such as BPOINT (Commonwealth Bank of Australia, n.d.) and POSTbillpay (Australia Post, n.d.).

Furthermore, there are nine WA councils who have their own online payment systems which provide online payment services to residents. Some examples of the councils who provide these services include the City of Joondalup, the City of Mandurah, the City of Melville, the City of Perth, the City of South Perth, the City of Swan and the town of Vincent. These online payment systems are provided either through third-party application software or in-house application software that is developed and managed internally.

2.1.3 The online library system

There are 114 WA councils who provide an online library system using a third-party service provider such as the State Library in WA. However, there are 26 WA councils who provide their own online library services direct to residents via the Internet. The City of Albany, the City of Armadale, the City of Joondalup and the City of Melville are some examples where this is done.

The online library system allows anyone to do catalogue searches such as author, title and subject. It also allows a library member to reserve, request or check the availability of the required books, Compact Discs (CDs) or other materials. Network enabled online public access catalogue (NetOpac) is one of the more popular online library applications being used in some of the libraries of the WA councils.

2.1.4 The online GIS

GIS is being used at some of the WA councils to provide a wide range of spatial and mapping services which include data capture, map production and GPS technologies. There are several WA councils which provide a useful online interactive mapping system to its residents or anyone to view street trees, properties, plans and aerial photos via the web. The City of Armadale, the City of Cockburn, the City of Melville, the City of Swan and the Town of Victoria Park are some of the WA councils who provide this online GIS service.

IntraMaps is one of the most popular online GIS application software packages being used at all the above mentioned WA councils. IntraMaps was developed by the Digital Mapping Solutions (DMS) and runs on either MS Windows Servers 2003 or 2008. IntraMaps supports various spatial data formats such as MS and Oracle spatials (DMS, n.d.).

2.1.5 The online GPS

Presently, GPS technology is being widely used in navigation and positional tools. With the combination of GPS and the Internet, GPS tracking or monitoring has been made possible.

For example, the online vehicle GPS tracking software is a tool which has the benefit of increasing the productivity, safety and security to council services such as bin collection and security patrol. The City of Melville has merged its GPS technology services with its ICT system in order to provide an online GPS service for its security patrol vehicles. This online GPS system allows for online monitoring of the activity of the vehicles in real-time.

Nevertheless, the objective of this research was to place emphasis on the email and online web systems as they provide a good test case study for the investigation. This is due to the fact that these two selected systems are the main online services used within the local councils in WA.

In terms of business criticality, email and online web systems can be considered as important online services due to their inherent popularity as well as functionality. Email communication has largely superseded fax and traditional mail communication due to its efficiency and cost benefits. As such email communication has become fundamental to business operations in most organisations. Data communicated via email has the added benefit of security as there is no consequent need to shred sensitive information as would be the case for hardcopy communications. All WA councils utilise email services for communication between their staff, residential and other organisations.

Furthermore, online web systems (static, dynamic and payment) also play a critical role in terms of providing services to several WA councils' residential and other organisations. Councils provide these various online web services in the form of online tendering, online web information, online feedback forms, online rate payments and online voting. These services are critical to their large business operations and provide a level of data security as they are robust enough to protect against interruption of services and loss of any sensitive data.

In addition, the email system is deployed in all local councils in WA whereas the online web system including the online payment services may be adopted in all major local councils in WA in the near future as a distinct possibility. Consequently, the findings from these two systems may be used as a guideline for other councils or organisations for further consideration, adaptation and implementation.

2.2 The studies on general risks analysis associated with the online services deployment

Several local councils in WA provide online payment services by utilising a 128 bit Secure Sockets Layer (SSL) technology over Hypertext Transfer Protocol Secure (HTTPS) (personal communications with the local councils in WA, 2005, 2006, 2007, 2008, 2009). Rates, fees, licence renewals, invoices, infringements are specific examples of these payment services.

Nevertheless, the significant missing part from the SSL transaction is a method for the resident to confirm his/her identity as a valid user to the council while using the online services (personal communications with the local councils in WA, 2005, 2006, 2007, 2008, 2009).

Furthermore, there is no method for the council to ensure the legitimacy of the identity of the resident. Even though SSL provides a secure communication channel, it does not provide a way to verify the uniqueness of each resident when dealing with the online services (personal communications with the local councils in WA, 2005, 2006, 2007, 2008, 2009; Secure Computing Corporation, 2006).

In terms of the number of perceived risks to the three selected councils, the followings are some examples of the past security concerns which occurred between the year 2006 and 2009:

- In the year 2007, Council A's email system was subjected to a flood of spamming incidents. These occurrences caused significant problems in terms of the accumulation of massive amounts of junk mail and a consequent reduction in internet speed. As a result, two Symantec spam filtering servers were deployed into their email system (personal communications with Council A, 2008);
- Council C experienced a similar incident of email spamming in the year 2008. These occurrences caused Council C's IT staff a lot of time and effort to manage the issue which also consequently led them to deploy an external spam filtering system to filter their email network traffic (personal communications with Council C, 2009); and
- In the year 2009, the frontend web server (IIS 6.0) of Council B was compromised due to the fact that the server had not installed the most up-to-date patches (personal communications with Council B, 2009).

In addition, various local councils in WA have deployed wireless network technologies to provide the online services that facilitate real-time online access to the councils' information systems, such as Internet access, surveillance cameras and mobile computing (personal communications with the local councils in WA, 2005, 2006, 2007, 2008, 2009).

Nonetheless, the nature of a wireless network technology is less secure than a wired network technology or a conventional technology counterpart (Australian Government: Attorney-General's Department, 2006; Limwiriyakul, 2009; Stanford University Residential Computing, 2007). Therefore, a wireless network technology may introduce a new level of potential risks during online access to services (Limwiriyakul, 2009).

There are several potential risks and threats associated with the online services usage such as viruses, hackers, Denial of Service (DoS), Distributed Denial of Service (DDoS), fake websites, identity theft or online Identity (ID) theft and data integrity. Furthermore, Domain Name Server (DNS) vulnerability is another potential risk where an intruder gains control of the DNS, to do phishing and farming attacks thereby misleading all other users of the DNS (Fontana, 2007). The following lists some examples of services and their associated risks specific to the online services provided by the local councils in WA:

1) *Data integrity:* This includes data loss and data corruption that may be caused by virus infected emails or through intruders who infiltrate the database of a council;
2) *DoS and DDoS:* These denial of services are usually caused when the website, firewall, database, library and online payment systems of a council are affected by severe interruptions or delays as experienced by both the staff and residents of the council;
3) *Data security:* The councils' databases contain personal information relating to the staff and residents that may be stolen, intercepted or exploited by an intruder using spyware or other mechanism and which may or may not be detected;
4) *Misuse of resources:* The council library and community centres may be at risk through the general misuse of the online services by the staff, residents and the public such as the possible unauthorised browsing of pornography, racism, strong violence and crime websites; and
5) *System penetration security risks:* The councils may be at risk from infected Internet download files or executables containing potential viruses that may compromise the information systems.

Consequently, it is essential for the local councils in WA to apply a powerful ICT security strategy in order to shield their systems from intrusion, corruption and exploitation of information. The ICT security should be performed through well-articulated policies and procedures and technical solutions for the staff including training, controlling, monitoring and enforcement (Allen et al., 2007).

Risk assessment typically refers to a security analysis carried out through interviews and research which includes business, legal and industry specific criteria. Security testing is a project-oriented risk assessment of systems and networks through the application of a professional analysis on a security examination where penetration is habitually utilised to validate false positives and false negatives (Herzog, 2006).

Table 2.1 illustrates the potential threats, assets, impacts, countermeasures or contingencies and policy recommendations of the online services provided by the local councils in WA. (L represents low, M represents medium and H represents high). The following summary has been adapted from Whitman and Mattord (2007, pp. 57-59).

Table 2.1 *A summary of threats, assets, impacts, countermeasures or contingencies and policy recommendations for the online services of the local councils in WA*

Threats	**Assets**	**Impacts**	**Countermeasures or contingencies**	**Policy recommendations**
1. Brute force and dictionary attacks	Email, online web, online library, online GIS, online GPS systems and information reputation	M	Security education for user System passwords change frequency Strong system password policy Control and encryption of all communication ports by the councils' IT teams Filter/disable unnecessary ports and protocols on the Internet gateway firewall Audit trail software to show logins and failed logins Use of encryption technology to protect all transmitted and stored information	Staff to undertake security education on induction Regularly review and ensure that the insurance policy covers replacement due to brute force and dictionary attacks Backup media stored in an external location Regularly update the software, patches of all online systems Using encryption technology to protect information in all online systems

Table 2.1 *A summary of threats, assets, impacts, countermeasures or contingencies and policy recommendations for the online services of the local councils in WA (continued)*

Threats	**Assets**	**Impacts**	**Countermeasures or contingencies**	**Policy recommendations**
2. DoS/DDoS attacks	Email, online web, online library, online GIS, online GPS systems and information reputation	M/H	Security education for user Filter/disable unnecessary ports and protocols on the Internet gateway firewall Guidelines on regular backups of critical data to be issued, audited and verified Software and hardware configurations to be controlled by the councils' IT teams only Control and encryption of all communication ports by the councils' IT teams Regular patching of all the applications and OS software of all the online services	Staff to undertake security education on induction Random audits of both software and hardware are to be conducted Removal of any IT equipments is to be authorised by the councils' IT teams Regularly review and ensure that the insurance policy covers replacement due to DoS attacks Backup media stored in an external location All ICT configurations are to be controlled by the councils' IT teams
3. Dust and temperature damage	Email, online web, online library, online GIS, online GPS systems	L/M	Security education for user Check/clean all online IT systems and devices/equipment to ensure there is no dust Install air condition controls and dust filtering systems or position the equipment to take advantage of the prevailing environmental conditions Insure all assets	Staff to undertake security education on induction Regularly review and ensure that the insurance policy covers replacement due to dust contamination Backup media stored in an external location Regular maintenance on air conditioning and filtering systems or environmental area
4. Electrical power fail /unstable/ surge	Email, online web, online library, online GIS, online GPS systems	H	Security education for user Backup all software and configurations files of all online systems and store in different off-site locations Check/monitoring/test Uninterruptible Power Supply/Uninterruptible Power Source (UPS) or surge protector on regular basis Insure all assets	All assets must be insured Staff to undertake security education on induction Regularly review and ensure that the insurance policy covers replacement due to electrical power failure

Table 2.1 *A summary of threats, assets, impacts, countermeasures or contingencies and policy recommendations for the online services of the local councils in WA (continued)*

Threats	**Assets**	**Impacts**	**Countermeasures or contingencies**	**Policy recommendations**
5. Eaves-dropping attacks	Email, online web, online library, online GIS, online GPS systems	M/H	Security education for user Control and encryption of all communication ports by the councils' IT teams Filter/disable unnecessary ports and protocols on the Internet gateway firewall	Staff to undertake security education on induction Regularly update the software, patches of all online systems Using encryption technology to protect information in all online systems Regularly review and ensure that the insurance policy covers replacement due to eavesdropping attacks
6. Fires, flooding, earthquake or any other natural hazards/ disasters	Email, online web, online library, online GIS, online GPS systems and information reputation	H	Security education for user Backup all software and configuration files of all online systems and store in different off-site locations Permanently mark all online systems equipment as council property retrieval message Contingency plan in place in case of emergency Insure all assets	All assets must be insured Staff to undertake security education on induction All councils' assets must be clearly labelled as the council property and audited twice a year Regularly check drains, water pipes, for fire hazards or earthquake proofing. Regularly review and ensure that the insurance policy covers replacement due to natural hazards/disasters

Table 2.1 *A summary of threats, assets, impacts, countermeasures or contingencies and policy recommendations for the online services of the local councils in WA (continued)*

Threats	**Assets**	**Impacts**	**Countermeasures or contingencies**	**Policy recommendations**
7. Hacker attacks	Email, online web, online library, online GIS, online GPS systems and information reputation	M/H	Security education for user Filter/disable unnecessary ports and protocol on the Internet gateway firewall Install IDS/IPS at the Internet gateway system Guidelines on regular backups of critical data to be issued, audited and verified Software and hardware configurations to be controlled by the councils' IT teams only Control and encryption of all communication ports by the councils' IT teams Patching all applications and Operating System (OS) software of all online services systems regularly	Staff to undertake security education on induction Physical and software measures are to be used on all online systems to minimise modification and unauthorised access Random audits of both software and hardware are to be conducted Removal of any IT equipments is to be authorised by the councils' IT teams Regularly review and ensure that the insurance policy covers replacement due to hacker attacks Using encryption technology to protect information in all online systems Deploy IDS/IPS Backup media stored in an external location All ICT configurations are to be controlled by the councils' IT teams
8. Interference and jamming and attacks	Online GPS system and information reputation	M/H	Security education for user Implement filtering/detecting system to monitor or detect any strong interference signals	Staff to undertake security education on induction Regularly review and ensure that the insurance policy covers replacement due to jamming and interference attacks Regularly review and update the facilities policy and GPS usage devices policy Backup media stored in an external location

Table 2.1 *A summary of threats, assets, impacts, countermeasures or contingencies and policy recommendations for the online services of the local councils in WA (continued)*

Threats	**Assets**	**Impacts**	**Countermeasures or contingencies**	**Policy recommendations**
9. Internal theft of online systems devices/ equipments at the selected councils' premises	Email, online web, online library, online GIS, online GPS systems and information reputation	M/H	Security education for user Lock up all laptops when not in use Background/identity checks conducted on staff/contractors Access controls within the company buildings Permanently mark all online systems equipment as council property retrieval message Regular audits of hardware by the councils' IT teams	All assets must be insured Staff to undertake security education on induction Random audits of both software and hardware are to be conducted Removal of any IT equipments is to be authorised by the councils' IT teams All councils' assets must be clearly labelled as the council property and audited twice a year Background/identity checks will be conducted on staffs/contractors Physical and software measures are to be used on all systems to minimise modification and unauthorised access All ICT configurations are to be controlled by the councils' IT teams
10. Malicious active code attacks	Email, online web, online library, online GIS, online GPS systems	M	Enable filtering features on the councils' firewalls systems to filter/limit Java applets and Active X objects Minimise the number of users access to Java applets or Active X objects on all councils' online services systems	Staff to undertake security education on induction Regularly review and ensure that the insurance policy covers replacement due to malicious active code attacks
11. Social engineering attacks	Email, online web, online library, online GIS, online GPS systems	L/M	Security education for user Background/identity checks conducted on staffs/contractors The councils' IT staff are not permitted to give out information to unauthorised personnel Restrict/minimise access to confidential information regarding all online services systems	Staff to undertake security education on induction Only authorised personnel to access security information Regularly review and ensure that the insurance policy covers replacement due to social engineering attacks

Table 2.1 *A summary of threats, assets, impacts, countermeasures or contingencies and policy recommendations for the online services of the local councils in WA (continued)*

Threats	**Assets**	**Impacts**	**Countermeasures or contingencies**	**Policy recommendations**
12. Staff damage	Email, online web, online library, online GIS, online GPS systems	H	Security education for user Backup all software and configuration files of all online systems and store in different off-site locations	Staff to undertake security education on induction All assets must be insured Regularly update the policy
13. Virus, malware and worm introduction through Internet usage	Email, online web, online library, online GIS, online GPS systems	H	Automatic malware, virus and worm and protection software used and automatically updated Security education for user Guidelines on regular backups of critical data to be issued, audited and verified Software and hardware configurations to be controlled by the councils' IT teams only Control and encryption of all communication ports by the councils' IT teams Patching all applications and OS software of all online services systems regularly	Staff to undertake security education on induction Physical and software measures are to be used on all online systems to minimise modification and unauthorised access Random audits of both software and hardware are to be conducted Removal of any IT equipments is to be authorised by the councils' IT teams Backup media stored in an external location All ICT configurations are to be controlled by the councils' IT teams

(Source: Adapted from Whitman & Mattord, 2007, pp. 57-59)

2.3 The standard online services systems testing

This research specifically examined the level of security of the email and online web systems that are presently employed at the selected councils. Adaptations from various testing techniques, open source information security standards, guidelines and recommendations from recognised organisations have been utilised.

An example of the IT security testing techniques was the OSSTMM 2.2 Section C: Internet technology security as a main testing benchmark methodology model. The IT testing techniques from other sources included NIST, CIS, ISSAF combined with related ICT network and security websites such as CERT, CheckPoint, Cisco, GFI,

Juniper, MS, NESSUS and NMAP. Other testing information was compiled from related books and journals and personal interviews were also used as a source of information gathering.

In addition, there were several testing techniques covering a range of different security categorisations of ICT. Examples of the security objects were email systems, DoS, firewall systems, web applications, intrusion detection systems, port scanning, password cracking, Internet border router systems, system fingerprinting and vulnerability. Details of these testing techniques are provided in Table 2.2 which has been adapted from Herzog (2006, pp. 49-67).

Table 2.2 *A summary of the common testing techniques*

Testing techniques	**Descriptions**	**Sample tasks and expected results utilised in the testing process**
1. Email system testing	Email system specification details together with any weaknesses that may cause information leakage such as email server types, footers, encryption techniques, Simple Mail Transfer Protocol (SMTP) server paths and bounced mails.	Investigate email headers, read receipts and bounced mails for the email server trails Examine email spoofing for an internal connect, egression, and internal and external relaying
2. DoS and DDoS testing	This DoS and DDoS testing is to ensure that the network and server system is capable of handling the several types DoS attacks such as ping of death, teardrop, SYN flooding and the User Datagram Protocol (UDP) flooding (Fadia, 2006).	Examine the exposure restrictions of systems to distrusted networks Investigate the extent of load bearing of server and network for hits and traffic Inspect detail of weaknesses in the online availability including identification of any single points of failure Inspect detail of DoS vulnerable systems testings
3. Firewall testing	Firewalls are deployed to control and manage the flow of the network traffic between internal networks, the Demilitarised Zone (DMZ) servers and the Internet based on the security policies of the organisations. It utilises ACLs to allow or deny network packets. The objective of firewall testing is to guarantee that only authorised network traffic is allowed to gain access into the network, and all other traffic be denied.	Indicate information on the firewalls as services and system as well as the features performed on the firewalls Outline of the network security policy by Access Control Lists (ACLs) Test ACLs against the network security policy or against the "Deny All" rule Verify that the firewalls actively filter local network traffic Verify that the firewalls perform address spoof detection Validate Transmission Control Protocol (TCP) and UDP scanning to server logs

Table 2.2 *A summary of the common testing techniques (continued)*

Testing techniques	**Descriptions**	**Sample tasks and expected results utilised in the testing process**
4. Internet application testing	The purpose of this Internet application testing is to search for "security bugs" in client-server applications of the systems, ability to defend against any internal or external threats. Note: This testing was not conducted due to time constraints.	Decompose the binary codes where accessible Locate potential brute force password guessing access points in the client-server applications Find legitimate login credentials with password grinding if possible Trace the authentication system using spoofed tokens Assemble sensitive information with Man-In-the-Middle attacks Insert excess/fake information with session-hijacking techniques Collect excessive information with a direct Uniform Resource Locator (URL), direct instruction, action sequence jumping and/or page skipping
5. IDS testing	The focus of this IDS testing is on the IDS performance and sensitivity.	Inspect any packets and protocols which were not scanned by the IDS Examine a list of IDS false positives and missed alarms Investigate the IDS architecture and a list of unmonitored paths into the network Investigate the IDS sensitivity, the reaction time and the IDS performance under a heavy load
6. Password cracking testing	This password cracking testing technique is a process to check for password validation and strength by deploying automated password-testing tools. **Note:** This testing was not conducted due to time constraints.	Execute automated dictionary and brute force attacks on the password file where applicable Execute automated password crackers on encrypted files such as Portable Document Format (PDF) or MS Word documents Obtain the password file containing usernames and passwords using smbpasswd for Unix systems and Sam._ for Windows NT systems Examine the list of systems and documents that are potentially vulnerable to crack
6. Port scanning testing	It is the invasive probing of the network and transport level of the system ports. Various network port scanning tools are employed to gather and check the information of the network system.	Inspect details of open, closed or filtered ports Inspect Internet Protocol (IP) addresses of all live systems Inspect the internal system network addressing Examine the list of discovered tunnelled and encapsulated protocols Investigate the list of discovered routing protocols supported Inspect the active services and the network map

Table 2.2 *A summary of the common testing techniques (continued)*

Testing techniques	**Descriptions**	**Sample tasks and expected results utilised in the testing process**
7. Internet border router testing	The action of this Internet border router testing technique is to protect, control and filter the network traffic flow for both the Intranet and the Internet is based on the security policy. It runs ACLs to facilitate the permission or blockage of the network traffic packets.	Examine the router type and its specified features Verify that the router is implementing the address spoof detection Check and confirm which router provides Network Address Translation (NAT) Check the ACLs against the written security policy or the "Deny All" rule Check the router outbound capabilities from the inside
8. System fingerprinting testing	The purpose of this system fingerprinting testing technique is to test system responses.	Verify the patch level Verify the type of the OS Verify the type of the system Verify the system enumeration Verify internal system network addressing
9. Vulnerability testing	Various automated tools have been deployed in this vulnerability testing technique.	Determine feasible DoS vulnerabilities Determine loops and holes of the systems

(Source: Adapted from Herzog, 2006, pp. 49-67)

Although the focus of this research was on the email and online web systems only, it was necessary to utilise firewall, IDS/IPS, Internet border router, port scanning, system fingerprinting and vulnerability testing techniques as they are all related and required for as part of comprehensive testing of these systems. Nevertheless, DoS and DDoS techniques were not fully covered in the review as this type of testing was not conducted in the current research due to the possible interruption to the councils' network systems and the associated disruption to normal business operations.

In addition, a review of both the Internet application itself and password integrity tests were not conducted as they were deemed to be out of the scope of this research.

2.4 Studies on the email system

This section is divided into two subsections, which include email vulnerabilities and risks as well as a general description of the email system testing

2.4.1 Types of email vulnerabilities and risks

The email vulnerabilities and risks in terms of attack techniques frequently used by hackers are described in this section. This is followed by detailing the testing of each stage such as network surveying and its architecture, Internet border router, firewall, IDS, switches review, services and system identification, port scanning, vulnerabilities, spoofing, vendor security benchmark auditing and security policy reviews. The email system is one of the most common targets that attackers aim at and it includes both the email system and the email clients.

Typically, an email system consists of email server(s) and its network infrastructure such as firewall and IDS. All of these devices have vulnerabilities that can be protected through the use of proper configuration. Furthermore, potential risks can be minimised by simply designing and applying a good security practice policy. Table 2.3 displays a summary of the common methods of attacks to the email system.

Table 2.3 *A summary of the common methods of attacks to the email system*

Attacking techniques	**Descriptions**
Email bomber	Massive emails generated which can be the same or different messages from an individual sender or a group of senders.
Email spamming	Any unwanted advertisements for services or products which were included in an email message.
Email sniffing and spoofing	A way of intercepting email traffic using a network sniffer tool which allows the attacker to capture all the email contents.
Email scam	Fraud or unwanted email that usually claims the prospect of a bargain or something for nothing.
Email phishing	Emails which were created to collect (phish) personal information (identity theft) such as usernames, passwords, credit card and bank account.
Email borne viruses	Emails that have an attached virus, worm or Trojan.
Buffer overflows	By sending a long HELO command or long email names in MAIL or RCPT commands to the target email server can create a buffer overflow and possibly interrupt the email system (Basta & Halton, 2008).
DoS	This attack may crash or destabilise the target email server by attempting to open multiple connections to the server (SMTP flooding).
Third-party mail relay	Or open relay is a target email server which receives email from an unknown sender. Then sending it on to recipient(s) which are not users of the email system (Stewart, 2003).

2.4.2 A general description of the email system testing

The email system testing can be categorised into five stages as described briefly in the following.

1) *Network surveying:* This network surveying stage is utilised to gather information relating to the council's email system such as network architecture, email server, reverse proxy server and spam blocker. In addition, both identified issues and recommendations are included as part of the information gathering.
2) *Email system's infrastructure (Internet border router, firewall, IDS/IPS and switches) review:* This email system's infrastructure stage is used to collect specifications and configuration codes of the email system infrastructure devices.
3) *Services and system identification, port scanning and vulnerability testing:* This services and system identification, port scanning and vulnerability testing stage is employed to audit and review the email server, the spam blocker appliance and the reverse proxy server (if any) on services, system identifications, patching status, TCP and UDP ports and possible vulnerabilities.
4) *Spoofing testing and vendor security benchmark on the email server application software:* Spoofing testing covers the testing on internal connectivity, internal and external relaying on the email system of the council. In terms of vendor security benchmark on the email server application software, it benchmarks against the council's email application software using open source benchmark guideline such as the CIS benchmark for MS Exchange 2007 for Windows Server 2003 version 1.0. In addition, any modifications to the benchmark made to suit the council's email system.
5) *Email security policy reviews:* This email security policy reviews stage is concerned with a review of the related email information security policy including the technical policy that is in current use at the council.

2.5 Studies on the online web system

The two subsections in this section include the types of online web vulnerabilities and risks and a general description of the online web system testing.

2.5.1 Types of online web vulnerabilities and risks

Tracy et al. (2007, p. ES-1) states that "web servers are often the most targeted and attacked hosts on organizations' networks". It follows therefore that public web servers such as the online web servers, frontend web servers, application web servers will be even more targeted. A summary of specific security risks, threats and vulnerabilities on the common web servers is shown in Table 2.4.

Table 2.4 *A summary of the common online web's attack/threat techniques*

Attack/threat techniques	**Descriptions**
Web pilfering	Attackers search through web pages for key flaws and vulnerabilities manually or with automated tools (Scambray et al., 2001).
DoS	Attackers may directly or indirectly attack web servers or the supporting network infrastructure such as firewalls or routers. This may result in denying or interrupting customers or users accessing its services.
Input validation (injection)	These intrusions include Hypertext Markup Language (HTML) injection, Cross-Site Scripting (XSS), Structured Query Language (SQL) and Lightweight Directory Access Protocol (LDAP) injections. Attackers target sensitive information of web applications which normally provide links to its supported backend database servers. This can cause loss of confidential data, open the data to manipulation (insert, delete, update), or interrupt the use of the database application.
Interception	Attackers may intercept transmissions of unencrypted information between the web server and the browser. The information may include sensitive data such as login names and passwords.
Exploiting software	Attackers may take advantage of software bugs in the web server platform. Some examples are the security holes in Internet Information Services (IIS), Apache Tomcat, Active Server Page (ASP) and Hypertext Preprocessor (PHP) applications. This may allow attackers access to private files or folders in the web server.
Buffer overflows	"Attackers use buffer overflows to corrupt the execution stack of a web application" (The Open Web Application Security Project or OWASP, 2009, p. 2). This can also cause interruption to web servers and can create significant risks to users mainly centred around the manipulation of the system applications and data.
Web authentication threats	Examples are username/password threats, username enumeration, password guessing and eavesdropping (Scambray et al., 2006). This can lead to identity theft.
Web authorisation threats	Fingerprinting authorisation and both attacking ACLs and tokens are classic examples of web application threats (Scambray et al., 2006). This can lead to part or full control of the compromised web application and its backend system.
Web services vulnerabilities	This includes attacking Extensible Markup Language (XML) web services including Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) and Universal Description, Discovery, and Integration (UDDI) for vulnerabilities.

2.5.2 A general description of the online web system testing

The online web system testing can be classified into five stages as depicted briefly in the following.

1) *Network surveying*: This network surveying stage is used to gather information relating to the council's online web system such as network architecture, web server(s), application server(s), backend database server(s) and Content Management System (CMS) server(s) (if they exist). In addition, both identified issues and recommendations are also included.
2) *Online web system's infrastructure (Internet border router, firewall, IDS/IPS and switches) review:* This online web system's infrastructure review stage is employed to collect specifications and configuration codes of the online web system infrastructure devices.
3) *Services and system identification, port scanning and vulnerability testing:* This services and system identification, port scanning and vulnerability testing stage is deployed to audit and review the related servers such web, application, backend database and CMS server(s) (if they exist) to audit on services, system identifications, patching status, TCP and UDP ports and feasible vulnerabilities.
4) *Vendor security benchmark online backend database server:* This vendor security benchmark online backend database server stage is utilised to do benchmark test against the council's online backend database application software employing open source benchmark guideline such as the CIS – security configuration benchmark for MS SQL Server 2005 version 1.2.0. In addition, details of modifications to the benchmark made to suit the council's online backend database server.
5) *Online web system security policy reviews:* This online web system security policy reviews stage is used to review the current related online web system including the online payment system security policy of the selected councils.

2.6 Summary

Findings from the literature review point to a need for a process of enhancing the level of security for common Internet technologies in a comprehensive way as it appears there is possibly no facility for this in the local councils in WA. It is also apparent from the number of personal interviews with the local councils in WA during the period 2005 to 2009 with respect to improving the level and strength of security in Internet technologies such as the email and online web systems; this has not been achieved to any significant level of satisfaction. Consequently, further research studies into these aspects may be warranted as they may serve to expand general knowledge in this area and increase the level of confidence in the security of these objects.

In relation to the face-to-face formal interviews, all the three IT managers from the selected councils were agreed that there was a need of enhancing the level of security of their email and online web systems. For examples, Council A's IT manager had a strong concern about their current online payment system particularly in security of their SQL database servers (personal communications with Council A, 2007, 2008, 2009). Council B's IT manager was also concern on their online in-house payment system particularly in security setting on the frontend payment web server (personal communications with Council B, 2009). Furthermore, both the IT manager and system administrator of Council C were seriously concern about security of their newly deployed online payment system (Epathway) (personal communications with Council C, 2009, 2010).

In addition, it is feasible that this research may serve as a framework on which to base security testing for similarly structured organisations using the email and online web systems. The uncovering of the deficiency in the level of security is exactly the novelty in this research, as there has been no efficient set of criteria that address the potential risks that may occur while using the email and online web systems as used by the local councils in WA. Therefore, an investigation undertaken through the use of well-known software may prove beneficial in testing the developed information security frameworks at the selected local councils in WA. The details on the method and materials utilised in this research are presented in Chapter 3.

As a result, it may provide the useful and practical information security frameworks as a guide or model that may enhance the level of security in the councils' systems in terms of planning, monitoring, controlling, managing and implementation.

CHAPTER 3. RESEARCH METHODOLOGY AND THE DEVELOPED INFORMATION SECURITY FRAMEWORKS

This chapter aims to present the interpretive multiple-case study principles, as well as the research method and techniques applied in this research. It also defines the scope and limitations of the research design. A description of how this research was implemented is presented in seven subsections. Firstly, the background to the research method is detailed to demonstrate how the research method was derived in Section 3.1. The following Section 3.2 deals with introducing the interpretive multiple-case study principles wherein the seven principles of case study research are described. The subsequent Section 3.3 is concerned with research design and procedures. It covers the reasons for selecting the organisations, data sources, research analysis process, data collection and analyses. Research materials including primary and secondary data sources and open-source and propriety software are also covered in Section 3.4. This is followed by a review of the theoretical frameworks and conceptual adaptations in Section 3.5. Section 3.6 examines the limitations to the research and a brief summary of the chapter is finally presented in Section 3.7.

3.1 Background to the research method used in the research

Qualitative research involves an in-depth understanding of certain behaviours and the reasons that control them. It relies on rationales behind a range of aspects of behaviour and focuses on samples, and categorises data into patterns for organising and reporting results (Cacho-Elizondo & Loussaïef, 2009). The most common qualitative research method in Information Systems (IS) research is the case study method (Alavi & Carlson, 1992; Myers, 2009; Orlikowski & Baroudi, 1991).

According to Klein & Myers (1999, p. 68), “IS research can be classified as interpretive if it is assumed that our knowledge of reality is gained only through social constructions such as language, consciousness, shared meanings, documents, tools, and other artefacts”.

Similarly, another quotation states that “interpretive researchers start out with the assumption that access to reality is only through social constructions such as language, consciousness and shared meanings” (Limwiriyakul, 2009, pp. 132-133; Myers, 1997, p. 2). Interpretive research method in IS is declared by Walsham (1993, pp. 4-5) as “aimed at producing an understanding of the context of the IS, and the process whereby the IS influences and is influenced by the context”.

In general, such interpretive research concentrates on the entire complexity of human sense making, since the incident becomes manifest in which there are no requirements for pre-identified dependent and independent variables (Glanz, 2003; Kaplan & Maxwell, 1994; Klein & Myers, 2001).

Myers and Walsham (1998) classified the interpretive research approach into three categories as positivist, interpretive and critical. Similarly, Guba and Lincoln (1994) clarified this research approach into four types, namely positivist, post-positivist, constructivist and critical. This research applied Orlikowski and Baroudi (1991)’s framework in order to decide whether the research categorisation was positivist, interpretive or critical. The positivist approach is used to determine the prior fixed relationships within phenomena examined by employing structured techniques. It assists researchers to do theory testing and enhance understanding in predictive occurrences. Propositions’ evidence, scientific measurement of variables, hypotheses testing and the inferences of phenomena depiction retrieved from a sample to a population, are some examples of the positivist category Guba & Lincoln (1994).

Interpretive approach supposes that people generate and correlate their thoughts by interrelation with others around the world. Furthermore, it is suitable for natural setting studies that have social interactions between researchers and people to learn from the background of their actions and attempt to understand the ideas and feelings of target subjects or an understanding of the subjective or people experience. Therefore, it supports researchers in the complete understanding of phenomena through the meanings that people allocate to them (Berger & Kellner, 1981; Guba & Lincoln, 1994; Neuman, 1997).

The critical category of research is used to assess the status quo by revealing the history, the beliefs and the contradictions of existing social systems for the purpose of facilitating their liberation. Critical evidence towards assumptions on organisations and IS, and a dialectical analysis are samples of the critical category (Guba & Lincoln, 1994).

Given the previous definitions and precepts, this research followed on from a traditional theoretical background to generate a theoretical formulation or a phenomenal interpretation as a construct in the form of a framework. In addition, there was an emphasis on the "subjective" as justification for the research. Multiple-case studies are classically included in the interpretive study and as a result it was the main research method used in this research.

Interpretive multiple-case studies were selected in order to validate the findings, as they were not simply a consequence of the unconventional behaviour of a specific case (Miles & Huberman, 1984). Thus the selection of the various independent local councils served to enhance critical, social and organisational understandings, which were linked to the ICT adjustment and/or implementation in all organisations. Conducting and depicting common implications in the test cases physically allowed for logical replication in other environments in order to obtain external validation. The reason for using multiple-case studies was because multiple experiments inherently have the capability to strengthen research findings (Benbasat et al., 1987; Limwiriyakul, 2009; Williamson, et al., 2002).

Furthermore, it allowed the researcher to examine a particular phenomenon in diverse settings and conduct cross-case analysis and comparison (Limwiriyakul, 2009; Williamson, et al., 2002). Therefore, the research method adopted in this research after a detailed examination of related research methods was to conduct interpretive multiple-case studies (Benbasat & Weber, 1996; Cavaye, 1996; Davis et al., 1992; Klein & Myers, 1999; Lee, 1989; Walsham, 1995) in the selected local councils in WA during the period between July 2009 and September 2010. Three designated local councils were selected for this research. It is believed that this selection was sufficient to achieve the objectives of this research due to the extensiveness of the data collection and collation, and subsequent analyses stages.

The majority of data collection techniques used in this research was semi-structured interviews, participant observation, group discussion and documentation analyses. These appropriate and qualitative tools were used to increase the richness and reliability of the case study.

In addition, two developed information security frameworks for the email and online web systems were implemented for the initial testing of each selected test case. Nevertheless, further testing should be developed according to individual organisational constraints, as each of the test cases was an independent research with decided individuality.

3.2 Seven principles for the interpretive multiple-case studies

Klein and Myers (1999) proposed a set of seven principles for conducting and evaluating interpretive case studies in IS research based on hermeneutic orientation. This may assist the researchers and may be used as a guide to gain understanding of the fundamental ideas of interpretive study. Based on their suggestion, the researchers should figure out how and what principles are suited for their research conditions. These seven principles were adopted to formulate the research design as follows:

- The fundamental principle of the hermeneutic circle;
- The principle of contextualisation;
- The principle of interaction between the researchers and the subjects;
- The principle of abstraction and generalisation;
- The principle of dialogical reasoning;
- The principle of multiple interpretations; and
- The principle of suspicion.

The use of these seven principles may enhance the validity and clarity of the research. Details of these seven principles and how they applied to this research are outlined in the following sections.

3.2.1 The fundamental principle of the hermeneutic circle

This principle recommends that subjective or people understanding is attained by considering the partial and entire meaning of their actions (Klein & Myers, 1999). Klein and Myers (1999, p. 71) stated that “the process of interpretation moves from a precursory understanding of the parts to the whole and from a global understanding of the whole context back to an improved understanding of each part”. Therefore, the research method in each case study necessitates being the partial and total understanding of the subjective or people experience, namely the performance and management of the IT managerial and IT operational staff incorporated with the current ICT system security patterns or policies of the selected councils in WA. This requirement provides a better understanding of the interchange patterns of each part as a whole depiction.

Additionally, Klein and Myers (1999, p. 73) suggest that “during repeated cycles of the hermeneutic circle, all of the suggested principles can be applied iteratively, forming a complex web of interpretations”. Consequently, this research deployed several stages of data analysis with the use of several analysis tools to facilitate the iterations.

In addition, this research is proposed to be interpretive research as it works on the contextual and is limited within the selected councils in WA. There are several significant factors that have an effect on the performance and management of the IT managerial and IT operational staff within the selected councils.

These include a wide range from hard technical issues such as network surveying, internetwork infrastructure review, services and system identification, port scanning and vulnerability testing, and vendor security benchmark auditing, through to soft social issues such as performance and management style, and ICT system security policy enforcement. Thus, there has to be consideration of all issues individually together with a combination into one piece in order to achieve an understanding of the total problem situation.

3.2.2 The principle of contextualisation

This principle relates to the critical explanation of the social and historical background or the context of the research setting. It describes how the circumstances have been

developed and occurred (Klein & Myers, 1999). In this research, the concept of a digital community or ICT including system security threats and risks is related to this principle as it intensely describes the situation background that occurs within the selected councils.

Additionally, this research collects security policy documents, personal interviews and computer data as research artefacts in order to produce an intensive understanding of the contexts that arise within the selected councils. Consequently, these may lead it to be a more crucial and concentrated consideration of the research circumstances particularly on the social and historical background in each of the selected councils.

3.2.3 The principle of interaction between the researchers and the subjects

This principle relates to the association between the researchers and the subjects as it necessitates that the researchers place themselves and the research subjects within a historical context. The researchers examine and interpret the interaction of the research subjects and data in order to produce the facts, documents or artefacts. Generally, the researchers need to consider carefully their actions as they may influence and affect the subjects while conducting the research (Klein & Myers, 1999). Nevertheless, the impact of this interaction for this research was reduced, as it did not relate directly to human subjects. Consequently, it may eliminate the feasibility of Hawthorne effects (Mayo, 1933) by the subjects.

In addition, this research utilised both primary and secondary data sources to obtain the results and findings. Furthermore, it employed the accredited software to analyse the primary data from each selected council (see Section 3.3.2 for further detail on the data analysis procedures).

The interviews, as one of the primary data sources, and documentation, as the secondary data source, from each selected council were used to compare and support in the analysis of the empirical data obtained from the software. This was deemed to be a good opportunity to assist the researchers in adjusting the interpretation in order to gain a better and clear understanding on the research subjects and/or data.

3.2.4 The principle of abstraction and generalisation

Klein and Myers (1999, p. 72) stated that this principle "requires relating the idiographic details by the data interpretation through the application of principles one and two to theoretical, general concepts that describe the nature of human understanding and social action".

Furthermore, they suggested that theory and its formation including concepts, contents, frameworks and processes play an essential role in interpretive research to receive abstraction and generalisation from the findings. Therefore, the analysis in each case or council may display comprehensively how the developed information security frameworks had been adopted and implemented as the practical models are the significant issues in the interpretation. The in-depth information in each case may be disclosed by the interpretation that associated with theory and its general concepts. The case may be employed to simplify the concepts from theory (Klein & Myers, 1999).

3.2.5 The principle of dialogical reasoning

This principle requires the sensitivity of the researchers to deal with the feasible contradictions among the theoretical preconceptions, which lead the research design and the actual findings (Klein & Myers, 1999). This may be revised and done several times in the cycle of the research process to enhance the understanding of each subsequence stage in the research process. While conducting the data analysis procedures, the outcomes from some of the analyses were different from the theoretical preconceptions. As a result, several tests were required to be repeated in order to investigate and clarify the differences.

3.2.6 The principle of multiple interpretations

This principle requires sensitivity from the researchers to observe and investigate the potential dissimilarities or contradictions in interpretations in conjunction with the reasons from different participants in the research setting (Klein & Myers, 1999). Each participant may understand and interpret in a variety of ways of thought even if they confront the same situations or problems.

This principle was applied to this research by comparing and evaluating the interview data and the data obtained from the software that effectively present the differentiation between the recognition and actuality of the circumstances. In the same council, employees may have different viewpoints on a situation or problem, which is based upon their individual theoretical perspective. This perspective may have an influence on their interpretations in a situation or problem in which it may depict or guide towards any potential conclusions, ideas or even generate principles or fundamentals.

For instance, the IT operational staff may have different visions of the circumstances in comparison with the IT managerial staff. Nevertheless, when investigating and presenting the findings to the council both of the viewpoints were collated into the statement.

3.2.7 The principle of suspicion

This principle requires the sensitivity about the probable biases and systematic distortion from the researchers in narration and data gathered from the participants (Klein & Myers, 1999). This principle may relate to the various sources of context which may lead to be regarded with suspicion such as personal biases, personal opinions or comments that may influence other people's thoughts, and/or infer inaccuracy or unreliability of data.

Even though, this research conducted the interviews from the IT managerial and IT operational staff, it did not have any inherent suspicions due to the nature of the research. The interview data obtained from each council were merely the minor components with respect to the use of software in data analysis, which was the major component in this research. Therefore, the findings attained from the software may be claimed to be unbiased and/or accurate data.

In conclusion, this research deployed both quantitative and qualitative methods in order to enhance validity and reliability of the research findings. The use of these methods may generate a better and solid understanding of the research context under the investigation (Cavaye, 1996). The document review as the quantitative method was utilised to validate and triangulate the findings derived from the use of software and interviews as the qualitative method.

According to Cavaye (1996), there is no preset amount of cases that is required to be studied. Consequently, three to five councils would be deemed sufficient for this purpose. Thus, for this research, it was decided to select three councils as these particular councils have the potential to provide useful and appropriate data and information for subsequent testings and analyses.

3.3 Case study research design and procedures

3.3.1 Selection of local councils in WA

The case studies were selected from a number of local councils. The selection was limited to WA because of the accessibility to the organisations. Two of the main attributes within each of the case studies were the various Internet services such as WWW, email, GIS, GPS, VoIP and wireless LAN provided, and in-house network infrastructure of the organisations. Accordingly, the selected councils were deemed suitable in that they would provide sufficient and relevant data for testing and analysis and subsequent interpretation and evaluation of the results.

In addition, the selected councils were willing to provide real-time data, due to the fact that they would in-turn derive some benefits in the way of a measure of their security robustness and tightening through the post evaluation recommendations.

Furthermore, there was an element of trust and confidence in the researcher as a result of previous work done by the researcher for the selected councils.

3.3.2 Data analysis procedures

This research specifically examined the level of security of the email system that is currently deployed at the selected councils in WA. Various testing techniques such as open source information security standards, guidelines and recommendations from recognised organisations, were adapted for the purposes of this research. Some of these techniques were derived from sources such as the OSSTMM 2.2 Section C: Internet technology security and which was specifically used as a model for benchmark testing.

Other information security standard resources include CIS, ISSAF, NIST together with a host of information from other media such as WWW, journals, books and personal interviews integrated with information from CERT, CheckPoint, Cisco, GFI, Juniper, MS, NESSUS, NMAP and related ICT network and security websites.

The two data analysis procedures employed for testing purposes were for the email and online web systems. Each data analysis procedure consisted of five stages, which covered (1) network surveying; (2) internetwork infrastructure review; (3) services and system identification, port scanning and vulnerability testing; (4) vendor security benchmark auditing; and (5) security policy review.

The data analysis framework procedures for the email and online web systems were exactly the same except for Stage 4. The email system analysis procedure contained both vendor security benchmark auditing and email spoofing testing (Figure 3.1), whereas the online web system analysis procedure tested only the backend database server of each of the selected councils (Figure 3.2).

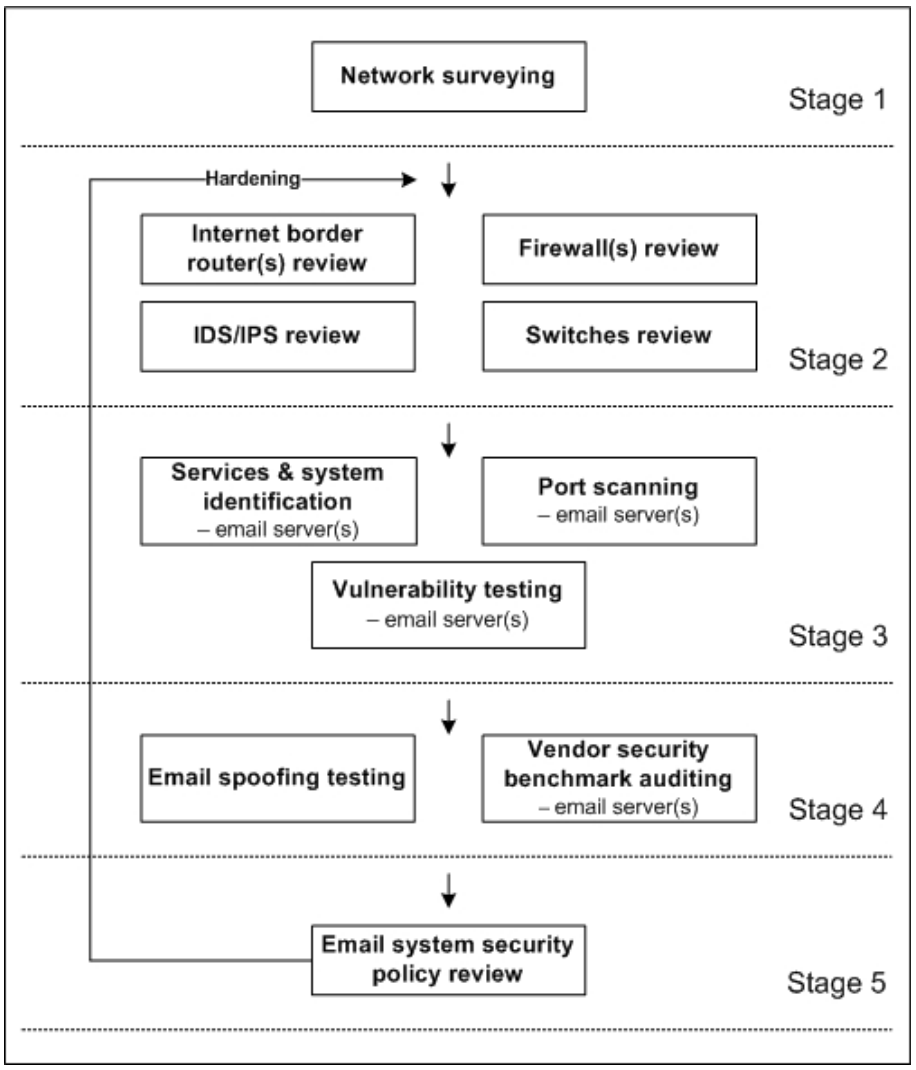

Figure 3.1. Data analysis framework: A stage module diagram for the analysis of the email system

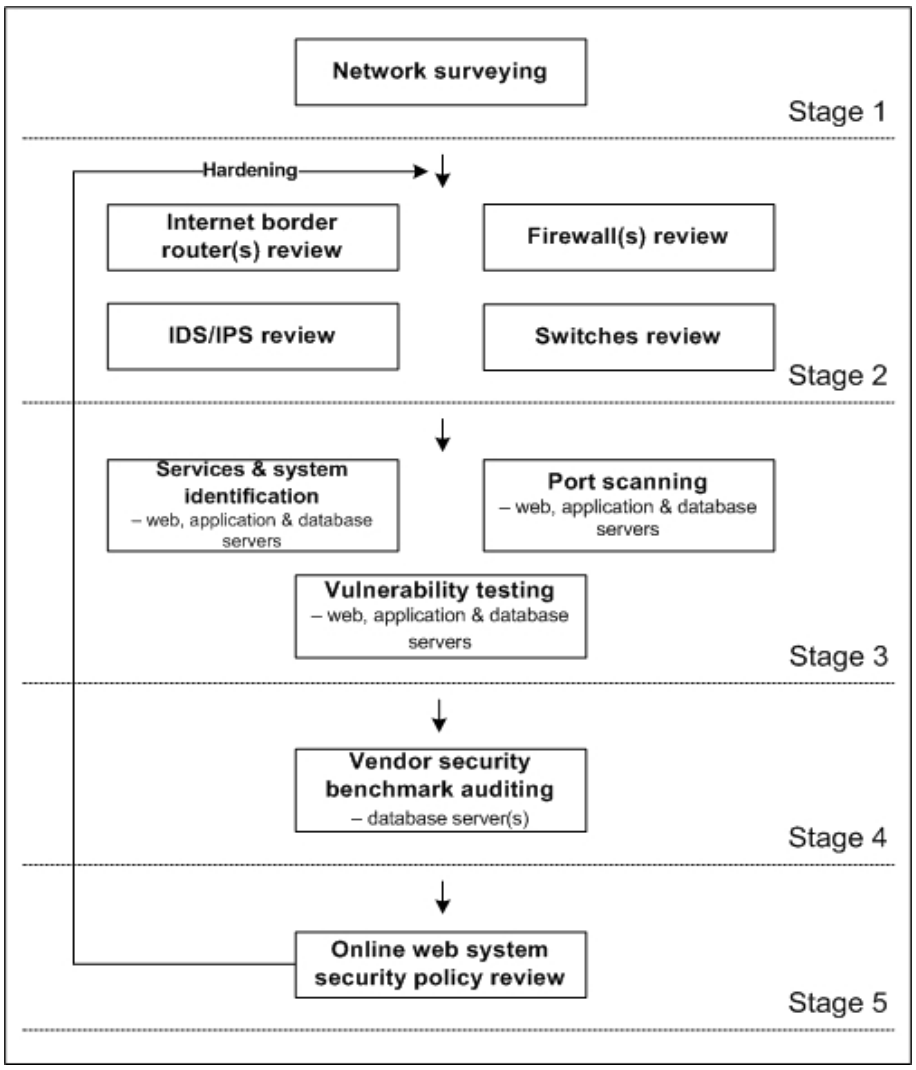

Figure 3.2. Data analysis framework: A stage module diagram for the analysis of the online web system

Details of each of the five stages of data analysis procedures for both the email and online web systems are explained below.

Stage 1: Network surveying

There were two sets of network surveying stages for each of the selected councils. Each network surveying stage consisted of specific internetwork data and information collection related to either the email or online web systems collected from each of the selected councils through the use of the following three artefacts:

- Overall network diagram for the internetwork link, the DMZ infrastructure connectivity of the related email or online web systems;
- Configuration codes of all internetwork devices such as the Internet border router, the Internet firewall(s), the DMZ's switch(s), the reverse proxy server and the related email or online web systems; and
- Device specifications of all internetwork devices, namely the Internet border router, the Internet firewall(s), the DMZ's switch(s), the reverse proxy server and the related email or online web systems.

The network surveying stage for the email system collected information on specifications of the email server(s) and the spam blocker appliance(s). Conversely, the network surveying stage for the online web system collected information from the static web and application servers. Information from the CMS (if applicable) and the backend database system were also collected in this network surveying stage.

All the public IP addresses of the network of the selected councils were concealed through the use of alias names to prevent any potential security risks. These designations were as follows:

- "A" represents subnetwork group 1;
- "B" represents subnetwork group 2;
- "C" represents subnetwork group 3; and
- "D" represents subnetwork group 4.

Stage 2: Internetwork infrastructure review

This internetwork infrastructure stage involves a review of the related specification and configuration codes data collection of the internetwork infrastructure devices for both the email and online web systems at the selected councils. The devices included the Internet border router, the IDS/IPS, the firewall(s), the DMZ switch(s) for all selected councils and the reverse proxy server for Council C only. This information was securely recorded on a workstation and later analysed for the purposes of this research only.

Stage 3: Services and system identification, port scanning and vulnerability testing

In this third testing stage, a network scanning technique was used for all three testing steps (services and system identification, port scanning and vulnerability testing). Both NMAP and GFI LANguard network scanning tools were used for scanning the email and online web systems. These software applications are well known and widely used in the network industry. NMAP is a free open source application whereas GFI LANguard is a commercial application.

NMAP with GUI standard (open source Zenmap version 5.0) for MS Windows XP version was run. The slow comprehensive scan option was used in the test in order to collect as much information as possible from the email and online web systems relating to TCP, UDP ports, vulnerabilities, patches, services, software and hardware. In addition, GFI LANguard version 9.0 with the full scan option was run in order to fully test and gather the target email and online web systems information.

The services and system identification were categorised into two groups. These were the system information policy results and the system patching status results. The system information policy results was further summarised into three groups. These groups were the services, the password policy and the security audit policy. Additionally, the system patching status results were categorised into two groups. These groups were the missing service packs and the missing patches.

The port scanning testing on the target servers of both the email and online web systems were run with the following options:

- Full comprehensive scan in NMAP testing of all TCP and UDP ports; and
- Comprehensive scan in GFI LANguard testing on all TCP and UDP ports.

Stage 4: Vendor security benchmark auditing

The email system testing involved two steps which included the general email spoofing testing and vendor security auditing as follows:

- *Email spoofing testing:* This step was adapted from an email spoofing template from the OSSTMM 2.2 Section C: Internet technology security as a guideline. The purpose of this email spoofing testing was to discover generally whether the email server was secured against any spoofing attacks; and
- *Email vendor security auditing:* This specific auditing was modified to suit the email application server system of each of the selected councils. However, as each of the selected councils used the same template from CIS Benchmark for Exchange 2007 for Windows Server 2003 version 1.0 – Recommended Security Setting for Exchange Controls, there was no need for further adaptation.

On the other hand, there was only one testing step carried out for the online web system as shown in Figure 3.2: Testing stage 4. This fourth testing stage was the vendor (database) security benchmark auditing on the backend database server of the selected councils. The database auditing template was designed to suit the application platform of the backend database in each of the selected councils.

However, as each of the selected councils deployed the Security Configuration Benchmark for MS SQL Server 2005 version 1.2.0 from CIS, the database auditing template was the same for all.

Stage 5: Email and online web systems security policy review

The purpose of this email and online web systems security policy review stage was to review the IT security policy in relation to the email and online web systems. This email and online web systems security policy review stage included the investigation of the security related to the internetwork infrastructure and its devices, the email server(s), the backend database server(s) and the web server(s).

Furthermore, this review covered an information security policy in general for the overall enterprise and technical security policy particularly on issue-specific and systems-specific security policies of the email and online web systems in each of the selected councils.

3.4 Research materials

The sources of data and materials utilised in this research are described below.

3.4.1 Primary data

The primary data was made up of interviews and testing analysis as presented below in details.

3.4.1.1 Interviews

Several semi-structured interviews were conducted with the IT managerial staff (IT managers) and the IT operational staff (application, database, network, system, telecommunication and web administrators).

The IT managerial staff were selected for this exercise as the responsibility of the decision making rested with them. This responsibility included advising the IT operational staff and providing direction for the protection of the organisations' ICT systems. It also included the potential to support IS implementations and managerial judgement to enforce organisation policy for the success of the organisation (Pinto & Slevin, 1989; Robey, 1979).

The inclusion of the IT managerial staff for the interviews was important as they were also responsible for the following activities associated with the security testing:

- "Coordinating the development and maintenance of the organisation's information security policies, standards and procedures;
- Ensuring the establishment of, and compliance with, consistent security evaluation process for departments throughout the organisation; and
- Participating in developing processes for decision-making and prioritisation of system for security testing" (Wack et al., 2003, pp. 2-4).

In addition to the IT managerial staff, the IT operational staff were selected as key stakeholders because of their day to day responsibilities such as network and system monitoring and maintenance. Their responsibilities included the implementation of the network and system securities and guidelines derived from the organisation policy for the utilisation of the IT system. It was considered important to include them in the interviews, as their security practices would facilitate better understanding of any security issues faced by the selected councils.

Semi-guided interviews were deployed as an outline for open-ended answers. These were carried out in two steps with the IT managerial and IT operational staff at each of the selected councils. These interviews formed an initial baseline prior to the analysis of the data. The initial baseline interview was to establish the level of security policies for the email and online web systems technologies and the associated enforcement by the key stakeholders. The testing analysis interviews with post-interview reporting were designed to obtain the feedbacks or comments on the findings of the initial testing analyses with the aim of suggestions for further improvements.

Additionally, no interviews were conducted with general end-users due to time constraints as well as the fact that such an exercise would be beyond the scope and reach of the charted research.

3.4.1.2 Testing analysis

There were two data gathering phases to obtain security data and information of the email and online web systems for the testing at each of the selected councils. This was to identify any potential security vulnerabilities or risks at these sites. Additional details were discussed and provided in Section 3.3.2.

3.4.2 Secondary data

The secondary data was made up of the document review. This review was a detailed inspection of all existing information, network diagrams and related IT security policies, and procedures documentation in both paper-based and electronic-based formats was done as permitted by each of the selected councils.

These documentations were used for analysis and comparison with particular references, for the internetwork infrastructure, system details and security policy of both the email and online web systems at each of the selected councils. They were later used as suitable guidelines for these councils in the reporting stages of the research.

3.4.3 Software

The software used to test both the email and online web systems were NMAP, GFI LANguard and Telnet. Both NMAP and GFI LANguard are well-known network scanning tools, which are powerful and widely used by IT security professionals. In addition, both NMAP and GFI LANguard use different algorithms for testing the network and extracting system information such as hardware, software, service(s), patch(s), port(s) and vulnerability(s) (personal communications with Professor Dr. Craig Valli and Dr. Andrew Woodward, 2008, 2009), thereby complementing each other.

3.4.3.1 NMAP

NMAP is the open source software available freely from the Internet. NMAP with GUI standard called Zenmap version 5.0 for MS Windows XP version was used. In order to obtain as much information as possible from the email and online web systems' servers, the slow comprehensive scan option was used in all tests. This option returned all relevant information about TCP, UDP ports, vulnerabilities, patches, services, software and hardware (Lyon, 2009).

3.4.3.2 GFI LANguard

GFI LANguard version 9.0 is the commercial software that was deployed in all of the tests. The full scan option of GFI LANguard was used in order to fully test and collect the email and online web systems information. The software collected TCP, UDP ports, vulnerabilities, patches, services, software and hardware information. It also provided the vulnerability information which assisted in the analysis of both the email and online web systems (GFI, 2009).

3.4.3.3 Telnet

MS Telnet software was employed to test against the email system for spoofing of email at each of the selected councils. This was conducted by telnetting to port 25 (SMTP) and manually probing the systems.

3.5 Conceptual framework

Figure 3.3 is the conceptual framework for each interpretive case study within the selected local councils in WA. This conceptual framework demonstrated a process as well as some techniques to collect and analyse data from a variety of sources. The use of interviews, document review and systems testing results and analyses provided a context for the examination and interpretation of the level of security information from a variety of perspectives, and was used to generate the report details of the testing analyses back to the selected councils.

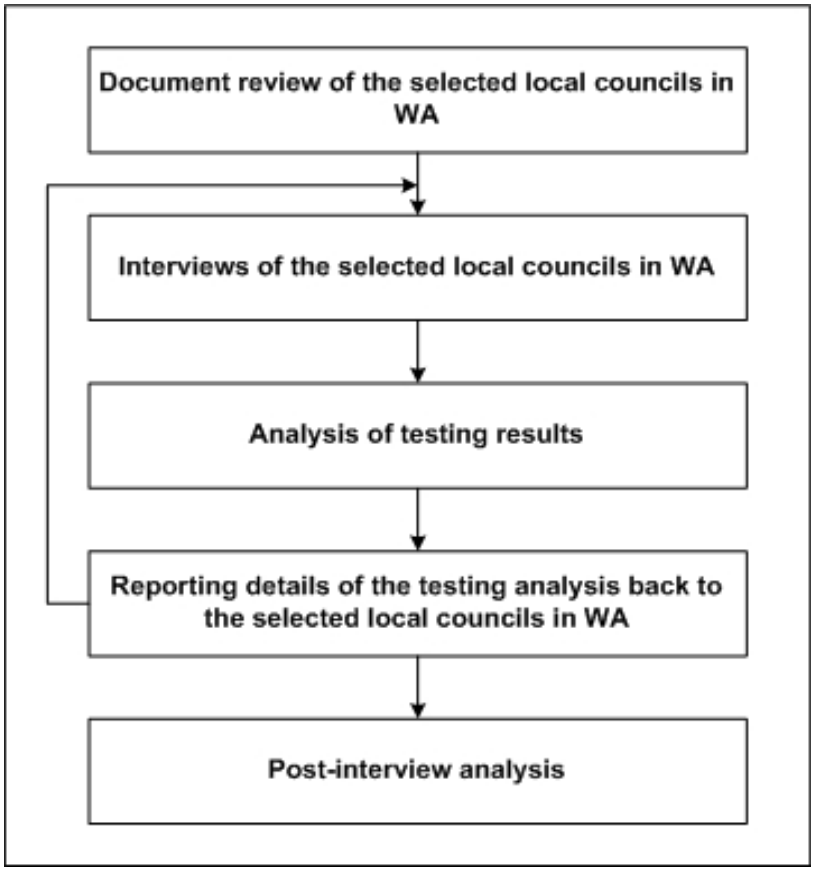

Figure 3.3. A conceptual framework for the processes involved in the audit of any case study

There were five main procedures in the conceptual framework and details are as below.

1) *Document review of the selected local councils in WA:* This procedure related to the review of the current internetwork diagrams, the specifications and the configuration codes of internetwork devices, the policy documentations and the literature relating to the use of the email and online web systems in the selected councils.
2) *Interviews with the selected local councils in WA:* This procedure focused on the interviews of the IT managerial and IT operational staff regarding and relating to the use of the email and online web systems in the selected councils.
3) *Analysis of testing results:* This procedure involved the use of three network application analysis tools to investigate the email and online web systems for further assessment. These tools were NMAP, GFI LANguard and Telnet.
4) *Reporting details of the testing analysis back to the selected local councils in WA:* This procedure was about the findings from the testing analysis of the email and online web systems that were reported back to the selected councils for further assessment, consideration and implementation.
5) *Post-interview analysis:* This procedure involved the post-interview analysis of the IT managerial and IT operational staff about their perceptions and thoughts about the findings from both the email and online web system testing analyses.

3.6 Limitations of the research

There were two major factors that limited the research. A common criticism of case study methodology is that its dependence on a single case renders it insufficient and incompetent of providing a generalising conclusion (Hamel et al., 1993; Myers, 2000; Tellis, 1997; Yin, 1984, 1993, 1994). However, this limitation was offset as the findings were replicated from the multiple-case studies. Due to the extensiveness of data collection and collation and its subsequent analysis, it is believed that three to four case studies may provide a good logical model of information security frameworks for local councils in WA. Although the selected councils needed to have had reasonable Internet infrastructure and related technologies installed, this situation may not be applicable to small regional councils/shires.

However, the information security frameworks developed as results of this research, provide recommendations which may be adopted by any other councils and/or organisations for their information security implementation.

Another limitation of this research was that the selected councils have moderately been alerted to the existing security problems of their email and online web systems. As a result, it would probably have introduced some bias into the selection and subsequent assessment of the cases.

3.7 Summary

This chapter described the research method, background and the developed information security frameworks for the email and online web systems deployed in this research. Klein and Myers (1999)'s principles of interpretive multiple-case studies was the design model used for conducting this research.

Case study research design and procedures were served to integrate a proper alternative of qualitative techniques to raise the prosperity, validity and reliability of the research. Research materials were then explained in detail in Section 3.4. An outline of the possible limitations in case study research design and procedures, together with a strategy to minimise these weaknesses have also been provided.

Accordingly, the research method deployed in this research was adopted and applied into each case which can be leaded to the results and fidings to the following chapters.

CHAPTER 4. EXPERIMENTAL EVALUATION AND ANALYSIS: A CASE STUDY OF COUNCIL A

This chapter aims to illustrate the results and findings from Council A's email and online web systems investigated in the research. It consists of five subsections as (1) background information; (2) methodology; (3) CouncilA's email system results; (4) Council A's online web system results; and (5) analysis and discusion.

4.1 Background information

Council A is a WA local government council which has its own IT department. Currently, the council's main computer network is located at the external host Internet Service Provider (ISP) location which is connected to all the council sites including central and remote sites via fibre optic, Digital Subscriber Line (DSL) and Asymmetric Digital Subscriber Line (ADSL) connections. The council is connected to the outside world or the Internet through the external ISP via a fibre optic connection. The network architecture of Council A is identified as star topology architecture. All the council's IT service systems such as email, Intranet, property, GIS, financial and online web systems are located at the external host site. In addition, all the IT systems including both email and online web systems are managed by its own internal IT staff members.

Council A's email system has over 1,000 mailboxes which serve mainly its staff as well as the councillors and external contractors. MS Exchange 2007 is used by the council as an email application server whereas MS Outlook 2007 is used as the email client and personal information management tool. Furthermore, webmail or the web-based email (OWA – Outlook Web Access) feature is available to its staff for accessing the mailboxes externally from the web.

In terms of the online web system services, the council provides general information, mailing lists and online community groups to its residents and interested persons. In addition, the council provides online payment services to its registered residents and it uses a third-party software called "Epathway" (Infor, 2009) for its online payment system.

4.2 Methodology

This subsection aims to provide the details on methodology utilised in this research. It is categorised into six parts: (1) pre-interview consultation; (2) document review; (3) interview investigation; (4) existing architecture discovery; (5) email system testing; and (6) online web system testing.

4.2.1 Pre-interview consultation

Firstly, there was an initial open-ended meeting between the researcher, the principal supervisor and the council's IT manager in order to determine the scope of the project. As a result, all involved parties agreed that both email and online web systems would be audited in order to determine any potential risks and recommendation solutions.

The council agreed to an overall time frame of six months which included an estimate of three months for each report produced. Furthermore, the IT manager stipulated that this project was to be undertaken at no cost to the council and the council could end or abort this project at anytime as desired. It was also agreed that two reports with recommendations would be presented and distributed to the council in succession which were email and online web systems respectively.

4.2.2 Document review

Two types of related documents, which were specification documents hardware and software and the council policy documents were available.

Several documents relating to Council A's email and online web systems were collected. For example, configuration codes and specifications of the Internet border router, the IDS/IPS, the Internet border switch, the DMZ switch, the internal switch, the firewalls, the email server, the spam blocker appliances, the web servers and the backend database server. In addition, copies of the DMZ internetwork and overall network diagrams were collected.

In terms of IT security in relation to the email and online web systems, it was advised that both the enterprise information security and technical (both issue-specific and systems-specific) security policies were non-existent. Currently, Council A has the internet usage policy for a library community access to the internet (see Appendix A24).

4.2.3 Interview investigation

Several interviews were conducted with the three stakeholder groups as follows:

- The IT manager of Council A;
- The council's IT operational staff (network, application and telecommunication administrators); and
- The council's external IT staff (database administrator).

The face-to-face interview with the IT manager was used to obtain a general overview of Council A's overall network and services, particularly with regards to the email and online web systems. The scope of the project was discussed including any possible potential risk issues overall, while conducting the project.

Several ongoing interviews were conducted with the network, the Epathway application, the telecommunication and the database administrators. Several interview techniques were used such as face-to-face, telephone and email.

The interviews carried out with the council's network administrator and the telecommunication administrator were mainly related to discussions of the council infrastructure and its network connectivity which includes the firewalls, the Internet border router, the IDS/IPS, the switch, the virus protection system, the email server, the Active Directory (AD) and the DNS. In addition, the related configuration codes of all the related devices were discussed.

In terms of the web, application and database servers, there were several testing analyses and interviews conducted with the online payment application (Epathway) and the external database administrators. These testings covered the configurations of the council's online payment system servers which are the frontend web server, the application server and the backend database server.

4.2.4 Existing architecture discovery

This section details the discovery of the existing architecture and structural operation relating to the email and online web systems of Council A.

4.2.4.1 The existing email system architecture of Council A

The email system of Council A has one email server and one spam blocker appliance. Both devices are connected together within the council's network infrastructure at the data centre which is located at the council's ISP. The email server resides in the internal network while the spam blocker appliance is located in the DMZ area.

In terms of the infrastructure devices, the council has one Internet border router, one firewall, and three switches.

Figure 4.1 demonstrates the email system related devices connectivity and allowed email protocols in a high level network diagram.

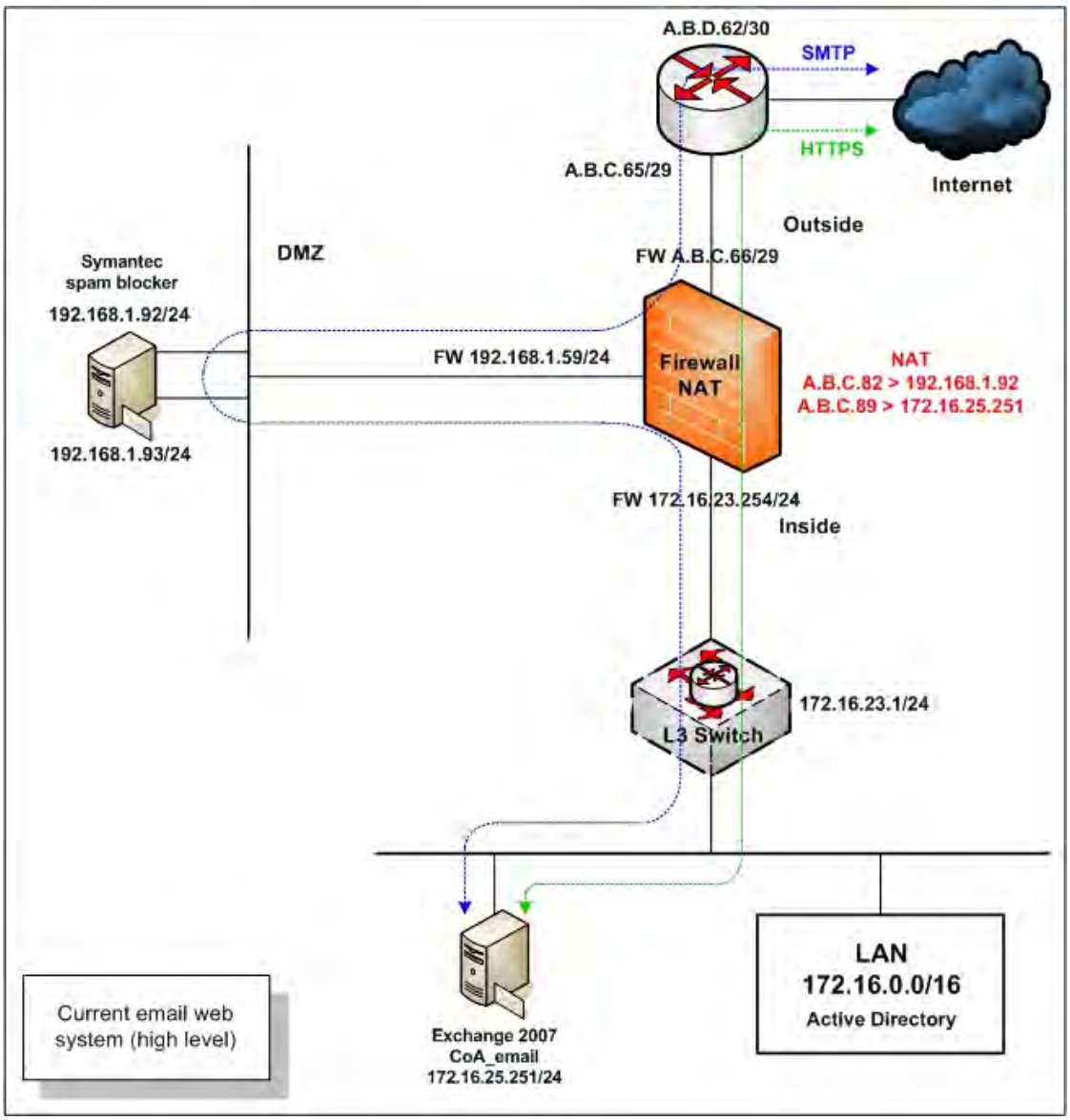

Figure 4.1. A current high level network diagram for the email system of Council A

In addition, two related email protocols, HTTPS and SMTP are allowed in the network. Both protocols provide typical email and secured webmail (HTTPS) services respectively to the council's staff. In terms of webmail, the current email server (MS Exchange 2007) is configured to support the Client Access Server (CAS) form via MS Outlook Web App/Outlook Web Access (OWA). Other CAS forms such as MS Outlook Anywhere and MS ActiveSync are not supported. Furthermore, Council A's webmail service uses 128-bit encryption with standard validation SSL certificate (Limwiriyakul & Valli, 2011c).

4.2.4.2 The existing online web system's architecture of Council A

Council A has two online web systems which are the static web system and the online payment system. The council's online web system (online payment system) serves its residents in terms of online payment services such as rates and infringements. The online web servers are located in the DMZ and the internal network areas. As previously mentioned, the council's online static web system was not tested. Therefore, the online static web system is only briefly discussed in the following section.

4.2.4.2.1 The existing static web system architecture

The council static web system consists of two web servers which are the Internet web server and the Intranet web server. The Internet web server is located in the DMZ and the Intranet web server is located in the council's internal network. Both the Internet web and the Intranet web servers interact with each other in a one-way direction from the inside through the DMZ area via HTTP web protocol. This means that only the Intranet web server can send HTTP web traffic to the Intranet web server. In addition, the council's media staff periodically pushes the updated data to the Internet web server.

4.2.4.2.2 The existing online payment system architecture

The council's existing online payment system can be considered as a multi-tiered (3) client-server architecture which consists mainly of a frontend web, application, and backend database servers (Microsoft Corporation, 2010).

The existing system is comprised of the frontend web server (CoA-DMZ-Epathweb), the application server (CoA-Pathway) and the backend database SQL server (CoA-SQL) as depicted in Figure 4.2.

The frontend web and application servers perform all of the application logic. The backend database server performs the data logic. In terms of application software, the council uses a third-party Pathway application with the online payment feature. Typically, three-tiered client-server architecture consists of the following three components:

- Presentation logic – displays information and content which is normally related to the user interface and user interactions via the client web browser;
- Application logic (business, middle tier, data access) – synchronises the application, processes necessary commands and calculations required from the web and application servers; and
- Data logic – deals with the storage and retrieval of information from the database or file server (Microsoft Corporation, 2010).

There are benefits of deploying a three-tier client-server architecture as compared to traditional application architectures (host-based and client-based architectures). They are as follows:

- Improved availability – redundant application servers can be deployed in case of hardware failure for critical applications;
- Scalability – the system can be expanded to deploy more application servers (Microsoft Corporation, 2010);
- Better security – no direct connection between client and database thereby ensuring data integrity. Moreover, the database is transparent;
- Reduced distribution – changes to application/business logic are done once only on the server with no requirement to be distributed to all the clients; and
- Easier to implement – "complex application rules are easy to implement in application server" (Kambalyal, n.d., p. 12).

In addition, the council used an external gateway security payment service to provide a secured online payment service for its residents. Both the council's online payment system and the external gateway security payment services communicate using the HTTPS protocol over a SSL connection which uses 128-bit encryption with standard validation SSL certificate same as its webmail system (Limwiriyakul & Valli, 2011c).

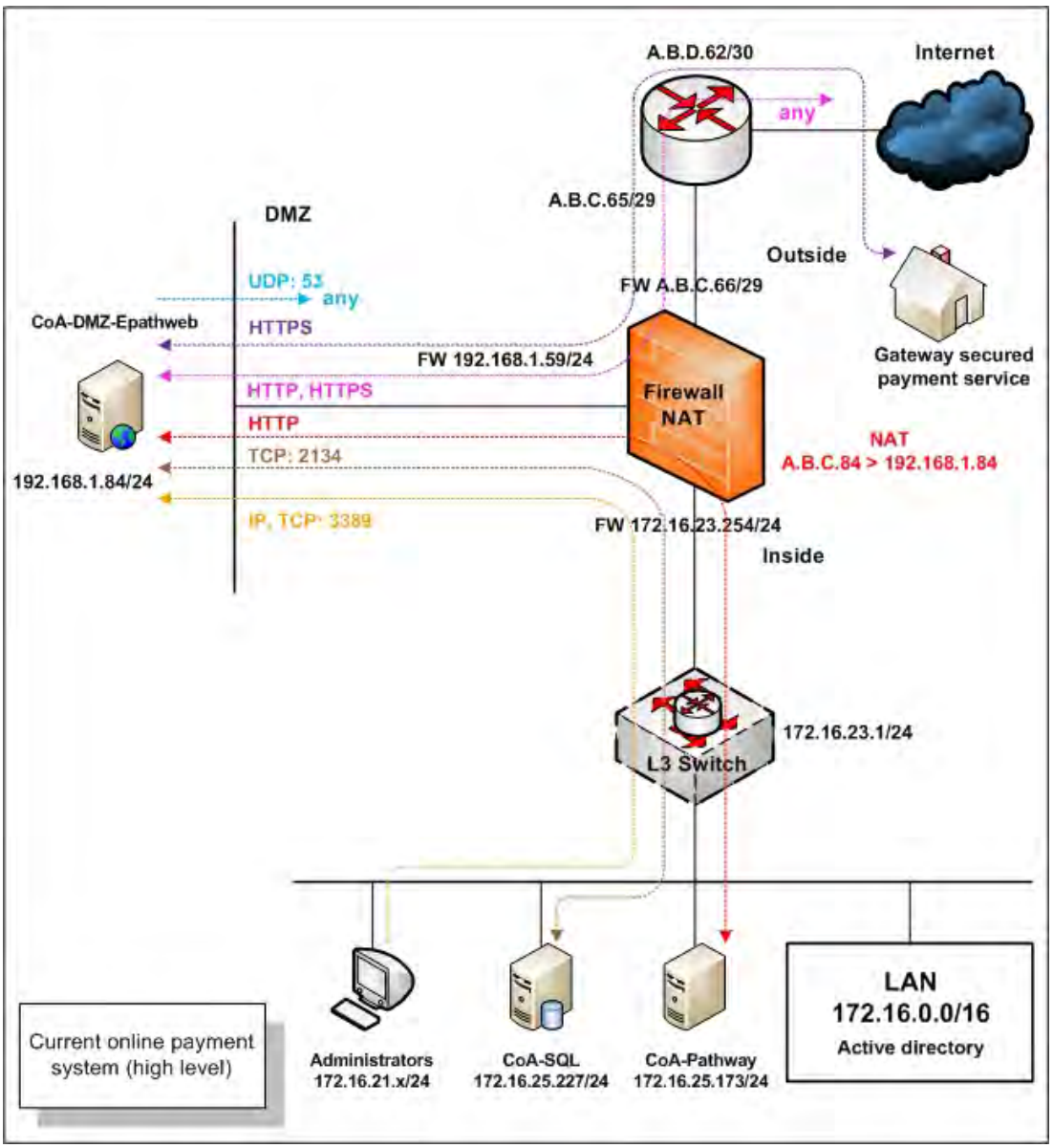

Figure 4.2. The high level online payment system including network traffic protocols currently in use by Council A

4.2.5 Email system testing

There were five stages which are summarised as follows:

- Network surveying includes discovery of the network architecture of the email system of Council. See Section 4.2.4.1 for more details. This testing stage also gathers information on the specifications of the email server and the spam blocker appliances of council A;

- Auditing and configuration codes review of the council's Internet infrastructure including Internet border router, IDS/IPS, firewalls and switching devices;
- Services and system identification, port scanning and vulnerability testing of the email server;
- Email spoofing testing and vendor security benchmark auditing on the email server and the spam blocker appliance; and
- Email system security policy review.

4.2.6 Online web system testing

The online web system of the council can be categorised into two distinct application profiles which are the static web system and the online payment system. Both the static web and online payment systems have their own separate hardware for servers.

However, the testing analysis was restricted to the on the online payment system as requested by the council's IT operational staff. This online web system testing analysis which was conducted consists of five stages which are summarised as follows:

- Network surveying: comprises the network architecture of the online payment system of Council A. See Section 4.2.4.2 for more details. This testing stage also gathers information from the static web, application and backend database servers related to the online web system of the council;
- Identified risks review for the council's internetwork infrastructure devices which related to Council A's online payment system;
- Services and system identification, port scanning and vulnerability testing of the council's online payment system's servers;
- Vendor security benchmark auditing on the council's online payment database server; and
- Reviewing the council's online payment system security policy.

4.3 Council A's email system results

The architecture design, the device configurations, the vulnerabilities of all the email system servers, the email spoofing, the vendor security benchmark and the security policy were successfully tested, audited and reviewed. The following sections describe all the results of these testings in detail.

4.3.1 Testing stage 1: Network surveying

In this first testing stage, information of the council's email system which includes the email and spam blocker appliances, the infrastructure architecture and devices were collected. The following information was collected:

- Overall network diagram for the Internet link, the DMZ infrastructure connectivity including the email system; See Section 4.2.4.1 for more details;
- The specification and related email configuration codes of the Internet border router, the Internet firewall, the Internet switch and two DMZ switches;
- The email server's specification summary; and
- The spam blocker appliance's specification summary.

The following sections describe the overall summary specifications of the email and spam blocker appliances and the associated identified risks.

4.3.1.1 The email system devices

There are two specific devices which are the email server (MS Exchange 2007) and the Symantec spam blocker appliance in Council A's email system.

4.3.1.1.1 The email server

The current email server of Council A was migrated from its old MS Exchange 2003 email server. The email server has MS Windows Server 2003 Enterprise Edition with service pack 2 as an OS. MS Exchange 2007 with service pack 1 is used as the email

application. The current MS Exchange 2007 email application configuration of the email server was configured as a simple single-server architecture which consisted of three of five server roles which are the Mailbox server, the Hub Transport server and the CAS roles.

Nevertheless, the other two MS Exchange 2007 feature server roles; the Edge Transport and the Unified Messaging servers were not installed. This was due to the fact that Council A uses the Symantec spam blocker and the Cisco Unity voice mail system which perform the same function as the Edge Transport server role and the Unified Messaging server role respectively. Table 4.1 summarises the email server specifications.

Table 4.1 *A summary of the email server specifications*

Attributes	**Details**
Email application software	MS Exchange 2007 with service pack 1
Email scanning software	None
OS	MS Windows Server 2003 Enterprise Edition with service pack 2
Hardware	8 Gigabyte (GB) Random Access Memory (RAM), Hard disks C: 20GB, e: 180GB, f: 200GB
IP address	172.16.25.251/24
MS Exchange 2007 server roles	Mailbox, Hub Transport, CAS combined
Email service protocols	SMTP and HTTPS
Other software	None

In addition, according to Microsoft TechNet (2007a), a simple single-server architecture (MS Exchange 2007) should only be deployed in Windows's Small Business Server (SBS) which is suitable for small network environments.

Figure 4.3 demonstrates MS Exchange Server 2007 architecture based on a single-role server.

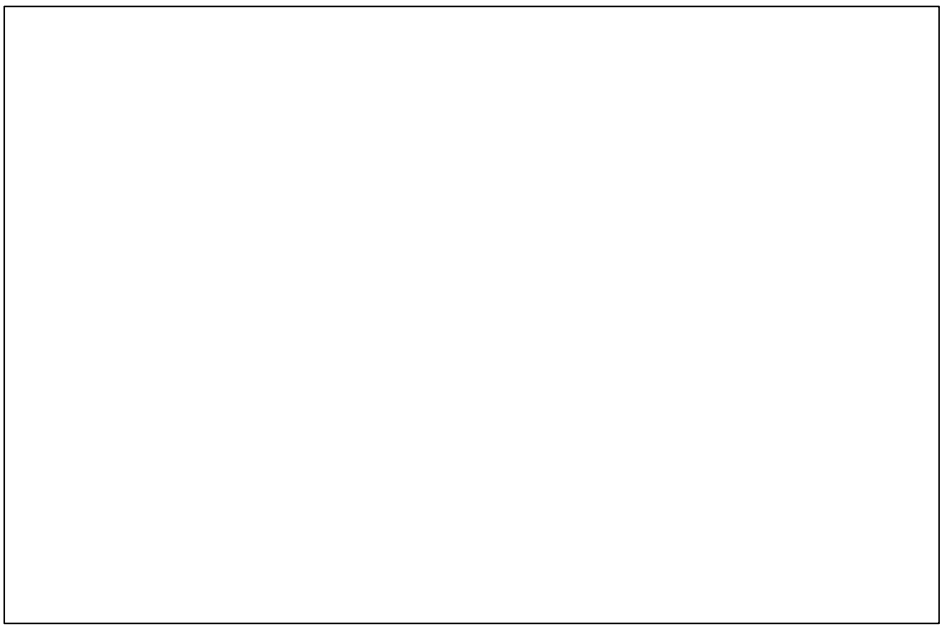

Figure 4.3. The MS Exchange Server 2007 architecture based on a single-role server *(Source: Microsoft TechNet, 2007a, p. 37)*

Furthermore, the following summarises the MS Exchange 2007's server roles (Microsoft Exchange Documentation Team, 2009).

- CAS(s): to support Post Office Protocol 3 (POP3) and Internet Message Access Protocol 4 (IMAP4) clients, MS Exchange ActiveSync, MS Office OWA and MS Outlook Anywhere and new MS Outlook 2007 client functions;
- Edge Transport server(s): to handle message traffic to and from the Internet, run spam filters and handle SMTP relay;
- Hub Transport server(s): to perform the internal message transfer, distribution list expansions, and message conversions between Internet mail and MS Exchange Server message formats;
- Mailbox server(s): to manage mailboxes, store databases and provide MS Office Outlook clients and CAS with access to the data; and
- Unified Messaging server(s): to integrate voice and fax with email messaging and run Outlook Voice Access.

4.3.1.1.2 The spam blocker appliance

The spam blocker appliance was running on a Symantec hardware appliance with mail security for MS Exchange Server 2007 software. The purpose of this box is to filter all incoming email (SMTP) against virus and worm threats and to block spam emails. The spam blocker appliance has two network interfaces which are 192.168.1.92 and 192.168.1.93. When incoming SMTP traffic enter the council's network it goes through the 192.168.1.92 interface of the spam blocker appliance. Then, the SMTP traffic is checked and cleaned by the spam blocker appliance before forwarding the cleaned SMTP traffic to the firewall via its 192.168.1.93 interface. See Figure 4.4 for the detail on the demonstrated network connectivity of the council's spam blocker appliance.

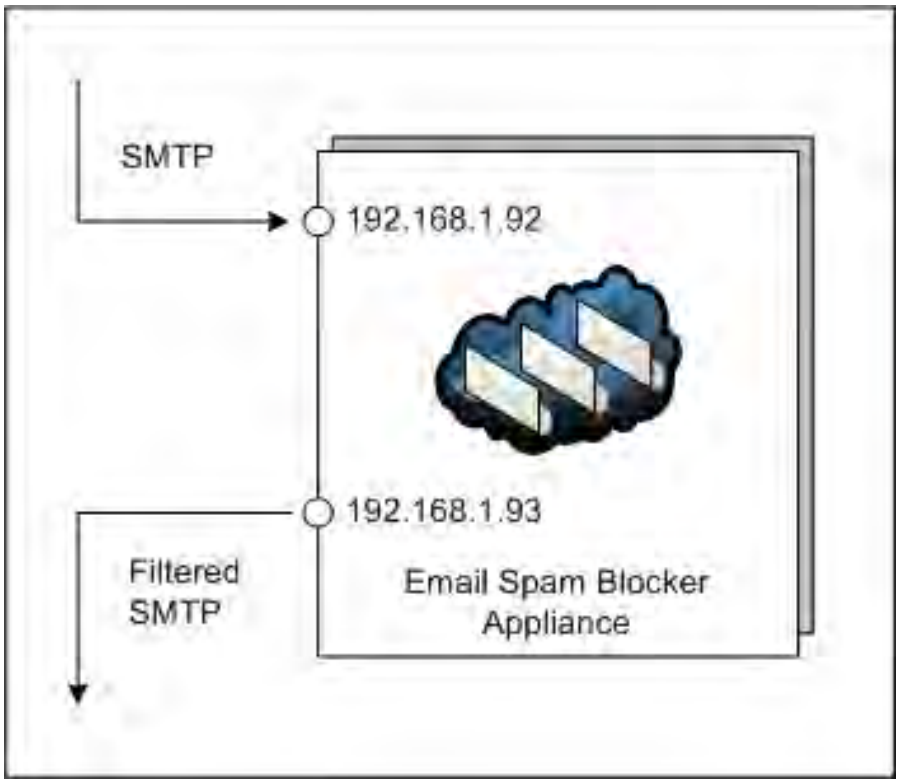

Figure 4.4. A high level diagram of Council A's email spam blocker appliance

As compared to MS Exchange 2007 server roles, this spam blocker appliance performs the same as the MS Edge Transport server role. Table 4.2 summarised the spam blocker appliance role.

Table 4.2 *A summary of the spam blocker appliance specifications*

Attributes	**Details**
Spam blocker application software	Symantec Mail Security Suite 5.0.0-36
OS	Symantec
Hardware	Stand alone appliance
Interfaces	192.168.1.92 for sending and receiving SMTP traffics between outside/external and DMZ networks 192.168.1.93 for sending and receiving SMTP traffics between the council A inside/internal and DMZ networks
Feature roles	Scan virus, block spam email, block emails blacklist

4.3.1.2 Testing stage 1: Identified risk issues

The identified risk issues of testing stage 1 for Council A's email system are described in the following sections.

- ***Risk 1: Virus protection software***

The current email server does not have any virus protection software installed. This may be a source of potential risks against virus and worm attacks.

- ***Risk 2: Single point of failure***

Council A's current email architecture may be considered as a simple single-server architecture as previously mentioned. As per recommended best practices by Microsoft Exchange Documentation Team (2009), a simple single-server (MS Exchange 2007) architecture should only be installed in MS Windows SBS which is typically designed for small network environments and low network loads. However, the current Council A's email system and its network environment are considered to be a medium-sized network as the email server handles over 1,000 mailboxes and provides email services to over 700 staff.

The current email server performs three MS Exchange 2007 server roles concurrently as previously mentioned. Therefore, this may be considered as being a single point of failure due to the single email server having to handle all three MS Exchange server roles.

- ***Risk 3: Same subnetwork***

The existing email server is positioned in the council's internal network and on the same subnetwork Virtual Local Area Network 5 (VLAN5) with all the other council's servers. This configuration may be exposing the council to potential risks as there are no filtering mechanisms in place to separate or isolate traffic between the email and the other council's servers.

This may cause possible direct or indirect interruptions to Council A's IT services in the case of the email server being compromised, thereby allowing any infections or intrusions to spread to other servers within the network. The filtering of network traffic to and from the email server may therefore prevent or reduce this risk. The network traffic filtering can be performed at Council A's core switch.

4.3.2 Testing stage 2: The email system's infrastructure – Internet border router, IDS/IPS, firewalls and switch reviews

The data collection of the device configuration codes for the Internet border router, the IDS/IPS, the firewall and the switch were reviewed and are presented in the following sections.

4.3.2.1 Internet border router configuration codes data collection and reviews

Council A's Internet border router is designed for routing purposes to route either forward or reverse the council's internetwork traffic or supported protocols such as Citrix server and client services, email and WWW. The current router is also configured to filter unnecessary traffic which means only permitted protocols are allowed to enter and leave the council's network. Table 4.3 summarises the specifications of the Internet border router.

Table 4.3 *A summary of the Internet border router specifications*

Attributes	**Details**
Device type	Cisco router 2811
OS	Cisco Internetwork OS (IOS) 12.4
Memory	256 Megabyte (MB) RAM, 64MB flash
Interface (2)	2 x Ethernet 10/100 full duplex
IP address	A.B.D.62/30, A.B.C.65/29

4.3.2.2 IDS/IPS configuration codes data collection and reviews

The Internet border router and the firewall of Council A have their own built-in IDS/IPS and IPS features respectively. However, the IPS features on both these devices were currently disabled. It is important to have an active IDS/IPS system to provide early warning information about intrusions or intrusion attempts to the network or system administrators.

This information may reduce any potential risks against the network including the email system by allowing the network or the system administrator ample time to counteract the intrusion threats.

4.3.2.3 Firewall configuration codes data collection and reviews

The firewall of Council A provides filtering of both incoming and outgoing internetwork traffic. The firewall also performs NAT. Table 4.4 summarises the specifications of the firewall. See previous Figure 4.1 for illustration of the firewall network architecture. In addition, the summary of the firewall configuration codes including NAT related to the email system are summarised in Appendix A1.

Furthermore, Appendix A2 shows the summary of the firewall codes with respect to Council A’s email system.

Table 4.4 *A summary of the firewall specifications*

Attributes	**Details**
Device type	Cisco ASA
OS	ASA version 7.1 (2)
Memory	512 MB RAM, 64MB flash
Interfaces	5 x Ethernet 10/100 full duplex
IP addresses	Interface gigabit 0/0: A.B.C.66 Interface gigabit 0/1.16: 172.16.23.254, Interface gigabit 0/1.69: 192.168.1.254 Interface gigabit 0/2.31: 172.33.0.1 (Virtual Private Network or VPN), Interface gigabit 0/2.67: A.B.C.x (VPN) Interface gigabit 0/3.10: LAN failover, Interface gigabit 0/3.11: state failover Interface management 0/0: 10.1.80.11

In addition, the access to the firewalls for administration purposes is already securely configured as it only allows authorised staff (IT administrators) access based on computer IP addresses. Both Secure Shell (SSH) and HTTPS are the only secure communication methods which only permit valid username and password combinations.

4.3.2.4 Switch configuration codes data collection and reviews

Council A has three Ethernet switches which provide connectivity for the council's internetwork. The Outside_sw provides connections between the Internet border router and the firewalls. The Fwswitch and DMZ_sw switches provide DMZ connections for the council's DMZ servers.

In addition, the Fwswitch is connected to the council's core switch (Cisco Catalyst 6500). The council's core switch provides backbone and internal server connectivity. The current overall hardware and software details of the three switches are depicted in Table 4.5. The details on ports, VLANs including its connectivity are provided in Figure 4.5.

Table 4.5 *Current switches hardware and software details of Council A's internetworking system*

Attributes	**Details**
Device name	Outside_sw
Device type	Cisco Catalyst 3650 SM switch
OS	Cisco IOS version 12.2
Memory	256 MB
Port	24 x 10/100 MB Unshielded Twisted Pair (UTP) Ethernet ports, 2 x GB Small Form-Factor Pluggable (SFP) ports
Operate at	Layer 2 Open Systems Interconnection (OSI)
IP address	A.B.C.69
VLAN number	1
Device name	Fwswitch
Device type	Cisco Catalyst 3650 SM switch
OS	Cisco IOS version 12.2
Memory	256 MB
Port	24 x 10/100 MB UTP Ethernet ports, 2 x GB SFP ports
Operate at	Layer 2 OSI
IP address	None
VLAN number(s)	20, 254
Device name	DMZ_sw
Device type	Cisco Catalyst 3650 SM switch
OS	Cisco IOS version 12.2
Memory	256 MB
Port	24 x 10/100 MB UTP Ethernet ports, 2 x GB SFP ports
Operate at	Layer 2 OSI
IP address	192.168.1.250/24
VLAN number(s)	1, 16, 31, 67, 69

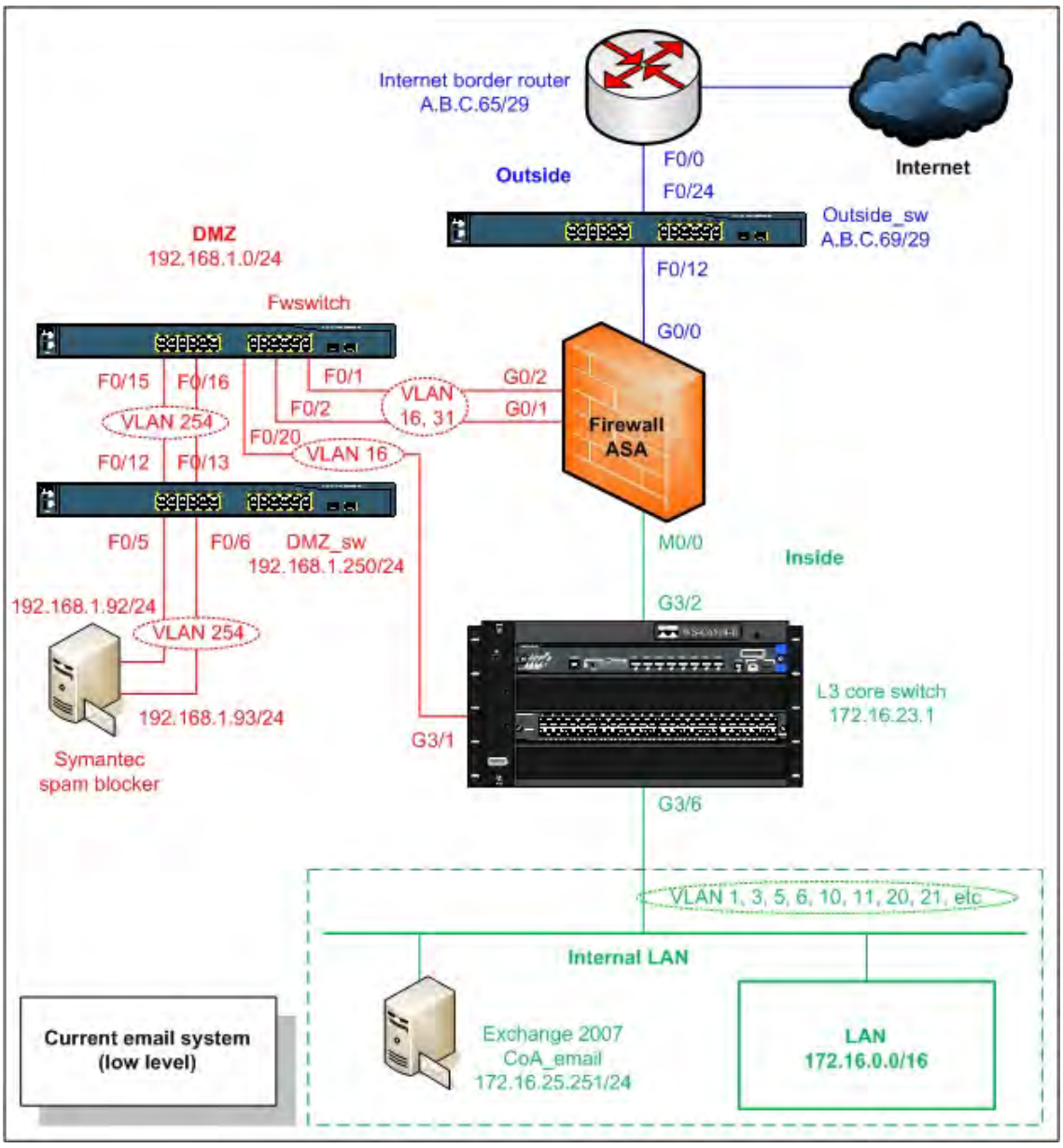

Figure 4.5. A current low level network diagram of the email system for Council A

4.3.2.5 Testing stage 2: Identified risk issues

The following section details the identified risk issue for the council's email infrastructure system (Internet border router, the IDS/IPS, the firewall and the switches).

- ***Risk 1: Unnecessary ACL coding on the Internet border router***

There was a single unnecessary configuration code (see Appendix A2: Policy number 3) uncovered on the Internet border router.

- ***Risk 2: Internet border router's IDS was disabled***

Currently, the built-in IDS/IPS feature of the Internet border router (Cisco 2811) is disabled which may be a potential security risk due to being vulnerable to scanning and spoofing attacks.

- ***Risk 3: Firewall's IPS was disabled***

The current IPS feature on the firewall (Cisco ASA) is disabled which means both incoming and outgoing SMTP and HTTPS email related protocols are not inspected. This may cause potential risks, such as DoS and malicious code attacks (Check Point Software Technologies Ltd., 2010) to the council's network and email system.

- ***Risk 4: Inadequate firewall ACL coding – HTTP and HTTPS***

The current firewall rule (see Appendix A2: Policy number 1) allows the spam blocker appliance (interface 192.168.1.92) access anywhere via HTTP and HTTPS ports.

- ***Risk 5: Unused firewall ACL coding – LDAP, MS-DS***

The current firewall rules (see Appendix A2: Policy numbers 4, 8 and 9) are configured to allow the decommissioned internal server (172.16.5.70) and the spam blocker appliance to communicate via LDAP and MS-DS ports.

- ***Risk 6: Inadequate firewall ACL coding – SMTP***

The current firewall rule (see Appendix A2: Policy number 10) allows the spam blocker appliance (interface 192.168.1.92) to directly access the email server via SMTP port, which is an inadequate configuration code.

- ***Risk 7: Unused firewall ACL coding – MS-WBT-Server***

The current firewall rule (see Appendix A2: Policy number 16) is configured to allow the email server to access the decommissioned server (192.168.1.89) in the DMZ via TCP port 3389.

- ***Risk 8: Overall inadequate switch code security configurations***

There were some insufficient switch security configuration codes on all the three Ethernet switches. These may cause potential security risks such as Address Resolution Protocol (ARP) spoofing, ARP poisoning and broadcast storm attacks to Council A's internetwork.

4.3.3 Testing stage 3: Services and system identification, port scanning, vulnerability testing and results

NMAP and GFI LANguard were the network scanning tools used for all three testing steps of this third testing stage. Both the software applications were run with full scan or comprehensive options in order to collect as much information as possible, as well as to fully test the council's email system at the same time. This use of the applications in this way creates scanning that is rigorous and intense.

4.3.3.1 Services and system identification results

The results of the services and system identification of Council A's MS Exchange 2007 email server are described in the following sections. However, there was no testing on the spam blocker appliance conducted as it was prohibited by the council's IT manager. More details are provided in Appendices A3 and A4.

4.3.3.2 Port scanning results

The port scanning testing analysis using both NMAP and GFI LANguard was successfully performed on the council's email server. However, no port scanning was performed on the council's spam blocker as requested by the IT staff.

Full details of the port scanning results of the council's email server are found in Appendix A5.

4.3.3.3 Vulnerability testing results

The vulnerability testing was successfully conducted on Council A's email server. However, as previously mentioned, testing of the spam blocker appliance was prohibited. Therefore, there was no vulnerability testing done on the spam blocker appliance. The vulnerabilities of the email server are categorised into four security levels which are high (H), medium (M), low (L) and potential (P) based on GFI LANguard analysis software. Full details of the vulnerability testing results of the council's email server are presented in Appendix A6.

4.3.3.4 Testing stage 3: Identified risk issues

The identified risk issues of Testing stage 3 for Council A's email system are described as follows.

- ***Risk 1: System information policy results for the email server***

There were inadequate measures of the system information policy's configuration of the council's email server which may cause potential risks to the council's email system.

- ***Risk 2: System patching status results for the email server***

Both GFI LANguard and NMAP network scanning tools were used to test the system patching status of the council's email server. There were vulnerability issues uncovered which may create possible threats to the email server. The scan uncovered that the service packs were current but there were nine missing patches on the email server. See Appendix A4 for more details.

- ***Risk 3: Unnecessary opened ports on the email server***

There were no issues found on the UDP ports. However, there were some issues uncovered on the TCP ports of the email server. These TCP ports were unnecessarily opened ports which pose potential risks to the council's email server. Table 4.6 displays the total numbers of TCP service ports opened on the email server. Furthermore, the full details of all both opened TCP and UDP service ports including the possible mitigation recommendations for the email server are listed in Appendix A5.

Table 4.6 *List of the number of open TCP and UDP ports on the email server*

Server name	Opened TCP ports	Opened UDP ports	Comment
Email server	31	5	Refer to Appendix A5

- ***Risk 4: Vulnerabilities found on the email server***

In terms of identified risk issues, there were two high, seven low and three potential risk categories uncovered issues found on the council's email server. For examples, there were unnecessary TCP services left opened such as File Transfer Protocol (FTP) and POP3. TCP services were inadvertently left opened which may cause potential risks to the council's email system. Table 4.7 shows the total numbers of the vulnerabilities found on the email server.

Table 4.7 *The overall of Council A's email server – vulnerabilities*

Server name	H	M	L	P	Overall vulnerability level	Comment
Email server	2	0	7	3	High (10/10)	Refer to Appendix A6

4.3.4 Testing stage 4: Spoofing testing and vendor security benchmark email server auditing

4.3.4.1 Email system spoofing testing results

There were several spoofing testings conducted on the email server. Furthermore, at this time the council's IT manager permitted testing the council's spam blocker appliance. Therefore, both interfaces (192.168.1.92 and 192.168.1.93) of the spam blocker appliance were also tested. A CIS template was used for the spoofing testings. There were identified risk issues found on the email server and the spam blocker appliance (interface 192.168.1.92). In terms of spoofing, there was no identified risk found on the spam blocker appliance (interface 192.168.1.93).

In addition, there was an egression testing on Council A's email system. As per best practice guidelines recommended by OSSTMM (Herzog, 2006) the council's email system correctly disallowed sending email from an internal address to either an internal or external address using a third-party POP3 server such as Yahoo Mail server. The egression testing result is presented in Table 4.8.

Table 4.8 *The egression testing result and recommendation for Council A's email system*

Testing technique	**Purpose**	**Result**	**Recommendation**
Sending an email from one internal address to either an internal or external addresses using an external, a third-party POP server.	To test egression	Unsuccessful	None

4.3.4.2 Specific email security vendor auditing results

CIS for MS Exchange 2007 for MS Windows Server 2003 version 1 was modified to suit Council A's email system. The modified auditing checklist was successfully tested on the council's email server. The current MS Exchange 2007 email server was not configured for both the Exchange Edge Transport and Unified Messaging server roles. Therefore, both server roles were not included in the modified auditing checklist.

The summary auditing results and mitigation recommendations of the MS Exchange 2007 email server are categorised into three server roles which are the Mailbox server, the Hub Transport server and the CAS roles. Tables 4.23, 4.24 and 4.25 on Section 4.5.1.1 provide details of these auditing results.

4.3.4.3 Testing stage 4: Identified risk issues

The identified risk issues for the email spoofing, the Mailbox server, the Hub Transport server and the CAS roles of the council's email server are presented as follows.

- ***Risk 1: The email server allowed relaying***

Both internal and external relaying was allowed to be sent internally on the email server. This mail relaying may be a cause of potential risks from internal spoofing attacks to the council's email server.

- ***Risk 2: The spam blocker appliance (interface 192.168.1.92) allowed relaying***

Similar to the situation on the email server, emails from both internal and external source addresses were allowed to be sent to the 192.168.1.92 interface destined for the council's internal or external email addresses. This situation is yet another cause of potential risks to the council's email system as the system allows anyone from the council's internal network to distribute email message via the spam blocker appliance without go to the council's email server.

- ***Risk 3: The Mailbox server role***

Council A's Mailbox server role has one mailbox. As per best practice guidelines recommended by CIS (2007), there were a number of mis-configurations on the council's Mailbox server role. For examples, both the email send and receive size were set to unlimited. This may a cause an unnecessary increase in the storage area of the email server. It may also create unnecessary network traffic to the council's network. This extra network traffic may affect the speed of the valid network traffic due to the increased volume caused by the extra load. See Table 4.23 for more details.

- ***Risk 4: The Hub Transport server role***

Council A's Hub Transport server role has one default group this is not optimal. As per best practice guidelines recommended by CIS (2007), the current setting on the Hub Transport server role of the council's email server should be reconfigured to provide better security to the MS Exchange 2007 email server of the council. See Table 4.24 for more details.

- ***Risk 5: The CAS role***

As previously mentioned, both the POP3 and IMAP4 related mail protocols are not being used at Council A. Therefore, both features of the CAS role were not included in this modified checklist. There were some inadequate settings on the council's CAS role. These inadequate settings may cause potential risks to the council MS Exchange 2007 email server. See Table 4.25 for more details.

4.3.5 Testing stage 5: The email system security policy review

There was only a community access to Internet policy (see Appendix A24) on library usage for the council. This library usage policy clarified the conditions of use for community access to the Internet via Council A's computer network. However, no other information security policy or any technical policy (either issue-specific or systems-specific security policy) was in existence for staff of the council. Consequently, there were no rules, policy or procedure guidelines for the IT operational staff of the council to follow.

4.3.5.1 Testing stage 5: Identified risk issues

The lack of any related email security guidelines can create a source of vulnerability to potential risks to the council's email and related systems in the form of unintended interruptions or intentional misuse of the email service.

- ***Risk 1: Interruption of the email service***

The lack of an email security guideline such as any email server configuration documentation may lead to misconfigration of the email server which may be a cause of potential downtime to the server and its email service to the staff of Council A.

- ***Risk 2: Misuse of the email service***

The lack of an email security guideline may also lead to poor communication of risk in terms of the email system which may create a cause of potential risk which can allow unauthorised persons to use the email server as a source to launch abuse or attacks in the form of spam email to the staff of Council A.

4.4 Council A's online web system results

The architecture design, the device configurations, the vulnerabilities of all the online system servers, the vendor security benchmark and the security policy were successfully tested, audited and reviewed for Council A. The following sections describe all the results of these testings in detail.

4.4.1 Testing stage 1: Network surveying

This network surveying stage was conducted in a similar way as completed in the Testing stage 1 of the email system. In summary, the following network specifications and policy documents of the council's online web system were collected:

- The overall network diagram for the Internet link, the DMZ infrastructure connectivity, and the ACL codes and specifications of the firewall which related to the council's online web system;
- The council's online web system related configuration codes for the Internet border, the IDS/IPS and the internetwork switches specifications; and
- The summary of three online payment servers (the DMZ frontend web, the application and the backend database servers) specifications.

The following sections describe the overall summary specifications of the online payment system devices at Council and the associated identified risks.

4.4.1.1 The online payment system devices

There online payment system comprised of three specific devices which were the frontend web server (the CoA-DMZ-Epathweb), the application server (the CoA-Pathway) and the backend database server (the CoA-SQL).

4.4.1.1.1 The frontend web server

The location of the council frontend web server is in the council's DMZ area. It provides the frontline interface to the client web browser. The council's residents can access the frontend web server through the council's website (https://services.coa.wa.gov.au) and make payments using their valid assessment number for rates, payment reference for applications or ticket numbers for infringements. The frontend web server synchronises with the application server via the HTTP port.

In addition, the application server performs SQL queries directly to the backend database server using the assigned specific TCP port (2134). Table 4.9 displays the overall details of the frontend web server specifications.

Table 4.9 *A summary of the frontend web server specifications*

Attributes	**Details**
Name	CoA-DMZ-Epathweb
Application software	Epathway, Epathweb
Other application software	Trend Micro virus protection software
OS	MS Windows Server 2003 Enterprise Edition with service pack 2
Hardware	IBM eServer BladeCenter
IP address	192.168.1.84/24

4.4.1.1.2 The application server

The application server functions as a middle tier application server which interacts with the frontend web server and the backend database server. It synchronises the transactions of the Pathway application, the processes commands and the calculations from the backend database server. Table 4.10 summarised the application server specifications.

Table 4.10 *A summary of the application server specifications*

Attributes	**Details**
Name	CoA-Pathway
Application software	Pathway
Other application software	Trend Micro virus protection software
OS	MS Windows Server 2003 Enterprise Edition with service pack 2
Hardware	IBM eServer BladeCenter
IP address	172.16.25.173/24

4.4.1.1.3 The backend database server

The backend database server is a physical MS SQL Server 2005 cluster which consists of two servers (the CoA-SQL1 and the CoA-SQL2). The two clustered servers work as part of a redundant system where one server is in active mode and the other one is in standby mode. The database server has most of the council‘s database applications such as accounting, human resources, building, and recreation systems. These software applications are running concurrently.

In terms of the online payment system, the backend database server keeps all the important information such as payment numbers, rate and infringement notice reference numbers, usernames, passwords and addresses. In addition, it holds sensitive information such as credit card numbers and an expiry dates. Table 4.11 presents the summarised of the backend database server specifications.

Table 4.11 *A summary of the backend database servers’ specifications*

Attributes	**Details**
Name	CoA-SQL1
Application software	MS SQL Server 2005
Other application software	Trend Micro virus protection software
OS	MS Windows Server 2003 Enterprise x64 Edition with service pack 2
Hardware	IBM eServer BladeCenter HS21, 4 x Central Processing Unit (CPU) EM64T 3 GHz, 16 GB RAM
IP address	172.16.25.222/24, 10.90.0.100/24 (Heartbeat: redundancy)

Table 4.11 *A summary of the backend database servers' specifications (continued)*

Attributes	**Details**
Name	CoA-SQL2
Application software	MS SQL Server 2005
Other application software	Trend Micro virus protection software
OS	MS Windows Server 2003 Enterprise x64 Edition with service pack 2
Hardware	IBM eServer BladeCenter HS20, 4 x CPU EM64T 3 GHz, 10 GB RAM
IP address	172.16.25.224/24, 10.90.0.101/24 (Heartbeat: redundancy)
Name	CoA-SQL
IP address	172.16.25.227/24
Role	SQL server cluster

4.4.1.2 Testing stage 1: Identified risk issues

The identified risk issues of testing stage 1 for Council A's online payment system are described in the following sections.

- ***Risk 1: Sensitive data stored in the backend database server***

As previously mentioned, the council's backend database server holds the council's resident sensitive information such as credit numbers, expiry dates and credit card types. These sensitive data have been entered manually by the council's payroll staff.

Furthermore, the sensitive data is kept in unencrypted (clear text) format and can therefore be viewed openly by anyone accessing the system. This means any staff members that have access to the backend database server are able to view the sensitive information. This scenario poses a very high risk in terms of staff access and may cause the council susceptibility to loss of trust, identity theft and damage to the council's reputation.

- ***Risk 2: The application and the backend database servers are located in the same subnet***

Both the online payment application server and the online payment backend database server are located in the council's internal network. Both the application and the backend database servers have the same subnet or IP address range and is also the same as the other internal servers. Common attacks such as viruses, Trojans and DoS may cause potential risks against the council's online payment system particularly to the backend database server and the other internal servers as well.

4.4.2 Testing stage 2: The infrastructure of the online web system – Internet border router, IDS/IPS, firewalls and switch reviews

This second testing stage consisted of the review of the software configuration codes for the router, IDS/IPS, firewalls and switches.

4.4.2.1 Internet border router configuration codes data collection and reviews

The council's Internet border router specifications were previously discussed in Section 4.3.2.1. In terms of the council's online payment system, the Internet border router was configured correctly providing routing connectivity.

4.4.2.2 IDS/IPS configuration codes data collection and reviews

As previously mentioned in Section 4.3.2.2, both the current IDS and IPS features have been disabled.

4.4.2.3 Firewall configuration codes data collection and reviews

The details of the Internet firewalls specifications can be found in the previously discussed in Section 4.3.2.3.

4.4.2.4 Switch configuration codes data collection and reviews

Council A's internetwork has three switches as previously mentioned. Details of the architecture, the configuration codes and the hardware specifications are previously discussed and addressed in Section 4.3.2.4. Nevertheless, details on ports and VLANs, including connectivity for the council's online payment system are displayed in Figure 4.6.

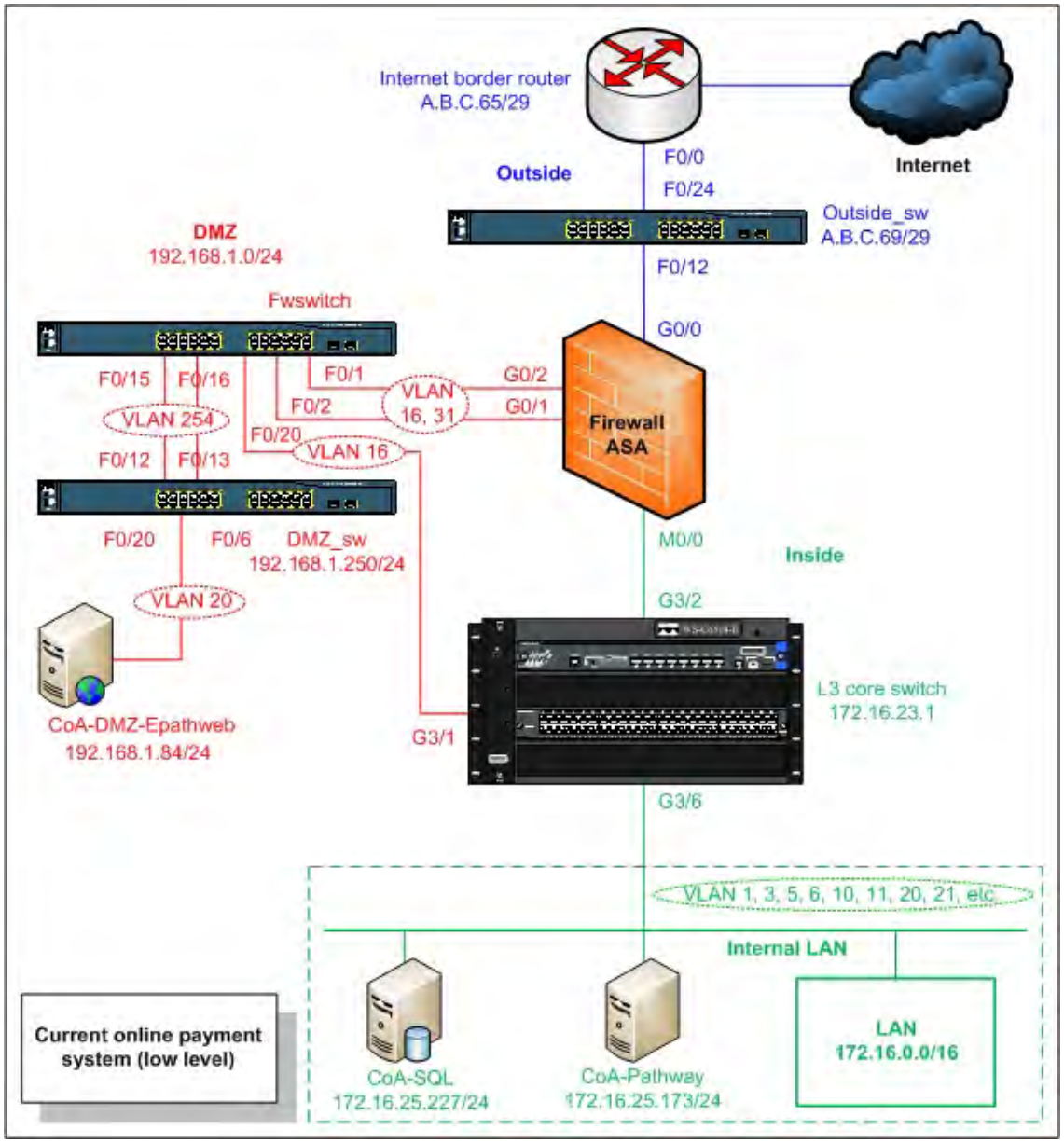

Figure 4.6. A current low level network diagram of the online payment system for Council A

4.4.2.5 Testing stage 2: Identified risk issues

The following section details the identified risk issues for the online payment infrastructure system (Internet border router, the IDS/IPS, the firewall and the switches) of the council.

- ***Risk 1: Firewall's IPS was disabled***

As previously explained in Section 4.3.2.5, the IPS of the council was disabled which meant that incoming online payment web traffic (HTTPS) was not inspected for abnormal patterns. According to Check Point Software Technologies Ltd. (2010) security guidelines, this can cause potential risks such as DoS attacks, to the council's online payment system.

- ***Risk 2: Inadequate firewall ACL coding – HTTPS inwards***

Currently, the firewall permits HTTPS traffic from anywhere (see Appendix A7: Policy number 1), allowing access to the online payment frontend web server. As per standard firewall configurations best practice, this can be a cause of potential risks to the frontend web server.

- ***Risk 3: Inadequate firewall ACL coding – Allows IP protocol from specific computer to the frontend web server***

The firewall permits two specific internal IP addresses (the IT operational staff's computers) to access the online frontend web server via IP protocol (see Appendix A7: Policy numbers 5 and 6). This may cause potential risks in the form of an internal attacker taking control of the IT operational staff's computers.

- ***Risk 4: Inadequate firewall ACL coding – Allows two-way communications via TCP port 2134 between the frontend web server and the internal backend database server***

The firewall rule allows two-way communications between the frontend web server and the internal backend database server (the CoA-SQL) via the assigned TCP port 2134 (see Appendix A7: Policy numbers 9 and 21). This allows an SQL query from the CoA-DMZ-Epathweb server to the CoA-SQL server directly (personal communications with

Council A, 2009). This may cause potential risks such as a DoS and SQL injection into the council's CoA-SQL backend database server which could lead to corruption, extraction or possible manipulation of data from any database being served.

For example, an attacker may use a SQL injection manipulation or function call injection attack technique to manipulate or modify the contents of the online payment database of the council (Joshi, 2011). The manipulation of the database file contents can be in the form of deletion or modification of the individual record details of residents of the council. Preventing this two-way communication on the firewall will prevent this type of vulnerability. See Figure 4.7 for more details.

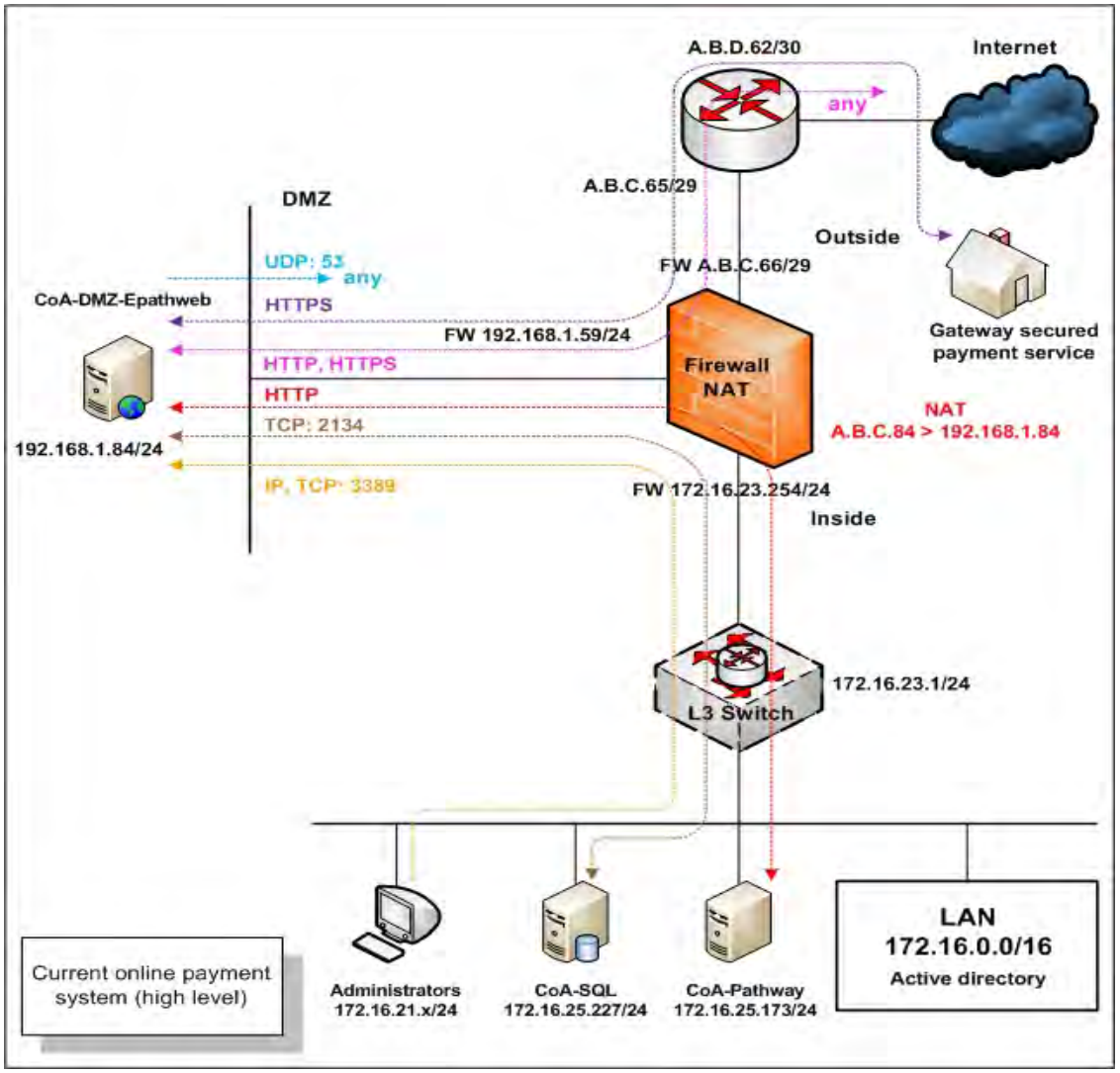

Figure 4.7. The high level online payment system including network traffic protocols currently in use by Council A

- ***Risk 5: Inadequate firewall ACL coding – HTTP and DNS outwards***

The firewall permits the CoA-DMZ-Epathweb server access to anywhere via HTTP and DNS (UDP port 53) (see Appendix A7: Policy numbers 13 and 14). This may be a source of potential risk in case of the CoA-DMZ-Epathweb server being used as a proxy for staging further attacks on systems internal and external to the council.

- ***Risk 6: Inadequate firewall ACL coding – HTTP inter-devices***

The firewall allows the CoA-DMZ-Epathweb server access the internal servers (IP 172.16.25.214, 172.16.25.194, 172.16.25.193) via HTTP port 80 (see Appendix A7: Policy numbers 17, 19 and 20). As per best practice recommendations to standard firewall configurations, this may be a cause of potential risks as the DMZ web server may directly access to the internal servers via HTTP port. This HTTP port may consider as an unsecure web port when compared with HTTPS.

- ***Risk 7: Overall inadequate switch code security configurations***

This point has been previously discussed in Section 4.3.2.5

4.4.3 Testing stage 3: Services and system identification, port scanning, vulnerability testing and results

Similarly techniques in Section 4.3.3 of the email system were used in this third testing stage. Both network scanning tools (NMAP and GFI LANguard) were conducted on all the testings steps (services and system identification, port scanning and vulnerability testings).

4.4.3.1 Services and system identification results

Appendices A8, A9, A10 and A11 provide the full details of the services and system identification testing results for the CoA-DMZ-Epathweb, the CoA-Pathway and the CoA-SQL servers. Furthermore, this section can be identified issues into two groups (system information policy results and system patching status results) similar to Section 4.3.3.1.

4.4.3.2 Port scanning results

Similarity to Section 4.3.3.2, both NMAP and GFI LANguard were used to scan the council online payment web servers. Moreover, both unnecessary TCP and UDP ports were identified in all the three servers (the CoA-DMZ-Epathweb, the CoA-Pathway and the CoA-SQL servers). Full details of the port scanning results are found in Appendices A12, A13 and 14.

4.4.3.3 Vulnerability testing results

Similar to Section 4.3.3.3, the vulnerability testing result can be categorised into four groups which are the high, medium, low and potential security risks based on the GFI standard. There were vulnerabilities identified on all the three servers of the online payment system. Full details of the vulnerability testing results are found in Appendices A15, 16 and 17.

4.4.3.4 Testing stage 3: Identified risk issues

The identified risk issues of Testing stage 3 for Council A's online payment system are described as follows.

- ***Risk 1: System information policy results for all the three servers***

There were some insufficiently secured services, poor password and security auditing policies presented in the MS Windows configuration settings on all three online payment servers at Council A. These configurations may create potential vulnerabilities to the council's online payment system. More details are provided in Appendices A8, A9 and A10.

- ***Risk 2: System patching status results for all the three servers***

There were no missing service packs and patches on the CoA-Epathweb and the CoA-SQL servers. However, there were missing service packs as well as patches on the CoA-Pathway server. These missing service packs and patches are a source of potential risks to the council's online payment system.

- ***Risk 3: Unnecessary opened ports on all the three servers***

There were 22 TCP and 11 UDP opened ports which include unnecessary ports on the CoA-DMZ-Epathweb server. On the CoA-Pathway server, there were 22 TCP and nine UDP opened ports which include unnecessary ports. Furthermore, there were 23 TCP and 14 UDP opened ports on the CoA-SQL server. These unnecessary opened TCP and UDP ports are a cause of potential risks such as manipulation of the database, unauthorised access and DDoS attacks to the council's online payment servers.

Table 4.12 displays the overall opened TCP and UDP ports of three servers of the council's online payment system. The overall opened TCP and UDP ports together with the recommended opened ports for the CoA-DMZ-Epathweb, CoA-Pathway and CoA-SQL servers are provided in Appendices A12, A13 and A14 respectively.

Table 4.12 *Overall opened TCP and UDP ports of all Council A's online payment servers*

Server names	**Opened TCP ports**	**Opened UDP ports**	**Comments**
CoA-DMZ-Epathweb	22	11	Refer to Appendix A12
CoA-Pathway	22	9	Refer to Appendix A13
CoA-SQL	23	14	Refer to Appendix A14

- ***Risk 4: Vulnerabilities found on all the three servers***

There were Ports 1 and 8012 opened on the CoA-DMZ-Epathweb server which may lead to a source of potential risks from Trojan attacks. Table 4.13 depicts the summary of the overall vulnerability testing results of the three servers, whereas the full details of vulnerability testing results and possible mitigation recommendations of the three online payment servers are provided in Appendices A15, A16 and A17 respectively.

Table 4.13 *Overall vulnerability of the three online payment servers of Council A*

Server names	**H**	**M**	**L**	**P**	**Overall vulnerability levels**	**Comments**
CoA-DMZ-Epathweb	6	0	7	2	High (10/10)	Refer to Appendix A15
CoA-Pathway	1	0	2	0	High (8/10)	Refer to Appendix A16
CoA-SQL	2	0	2	2	High (8/10)	Refer to Appendix A17

4.4.4 Testing stage 4: Vendor security: Database security benchmark auditing

This fourth testing stage pertains to the audit and analysis of database security on the council's backend database server (the CoA-SQL).

4.4.4.1 Database security benchmark results

MS SQL server 2005 is the database application software which is used in Council A's backend database server. The Security Configuration Benchmark for MS SQL Server 2005 version 1.2.0 January 12th, 2010 from CIS Benchmark was used and adapted as a prime benchmark auditing tool. According to CIS (2010), the CIS benchmark auditing tool consists of nine categories as follows:

1. OS and network specification configuration;
2. SQL server installation and patches;
3. SQL server settings;
4. Access controls;
5. Auditing and logging;
6. Backup and disaster recovery procedures;
7. Replication;
8. Application development best practices; and
9. Surface area configuration tool.

Furthermore, the risk rating can be categorised into four groups as follows:

- "H" represents a high risk level which may cause highly impact interruption to the council backend database server and related system;
- "M" represents a medium risk level which may cause negatively impact performance and utility to the council backend database and its applications;
- "L" represents a low risk level which may cause minor or little impact to the council backend database server and its applications; and

- "P" represents a potential risk level which may be a cause of potential risks to the council backend database server and its database applications.

Group one to six were successfully audited. However, group seven to nine were not audited as they were not applicable to the council's backend database environment.

4.4.4.2 Testing stage 4: Identified risk issues

The identified risk issues for the configuration of the MS SQL 2005 database on the council's backend server are presented as follow.

- ***Risk 1: Inadequate configuration for the database application of the backend database server***

There were some identified security issues on the CoA-SQL server from the auditing. These security issues are a cause of potential risks to the backend database server. The overall security issues uncovered (unsatisfactory) together with the risk rating of Council A's online payment backend database server based on the six audited category groups are presented in Table 4.14. Appendices A18, A19, A20, A21, A22 and A23 provide the full details of all the findings and the possible mitigation recommendations.

Table 4.14 *The overall risks of the six audited categories of the online payment backend database server (the CoA-SQL)*

Category no.	**Risks (H)**	**Risks (M)**	**Risks (L)**	**Risks (P)**	**Comments**
1) OS and network specification configuration	1	0	6	3	Refers to Appendix A18
2) SQL server installation and patches	0	2	0	1	Refers to Appendix A19
3) SQL server settings	1	2	4	8	Refers to Appendix A20
4) Access controls	1	3	0	0	Refers to Appendix A21
5) Auditing and logging	0	0	0	43	Refers to Appendix A22
6) Backup and disaster recovery procedures	0	1	3	1	Refers to Appendix A23
7) Replication	N/A	N/A	N/A	N/A	None
8) Application development best practices	N/A	N/A	N/A	N/A	None
9) Surface area configuration tool	N/A	N/A	N/A	N/A	None

4.4.5 Testing stage 5: The online web system security policy review

In terms of the online payment system, there is currently no existing information security policy including any technical and specific system security policies.

4.4.5.1 Testing stage 5: Identified risk issues

The lack of policy guidelines can be a cause of serious risks to the council's online payment system. The cause of these risks could be attributed to the following issues.

- ***Risk 1: Poor communication of risk***

This was evident from the lack of discussion and discourses related to risk assessment and risk management as these topics were notably absent from the weekly IT operational staff meetings (personal communications with Council A, 2009, 2010).

Nevertheless, there were some specific verbal discussions in relation to the lack of IT security policy issues between the network administrator and the telecommunication officer during the beginning of year 2010 (personal communications with Council A, 2010). However, there was no written outcome or action plan instituted in order to address this shortcoming.

- ***Risk 2: Possible misdirection of resources***

The lack of IT information security policies could also be ascribed to a misdirection of funds and resources directed to the establishment and maintenance of a security policy. The budgetary constraints of the council permitted some of the IT operational staff to work on a part-time basis (one day per week). The staff affected by this constraint included the network administrator, the online payment application administrator, the database administrator and the GIS officer.

Moreover, each staff was assigned on a different day of the week. Not only did this constraint affect the formulation of an information security policy, but it also resulted in a lack of communication between the affected staff in having discussions about information security policy.

Consequently, there was no allocation of budget, time and resources towards developing any IT security related policy up until the beginning of 2011, at which point the council's executive management team began allocating funds for the development of an organisational IT security policy.

- ***Risk 3: Poor understanding of the risks that are in the system as a result of poor management/strategic oversight***

This factor was evident from the fact that some of the council's IT staff not being fully aware of potential risks and their impact to the council's online payment system. For example, the online application software (Pathway) administrator was unaware that the council residents' confidential information was not stored in a secure format (encryption).

Another instance of the lack of understanding of the risk was the fact that over 100 database file systems were located on a single cluster server. These cost saving measures were implemented at the expense of the risk of a single point of failure. An implemented security policy would have rated the risk of a single point of failure higher than any cost saving initiative (personal communications with Council A, 2010).

4.5 Analysis and discussion

The analysis and discussion on both Council A's email as well as online payment systems are detailed in the following sections.

4.5.1 Analysis

The analysis can be separated into two sections for each of the analysis of Council A's email and online payment systems.

4.5.1.1 Council A's email system analysis – possible mitigations

The possible mitigation recommendations for the identified issues of Council A's email system are described in the following sections. Each of the mitigations described relate to the identified risk issue number.

4.5.1.1.1 Testing stage 1: Possible mitigation

- ***Risk 1***

A virus protection software server version is recommended to be installed on the email server in order to minimise potential attacks from virus and worms. Where possible this should use a different antivirus scanner than the client computer.

- ***Risk 2***

It is recommended that the council deploy an extra dedicated server to perform as a CAS. This additional server may reduce the potential risk of a single point of failure. The new CAS server can be a physical server or a Virtual Machine (VM) but on independent hardware. The network connection between both the new CAS and the existing email server should ideally be a gigabit connection with a high network bandwidth and low-latency as per recommended best practices by Microsoft Corporation (Microsoft Exchange Documentation Team, 2009).

In addition, virus protection software for the new CAS server is recommended to be included in the new CAS. Table 4.15 displays the summary specifications of a new dedicated CAS. Figure 4.8 illustrates details of its architecture including the new CAS.

Table 4.15 *Recommended summary of the new CAS specifications*

Attributes	**Details**
Email application software	MS Exchange 2007 with service pack 1
OS	MS Windows Server 2008 Enterprise Edition with service pack 1
Hardware	8GB RAM, Hard disks C: 20GB, e: 100GB
MS Exchange 2007 server role	CAS
Exchange support	MS OWA, MS Outlook Anywhere, MS ActiveSync
TCP protocols	HTTPS, Remote Procedure Call (RPC), LDAP
IP network	Different subnet with other email servers (isolate)
Network connection	Gigabit link between Client Access and Mailbox servers
ACL	Permits only allowed or required protocols
Other software	Virus protection software

- ***Risk 3***

A new CAS may be installed on a different subnetwork in order to minimise any potential risks that may take place. The current internal router (the layer 3 core switch) may also be configured using an ACL to only allow the required network communication protocols between the new CAS and the council's network. See Figure 4.8 for more details. Figure 4.8 demonstrates the council's email network diagram with an extra MS Exchange Server 2007.

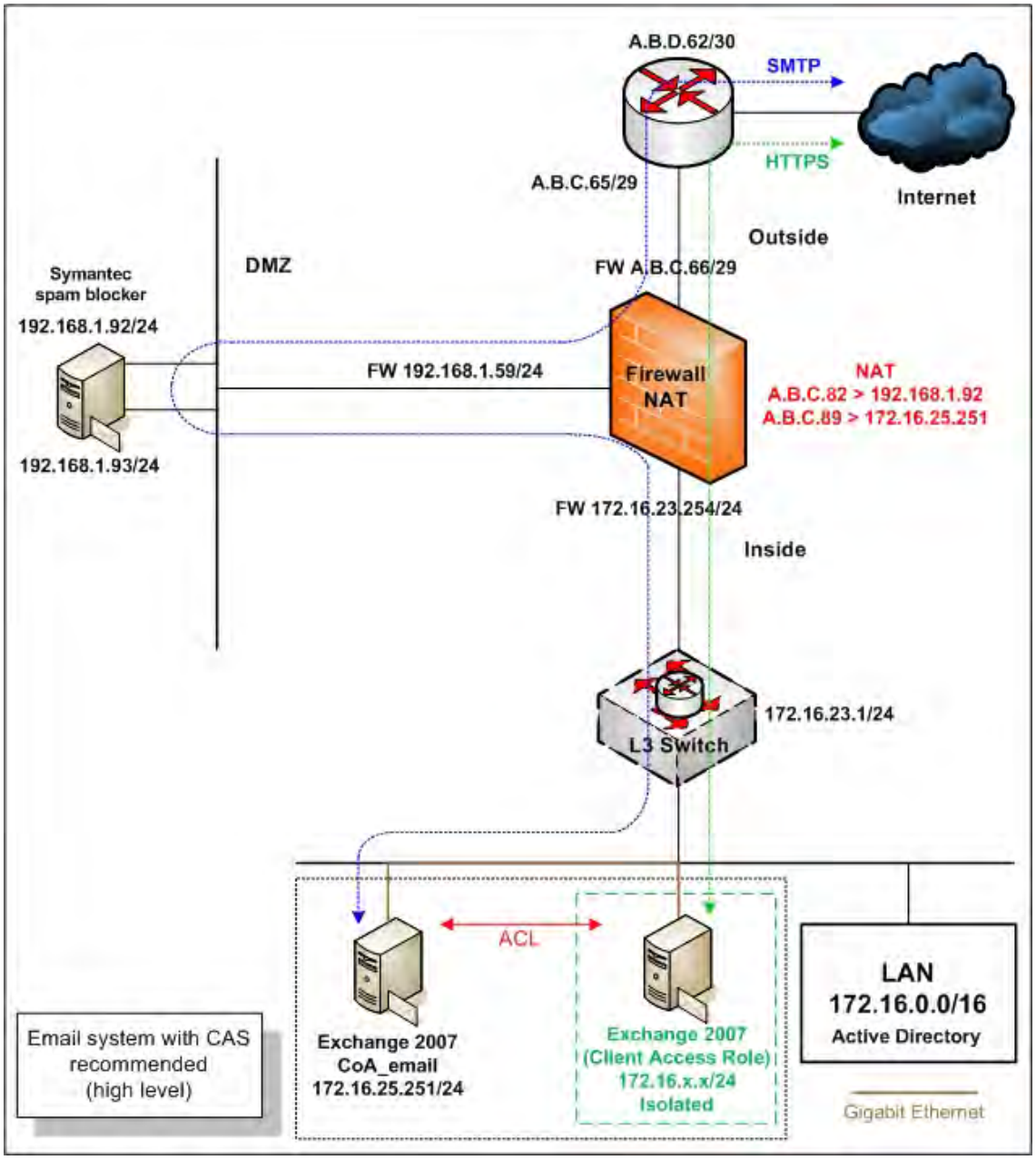

Figure 4.8. A recommended MS Exchange Server 2007 architecture with an extra MS Exchange Server 2007 (CAS role) for Council A

4.5.1.1.2 Testing stage 2: Possible mitigation

- ***Risk 1***

The current router allows anyone access to the external IP address (A.B.C.89) of the email server via the web or Hypertext Transfer Protocol (HTTP) traffic. This is considered to be unnecessary as the required and allowed protocol should be HTTPS only. Therefore, this configuration code could be removed. See Table 4.16 for more details.

Table 4.16 *The ACL configuration codes recommendation for Council A's Internet border router*

Policy no.	**Rules**	**Protocol types**	**From (source)**	**To (destination)**	**Ports (service)**	**Recommendations**
1	Permit	TCP	Any	A.B.C.82	SMTP	Satisfactory
2	Permit	TCP	Any	A.B.C.89	HTTPS	Satisfactory
3	Permit	TCP	Any	A.B.C.89	HTTP	Remove

- ***Risk 2***

Enabling the IDS/IPS feature on the current Internet border router may provide an additional prevention from scanning and spoofing attacks. More details are provided in Table 4.17.

- ***Risk 3***

The existing firewall (Cisco ASA) can provide stateful packet inspection to external HTTPS traffic. This feature may serve to reduce any potential risks as previously mentioned. Therefore, the council may wish to enable IPS on the two firewalls for HTTPS inspection. See Table 4.17 for more details. However**,** managing traffic in this way may not be practical because of the size and dynamic nature of the Internet. Therefore, the council may consider using the existing old MS Internet Security and Acceleration (ISA) Server 2006 which is currently unused to provide stateful inspection and application-layer filtering on all HTTPS traffic. This technique enables the ISA server to block any HTTPS traffic that appears out of context.

With this option incoming traffic will not overload the current firewall and also add no cost to the council's IT budget. Figure 4.9 demonstrates the MS Exchange Server 2007 Client Access architecture for external clients via HTTPS using ISA. In addition, Figure 4.10 illustrates the council's email network diagram with the CAS and ISA Server 2006.

Figure 4.9. Client access architecture for external clients
(Source: Microsoft TechNet, 2007a, p. 55)

From Figure 4.9 above, it can be seen that the ISA Server analyses the payload in data packets, which requires ISA Server 2006 to decrypt the SSL stream. The SSL connections from external network (the Internet) terminates on the ISA server and "then re-establishes a new SSL connection between the ISA server and the Client Access server. This SSL bridging process enables ISA Server 2006 to filter invalid data packets before the traffic reaches the Client Access servers while maintaining the confidentiality of client-to-server communication as it transits both external and internal networks" (Microsoft TechNet, 2007a, p. 54). An external trusted SSL certificate must be installed on the ISA server. Furthermore, for connections between the ISA Server 2006 and the CAS either external or internal trusted SSL certificates may be used.

Table 4.17 *A summary of the IDS/IPS of the council's internetwork system*

Products	Current issues	Recommendations	Descriptions
IDS on the Internet border router	Disabled	Enable (turn on)	For blocking of any spoofing/scanning attacks.
IPS on the firewall	Disabled	Option 1: Enable (turn on)	For real-time inspection of HTTPS traffic for the purposes of blocking and preventing any malicious or unwanted behaviour in real-time.
IPS on the firewall	Disabled	Option 2: Deploy the existing ISA 2006	For real-time inspection of HTTPS traffic.

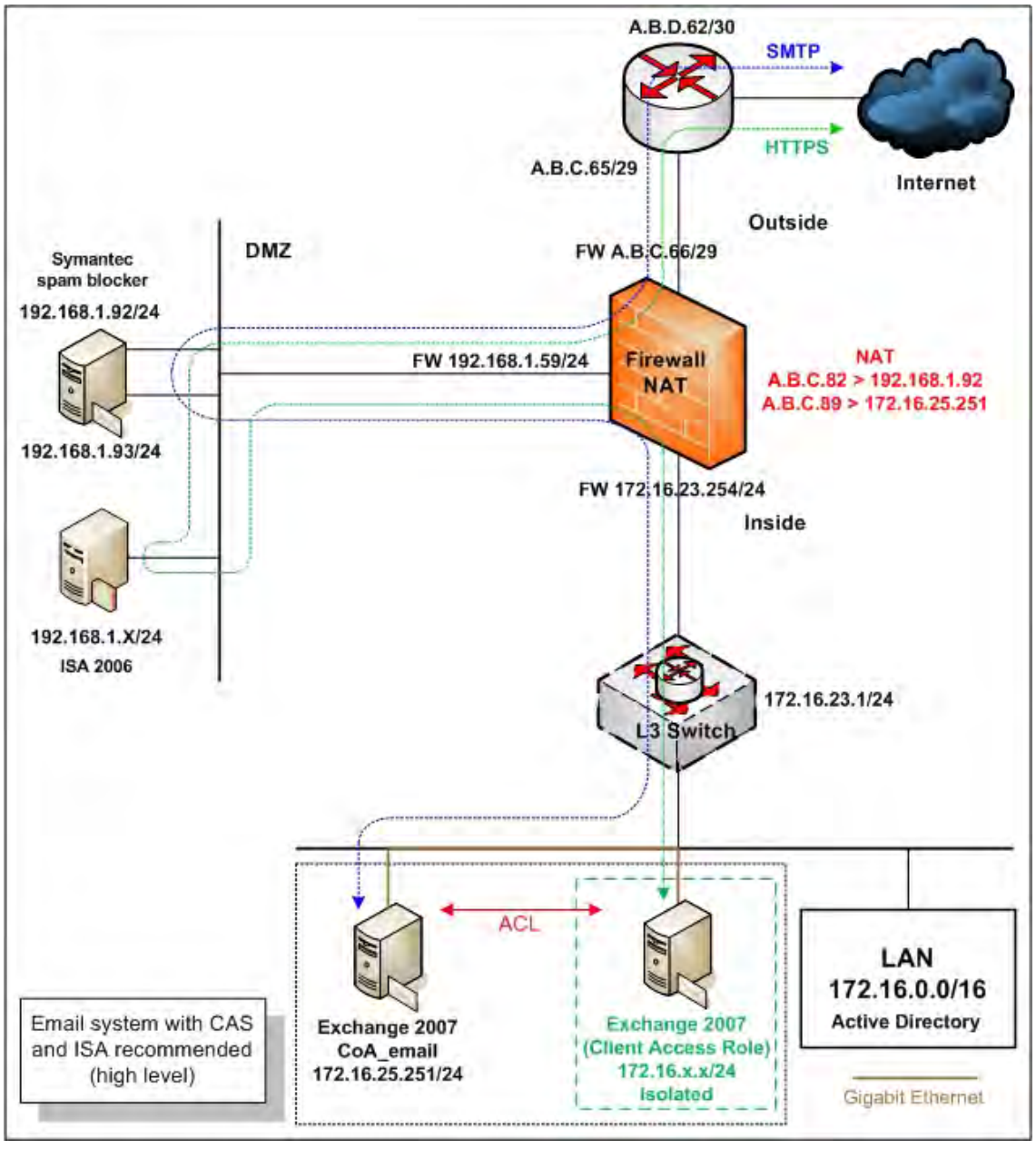

Figure 4.10. A recommended MS Exchange Server 2007 architecture with an extra MS Exchange 2007 (CAS role) and the existing MS ISA Server 2006 for Council A

- ***Risk 4***

As per best practice recommendations to standard firewall configurations, the council may allow the current spam blocker appliance access to only the required specific places either via HTTP or HTTPS ports.

- ***Risk 5***

These firewall rules may be removed as the internal server has been decommissioned. The removal of obsolete configuration codes serves to prevent any confusion that may arise in the future as to why a code which refers to a non-existent server is present. This allows clean and possible no confusion of the firewall configuration codes to the council's network administrator.

- ***Risk 6***

This firewall rule may be removed as the incoming SMTP traffic should forward traffic from the spam blocker appliance interface 192.168.1.93 rather than 192.168.1.92.

- ***Risk 7***

The firewall rule may be removed as the DMZ server (192.168.1.89) has been decommissioned.

- ***Risk 8***

The overall configurations including the possible mitigation recommendations are presented in Table 4.18. As per best practice recommendations of switch configurations and ISSAF (Rathore, 2006) guidelines, all the measures that are currently not implemented may be activated in order to protect against such attacks as previously mentioned.

Table 4.18 *Switches security identified issues and recommendations for Council A*

Security features	**Recommendations**		
	Outside_sw	**Fwswitch**	**DMZ_sw**
ACL applied to block unwanted devices	To do	To do	Satisfactory
Access to the device via HTTP is disabled	Satisfactory	Not Applicable (N/A)	Satisfactory
Access to the device via Telnet is disabled	To do	N/A	To do
Activate Loop protection on all ports	To do	To do	To do
Apply appropriate log server	To do	To do	To do
Apply appropriate timestamps debug time	Satisfactory	Satisfactory	Satisfactory
Apply appropriate timestamps log time	Satisfactory	Satisfactory	Satisfactory
Apply appropriate time zone	Satisfactory	To do	To do
Appropriate Simple Network Management Protocol (SNMP) used	N/A	N/A	Satisfactory
Appropriate VLAN used	To do	Satisfactory	Satisfactory
Best practice user name and/or password used	To do	To do	To do
Configure appropriate warning banner message	To do	To do	Satisfactory
Disable/shutdown unused switch ports	To do	To do	To do
Disable trunking on ports that do not need it	To do	To do	To do
Enable feature against ARP poisoning attacks	To do	To do	To do
Enable feature against ARP spoofing attacks	To do	To do	To do
Enable port broadcast storm control	To do	To do	To do
Enable port security limits MAC address to a port	To do	To do	To do
Ports connected to identified devices that do not support spanning-tree should be configured with Bridge Protocol Data Unit (BPDU) filtering	Satisfactory	To do	Satisfactory
Ports not connected to anything yet should be configured with protection	To do	To do	To do
Set Data Tools Platform (DTP) on all ports not being used for trunking	To do	To do	To do
Set strong password (Message-Digest Algorithm 5 or MD5) for authenticating VTP message	To do	To do	Satisfactory
Strong password encryption (MD5) used	To do	To do	Satisfactory
Trivial File Transfer Protocol (TFTP) service is disabled	To do	N/A	To do

4.5.1.1.3 Testing stage 3: Possible mitigation

- ***Risk 1***

Table 4.19 displays the summary of the overall system information policy testing result of the Council A's email system server. Furthermore, Appendix A3 provides the overall system information policy testing results, uncovered issues and possible mitigation recommendations of the council's email server.a

Table 4.19 *Overall system information policy of Council A's email server*

Server name	**Password policy**	**Security audit policy**	**Comment**
Email server	Unsatisfactory	Unsatisfactory	Refer to Appendix A3

- ***Risk 2***

Appendix A4 provides the specific details of the missing service pack and patches information as well as recommendations for updating of the email server.

- ***Risk 3***

Table 4.20 presents the total number of recommended open TCP and UDP ports on the email server.

Table 4.20 *The total number of recommended open TCP and UDP service ports on the email server*

Server name	**Recommended open TCP ports**	**Recommended open UDP port**	**Comment**
Email server	8	1	Refer to Appendix A5

- ***Risk 4***

Refer to Appendix A6 for full details of the identified risk issues and the possible mitigation recommendations.

4.5.1.1.4 Testing stage 4: Possible mitigation

- ***Risk 1***

The overall spoofing testing results including possible mitigation recommendations are presented in Table 4.21.

Table 4.21 *The spoofing testing results and mitigation recommendations for Council A's email server*

Testing techniques	**Purposes**	**Results**	**Recommendations**
Telnet to the email server and sending an email from one internal address to another internal address.	To test internal connectivity of the email server	Successful (allows relaying)	Should not allow mail relaying
Sending an email from one external address to another external address using the target email server.	To test external relaying of the email server	Successful (allows relaying)	Should not allow mail relaying
Sending an email from one internal address to an external address using the target email server.	To test internal relaying of the email server	Successful (allows relaying)	Should not allow mail relaying
Sending an email from one external address to an internal address using the target email server.	To test email relaying of the email server	Successful (allows relaying)	Should not allow mail relaying

- ***Risk 2***

The overall results and mitigation recommendations are provided in Table 4.22.

Table 4.22 *The spoofing testing results and mitigation recommendations for Council A's spam blocker appliance (interface 192.168.1.92)*

Testing techniques	**Purposes**	**Results**	**Recommendations**
Telnet to the spam blocker appliance (interface 192.168.1.92) and sending an email from one internal address to another internal address.	To test internal connectivity of the email server	Successful (allows relaying)	Should not allow email relaying
Sending an email from one external address to another external address using the spam blocker appliance (interface 192.168.1.92).	To test external relaying of the email server	Unsuccessful (does not allow relaying)	None
Sending an email from one internal address to an external address spam blocker appliance (interface 192.168.1.92).	To test internal relaying of the email server	Successful (allows relaying)	Should not allow email relaying
Sending an email from one external address to an internal address spam blocker appliance (interface 192.168.1.92).	To test email relaying of the email server	Successful (allows relaying)	Should not allow email relaying

- ***Risk 3***

Table 4.23 lists overall of the default settings, auditing results and mitigation recommendations based on the CIS suggestions.

Table 4.23 *The overall results of auditing and recommendations Mailbox server role of Council A's email server*

References	**Defaults**	**Council A**	**Recommendations**
Restrict email deletion retention	7 (days)	14 (days)	7 (days)
Restrict mailbox deletion retention	30 (days)	30 (days)	30 (days)
Restrict deletion of mail or mailboxes until archival	Unchecked	Unchecked	Checked
Mounting of mailbox database at startup	Unchecked	Unchecked	Unchecked
Ensure mailbox database cannot be overwritten	Checked	Unchecked	Unchecked
Verify default mailbox storage limits (issue warning at, prohibit send at, prohibit send and receive at)	Custom	1991680 Kilobyte (KB) 209752KB 2411520KB	Custom
Ensure public folder database cannot be overwritten	Checked	Unchecked	Unchecked
Verify default public folder storage limits (issue warning, prohibit send and receive at (KB)	Custom	1991680KB, -, 10240KB	Custom
Audit public folder client access	Custom	Custom	Custom
Audit public folder administrative access	Custom	Custom	Custom
Verify proper permissions on public folder database	Custom	Custom	Custom
Mounting of public folder database at startup	Unchecked	Unchecked	Unchecked
Restrict email send size (mailbox identity, mail contact identity and distribution group identity)		Unlimited Unlimited Unlimited	10MB 10MB 10MB
Restrict email receive size (mailbox identity, mail contact identity and distribution group identity)		Unlimited Unlimited Unlimited	10MB 10MB 10MB
Restrict max recipients	5000	Unlimited	2000
Audit mailbox spam bypass settings	False	False	False
AntiSpam updates	Disabled	Disabled	Disabled
Zero out deleted database pages	False	False	True

- ***Risk 4***

Table 4.24 lists overall default settings, results of auditing and mitigation recommendations based on the CIS suggestions.

Table 4.24 *The overall results of auditing and recommendations the Hub Transport server role of Council A's email server*

References	**Defaults**	**Council A**	**Recommendations**
Audit DNS lookup servers	None	Custom	Custom
Restrict email send size (max send size, max message size)	30MB 30MB	30 MB 30 MB	10MB 10MB
Restrict max recipients (max recipients per message)	5000	5000	2000
Restrict email receive size (max receive size, max message size, external Delivery Status Notification (DSN) max message attach size and internal DSN max message attach size)	30MB 30MB 10MB 10MB	30MB 30MB 10MB 10MB	10MB 10MB 10MB 10MB
Restrict IP range for receive connectors	None	None	Custom

- ***Risk 5***

The overall results of auditing, factory default settings and mitigation recommendations based on the CIS suggestions are presented in Table 4.25.

Table 4.25 *The overall results of auditing and recommendations CAS role of Council A's email server*

References	**Defaults**	**Council A**	**Recommendations**
Remove legacy web applications	Installed	Installed	Removed
Restrict web authentication methods*	See note	See note	See note
Require SSL for web applications	Checked Unchecked	Checked Unchecked	Checked Checked
Disable web anonymous access	Unchecked	Unchecked	Unchecked
Enable logging for default website	Checked	Checked	Checked
Enable policy for MS ActiveSync**	None	See note	See note
Forbid MS ActiveSync NonProvisionable devices	Checked	Checked	Unchecked

Table 4.25 *The overall results of auditing and recommendations CAS role of Council A's email server (continued)*

References	Defaults	Council A	Recommendations
Forbid MS ActiveSync simple device password	Checked	Checked	Unchecked
Disable MS ActiveSync Windows SharePoint Services (WSS)/Universal Naming Convention (UNC) access	Checked Checked	Checked, Checked	Unchecked Unchecked
Require MS ActiveSync password	Unchecked	Unchecked	Checked
Require MS ActiveSync alphanumeric password	Unchecked	Unchecked	Checked
Require MS ActiveSync minimum password length	Checked, 4	Checked, 3	Checked, 8
Require MS ActiveSync password expiration	Unchecked	Unchecked	60
Restrict MS ActiveSync attachment size	Unchecked	Unchecked	Unchecked 3MB
Require MS ActiveSync policy refresh	None	None	24.00:00:00
Restrict MS ActiveSync maximum password attempts	8	8	8
Require MS ActiveSync Certificate Based Authentication	Ignore Client Certs	Ignore Client Certs	Require Client Certs
Require MS ActiveSync inactivity lockout time	Enabled	Enabled	Disabled

Note:

Refers to restricted web authentication methods*

This task is to ensure that unneeded authentication methods for the MS Exchange web applications should be disabled. Refer to CIS (2007, p. 76), the MS Exchange 2007 recommendation "for web services and applications that cannot be disabled and removed from IIS ensure reasonable authentication methods are selected. These include Autodiscover, Exchange, Exchange Web Services (EWS), Exadmin, Exchweb, Microsoft-Exchange-ActiveSync, Offline Address Book (OAB), OWA, Public, and Unified Messaging (UM)". By doing this you limit the opportunity for unknown clients to connect to unneeded services. See more details in Table 4.26.

Table 4.26 *The overall results and recommendations of auditing web authentication and access control of Council A's email server*

Council A	**Integrate**	**Digest**	**Basic**	**Passport**
Autodiscover	X		X	
Exchange	X		X	
Exchange Web Services (EWS)	X			
Exadmin	X		X	
Exchweb	X		X	
MS-Exchange-ActiveSync			X	
Offline Address Book (OAB)	X			
Outlook Web Access (OWA)			X	
Public	X		X	
Unified Messaging (UM)	X			
Recommendations	**Integrate**	**Digest**	**Basic**	**Passport**
Autodiscover	X			
Exchange	X			
Exchange Web Services (EWS)	X		X	
Exadmin	X			
Exchweb	X			
MS-Exchange-ActiveSync			X*	
Offline Address Book (OAB)			X	
Outlook Web Access (OWA)			X	
Public	X		X	
Unified Messaging (UM)	X			

X represents enabled

X* represents only if not using Certificate

Refers to enable policy for MS ActiveSync**

This task creates and assigns policy for the MS ActiveSync service. Enabling and configuring the MS ActiveSync policy may assist to ensure that all corporate (Council A's) mobile devices are in line with its policy. This therefore may reduce the potential risks to the MS Exchange infrastructure in case of a mobile device disappearing (out of sync) from the network (CIS, 2007).

4.5.1.1.5 Testing stage 5: Possible mitigation

- ***Risks 1 and 2***

As per general best practice guidelines, a technical policy such as firewall and server (email) rules should be implemented in order to provide better security of the council's email and related system.

4.5.1.2 Council A's online payment system analysis – possible mitigations

The possible mitigation recommendations for the identified issues of Council A's online payment system are described in the following sections. Each of the mitigations described relate to the identified risk issue number.

4.5.1.2.1 Testing stage 1: Possible mitigation

- ***Risk 1***

In the interest of best practices suggested by Kiely (2006), it is recommended that the council deploys or applies an encryption method in order to secure the sensitive data after it is entered. There are two important factors when considering using encryption in a database. These two factors are performance and data bloat (or increase in size) (Kiely, 2006).

- *Performance:* Typically, "the more secure the algorithm and the larger the key size, the more processing cycles are required" (Kiely, 2006, p. 3). Therefore, it is recommended that only the sensitive data be encrypted; and
- *Data bloat:* How much bloat really "depends on the algorithm, key size, and the clear text that is being encrypted" (Kiely, 2006, p. 3). Table 4.27 represents the increase in size of the encrypted data over the clear text.

Table 4.27 *Increased sizes of encrypted data over its clear text*

Encryption types	**Algorithms**	**Maximum increase**	**Minimum increase**	**Average increase**
Symmetric	Triple Data Encryption Standard (DES)	3.80	0.45	1.77
Symmetric	Advanced Encryption Standard (AES) 128	5.40	0.54	2.51
Symmetric	AES 192	5.40	0.54	2.51
Symmetric	AES 256	5.40	0.54	2.51
-	Certificate	11.80	0.54	5.16
Symmetric	DES	3.80	0.45	1.77
Symmetric	Data Encryption Standard XORed (DESX)	3.80	0.45	1.77
Symmetric	Rivest Cipher (RC)2	3.80	0.45	1.77
Symmetric	RC4	3.60	0.43	1.73
Asymmetric	Rivest Shamir Adleman (RSA) 1024	11.80	0.54	5.16
Asymmetric	RSA 2048	24.60	2.08	11.31
Asymmetric	RSA 512	5.40	1.06	3.23

(Source: Adapted from Kiely, 2006, p. 3)

It is recommended that asymmetric encryption keys with RSA 1024 algorithm on the sensitive data be used. This method will selectively restrict access to the sensitive data, thereby allowing only holders of the private key to decrypt and view the data.

In addition, the encryption method may apply only to the council's sensitive data (customer credentials) rather than the entire database and all its tables. This will consume fewer loads and space on the backend database server (MS SQL 2005) (Dave, 2008; Microsoft Corporation, 2005).

- ***Risk 2***

Both the online payment application and the backend database servers should be configured into different subnetworks or a VLAN. Additionally, appropriate ACLs should be configured to tighter or filter network traffic between the application and the backend database servers as well as the subnets. This technique may mitigate the above mentioned potential risks.

4.5.1.2.2 Testing stage 2: Possible mitigation

- ***Risk 1***

The HTTPS traffic should be inspected in order to provide better security to the council's online payment system.

- ***Risk 2***

The firewall rule may be reconfigured to allow from anywhere (any) to outside (external). This may minimise potential risks against the online payment frontend web server (the CoA-DMZ-Epathweb) from both the DMZ and the internal networks. The purpose of the council's frontend web server is to serve its residents to access the frontend web server from outside of the network only.

Therefore, allowing access to the frontend web server from both the DMZ and the internal networks is unnecessary as it will increase the chance of potential risks such as virus and DoS attacks from either the DMZ or the internal networks in the event that attackers gained access to the internal network or the DMZ.

- ***Risk 3***

This rule may be tightened by allowing only the required TCP or UDP ports to the two IP addresses. For example, TCP ports 22 for SSH and 443 for HTTPS connections to be designated for administration purposes only.

- ***Risk 4***

In order to mitigate the potential risks, as per discussion with the network administrator and the online payment application administrator, the firewall rule may be disabled. Therefore; no communication will be allowed between the CoA-DMZ-Epathweb and the CoA-SQL servers. On the one hand, the current Epathweb software configuration on the CoA-DMZ-Epathweb server may be reconfigured for SQL queries to the CoA-Pathway rather than to the CoA-SQL server. The Pathway software configuration on the CoA-Pathway server may also be reconfigured to allow SQL queries with the CoA-SQL backend database server.

This can minimise any potential risks of direct access from the frontend web server to the internal backend database server. In addition, as per best practice recommendations to standard firewall configurations, no network traffic communication should be permitted between both the frontend web server and the backend database server.

- ***Risk 5***

This potential risk can be mitigated by reconfiguration of the firewall rules from the current destination setting which is anywhere (any), to outside (external) the network.

- ***Risk 6***

As per discussion with the council's network administrator, these firewall rules were unnecessary and were subsequently removed by the network administrator except for the firewall rule which, allows HTTP traffic between the frontend web server (the CoA-DMZ-Epathweb) and the Pathway application server (the CoA-Pathway). This was due to the fact that, HTTP is the required protocol for the frontend web server for communication with the Pathway application server.

In order to minimise the potential risk associated with the HTTP protocol, the council should consider using the existing old MS Internet Security and Acceleration (ISA) Server 2006 to provide stateful inspection and application-layer filtering on all HTTP traffic. This practice allows the ISA server to filter any HTTP traffic that appears out of context.

Figure 4.11 demonstrates the recommended high level online payment system including network traffic protocols and the existing MS ISA Server 2006 for the council.

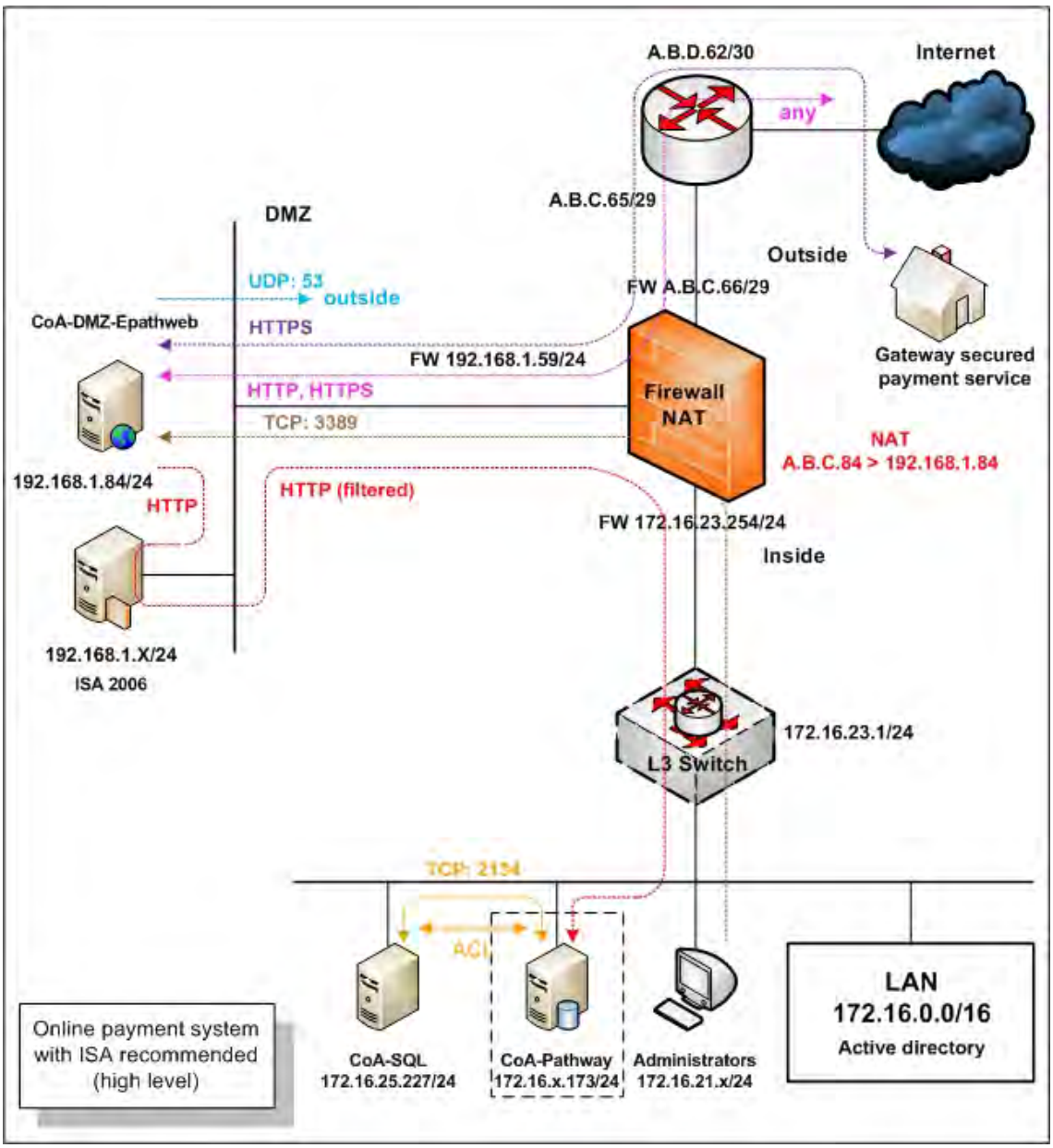

Figure 4.11. The recommended high level online payment system including network traffic protocols and the existing MS ISA Server 2006 for Council A

- ***Risk 7***

See previously discussion on Section 4.5.1.1.2 for more details.

4.5.1.2.3 Testing stage 3: Possible mitigation

- ***Risk 1***

In order to prevent any potential vulnerability that may arise as a result of poor configuration on both the password and security auditing policies at all of the three online payment system servers (the CoA-DMZ-Epathweb, the CoA-Pathway and the CoA-SQL), it is recommended that the MS Windows password be reconfigured. In addition the auditing policies should be reviewed at CoA-SQL server only as the DMZ server is governed by a satisfactory audit policy as indicated in Appendix A10.

Appendices A8, A9 and A10 depict the system information policy review including possible mitigation recommendations of the online payment servers pertaining to Council A's online payment system.

- ***Risk 2***

There was one missing service pack and two missing patches on the Council A's CoA-Pathway server as indicated in Appendix A11. One of these missing patches is categorised as critical. It is therefore, recommended to install the patch to the server as soon as possible. Furthermore, Appendix A11 displays the system patching testing analysis and possible mitigation recommendations of the council's CoA-Pathway server.

- ***Risk 3***

Table 4.28 presents the total number of recommended open TCP and UDP ports on all the council's online payment servers.

Table 4.28 *The total number of recommended open TCP and UDP service ports on all Council A's online payment servers*

Server names	**Recommended open TCP ports**	**Recommended open UDP ports**	**Comments**
CoA-DMZ-Epathweb	3	1	Refer to Appendix A12
CoA-Pathway	6	1	Refer to Appendix A13
CoA-SQL	9	2	Refer to Appendix A14

- ***Risk 4***

Refer to Appendices A15, A16 and A17 for full details of the identified risk issues and the possible mitigation recommendations.

4.5.1.2.4 Testing stage 4: Possible mitigation

- ***Risk 1***

Appendices A18, A19, A20, A21, A22 and A23 provide the full details of all the findings (satisfactory and unsatisfactory) and the possible mitigation recommendations.

4.5.1.2.5 Testing stage 5: Possible mitigation

- ***Risks 1, 2 and 3***

As per general recommendations to best practices, the council may wish to implement a related general information security policy together with associated technical security policies and procedures. The policies and procedures should cover the areas of the internetwork infrastructure, the web server and the database server. The implementation of these recommendations will serve to enhance the level of the information security of the online payment system of the council.

4.5.2 Discussion

The research activities carried out at Council A revealed that the implementation of both the email (MS Exchange 2007) and the online payment system were lacking in meeting both national and industry standards. Consequently, these sub-standard implementations pose a potential risk to the email, the online payment as well as the other related systems of Council A. However, the recommendations to mitigate the risks have been provided in the analysis section of this thesis.

Furthermore, the recommended frameworks for both the email and the online payment systems demonstrated that these frameworks can be used in order to improve or audit the security of systems within a similar environment. More details with references to the research questions and examples are provided in Chapter 8: Section 8.3.

There were seven main factors identified which may be a cause of potential risk to the Council A's email, online payment and other related IT systems. The risks can result in interruptions, extraction of personal details and destruction of data to the council's email as well as the online payment systems.

For example, a lack of specific knowledge by staff in proper configuration of the firewall will result in potential interruptions, modifications and destruction of the councils email and online payment data. Any consequential compromise to the integrity of the systems concerned will result in downtime while the systems become unavailable during repair.

Furthermore, extraction of the personal details of the council's residents becomes a distinct possibility as IT staff were unaware that residents' personal details information should be stored in an encrypted format for security. Non encryption of such personal detail information will result in a compromise to the confidentiality aspect of the security of information held within these databases and systems.

The seven factors were the lack of IT security standards awareness, inadequate domain or service specific knowledge, inefficient communication, limited IT training as a result of restricted training budget, insufficient time for task completion, reliance on external consultant for specific IT projects and no valid testing environment in place. The following paragraphs provide an explanation of the seven factors in full detail.

Firstly, the lack of IT security standards awareness was examined. There were several discussions with the council's IT operational staff (the network administrator, the Pathway application administrator, the system administrator, the telecommunication administrator and the external database administrator) over a period of several months. There were a number of potential risks apparent due to the lack of IT security standards awareness disclosed in the investigation.

For example, the email (MS Exchange 2007) system's architecture was not designed following the MS Exchange 2007 architecture recommendation. The MS SQL Server 2005 database configuration on the backend database server was also not following the industrial best practices standard recommended by CIS (2010).

In addition, the Pathway application administrator was not aware that the sensitive information (the client's credentials) should be recorded in encryption format. These represent serious knowledge gaps in human resource and should be addressed by further training or supplementing through consultancy. Table 4.29 summarises the findings related to the lack of IT security standards or general industrial best practices by the staff of Council A

Table 4.29 *The summary of the issues uncovered related to the lack of IT security standards awareness by the IT staff*

Results related to lack of IT security standards awareness by IT staff of the council	**Council A**
Internet border router redundancy/alternative Internet link deployed	No
IDS/IPS deployed and currently in use	No
Encryption of client sensitive information	No
Design of email server architecture based on the MS Exchange 2007 recommendations to best practices	No

Secondly, the inadequate domain or service specific knowledge was outlined. This was evident from the inadequate configuration on the three internetwork switches configuration codes, the firewall rules, the unnecessary ports and the services installed on the related servers. According to the network and system administrators, the council's IT operational staff have never been trained in specific knowledge such as email (MS Exchange 2007) server and firewall (Cisco ASA) related courses. See the following table for more details.

Table 4.30 *The summary of results uncovered related to the inadequate specific knowledge*

Results related to inadequate domain or service specific knowledge by the IT staff of the council	**Council A**
Firewall configuration related to the email and online web systems	Insufficient
Switch configuration related to the email and online web systems	Insufficient
Setup and configuration of the email server application (MS Exchange 2007)	Incorrect
Setup and configuration of the online database application (MS SQL Server 2005)	Incorrect
Application of updated software patches on the email server	No
Application of updated software patches on the online web server	No

Table 4.30 *The summary of results uncovered related to the inadequate specific knowledge (continued)*

Results related to inadequate domain or service specific knowledge by the IT staff of the council	**Council A**
Application of updated software patches on the online payment server	No
Internal email spoofing allowed	Yes
Unnecessarily opened or unused service ports on the email server	Yes
Unnecessarily opened or unused service ports on the online web server	Yes
Unnecessarily opened or unused service ports on the online payment server	Yes
Vulnerabilities uncovered on the email server	Yes
Vulnerabilities uncovered on the online web server	N/A
Vulnerabilities uncovered on the online payment server	Yes

Thirdly, the inefficient communication was highlighted. It was noticeable that there were mis-configurations on the ACL codes of the firewall related to the online payment system as a result of personal communications between the network administrator and the Pathway application administrator.

Furthermore, currently there were no change management procedures. There was also no apparent IT record of auditing systems in place. Introduction of a change management will assist the council's IT manager as well as operational staff to manage, plan, track and predict any changes that may occur efficiently. IT record auditing systems and documentation such as simple log books for firewall, email, database and web servers would also provide benefits to the IT operational staff.

For example, properly maintained system log books will allow IT staff to review, report or audit changes made, roll back changes made to previous states and minimise any risks of inaccurate data and configurations.

In addition, both change management procedures and IT record auditing systems and documentation procedures will also serve to increase the lack of communication between the IT operational staff. Table 4.31 summarises the issues uncovered that can contribute to the inefficient communication between the council's IT operational staff.

Table 4.31 *The summary of results uncovered that can contribute to the inefficient communication*

Results uncovered that can contribute to the inefficient communication	**Council A**
Existence of change management procedures	No
Availability of simple specific technical log books	No
Updated documentation of the IT email system	No
Updated documentation of the IT online web system related	No

Fourthly, the limited IT training as a result of a restricted training budget was examined. According to the council's IT manager, each year the IT department receives a restricted IT training budget resulting in each individual IT operational staff not being able to attend specific IT training courses every year. This deficiency in funded training would contribute further to the lack of specific IT knowledge within the council's IT department. See details in Table 4.32.

Table 4.32 *The summary results related to the limited IT training as a result of limited training budget*

Issues uncovered in relation to the limited IT training budget	**Council A**
Formal industry or equivalent firewall training of the IT operational staff	No
Formal industry or equivalent training of the email application (MS Exchange 2007) of the IT operational staff	No
Formal industry or equivalent training of database application (MS SQL Server 2005 or equivalent) of the IT operational staff.	No
Formal IT Security training of the IT operational staff	Partly
IT training yearly budget allocation for each IT operational staff member	Partly
Support of the council for self-costed self study of IT operational staff	Yes

Fifthly, the matter of insufficient time for task completion was looked at. The council's IT team has one IT manager, six IT operational staff and two part time staff (network and database administrators). Both the network and database administrators are contractors and only work one day per week. The council's IT team has to manage a wide range of ICT areas such as GIS, GPS, library, email, Intranet, online payment, online website, payroll, property, telecommunication and telephony systems. According to the telecommunication, the network and system administrators, only just enough time is available for them to complete their day to day operation tasks.

Additionally, they do not have any time left for documentation. This was evident from the uncompleted or partly completed network and system documentation. Table 4.33 summarised the insufficient time for task completion by the council IT operational staff.

Table 4.33 *Results uncovered related to the inefficient time for task completion*

Issues uncovered in relation to the inefficient time for task completion	**Council A**
The IT operational staff manages several complex IT systems task simultaneously	Yes
Use of enterprise information security policy	No
Use of technical (issue-specific and systems-specific) security policy	No
Updated documentation of the IT email system	No
Updated documentation of the IT online web system	No

Sixthly, the factor of the reliance on external consultants for specific IT projects was analysed. The council's IT team always relies on outsourcing to solve the expertise problems that may arise. This may result in a lack of knowledge transfer between the external contractors to the council's IT operational staff.

For example, in the projects which were completed by the contractors, there was a distinct lack of documentation such as for the email system (MS Exchange Server 2007) and the online payment system (Epathway). This indicates poor contract management by the council when initiating and finalising projects as these basic elements should be in the performance contract. See Table 4.34 for more details.

Table 4.34 *Summary of issues uncovered relating to the reliance on external consultants for specific IT projects*

Issues in relation to the reliance on external consultants for specific IT projects	**Council A**
Implementation of the firewall system by external consultants	Yes
Appropriate documentation for the firewall installation and management provided by the external consultants	No
Deployment of the email (MS Exchange 2007) application server by external consultants	Yes
Appropriate documentation for the email (MS Exchange 2007) installation and management provided by the external consultants	No
Deployment of the online payment system by external consultants	Partly
Appropriate documentation for the online payment system (Epathweb) installation and management provided by the external consultants	Partly

Finally, there was no valid testing environment in place at Council A. The IT department did not have any proper testing systems in place even though specific VM servers were allocated as testing servers for the database, and online payment systems.

Additionally, there was no testing system for the network communication equipment that would accurately match the testing environment to the architecture of the production system in totality. A totally mirrored testing environment would minimise any potential risks to down time and loss of productivity due to hapless mis-configurations, faulty installations or upgrades to the IT system carried out directly on the production environment, as these would be fully tested in the testing environment prior to a scheduled replication on the production system. The following table presents more details of the summary of issues uncovered related to the lack of a valid testing environment.

Table 4.35 *Summary results uncovered related to no valid testing environment on place at the council*

Summary results related to the lack of a valid testing environment	**Council A**
Existence of a testing environment for the infrastructure	No
Existence of a testing environment for the email system	Partly
Existence of a testing environment for the online payment system	Partly

CHAPTER 5. EXPERIMENTAL EVALUATION AND ANALYSIS: A CASE STUDY OF COUNCIL B

This chapter is presented in five subsections: (1) background information; (2) methodology; (3) Council's B email system results; (4) Council's B online web system results; and (5) analysis and discussion. Its objective is to exemplify the results and findings from the examination of Council B's email and online web systems in this research.

5.1 Background information

Council B is a local government council in WA which runs its own IT department. The council has an Ethernet network which connects its central and remote sites via fibre optic, DSL and ADSL. The council's central site is connected to the outside world or the Internet via a fibre optic connection. The council's network architecture is considered to be structured in a star topology format. Council B runs an in-house email system which provides email service to its staff. The council's email system has over 1,000 mailboxes, the majority of which serves its staff. Furthermore, the email system provides service to other indirect staff such as the councillors and external contractors as well. The council's email server is MS Exchange 2007 and MS Outlook 2007 is used as an email client and personal information management tool.

In addition, the email system has a web-based email or webmail feature, which allows the council's authorised personnel to access their email via a web browser anywhere over the Internet.

Council B also offers an online web system service to its residents. This online web system provides general information, mailing lists, online community groups and online payment services. Anyone can view the general information, join the online mailing lists and become part of the community groups.

Additionally, the council offers online payment system to its residents for paying their rates, applications, infringements, licence renewal and other invoices using their valid type of payment numbers as follows:

- Assessment number for rate payment;
- Payment reference number for application and licence renewal;
- Reference and invoice numbers for other invoices as meals on wheels payments; and
- Ticket number for infringements such as dog, litter and parking fines.

These valid types of payment numbers are assigned to the council's residents based on their individual application. In addition, both the email and online web systems are managed in-house by the council's IT staff.

5.2 Methodology

The purpose of this subsection is to provide a detailed description of the methodology used in this research. All the facets of the methodology including pre-interview consultation, document review, interview investigation, existing architecture discovery, email system testing and online web system testing are presented in the six sections.

5.2.1 Pre-interview consultation

Prior to the detailed analysis provided herewith, a pre-interview consultation was conducted in order to determine the scope of the project. This interview was in the form of initial open-ended meetings and discussions that were undertaken between participants including the researcher, both the principal and associate supervisors, the council's IT managerial staff and IT operational staff.

All involved parties agreed that both the email and online web systems would be audited as the findings may prove both useful and also serve to enhance security for both the email and online web systems. In addition, all parties agreed that this investigation may serve to increase the security awareness for the council's IT staff. Furthermore, the reports produced would serve to highlight any improvements to the systems that may be required in order to fine tune the efficiency and security of the email and online web systems.

Council B agreed to an overall time frame of five months based on the estimate of two and half months for each report produced. Additionally, the council agreed upon the recommendation that the analysis be done in stages in order to minimise the disruption to normal services.

It was also agreed that this project was to be undertaken at no cost to the council and the recommendations would be presented to the council as a set of two reports: 1) the email system and 2) the online web system. Additionally, the council would be under no obligation to implement any of the recommendations contained in the reports and the council may at its discretion, elect to abort the project at any time as desired.

5.2.2 Document review

There were two types of documents describing the email and online web systems that were available. These were the hardware and software specification documents and the organisation policy documents. The software documents consisted of in-house software systems as well as the third-party software systems.

Several documents relating to both the council's email and online web systems were collected. These documents included specifications and records of configuration codes of the Internet border router, the IDS/IPS, the DMZ switch, the firewalls, the email server, the spam blocker appliances, the static web servers, the application server and the backend database server. Furthermore, a copy of the DMZ internetwork diagram was collected.

From the interviews conducted it was established that both the email and online web systems technical security policies were non-existent apart from a general email usage policy. These omissions were due to the lack of time required for the implementation of security policies for these systems.

5.2.3 Interview investigation

Several interviews were conducted with the two main stakeholders as follows:

- Council B's IT managerial staff (IT manager); and
- The council's IT operational staff (database, network, Pathway application, system and web administrators).

The interview with the IT managerial staff were a face-to-face interview to ascertain a general overview of the council's email and online web systems. In terms of outcomes, an outline of the council's expectation from the project was discussed. It emerged that the council was interested in overall system documentation and risk analysis of both the email and online web systems.

Ongoing testing analysis interviews were conducting using several interview techniques such as face-to-face, telephone and email between the researcher, the network and the web administrators.

Interviews conducted with the network administrator were related to discussions of network connectivity of the various hardware entities. These included the firewalls, the Internet border router, the switch, the static web servers, the email, the AD, the DNS and the database servers. The ACL and configuration codes pertaining to the relevant devices were also discussed.

Testing analysis interviews were conducted with the web administrator, relating to the configurations of the backend database server, the static web servers, as well as the application logic surrounding the online web payment system.

5.2.4 Existing architecture discovery

This section describes the discovery of the existing architecture at Council B in relation to their email and online web systems.

5.2.4.1 The existing email system architecture of Council B

Council B's email system consists of one email server, and two spam blocker appliances. These devices are connected together within the council's internetwork infrastructure. The email server is located in the council's internal network whereas both the spam blocker appliances are located in the council's DMZ area. The infrastructure has one Internet router, two firewalls and one switch as its components. The only two email related network traffic protocols allowed in the network are HTTPS and SMTP which are used for webmail and traditional email respectively. In terms of HTTPS, Council B uses 128-bit encryption with standard validation SSL certificate for its webmail connectivity (Limwiriyakul & Valli, 2011c).

Figure 5.1 illustrates all the devices connectivity and allowed email network traffic protocols in a high level network diagram.

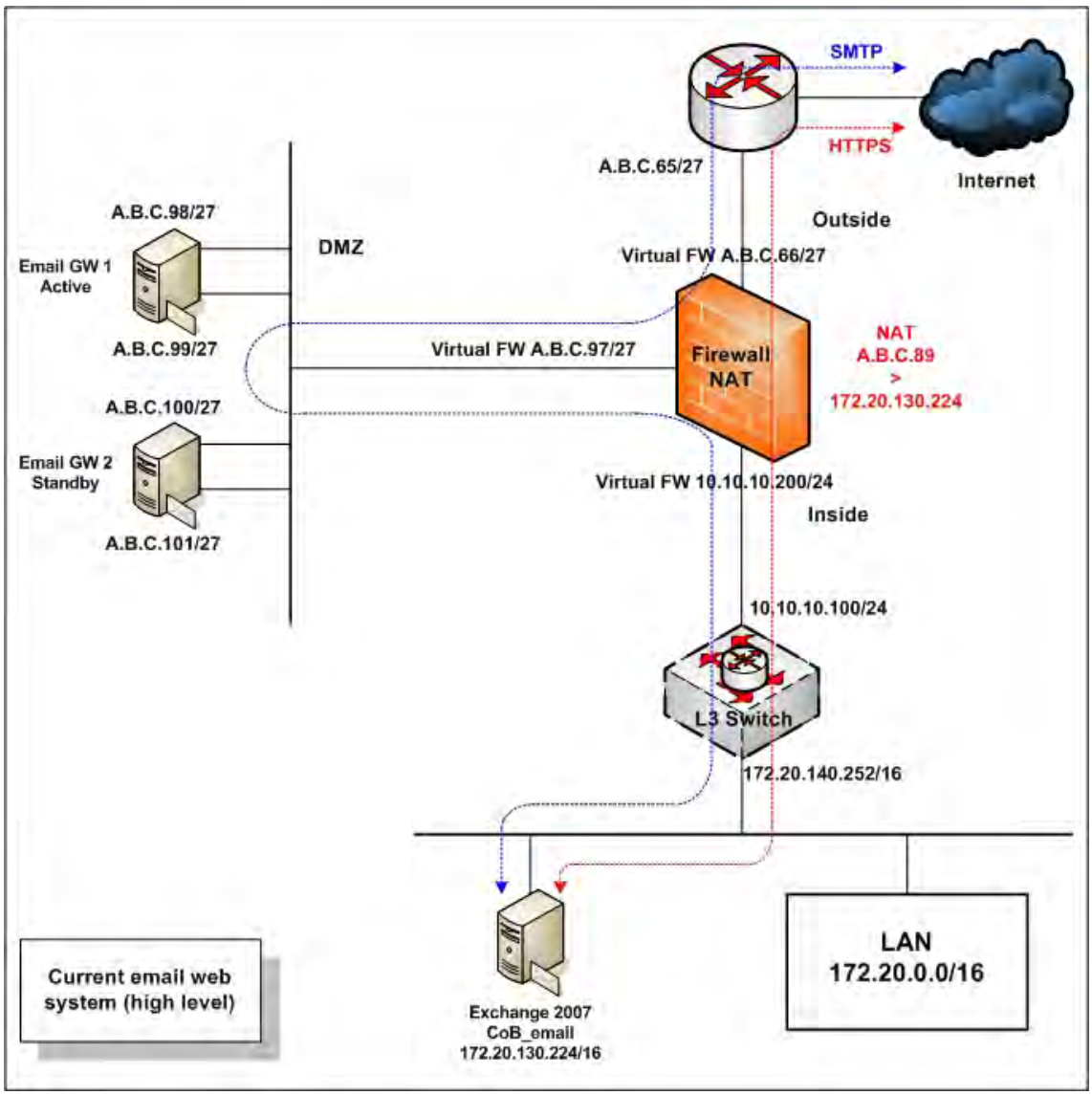

Figure 5.1. A current high level network diagram for the email system of Council B

5.2.4.2 The existing online web system's architecture of Council B

The council's current online web system provides the council's general information such as rates, libraries, events, facilities and jobs. Council B's online web system can be categorised into three different groups based on their features and architectures. These three groups are as follows:

- The static web system;
- The CMS web system; and
- The online payment system.

5.2.4.2.1 The existing static web system architecture

The current static web system has two CoB-DMZ-Web and CoB-Web servers. The council's static web system provides both simple/standard static and form-based web pages. The CoB-DMZ-Web server is located in the council's DMZ area, whereas the CoB-Web server is located in the council's internal network.

Figure 5.2 depicts the council's current architecture on the static web system including network traffic protocols in a high level network diagram.

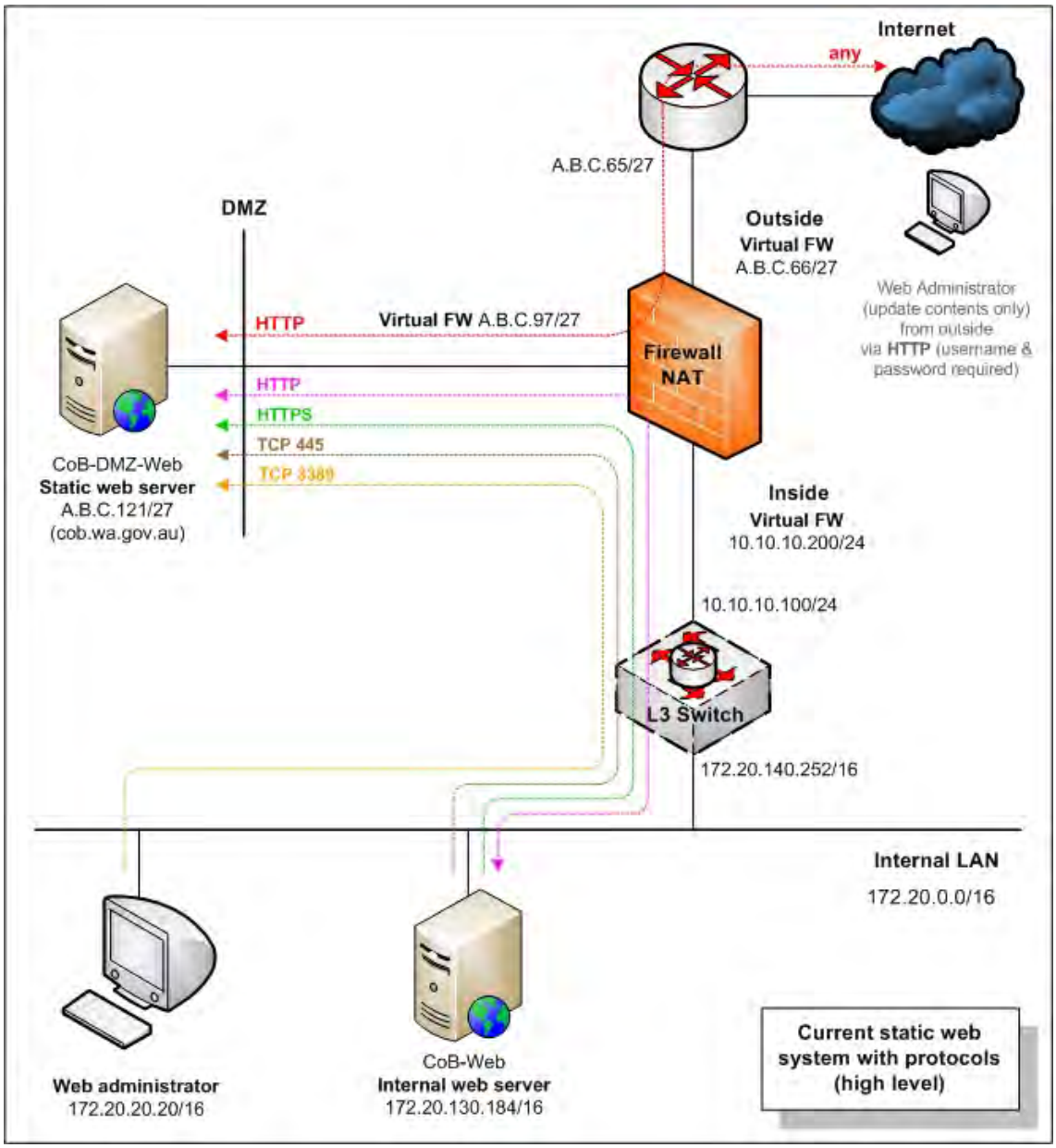

Figure 5.2. The high level static web system currently in use by Council B

5.2.4.2.2 The existing CMS web system architecture

The current CMS web system has two servers which are the CoB-DMZ-Web and the CoB-Database servers. It provides both simple/standard static and form-based web pages. The CoB-DMZ-Web acts as a CMS frontend web server whereas the CoB-Database acts as a CMS management server. The CoB-Database server is located in the council's internal network. Figure 5.3 illustrates the council's current CMS system architecture including network traffic protocols in a high level network diagram.

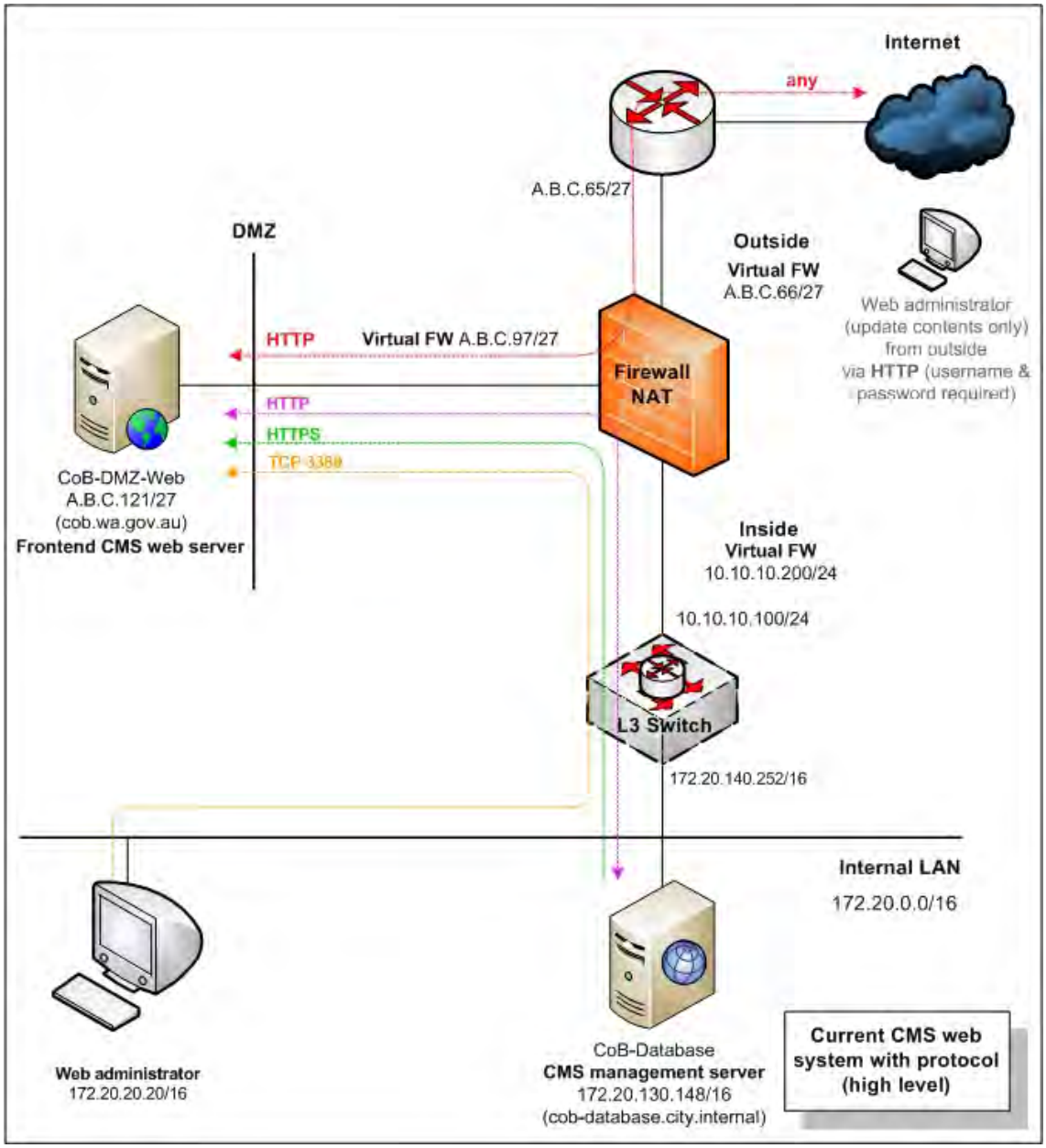

Figure 5.3. The high level CMS web system currently in use by Council B

Both the CoB-DMZ-Web and CoB-Database servers interact with each other as part of a Web Content Management System (WCMS). The CoB-Database permits the council's IT operational staff to manage and update web page information, prior to uploading the validated web pages from the CoB-Database server to the CoB-DMZ-Web server.

This arrangement provides good security as there is no direct connection between the client and the CMS management server. The council's residents, access general council information from the CMS frontend web server (the CoB-DMZ-Web) via the council's website (http://www.cob.wa.gov.au).

5.2.4.2.3 The existing online payment system architecture

The council's current online payment system is designed as a three-tiered client-server architecture. It consists mainly of two servers which include a frontend and web application server, and a backend database server as depicted in Figure 5.4. CoB-DMZ-Web performs the application logic function by covering both frontend and application web features. The backend database (the CoB-Database) server performs the data logic.

In addition, the external gateway security payment service (the online gateway) is employed by the council to provide a secured online payment system for its residents and is used for payments such as rates and infringements. The council's online payment system communicates with the external gateway security payment service using the HTTPS protocol.

Furthermore, the SSL protocol is used to provide an encrypted communication channel between the client's web browser and the council's online payment system. This method ensures secured private communications over the public Internet. The council uses 128-bit encryption with standard validation SSL certificate for its online payment SSL connection (Limwiriyakul & Valli, 2011c).

Figure 5.4 demonstrates the council's current online payment system architecture including network traffic protocols in a high level network diagram.

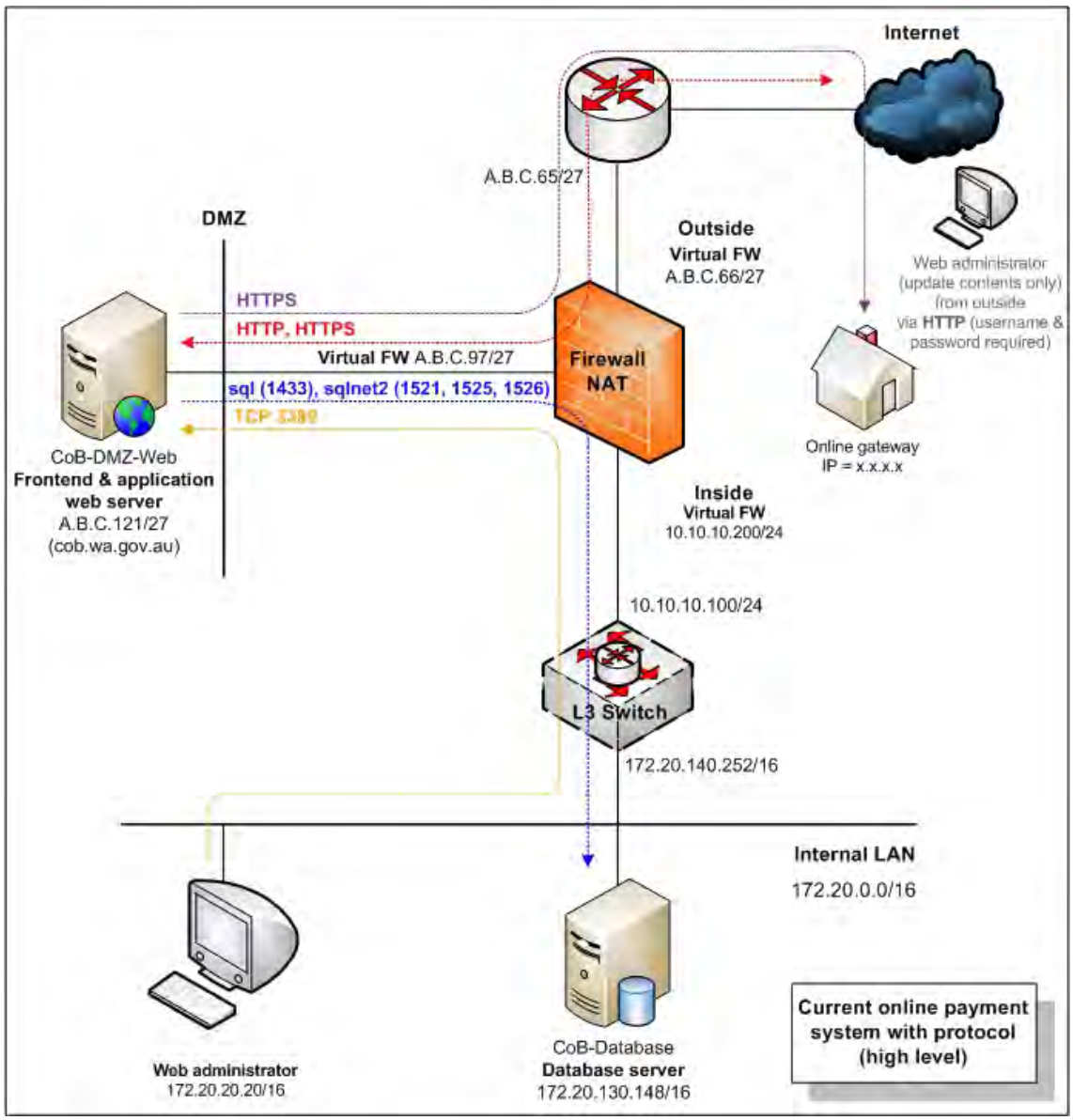

Figure 5.4. The high level online payment system currently in use by Council B

5.2.5 Email system testing

In this email system testing consists of five stages which are summarised as follows:

- Network surveying includes discovery of the current Council B's email system's network architecture;
- Auditing and configuration codes review of the Internet border router, the IDS/IPS, the firewalls and the switch devices;

- Services and system identification, port scanning and vulnerability testing of the email and webmail servers;
- Email spoofing testing and vendor security benchmark auditing on the email server; and
- Email system security policy review.

5.2.6 Online web system testing

The online web system of the council can be categorised into three distinct application profiles which are the static web system, the CMS web system and the online payment system. All of these online web systems share and partly share hardware for servers. More details of the servers are provided in the Testing stage 5.4.1.

This online web system testing analysis which was carried out consists of five stages which are summarised as follows:

- Network surveying, which includes the current Council B's online web system's network architecture, identified risks and mitigation recommendations;
- Auditing, configuration codes review, identified risks of the Internet border router, the IDS/IPS, the firewalls and the switch devices related to Council B's online web system;
- Services and system identification, port scanning and vulnerability testing of the online web system's servers;
- Vendor security benchmark auditing on the online payment server; and
- Online web system security policy review.

5.3 Council B's email system results

The following sections explain all the results of the review and testings for the architecture design, the device configurations, the vulnerabilities of all the email system servers, the email spoofing, the vendor security benchmark and the security policy in details.

5.3.1 Testing stage 1: Network surveying

This network surveying of the testing stage one consists of network surveying that collects information on the email system including the email server, the two spam blocker appliances, the current email architecture, identified issues and recommendations. Information for the following components of Council B's email system were collected:

- Overall network diagram for the Internet link, the DMZ infrastructure connectivity including the email system;
- The Internet border router, the two Internet firewalls, the DMZ's switch specification and the related email configuration codes;
- The email server's specification summary; and
- The two spam blocker appliances' specification summary.

5.3.1.1 The email system devices

The council's email system consists of two specific devices type. These are the MS Exchange 2007 email server and the Cisco IronPort spam blockers.

5.3.1.1.1 The email server

The current email server had MS Exchange 2007 with the newest service pack 1 as the email application software. The software was running on MS Windows Server 2003 Enterprise Edition with service pack 2.

According to Microsoft TechNet (2007a), the current email server configuration may be considered as a simple single-server architecture combining the Mailbox server, the Hub Transport server and the CAS roles. However, the Edge Transport server and Unified Messaging server roles were not included or installed for the same reasons as Council A in that Cisco IronPort spam blockers are used to perform the same function as the MS Edge Transport server role. Furthermore, Council B also uses the Notel VoIP system for the Unified Messaging server role. Summary details are provided in Table 5.1.

Table 5.1 *A summary of the email server specifications*

Attributes	**Details**
Email application software	MS Exchange 2007 with service pack 1
Email scanning software	Trend Micro ScanMail for MS Exchange version 8.0.1181
OS	MS Windows Server 2003 Enterprise Edition with service pack 2
Hardware	VMware server
IP address	172.20.130.224/16
MS Exchange 2007 roles	Mailbox, Hub Transport, CAS combined
Email service protocols	SMTP and HTTPS
Other software	Trend Micro OfficeScan Client

5.3.1.1.2 The spam blocker appliance

There are two spam blocker appliances (email GW1 and GW2) which are running on Cisco IronPort appliances. Each of the devices has two network interfaces for separating incoming and outgoing email network traffic. The two devices run concurrently as part of a redundancy strategy (active and standby mode). Table 5.2 summarises both the spam blocker appliance roles and specifications.

Table 5.2 *A summary of both the spam blocker appliance specifications*

Attributes	**Details**
Device name	Email GW1
Spam blocker application software	Cisco IronPort C150
OS	Cisco IOS
Hardware	2 GB RAM, 2 x 80 GB Serial Advanced Technology Attachment (SATA) drives
Interfaces (1, 2)	Gigabit Ethernet: A.B.C.98/27, A.B.C.99/27
Feature roles	Scan virus, block spam email, block email blacklist
Device name	Email GW2
Spam blocker application software	Cisco IronPort C150
OS	Cisco IOS
Hardware	2 GB RAM, 2 x 80 GB SATA drives
Interfaces (1, 2)	Gigabit Ethernet: A.B.C.100/27, A.B.C.101/27
Feature roles	Scan virus, block spam email, block email blacklist

The purpose of these appliances is to filter all incoming and outgoing emails (SMTP) against virus and worm threats and to block spam emails. As compared to MS Exchange 2007 server roles architecture (see previously discussed Section 4.3.1.1.1 for more details), these spam blocker appliances perform the same role as the MS Exchange 2007 Edge Transport server role.

5.3.1.2 Testing stage 1: Identified risk issues

The following sections describe the identified risk issues for the council's email system.

- ***Risk 1: Single point of failure***

As previously mentioned, the existing email architecture of Council B is made up of a simple single-server. According to Microsoft TechNet (2007a), the simple single-server (MS Exchange 2007) architecture should only be deployed in Windows's SBS which is suitable for small network environments. Council B's network is considered to be a medium size as it has over 1,000 mailboxes and over 600 staff (personal communications with Council B, 2010).

As the current council's email server performs three MS Exchange 2007 roles (CAS, Hub Transport and Mailbox Server roles). This may be considered as a single point of failure as all three MS Exchange Server roles are run by the single email server.

- ***Risk 2: Same subnetwork***

The email server is located in the council's internal network which has the same IP address group (subnet) as the other important servers with no additional ACL filtering for separation.

As the other important servers are the database, financial and file servers, they may be open to potential security risks, such as virus attacks. Virus attacks and threats arising on the email server may possibly infiltrate and infect other servers within the same subnetwork thereby leading to interruptions to the IT services of the council.

- ***Risk 3: MS ActiveSync – Authentication***

MS ActiveSync supports three different authentication types which are the basic, certificate and token forms. Council B currently uses the basic authentication together with a SSL connection. This means that username and password are transmitted in clear text whereas the connection on the other hand, is encrypted. Basic authentication can be considered as the simplest as it provides the lowest level of security as compared to both certificate and token form authentication methods (Luckett et al., 2008).

- ***Risk 4: MS Outlook Anywhere – Authentication***

MS Outlook Anywhere or RPC over TCP is disabled by default (Microsoft TechNet, 2007b, c). However, Council B's MS Outlook Anywhere is currently enabled. MS Outlook Anywhere deployed in Council B allows direct external access into the internal network using the basic client authentication method via the SSL connection. As the basic authentication method provides the lowest security, it is recommended that it be enhanced.

5.3.2 Testing stage 2: The email system's infrastructure – Internet border router, IDS/IPS, firewalls and switch reviews

This email system's infrastructure testing stage consists of a review of the council's email infrastructure data collections which are the Internet border codes, the IDS/IPS, the firewalls codes and the switch codes data collection.

5.3.2.1 Internet border router configuration codes data collection and reviews

According to the council's internetworking, the Internet border router acts as a gateway which allows the council network to be able to communicate with the outside world (the Internet). The Internet border router is designed for routing purposes in order to forward or route the internetworking traffics/protocols which serves the council network services such as email and WWW. In addition, the router provides the first layer of traffic filtering which means only permitted internetwork traffic or protocols are allowed to get in and out the council's network.

Table 5.3 summarised the specifications of the Internet border router and the ACL codes for the email system. In addition, the risk issues uncovered and the possible risk mitigation recommendations are also presented.

Table 5.3 *A summary of the Internet border router specifications*

Attributes	**Details**
Device type	Cisco 2811
OS	Cisco IOS version 12.2
Memory	128 MB
Interfaces (2)	External: A.B.D.x/30, Internal: A.B.C.65/27

5.3.2.2 IDS/IPS configuration codes data collection and reviews

IDS/IPS is a critical early warning system that may provide the necessary information to the network administrator/email administrator in order to protect the email server from attackers. The council's Internet border router has its own built-in IDS/IPS. However, the IDS/IPS feature on the router was disabled.

5.3.2.3 Firewall configuration codes data collection and reviews

In the council's internetworking, the two firewalls act as a main filtering for all incoming and outgoing internetwork traffic. In addition, they perform NAT as well. One of the firewall operates in an active mode and the other operates in a standby mode. Table 5.4 summarises the specifications of both the firewalls.

Table 5.4 *A summary of the firewall specifications*

Attributes	**Details**
Device type	CheckPoint Firewall-1
OS/model	UTM-1 272 (270 series)
Memory	512 MB
Interfaces	4 x Ethernet 10/100/100 full duplex, 1 sync port
IP address	See Figure 5.5 for full details

Refer to Appendix B2 for the summary of the firewall configuration codes with respect to NAT of the email system. In addition, Appendix B3 demonstrates the summary of the firewall configuration codes with respect to the email system.

5.3.2.4 Switch configuration codes data collection and reviews

Council's B has only one Ethernet switch which provides network communication and connectivity between the Internet border router, the firewalls, the DMZ servers and the council's internal network. The current overall hardware and software details of the switch are depicted in Table 5.5 whereas details on ports, VLANs including its connectivity are provided in Figure 5.5.

Table 5.5 *The email system: Current switch hardware and software details*

Attributes	**Details**
Device name	CoB-admin-central
Device type	Cisco Catalyst 3750G switch
OS	Cisco IOS version 12.2
Memory	128 MB
Port	24 x 10/100 MB UTP Ethernet ports, 2 x GB SFP ports
Operate at	Layer 3 OSI
VLAN number	1, 2, 3, 4, 6, 7

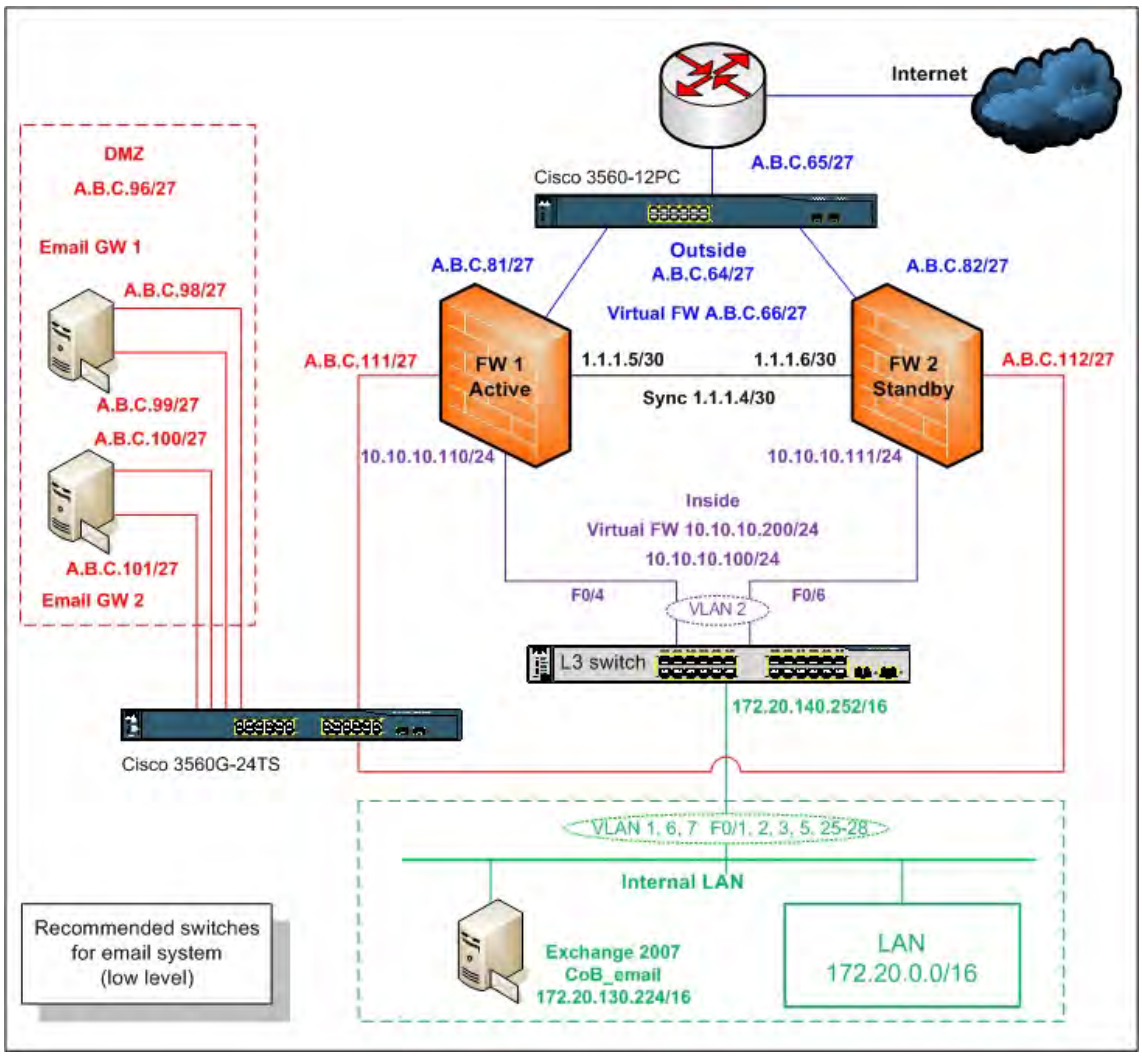

Figure 5.5. A current low level network diagram of the email system for Council B

5.3.2.5 Testing stage 2: Identified risk issues

The identified risk issue for the council's email infrastructure system (Internet border router, the IDS/IPS, the firewall and the switches) are detailed in the following sections.

- ***Risk 1: Poor ACL coding on the Internet border router***

The current Internet border router allows any IP traffic including TCP and UDP to get in and out the council network. This configuration may be considered contrary to the best practice recommendations of standard firewall configurations.

Nevertheless, the overall ACLs are sufficient to block some of the potential risky ports such as TCP port 161, 162, SNMP, Simple Network Management Protocol Trap (SNMPTRAP), Telnet, UDP port 259 as well as some private IP addresses. See Appendix B1 for details on a summary of the council's Internet border access list code for the email system.

- ***Risk 2: Internet border router's IDS was disabled***

The IPS software feature on the Internet border router (Cisco 2811) is currently disabled. This can be a cause of potential security risk to IP spoofing and scanning attacks. There are various types of security attacks which rely on the IP spoofing method in order to begin an attack such as SMURF or Internet Control Message Protocol (ICMP) flooding attack as well as DoS attacks (Network World, 2008). Such spoofing attacks may result in a loss of Internet connectivity for council's network as well as disrupt the council's community services.

- ***Risk 3: No IPS feature on both the firewalls***

Currently there is no software IPS feature implementation on the two CheckPoint firewall Unified Threat Management (UTM)-1 272 (270 Series) devices. Therefore, both the incoming and outgoing SMTP email traffic is not inspected making the network vulnerable to a broad range of threats including DoS, man in the middle and other malicious attacks (Check Point Software Technologies Ltd., 2010).

- ***Risk 4: Inadequate firewall ACL coding – spam blockers***

Both the two spam blockers (email GW1 and GW2) are currently accessible from anywhere within the council's internal network via both HTTP and Telnet remote communication ports (see Appendix B3: Policy number 3). Both these remote access communication methods are considered insecure, due to the fact that all data, including passwords, communicated through these ports is in a plaintext (Microsoft TechNet, 2004, 2005a, b).

Furthermore, communication traffic can be intercepted by hackers through packet sniffers and the password can be used later for further malicious purposes.

- ***Risk 5: Inadequate firewall ACL coding - HTTP***

The current firewall rule allows both the spam blocker appliances access anywhere via HTTP port (see Appendix B3: Policy number 4).

- ***Risk 6: Firewalls cannot provide deep inspection on HTTPS traffic***

The existing firewall (CheckPoint) cannot provide deep inspection on all HTTPS traffic (Check Point Software Technologies Ltd., 2010). This means that the council's webmail (HTTPS) traffic is directly allowed into the council's internal network without any inspection for potential unwanted malware.

- ***Risk 7: Overall inadequate switch code security configurations***

Similar to Council A, there were some inadequate switch code security configurations on the current Ethernet switch. These inadequate configurations may lead to potential risks such as ARP spoofing, ARP poisoning and broadcast storm attacks.

- ***Risk 8: Single point of failure***

As mentioned earlier, the council has only one switch which provides network communication and connectivity between the Internet border router, the firewalls, the DMZ servers and the council's internal network. This stand alone switch may be considered as a single point of failure. In addition, it can be a source of potential risk in that the council's internal network may be exposed to attack through the methods previously mentioned.

5.3.3 Testing stage 3: Services and system identification, port scanning, vulnerability testing and results

Similar testing steps conducted at Council A, NMAP and GFI LANguard network scanning tools were used for the scanning test of the council's email system. NMAP with GUI standard (open source Zenmap version 5.0) for MS Windows XP version was run. The slow comprehensive scan option was used in the test in order to collect as much information as possible from the email system relating to the TCP, UDP ports, vulnerabilities, patches, services, software and hardware.

In addition, GFI LANguard version 9.0 with full scan option was run in order to fully test and collect the council's email system information. Both these scanning techniques allow deep information collection on the council's email system.

5.3.3.1 Services and system identification results

The full results of the services and system identification of the MS Exchange 2007 email server are presented in Appendices B4 and B5. However, there were no testing results for the two email gateway spam blocker appliances as neither of the testing software (NMAP and GFI LANguard) could obtain any services and system information, including patching information, for the two email gateway spam blocker appliances.

5.3.3.2 Port scanning results

Both NMAP and GFI LANguard network scanning tools were used to perform port scanning on the email server and on the two email gateway spam blocker appliances GW1 (A.B.C.99) and GW2 (A.B.C.101).

Moreover, there were some issues uncovered such as the TCP and UDP ports which were found to be left opened unnecessarily. This was found to be the case on the email server but not on the two email gateway spam blocker appliances (GW1 and GW2). Full port scanning details of the council's email server is provided in Appendix B6.

5.3.3.3 Vulnerability testing results

Similar to the vulnerability technique of Council A, the vulnerability is categorised into four levels which are high (H), medium (M), low (L) and potential (P) security levels. The vulnerability analysis was successfully executed on the email server. However, there were no vulnerability analysis results for the gateway spam blocker appliances as both the GFI LANguard and NMAP software did not yield any vulnerability information from the vulnerability testing. Full vulnerability results are provided in Appendix B7.

5.3.3.4 Testing stage 3: Identified risk issues

The identified risk issues of Testing stage 3 for Council B's email system are described as follows.

- ***Risk 1: System information policy results for the email server***

There were inadequate measures of the system information policy's configuration which includes password policy, security auditing policy and services. This inadequacy may lead to the potential risk of attacks against the organisation's email system.

- ***Risk 2: System patching status results for the email server***

The overall system patching status testing analysis of the council's email server was carried out using GFI LANguard and NMAP scanning tools. A number of issues were uncovered. These related to missing and unimplemented system patching information thereby creating vulnerabilities and possible threats to the council's email server (the CoB-email). The scan revealed that there were two missing patches on the email server. See more details in Appendix B5.

- ***Risk 3: Unnecessary opened ports on the email server***

It was found that there were 22 opened TCP ports and eight opened UDP ports on the email server. These numbers include the unnecessarily opened ports. See Table 5.6 for more a total numbers of opened TCP and UDP ports of the council's email server. The overall opened TCP and UDP ports as well as the possible mitigation recommendations are presented in Appendix B6.

Table 5.6 *List of the number of open TCP and UDP ports on the email server*

Server name	**Opened TCP ports**	**Opened UDP ports**	**Comment**
Email server	22	8	Refer to Appendix B6

- ***Risk 4: Vulnerabilities found on the email server***

There were vulnerabilities discovered on the email server. As an example the TCP service port 110 (POP3) was left opened thereby presenting a vulnerability issue in the high security risk category. Table 5.7 displays the overall Council B's vulnerabilities. Furthermore, Appendix B7 provides full details of the identified risk issues for Council B's email server.

Table 5.7 *The overall of Council B's email server – vulnerabilities*

Server name	**H**	**M**	**L**	**P**	**Overall vulnerability level**	**Comment**
Email server	2	1	7	2	High (10/10)	Refer to Appendix B7

5.3.4 Testing stage 4: Spoofing testing and vendor security benchmark email server auditing

This spoofing testing and vendor security benchmark email server auditing stage consists of two testing steps which are the email system spoofing testing and specific vendor security benchmark auditing of MS Exchange 2007 on the email server.

5.3.4.1 Email system spoofing testing results

Several spoofing testings were carried out over the email server and both the network interfaces of each the email gateway spam blocker appliances (GW1 and GW2). The spoofing testings were all conducted using the CIS template. Moreover, a number of risk issues were identified from the spoofing testing.

In addition, the egression testing over the council's email system was successfully tested. This egression testing revealed that the council's email system correctly disallowed sending an email from an internal address to either an internal or external address via a third-party POP3 server. Table 5.8 presents the egression testing result and recommendation.

Table 5.8 *The egression testing result and recommendation*

Testing technique	Purpose	Result	Recommendation
Sending an email from one internal address to either an internal or external addresses using an external, a third-party POP server.	To test egression	Unsuccessful	None

5.3.4.2 Specific email security vendor auditing results

The overall modified auditing checklist tables were adapted and from the specific security recommendations – The CIS Benchmark for MS Exchange 2007 for MS Windows Server 2003 Version 1.0 to suit Council B's email system same as technique utilised in Council A. The Exchange Edge Transport and Unified Messaging server roles and all defaults with "N/A" status are not included in the overall modified auditing checklist tables. This is due to the fact that the existing MS Exchange 2007 architecture for Council B is not configured for the Edge Transport server role.

The overall summary of the email MS exchange 2007 security benchmark testing checklist for Council B can be categorised into three server roles which are the Mailbox server, the Hub Transport server and the CAS roles. In terms of the Council B's Mailbox server role, there were five mailboxes as follows:

1) First storage group > Private mailbox store 1;
2) Pub folders storage group > Public folder database;
3) Second storage group > Private mailbox store 2;
4) Temp storage group > Temp mailbox database; and
5) Third storage group > Private mailbox store 3.

In addition, Tables 5.28, 5.29 and 5.30 in Section 5.5.1.1.4 provide details of these auditing results relating to risks and mitigations.

5.3.4.3 Testing stage 4: Identified risk issues

The identified risk issues for the email spoofing, the Mailbox server, the Hub Transport server and the CAS roles of Council B's email server are presented as follows.

- ***Risk 1: The email server allowed relaying***

The email server allows emails to be sent from both internal and external source addresses to the council's internal email address destination. This email relaying can be a source of potential risk from spoofing attacks arising internally.

- ***Risk 2: The spam blocker appliance 1 (email GW1)***

Emails from both internal and external source addresses to the council's internal or external email address destinations are allowed to be sent from the outbound2 interface of the email GW1. This email relaying is a cause of potential risks to the council's email system as it will then be possible for an intruder to Telnet to the outbound2 interface and directly send unauthorised emails.

- ***Risk 3: The spam blocker appliance 2 (email GW2)***

Both internal and external relaying is allowed from the outbound interface of the email GW2. This mail relaying again may be a cause of potential risk to the council's email system.

- ***Risk 4: The Mailbox server role***

There were a number of mis-configurations on the Mailbox server role of the email (MS Exchange 2007) server. An example of this type of configuration error was the unlimited setting of the email send size. This unlimited setting could lead to a possible increase in unnecessary network traffic and may affect the speed of the council's network traffic, by inadvertently causing a filling up of the storage capacity of the email server as well as the backup system. See Table 5.28 for more details.

- ***Risk 5: The Hub Transport server role***

The council's Hub Transport server role has three groups which are the default CoB Gold, CoB Flourine and Client CoB Gold. In terms of following industry best practice recommendations by CIS (2007), the Hub Transport server role of the council's email server should be reconfigured in order to increase its security. As an example, the IP range could be restricted for receive connectors. See Table 5.29 for more details.

- ***Risk 6: The CAS role***

The CAS role with POP3 and IMAP related features are not included in the overall modified checklist auditing Table 5.30 as the email server is configured to support only SMTP and both POP3 and IMAP protocols are not supported.

There were some mis-configurations on the CAS role. As an example, the MS ActiveSync password options on both the default and executive Nokia policy were disabled. Consequently, passwords are not required, thereby exposing the council's email system to possible intrusion. See Table 5.30 for more details.

5.3.5 Testing stage 5: The email system security policy review

This email system security policy stage consists of the review of the email system security policy. There was no existing technical email system policy apart from a general information security which covered aspects of email usage (see Appendix B30).

5.3.5.1 Testing stage 5: Identified risk issues

The lack of any technical email system security policy can contribute to potential risks such as interruption and misuse of the email services as previously discussed in Section 4.3.5.1, to Council B's email as well as the related systems.

- ***Risk 1: Interruption of the email service***

Similarly to Council A, the lack of an email security guideline may be a cause of potential downtime to the email server as well as its services of Council B.

- ***Risk 2: Misuse of the email service***

As discussed in Chapter 4, the lack of an email security guideline at Council B can contribute to a cause of potential risks in terms of allowing unauthorised access as well as use of the email as a source to initiate email attacks to the council's staff.

5.4 Council B's online web system results

Council B's online web system (the static web system, the CMS web system and the payment system) was audited and tested for the architecture, the intrusion detection, the device configurations, the vulnerabilities of all the online web system servers, the vendor security benchmark auditing and the security policy review. The following sections describe all the results of these testings in detail.

5.4.1 Testing stage 1: Network surveying

This network surveying stage involved making an audit of the online web system architecture together with the networking devices such as the router, the firewalls and the switch. The following network specifications and policy documents were collected for the council's system:

- The overall network diagram for the Internet link and the DMZ infrastructure connectivity;
- The firewall device specification and ACL codes related to the council's online web system;
- The IDS/IPS, the Internet border, the DMZ switch specification and codes related to council's online web system; and
- The specifications summary of the online web system servers.

The following sections describe the overall summary specifications of the online web system devices (the static web system, the CMS web system and the payment system) at Council B as well as the associated identified risks.

5.4.1.1 The static web system devices

The static web system consists of two web servers (the CoB-DMZ-Web and the CoB-Web) as previously mentioned.

5.4.1.1.1 The CoB-DMZ-Web server

The CoB-DMZ-Web server is located in the DMZ so as to minimise any potential risks arising from attackers to the council's static web system. This web server provides the council's specific information via static web pages including forms, to its residents as well as others. The summary specifications of the CoB-DMZ-Web server are presented in Table 5.9.

Table 5.9 *A summary of the CoB-DMZ-Web server specifications*

Attributes	**Details**
Device name	CoB-DMZ-Web
Domain name	Cob.wa.gov.au
Web server software	MS IIS web server 6.0
Other application software	Trend Micro server protect
OS	MS Windows Server 2003 R2 with service pack 2
Hardware	Simple Standard Virtual Server (VMware) Small Computer System Interface (SCSI) C: 30 GB, E: 50 GB, F: 9 GB; memory physical 2 GB and virtual 3.85 GB
IP address	A.B.C.121/27

5.4.1.1.2 The CoB-Web server

The CoB-Web is an in-house server, custom built to suite the council's web system requirements. It is located in the council's internal network. It allows the council's IT operational staff (web administrator) to manage and update web pages information such as PDF and MP3 files, before pushing or uploading the validated web pages from the CoB-Web server to the CoB-DMZ-Web server. See Table 5.10 for more details.

Table 5.10 *A summary of the CoB-Web server specifications*

Attributes	**Details**
Device name	CoB-Web
Domain name (internal)	CoB-Web.city.internal
Web server software	MS IIS web server 6.0
Other application software	Trend OfficeScan
OS	MS Windows Server 2003 R2 with service pack 2
Hardware	VMware SCSI C: 20 GB, E: 60 GB; memory physical 2 GB and virtual 3.85 GB
IP address	172.20.130.184/16

5.4.1.2 The CMS web system devices

As previously discussed in Section 5.2.4.2.2, the council's CMS web system has two servers which are the CMS frontend web server (the CoB-DMZ-Web) and the CMS management server (the CoB-Database). The summary specifications of the CoB-Database server are described as follows. However, the CoB-DMZ-Web server's specifications are not included as it has been previously described in Section 5.4.1.1.

5.4.1.2.1 The CMS frontend web server

The specification details of the CoB-DMZ-Web server have been previously discussed in Section 5.4.1.1.

5.4.1.2.2 The CMS management server

The CoB-Database server works as the CMS management server as well as the backend database. It interacts with the CoB-DMZ-Web as part of a Web Content Management System (WCMS) as previously described in Section 5.2.4.2.2. Table 5.11 summarises the CMS management server (the CoB-Database) specifications.

Table 5.11 *A summary of the CMS management server specifications*

Attributes	**Details**
Device name	CoB-Database (CoB-Database.city.internal)
Web server software	MS IIS web server 6.0
Other application software	Trend OfficeScan
OS	MS Windows Server 2003 with service pack 2
Hardware	VMware SCSI C: 30 GB, E: 50 GB, F: 12 GB; memory physical 4 GB and virtual 7.27 GB
IP address	172.20.130.148/16

5.4.1.3 The online payment system devices

The overall brief summary specifications of the council's online payment servers (frontend web, application and backend database servers) are described as follows.

5.4.1.3.1 The frontend web server

The current frontend web server is located in the DMZ to diminish any potential risks which may take place from attackers to the council's online payment system. It performs the first part of the application logic which provides the front line interface to the client web browser. The council's residents can access the frontend web server through the council's website (http://www.cob.wa.gov.au/Live/PayOnline.aspx), using their valid reference number for rates or infringement payments, whereas a valid payment number is required for dog registration renewals. The details of the frontend web server (the CoB-DMZ-Web server) specifications have been described earlier in Table 5.9.

5.4.1.3.2 The application server

Typically, in the online web payment system environment, the application server functions as a middle tier which interacts with the frontend DMZ web server and the backend database server. It synchronises the transactions of the application, processes necessary commands, and performs all calculations and queries of the data to and from the SQL backend database server. As previously mentioned, the CoB-DMZ-Web server performs both the frontend and application functions.

5.4.1.3.3 The backend database server

The CoB-Database has the custom built database application running in conjunction with MS SQL Server 2005. The CoB-Database server works as the backend database which holds all the necessary information such as payment numbers, rates and infringement notice reference numbers, usernames, passwords and street addresses. Nevertheless, critical user information such as credit card numbers and expiry dates are not stored in the database tables.

In addition, users' data are stored in secured (encrypted) format. However, no further information about the encrypted details were provided by the council (personal communications with Council B, 2010). Furthermore, the CoB-Database server performs both functions which include the CMS and online payment backend database server functions. The backend database server specifications has been summarised earlier in the CMS section in Table 5.11.

5.4.1.4 Testing stage 1: Identified risk issues

The identified risk issues of Testing stage 1 for Council B's online payment system are described in the following sections.

- ***Risk 1: The online payment system***

As mentioned earlier that the council's online payment system consists of two servers (the CoB-DMZ-Web and the CoB-Database). The CoB-DMZ-Web provides both frontend and application features. This utilisation can be considered as a source of a potential risk due to the single point of failure in the case of the CoB-DMZ-Web server being compromised.

5.4.2 Testing stage 2: The infrastructure of the online web system – Internet border router, IDS/IPS, firewalls and switch reviews

This second testing stage is made up of the review of the software configuration codes for the router, switch, firewalls, IDS and IPS devices.

5.4.2.1 Internet border router configuration codes data collection and reviews

Details of the Internet border router specifications were previously discussed in Section 5.3.2.1. Moreover, the examination of the configuration codes from the Internet border router revealed the risk issue to be a vulnerability to an IP spoofing attack.

5.4.2.2 IDS/IPS configuration codes data collection and reviews

This section covers the data collection, reviews and recommendations for the IDS/IPS features on the Internet border router and the two CheckPoint firewall UTM-1 272 devices. Several risk issues were uncovered during the review process for these devices in relation to IDS and IPS in addition to the missing IPS software feature and the disabled IDS software feature.

5.4.2.3 Firewall configuration codes data collection and reviews

This firewall review section is separated into three groups which cover the static web, CMS web and online payment systems. More details of the council's Internet firewalls specifications are located in Section 5.3.2.3. Appendix B8 shows the summary of the firewall configuration codes relevant to the online static web system's servers (the CoB-DMZ-Web and the CoB-Web). Examination revealed that only the web administrator can access the CoB-DMZ-Web server via TCP port 3389 for remote administration purposes from the designated computer (172.20.20.20/16).

In addition, TCP port 445 MS file sharing protocol allows one-way access from the CoB-Web server to the CoB-DMZ-Web server. This allows the web administrator to upload web contents from the CoB-Web server to the CoB-DMZ-Web server. On the other hand, Appendix B9 shows the summary of the firewall configuration codes with respect to both the CMS web system servers. Furthermore, the issues that were revealed were associated with the firewall settings of the online payment system. Appendix B10 displays the full firewall coding details with respect to the council's online payment system.

5.4.2.4 Switch configuration codes data collection and reviews

As mentioned earlier, Council B has only one switch which provides network communication and connectivity between the Internet border router, the firewalls, the DMZ server and the council's internal network. For more details in terms of the architecture, the configuration codes, the hardware specifications and identified risk issues see Section 5.3.2.4. However, details on ports and VLANs, including connectivity for the council's online web system are provided in Figure 5.6.

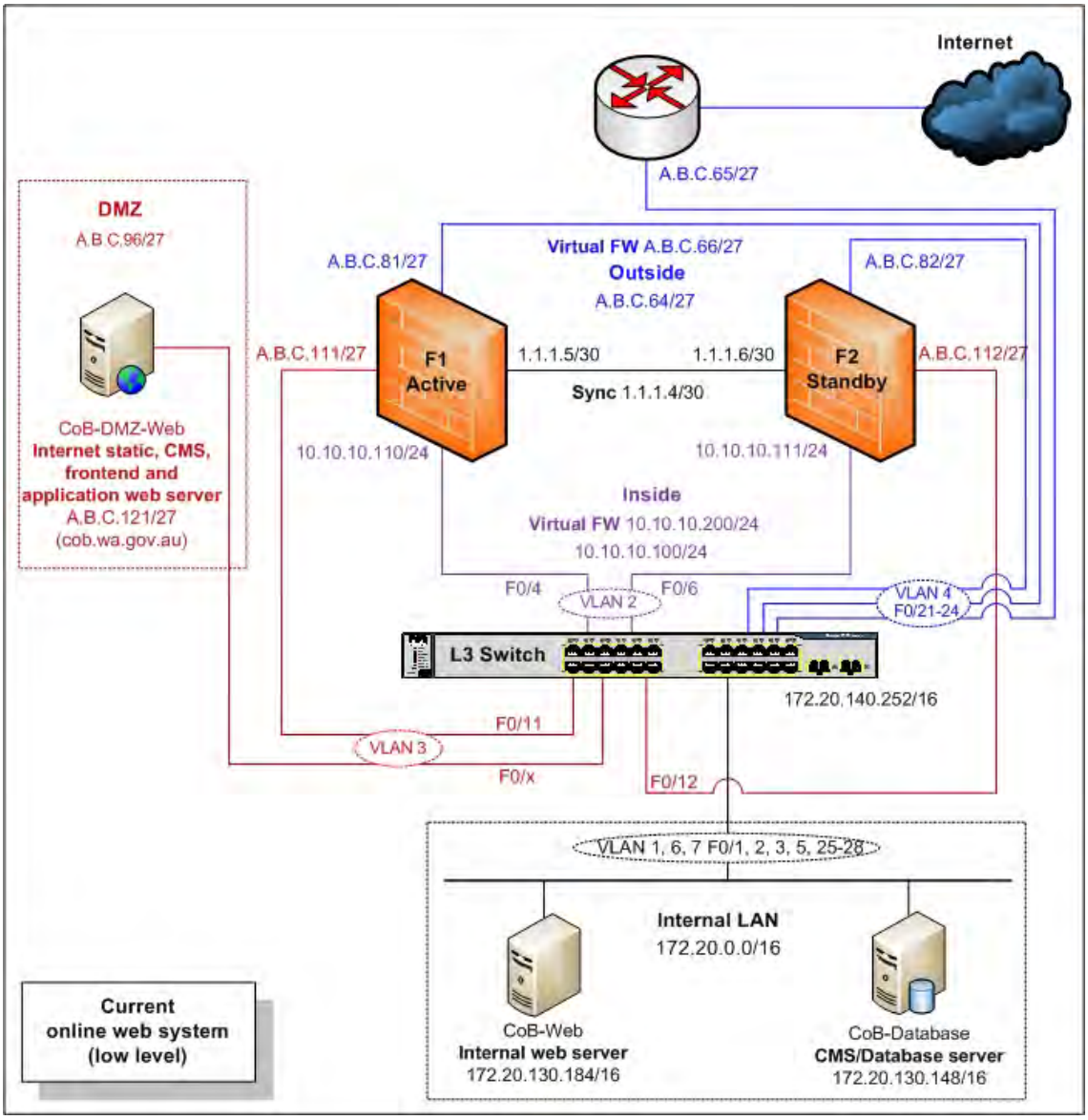

Figure 5.6. The low level online web system network diagram (including the static, the CMS and the online payment web systems) currently in use by Council B

5.4.2.5 Testing stage 2: Identified risk issues

The following section details the identified risk issues for the infrastructure of the online web system (Internet border router, the IDS/IPS, the firewall and the switches) of Council B.

- ***Risk 1: Poor ACL coding on the Internet border router***

The current ACL rule of the Internet border router allows any IP traffics get in and out the council's network. According to best practice recommendations to standard router configurations, this setting is considered to be opened to cyber attacks such as IP spoofing and unauthorised network probing.

- ***Risk 2: No inspection on web (HTTP) network traffic***

The incoming and outgoing web (HTTP) network traffic is not inspected (by IPS) which is a source of possible risks to attack from malware such as worms and Trojans.

- ***Risk 3: The static web system: inadequate firewall ACL coding – HTTP outwards***

The current ACL setting for the firewall allows the CoB-DMZ-Web server access to anywhere through the HTTP port 80 (see Appendix B8: Policy number 4). This ACL setting is a source of potential risk in terms of the CoB-DMZ-Web server being used as a launch pad for staging further attacks.

- ***Risk 4: The static web system: Inadequate firewall ACL coding – HTTP inter-device***

The current ACL setting for the firewall allows the CoB-DMZ-Web server access to the CoB-Web server which is located in the council's internal network via HTTP port 80 (see Appendix B8: Policy number 5). This can be a cause of potential risks as HTTP traffic from the DMZ network can directly access the internal network without any packet inspection.

- ***Risk 5: The static web system: Inadequate firewall ACL coding – HTTPS outwards***

The current ACL setting for the firewall allows both HTTP and HTTPS traffic from the internal CoB-Web server to the CoB-DMZ-Web server in the DMZ (see Appendix B8: Policy numbers 6 and 7). As per discussion with the web administrator, these ACL rules were not required as HTTP and HTTPS traffic should not be permitted in this direction.

- ***Risk 6:The CMS web system: Inadequate firewall ACL coding – HTTP inwards***

The current ACL setting for the firewall allows the CoB-DMZ-Web server which located in DMZ area access to the internal CoB-Database server via HTTP port 80 (see Appendix B9: Policy number 5). This is a source of potential risk as HTTP traffic from the DMZ network is able to access the internal network without any traffic inspection.

- ***Risk 7: The CMS web system: Inadequate firewall ACL coding – HTTPS inwards***

The current ACL setting for the firewall allows the CoB-DMZ-Web server access to the internal CoB-Database server via HTTPS (see Appendix B9: Policy number 6). This is a source of potential risk to the internal database server as the HTTPS traffic from the DMZ network can directly flow to the council's internal network without any completed or deep packet inspection.

For example, there exists a potential risk from malware being spread through the HTTPS traffic if deep packet inspection is not performed (Cisco, 2002; Websense, 2010).

- ***Risk 8: The online payment system: Inadequate firewall ACL coding – HTTPS outwards***

The current ACL setting for the firewall allows HTTPS traffic from the CoB-DMZ-Web server access to anywhere (any) (see Appendix B10: Policy number 4). This ACL setting is a source of potential risks in terms of the web server in the DMZ area being used as a launch pad for staging further attacks.

- ***Risk 9: The online payment system: Inadequate firewall ACL coding – Sqlnet2***

The current ACL setting for the firewall permits communications between the CoB-DMZ-Web server and the CoB-Database server in both directions (incoming and outgoing) via Oracle Sqlnet2 protocol (TCP ports: 1521, 1525 and 1526) (see Appendix B10: Policy numbers 6 and 7). This firewall rule is considered unnecessary due to the fact that the Oracle database server was decommissioned and is no longer in use having been replaced with the MS SQL server.

Furthermore, these ACL rules can be a cause of potential risk to the CoB-Database server via Sqlnet2 protocol ports such as multi-threaded operating system server issues and disclosure of important information on the CoB-Database server.

- ***Risk 10: Overall inadequate switch code security configurations***

This point has been previously discussed in Section 5.3.2.5.

5.4.3 Testing stage 3: Services and system identification, port scanning, vulnerability testing and results

In this third testing stage similar techniques which were used in Section 5.5.3 of the email system were used. Both NMAP and GFI LANguard network scanning tools were used for all three testing steps (services and system identification, port scanning and vulnerability testing) for Council B's online web system (including the static, the CMS and the online payment web systems) network scanning.

5.4.3.1 Services and system identification results

The results of the services and system identifications of the three servers which are the CoB-DMZ-Web (A.B.C.121), the CoB-Web (172.20.130.184) and the CoB-Database (172.20.130.148) are summarised in Appendices B13, B14 and B15.

5.4.3.2 Port scanning results

In this port scanning testing section, the techniques used were similar to Section 5.3.3.2 of the email system. Both NMAP and GFI LANguard were utilised to scan Council B's online web system servers. Moreover, there were unnecessary TCP and UDP ports discovered in all three servers (the CoB-DMZ-Web, the CoB-Web and the CoB-Database). Full details are provided in Appendices B16, B17 and B18.

5.4.3.3 Vulnerability testing results

The techniques that were used in this vulnerability testing phase were similar to Section 5.3.3.3. There are four vulnerability groups which include the high, medium, low and potential security risks. There were vulnerabilities uncovered on all three servers of the council's online systems (the CoB-DMZ-Web, the CoB-Web and the CoB-Database).

5.4.3.4 Testing stage 3: Identified risk issues

The identified risk issues of Testing stage 3 for Council B's online web system are described as follows.

- ***Risk 1: System information policy results for all the three servers***

The Windows configuration settings of all the three servers of the council's online web systems were lacking in some respects in term of services, password and security auditing policies. This can lead to vulnerabilities to the council's online web system.

- ***Risk 2: System patching status results for all the three servers***

Testing for this section was done using GFI LANguard and NMAP scanning tools. There were no missing service packs and patches on the CoB-DMZ-Web server. However, there were missing service packs and patches on both the CoB-Web and the CoB-Database servers. These can be a source of potential risks to the council, particularly the CoB-Database server which holds the council's client sensitive information.

- ***Risk 3: Unnecessary opened ports on all the three servers***

There were 20 TCP and nine UDP opened ports which include unnecessary ports on the CoB-DMZ-Web server. These unnecessary opened ports can lead to a cause of potential risks in terms of unauthorised access to the DMZ web server. Table 5.12 presents the overall opened TCP and UDP ports for all the three servers.

Additionally, Appendices B16, B17 and B18 provide the full details of the overall opened TCP and UDP service ports as well as the possible mitigation recommendations of the CoB-DMZ-Web, the CoB-Web and the CoB-Database servers respectively.

Table 5.12 *Overall opened TCP and UDP service ports of all the three servers*

Server names	**Opened TCP ports**	**Opened UDP ports**	**Comments**
CoB-DMZ-Web	20	9	Refer to Appendix B16
CoB-Web	9	9	Refer to Appendix B17
CoB-Database	10	9	Refer to Appendix B18

- ***Risk 4: Vulnerabilities found on all the three servers***

There were vulnerabilities discovered on the CoB-DMZ-Web server such as the guest user account having access to application, security and system log files. Table 5.13 lists the overall vulnerability testing results of the three servers.

The overall vulnerability testing results and the possible mitigation recommendations of the three servers are summarised in Appendices B19, B20 and B21 respectively.

Table 5.13 *Overall vulnerability of the three servers of Council B's online web systems*

Server names	**H**	**M**	**L**	**P**	**Overall vulnerability levels**	**Comments**
CoB-DMZ-Web	1	3	7	2	High (8/10)	Refer to Appendix B19
CoB-Web	1	0	6	1	High (10/10)	Refer to Appendix B20
CoB-Database	1	0	4	2	High (9/10)	Refer to Appendix B21

5.4.4 Testing stage 4: Vendor security: Database security benchmark auditing

This vendor security benchmark auditing stage consists of one testing step which is the database security benchmark auditing on the council's backend database server (the CoB-Database).

5.4.4.1 Database security benchmark results

Similarly to Council A, MS SQL Server 2005 is an online web database application which is deployed in the council's backend database server (the CoB-Database). The Security Configuration Benchmark for MS SQL Server 2005 version 1.2.0 January 12th, 2010 from CIS was used in this audit as a prime benchmark auditing tool.

The CIS benchmark auditing tool is categorised into nine groups as previously described in Section 4.4.4.1. The auditing was carried out on group one to six and group eight to nine. Group seven (replication) was not audited as there was no replication implemented in the council's database system.

5.4.4.2 Testing stage 4: Identified risk issues

The identified risk issues for the configuration of the MS SQL 2005 database on the council's backend server are presented as follow.

- ***Risk 1: Inadequate configuration for the database application of the backend database server***

There were some security issues uncovered from the auditing. These security issues may lead to possible interruptions to the CoB-Database server. Table 5.14 presents the overall security issues uncovered from the CoB-Database server based on the eight category groups.

See Appendices B22, B23, B24, B25, B26, B27, B28 and B29 for full details of all the results and findings including the possible mitigation recommendations based on the eight category groups respectively.

Table 5.14 *The overall risks of the eight audited categories of the CoB-Database server*

Category no.	**Risks (H)**	**Risks (M)**	**Risks (L)**	**Risks (P)**	**Comments**
1) OS and network specification configuration	1	3	10	2	Refers to Appendix B22
2) SQL server installation and patches	0	3	1	0	Refers to Appendix B23
3) SQL server settings	0	2	4	10	Refers to Appendix B24
4) Access controls	0	1	0	0	Refers to Appendix B25
5) Auditing and logging	0	0	0	43	Refers to Appendix B26
6) Backup and disaster recovery procedures	0	1	1	1	Refers to Appendix B27
7) Replication	N/A	N/A	N/A	N/A	None
8) Application development best practices	1	1	0	0	Refers to Appendix B28
9) Surface area configuration tool	0	1	2	1	Refers to Appendix B29

5.4.5 Testing stage 5: The online web system security policy review

There was a general information security policy for online services usage. This general information security policy covered acceptable and prohibited usages of email, internet, data confidentiality, logon accounts, passwords and electronic fax. However, there was no existing related technical policy for the online web system in place at the council such as a network infrastructure related policy and a data security policy (see Appendix B30).

5.4.5.1 Testing stage 5: Identified risk issues

This lack of related online web system security policy can create high risks to the council's online web system. Similar to Council A, the cause of these risks could be characterised as follows:

- Poor communication of risk;
- Possible misdirection or resources; and
- Poor understanding of the risks that are in the system as a result of poor management/strategic oversight.

- ***Risk 1: Poor communication of risk***

There was little or no discussion of ICT risk management in the weekly IT operation staff meetings (personal communications with Council B, 2010). The reasons for the non existence of risk management discussions was due to the lack of time as the council's IT operational team often have ample day to day operation tasks to manage, and the fact that the council has no ICT risk management plan in place.

- ***Risk 2: Possible misdirection of resources***

As a result of budget constraints in the council's IT department, there was no budget allocation for the development of an ICT security related policy, including a specific technical security policy. The council's IT department has fully allocated its budget, mainly to resources and day-to-day operations (personal communications with Council B, 2010). However, at the end of year 2010, general ICT and specific technical security policies were discussed due to the recommendations of the IT email and online web systems reports.

In addition, just before the Christmas 2010, the CoB-DMZ-Web server was hacked into as a direct consequence of missing patches in the CoB-DMZ-Web server (personal communications with Council B, 2010). This security break has raised ICT security awareness among the council's IT staff.

- ***Risk 3: Poor understanding of the risks that are in the system as a result of poor management/strategic oversight***

This aspect was due to the fact that some of the council's IT operational staff lack a reasonable knowledge of the details of IT security particularly in their area of responsibility. For example, the web system analyst has a good knowledge of web programming but little knowledge in web security related issues.

In addition, this research acted upon the concerns of management and staff with regards to the identified security risks as expounded earlier. The resulting report and recommendations provided as a result of this research serve to equip management with a basis for support of these concerns and therefore herald a "call to action" for the respective councils. The security recommendations serve as a justification for an

internal review of the respective councils and act as a case for introduction of some form of policy tightening especially in regards to the online systems. In addition, the fact that some of the security risks arose as a result of a lack of training and personal professional development of staff should serve as strong case for future budgetary allocations in the area of ongoing staff training and up skilling.

5.5 Analysis and discussion

The analysis and discussion on both Council B's email as well as online web systems (the static web system, the CMS web system and the online payment system) are detailed in the following sections.

5.5.1 Analysis

The analysis can be separated into two sections for each of the analysis of Council B's email and online web systems.

5.5.1.1 Council B's email system analysis – possible mitigations

The following sections (Testing stages 1, 2, 3, 4 and 5) describe the possible mitigation recommendations for the identified issues of Council B's email system. Each of the mitigations described relate to the identified risk issue number.

5.5.1.1.1 Testing stage 1: Possible mitigation

- ***Risk 1***

In order to mitigate this potential risk of a single point of failure, it is recommended that Council B deploys an extra dedicated server to only perform a CAS role. This additional server may be in the form of a VM or a physical server. In addition, the connection between the CAS and the Mailbox Server should be used with a high-bandwidth and low-latency connection as per Microsoft TechNet (2009, p. 2) which states that "the minimum recommended bandwidth is 100 Mbps, but a 1-Gpbs connection should be considered for enterprise data centres". Therefore, a gigabit connection is strongly

recommended. The summary specifications of a new dedicated CAS are provided in Table 5.15. Figure 5.7 provides details of its architecture including the new CAS.

Additionally, the existing email system does not currently have the Unified Messaging server role installed. However, in the medium to long term future Council B should consider combining or replacing it with the council's current voice mail product provided its features have been updated and the cost is justified.

Table 5.15 *A summary recommendations of the new CAS specifications*

Attributes	**Details**
Email application software	MS Exchange 2007 with service pack 1
OS	MS Windows Server 2008 Enterprise Edition with service pack 1
Hardware	VMware or equivalent 8 GB RAM, hard disks C: 20 GB, e: 100 GB
MS Exchange 2007 role	CAS
MS Exchange support	MS OWA, MS Outlook Anywhere, MS ActiveSync
TCP/IP protocols	HTTPS, RPC, LDAP
IP network	Different subnet with other email servers (isolate)
Network connection	Gigabit link between Client Access and Mailbox servers
ACL	Permits only allowed or required protocols
Other software	Virus protection software for server

- ***Risk 2***

In order to further minimise and control any other potential risks that may occur, due to the email server being on the same subnet, it is recommended that the dedicated CAS may be configured to a different sub-network. In addition, ACL filtering may be implemented to only allow the required network protocols for communication between the new CAS and the network. See Figure 5.7 for more details.

- ***Risk 3***

The use of either the certificate or token authentication methods may provide better mechanism security when compared with the basic authentication method (Luckett et al., 2008). In case of deploying certificate authentication method, it is recommended that Council B should ensure that its mobile clients still authenticate with the MS

ActiveSync protocol. This due to the fact that the “not all mobile devices can use certificate-based authentication” (Luckett et. al., 2008, p. 531).

Alternatively, implementing token authentication method as an additional layer of authentication typically requires a third-party authentication solution which comes with additional costs, time and manpower. Table 5.16 summarises the options and recommendations for enhancing the client access security methods for Council B.

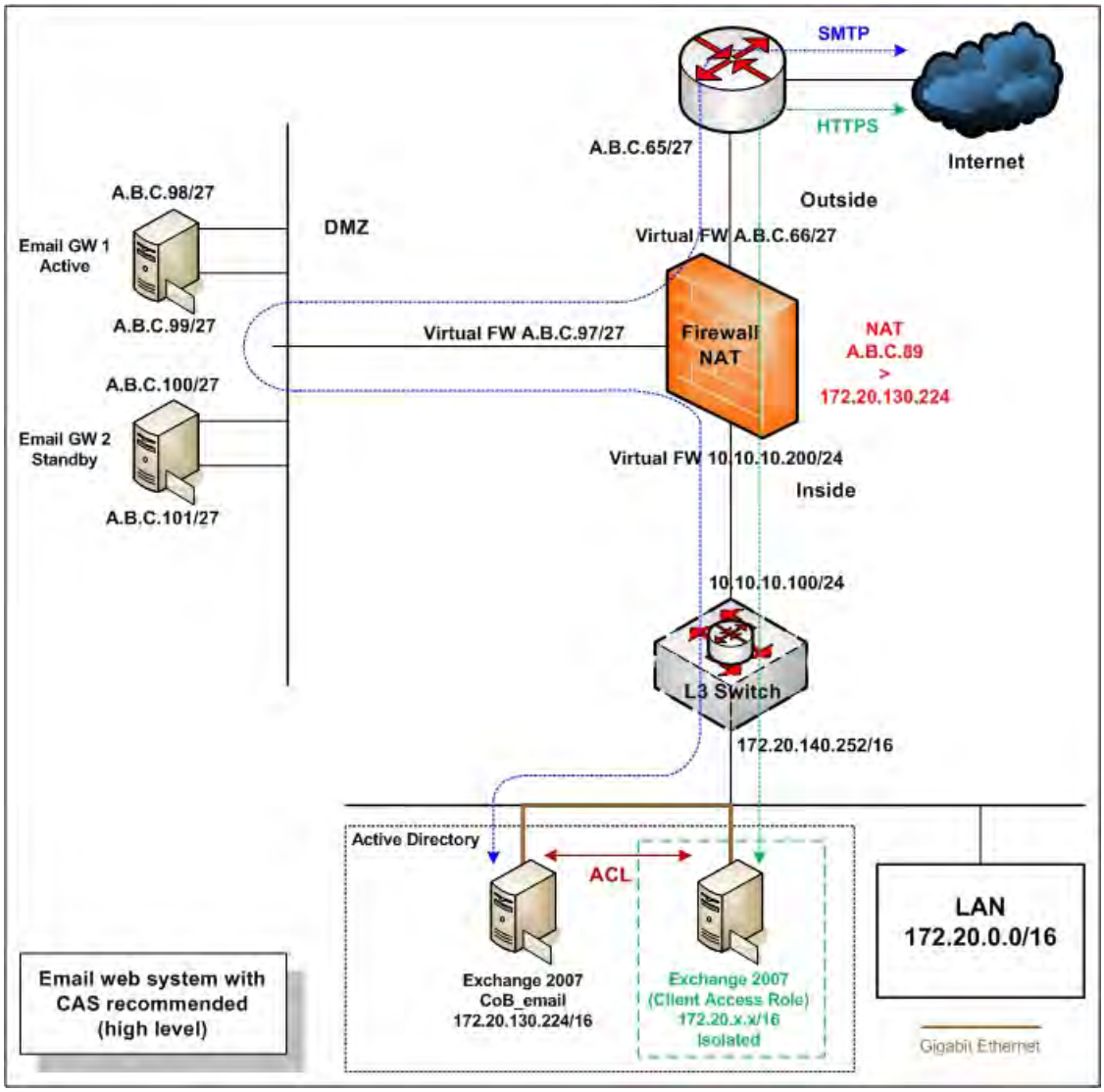

Figure 5.7. A recommended MS Exchange Server 2007 architecture with an extra MS Exchange 2007 (CAS role)

- ***Risk 4***

It is known that NT LAN Manager (NTLM) provides better security than basic authentication (Luckett et al., 2008). Therefore, NTLM authentication may be used in conjunction with the SSL connection.

Furthermore, the current firewall (CheckPoint Firewall-1) needs to be configured in order to handle NTLM authentication (Microsoft TechNet, 2007b, c). Table 5.16 identifies the MS Outlook Anywhere current authentication methods of Council B and the enhancement recommendations.

Table 5.16 *Overall current and recommendations client access security methods over SSL for the email system of Council B*

Client-to-server connections	**Authentication options**	**Council B current configuration**	**Recommended authentication for Council B**
MS OWA	Basic/form-based	Form-based	Form-based
MS ActiveSync	Basic/certificate/token	Basic	Certificate or token
MS Outlook Anywhere	Basic/NTLM	Basic	NTLM

5.5.1.1.2 Testing stage 2: Possible mitigation

- ***Risk 1***

The council may wish to tighten its ACL filtering; this may be achieved by creating each individual ACL for each individual service usage. Recommended examples for the email service are shown in Table 5.17.

Table 5.17 *Possible examples of the Internet border ACL for the email system*

Rules	**Protocol types**	**From (source)**	**To (destination)**	**Ports (service)**	**Recommendations**
Permit	TCP	Any	A.B.C.98-101	SMTP	Yes
Permit	TCP	Any	A.B.C.89	HTTPS	Yes

- ***Risk 2***

The Cisco IOS IPS software feature on the Internet border router (Cisco 2811) may be enabled in order to monitor and prevent potential IP spoofing and scanning attacks. Therefore, the Internet border router will act as a first protection layer for the Internetwork system of the council. More details are provided in Table 5.18.

- ***Risk 3***

The IPS feature can be added to the two current firewalls (UTM-1 272) to increase its security. According to Check Point Software Technologies Ltd. (2010, p. 5), IPS features on CheckPoint firewall UTM-1 270 can perform the following:

- "Network-layer protection blocks attacks such as DoS, port scanning and IP/ Internet Control Message Protocol (ICMP)/TCP-related;
- Application-layer protection blocks attacks such as DNS cache poisoning, FTP bounce and improper commands; and
- Detection methods signature-based, behavioural and protocol anomaly."

This added IPS feature may cause both the incoming and outgoing email (SMTP) traffic to be fully inspected. Consequently, vulnerability to the previously mentioned attacks will be minimised. In addition, the IPS can inspect other network protocols such as HTTP. Table 5.18 provides overall details of the identified issues and the recommendation solutions.

Table 5.18 *A summary of the IPS of the council's internetwork system*

Products	**Current issues**	**Recommendations**	**Descriptions**
IPS on the Internet border router	Disabled	Enable (turn on)	For blocking of any spoofing/scanning attacks.
IPS on the firewall	Non-existent	Add this optional feature	For real-time inspection of all required important network traffic (protocols) for the purposes of blocking and preventing any malicious or unwanted behaviour in real-time.

- ***Risk 4***

Accessing the two spam blocker appliances from the council's internal network via HTTP or Telnet ports should be avoided or prohibited in order to conform to general best practice recommendations. HTTPS and Secure Shell (SSH) protocols were recommended to the council as alternatives for secure encrypted remote access mechanisms to the two spam blocker appliances so that all communications through these ports is encrypted.

The HTTPS (TCP: 443) and SSH (TCP: 22) ports should both be opened on the firewalls for accessibility via the web interface as well as command line interface respectively. Moreover, both HTTPS and SSH services should also be enabled on the spam blocker appliances.

- ***Risk 5***

Access to anywhere via port HTTP from either of the spam blocker appliances (email GW1 and GW2) in the council's DMZ network should be limited or specified in order to match to best practice recommendations for standard firewall configurations.

- ***Risk 6***

The council may consider deploying third-party solutions such as Cisco IronPort S-Series web security appliance or Websense Content Gateway in order to perform full or deep inspection on the contents of HTTPS traffic (Cisco, 2002; Websense, 2010).

In addition, other web protocols such as HTTP can also be deeply inspected. Full scanning of the contents of HTTPS traffic allows the council to identify and stop any potential malware lurking in the HTTPS traffic. This security measure will increase the Internet security of the council.

Figure 5.8 illustrates all devices connectivity including the recommended CAS as well as the third-party solution in a high level network diagram.

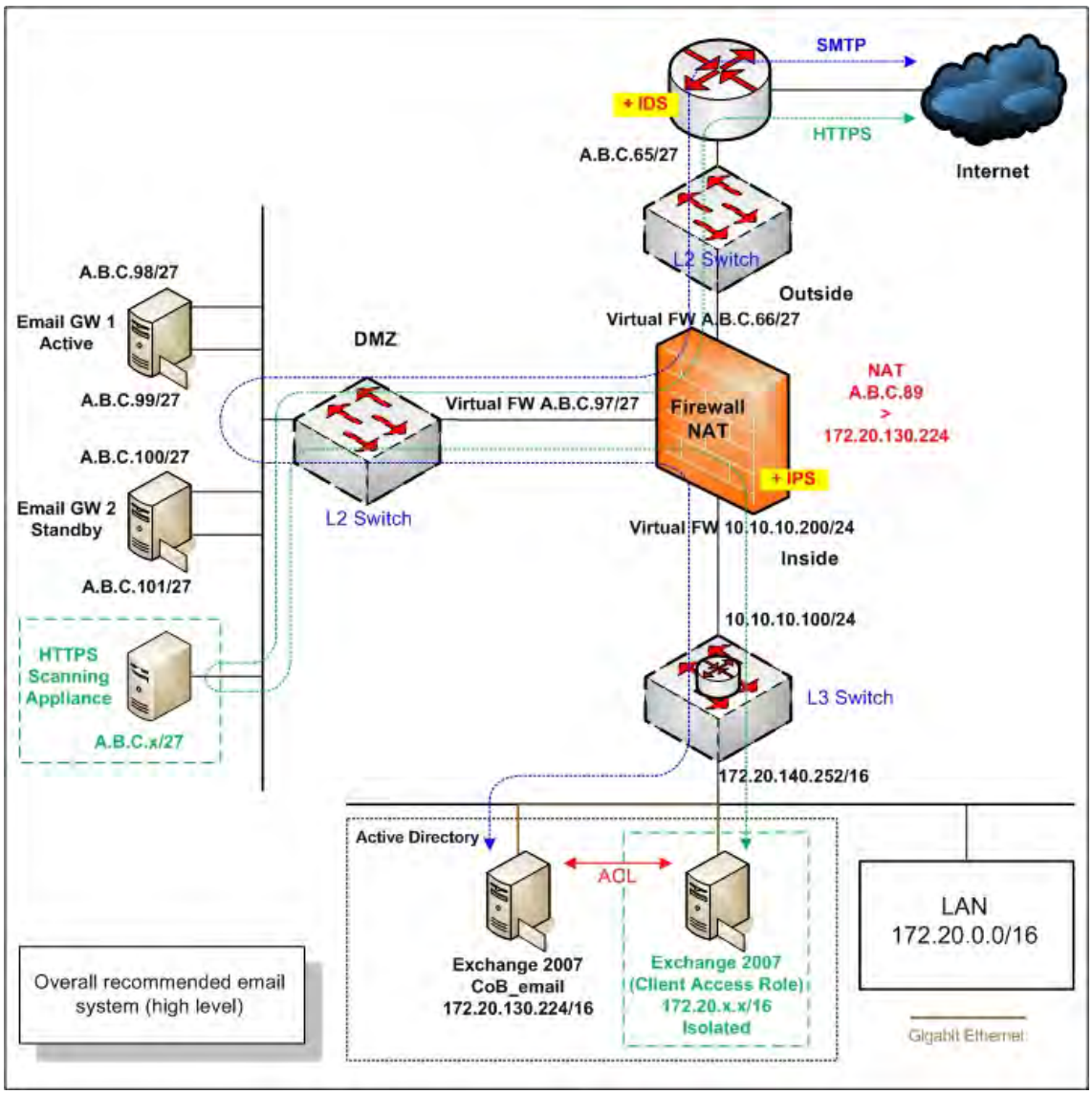

Figure 5.8. An overall recommended MS Exchange Server 2007 architecture with an extra MS Exchange 2007 (CAS role) and a third-party stateful device

- ***Risk 7***

With reference to Table 5.19, it is recommended that all the measures that are currently not implemented or enabled be activated for optimum security in order to protect attacks against the council's Ethernet switch.

Table 5.19 *Switch security identified issues and recommendations*

Security features	**Recommendations**
ACL applied to block unwanted devices	To do
Access to the device via HTTP is disabled	To do
Access to the device via Telnet is disabled	To do
Activate Loop protection on all ports	To do
Apply appropriate log server	Satisfactory
Apply appropriate timestamps debug time	Satisfactory
Apply appropriate timestamps log time	Satisfactory
Apply appropriate time zone	Satisfactory
Appropriate SNMP used	To do
Appropriate VLAN used	Satisfactory
Best practice user name and/or password used	To do
Configure appropriate warning banner message	To do
Disable/shutdown unused switch ports	To do
Disable trunking on ports that do not need it	Satisfactory
Enable feature against ARP poisoning attacks	To do
Enable feature against ARP spoofing attacks	To do
Enable port broadcast storm control	To do
Enable port security limits MAC address to a port	To do
Ports connected to identified devices that do not support spanning-tree should be configured with BPDU filtering	To do
Ports not connected to anything yet should be configured with protection	To do
Set DTP on all ports not being used for trunking	N/A
Set strong password (MD5) for authenticating VTP message	To do
Strong password encryption (MD5) used	To do
TFTP service is disabled	To do

- ***Risk 8***

It is recommended that two additional switches should be deployed as follows:

- The outside area: A new switch to connect the two firewalls and the Internet border router; and
- The DMZ area: A new switch to connect the two firewalls and the DMZ servers.

On the other hand, the current switch can be used to connect between the firewall and the council's internal network. The new switches recommendations are provided in Table 5.20. Figure 5.9 illustrates more details on ports, VLAN including its connectivity.

Table 5.20 *New switches hardware and software recommendations*

Attributes	**Details**
Device location	The council's outside network area
Device type	Cisco Catalyst 3560 switch (3560-12PC)
OS	Cisco IOS version 12.2 or higher
Memory	128 MB
Port	Ethernet 10/100 ports with Power over Ethernet (PoE) and 1 dual-purpose 10/100/1000 and SFP port
Operate at	Layer 2 OSI
Attributes	**Details**
Device location	The council's DMZ network area
Device type	Cisco Catalyst 3560 switch (3560G-24TS)
OS	Cisco IOS version 12.2 or higher
Memory	128 MB
Port	24 Ethernet 10/100/1000 ports and 4 SFP-based gigabit Ethernet ports
Operate at	Layer 2 OSI

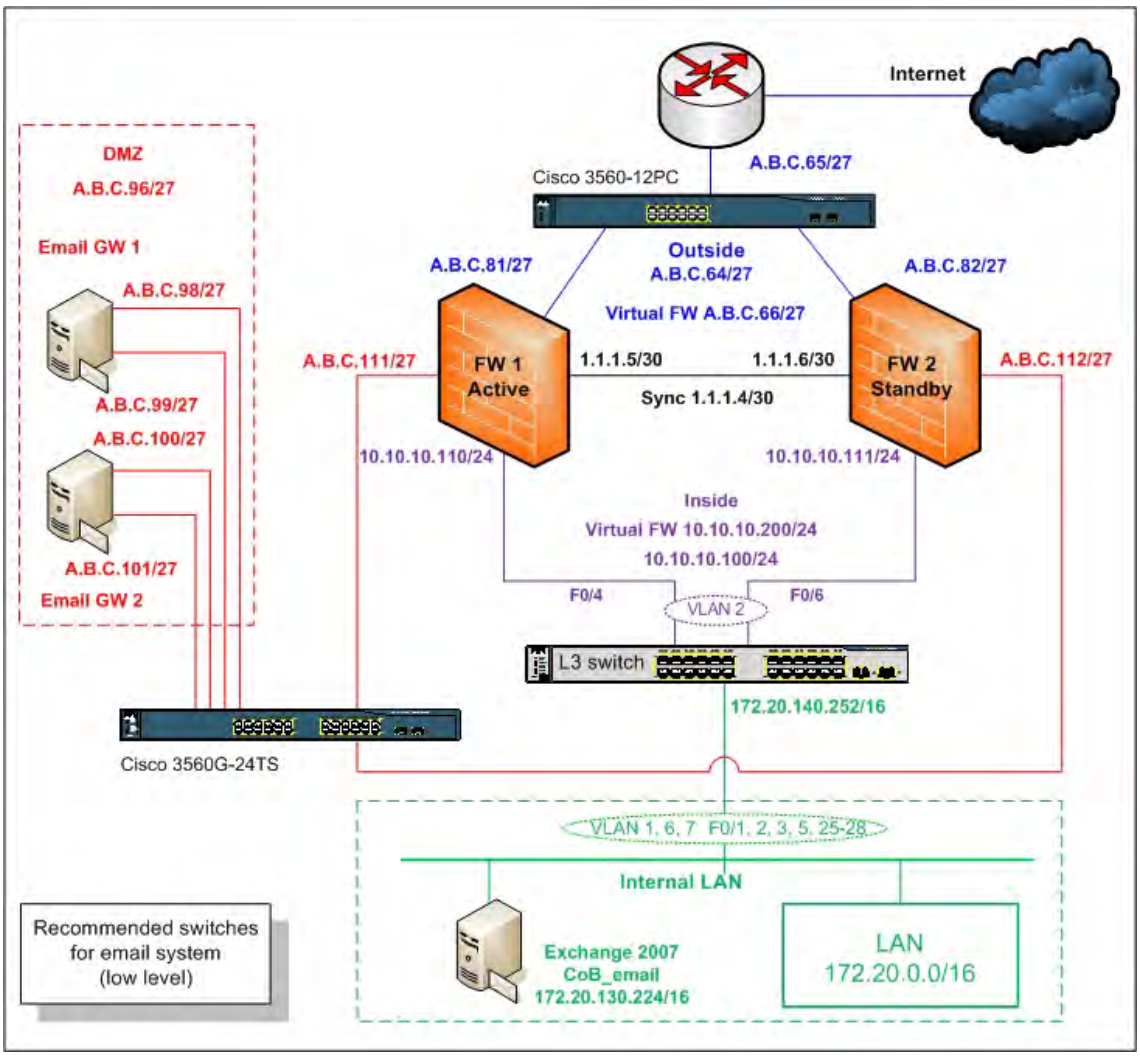

Figure 5.9. A current low level network diagram of the email system for Council B with the new recommended switches

5.5.1.1.3 Testing stage 3: Possible mitigation

- ***Risk 1***

The overall system information policy testing results of the council's email server are summarised in Tables 5.21 whereas full details of the overall system information policy testing results and recommendations are provided in Appendix B4.

Table 5.21 *Overall system information policy of Council B's email server*

Server name	**Password policy**	**Security audit policy**	**Comment**
Email server	Unsatisfactory	Unsatisfactory	Refer to Appendix B4

- ***Risk 2***

Appendix B5 provides the specific details of the missing patches and the possible mitigation recommendations of the email server.

- ***Risk 3***

As previously discussed, there were 22 opened TCP and eight UDP ports. These opened ports included unnecessary ports. Table 5.22 presents the total number of recommended open TCP and UDP ports on the email server.

Table 5.22 *The total number of recommended open TCP and UDP service ports on the email server*

Server name	**Recommended open TCP ports**	**Recommended open UDP port**	**Comment**
Email server	7	1	Refer to Appendix B6

- ***Risk 4***

Refer to Appendix B7 for full details of the identified risk issues and the possible mitigation recommendations.

5.5.1.1.4 Testing stage 4: Possible mitigation

- ***Risk 1***

The overall spoofing testing results for the council email server including possible mitigation recommendations are presented in Table 5.23.

Table 5.23 *The spoofing testing results and recommendations for the email server*

Testing techniques	**Purposes**	**Results**	**Recommendations**
Telnet to the email server and sending an email from one internal address to another internal address.	To test internal connectivity of the email server	Successful (allows relaying)	Should not allow mail relaying
Sending an email from one external address to another external address using the target email server.	To test external relaying of the email server	Unsuccessful (does not allow relaying)	None
Sending an email from one internal address to an external address using the target email server.	To test internal relaying of the email server	Unsuccessful (does not allow relaying)	None
Sending an email from one external address to an internal address using the target email server.	To test email relaying of the email server	Successful (allows relaying)	Should not allow mail relaying

- ***Risk 2***

The overall results and mitigation recommendations of both the network interfaces of the spam blocker appliance 1 (email GW1) are provided in Tables 5.24 and 5.25.

Table 5.24 *The spoofing testing results and recommendations of the email GW1 (inbound2.cob.wa.gov.au: A.B.C.98)*

Testing techniques	**Purposes**	**Results**	**Recommendations**
Telnet to the email GW1 and sending an email from one internal address to another internal address.	To test internal connectivity of the email GW1	Successful (allows relaying)	None
Telnet to the email GW1 and sending an email from one external address to another external address using the spam blocker appliance.	To test external relaying of the email GW1	Unsuccessful (does not allow relaying)	Block internal staff from directly accessing the device via Telnet and SMTP port.
Telnet the email GW1 and sending an email from one internal address to an external address using the spam blocker appliance.	To test internal relaying of the email GW1	Unsuccessful (does not allow relaying)	Block internal staff from directly accessing the device via Telnet and SMTP port.
Telnet to the email GW1 and sending an email from one external address to an internal address using the spam blocker appliance.	To test mail relaying of the email GW1	Successful (allows relaying)	None

Table 5.25 *The spoofing testing results and recommendations of the email GW1 (outbound2.cob.wa.gov.au: A.B.C.99)*

Testing techniques	**Purposes**	**Results**	**Recommendations**
Telnet to the email GW1 and sending an email from one internal address to another internal address.	To test internal connectivity of the email GW1	Successful (allows relaying)	Block internal staff from directly accessing the device via Telnet and SMTP port.
Telnet to the email GW1 and sending an email from one external address to another external address using the spam blocker appliance.	To test external relaying of the email GW1	Successful (allows relaying)	Block internal staff from directly accessing the device via Telnet and SMTP port.
Telnet the email GW1 and sending an email from one internal address to an external address using the spam blocker appliance.	To test internal relaying of the email GW1	Successful (allows relaying)	Block internal staff from directly accessing the device via Telnet and SMTP port.
Telnet to the email GW1 and sending an email from one external address to an internal address using the spam blocker appliance.	To test mail relaying of the email GW1	Successful (allows relaying)	Block internal staff from directly accessing the device via Telnet and SMTP port.

- ***Risk 3***

The overall spoofing testing results and mitigation recommendations of the spam blocker appliance 2 (email GW2) are provided in both Tables 5.26 and 5.27.

Table 5.26 *The spoofing testing results and recommendations of the email GW2 (inbound.cob.wa.gov.au: A.B.C.100)*

Testing techniques	**Purposes**	**Results**	**Recommendations**
Telnet to the email GW2 and sending an email from one internal address to another internal address.	To test internal connectivity of the email GW2	Successful (allows relaying)	None
Telnet to the email GW2 and sending an email from one external address to another external address using the spam blocker appliance.	To test external relaying of the email GW2	Unsuccessful (does not allow relaying)	Block the internal staff from directly accessing the device via Telnet and SMTP port.
Telnet the email GW2 and sending an email from one internal address to an external address using the spam blocker appliance.	To test internal relaying of the email GW2	Unsuccessful (does not allow relaying)	Block the internal staff from directly accessing the device via Telnet and SMTP port.
Telnet to the email GW2 and sending an email from one external address to an internal address using the spam blocker server.	To test mail relaying of the email GW2	Successful (allows relaying)	None

Table 5.27 *The spoofing testing results and recommendations of the email GW2 (outbound.cob.wa.gov.au: A.B.C.101)*

Testing techniques	**Purposes**	**Results**	**Recommendations**
Telnet to the email GW2 and sending an email from one internal address to another internal address.	To test internal connectivity of the email GW2	Successful (allows relaying)	Block the internal staff from directly accessing the device via Telnet and SMTP port.
Telnet to the email GW2 and sending an email from one external address to another external address using the spam blocker appliance.	To test external relaying of the email GW2	Successful (allows relaying)	Block the internal staff from directly accessing the device via Telnet and SMTP port.
Telnet to the email GW2 and sending an email from one internal address to an external address using the spam blocker appliance.	To test internal relaying of the email GW2	Successful (allows relaying)	Block the internal staff from directly accessing the device via Telnet and SMTP port.
Telnet to the email GW2 and sending an email from one external address to an internal address using the spam blocker appliance.	To test mail relaying of the email GW2	Successful (allows relaying)	Block the internal staff from directly accessing the device via Telnet and SMTP port.

- ***Risk 4***

Table 5.28 shows overall results of auditing the Mailbox server role of the council's email server including the possible mitigations based on the CIS suggestions.

Table 5.28 *The overall results of auditing and recommendations Mailbox server role of the council's email server*

References	**Defaults**	**Council B**	**Recommendations**
Restrict email deletion retention 1. Private mailbox store 1 2. Public folder database 3. Private mailbox store 2 4. Temp mailbox database 5. Private mailbox store 3	7 (days)	(days) 7 14 7 7 7	7 (days)
Restrict mailbox deletion retention 1. Private mailbox store 1 2. Public folder database 3. Private mailbox store 2 4. Temp mailbox database 5. Private mailbox store 3	30 (days)	(days) 30 30 30 30 30	30 (days)
Restrict deletion of mail or mailboxes until archival 1. Private mailbox store 1 2. Public folder database 3. Private mailbox store 2 4. Temp mailbox database 5. Private mailbox store 3	Unchecked	 Unchecked Unchecked Unchecked Unchecked Unchecked	Checked
Mounting of mailbox database at startup 1. Private mailbox store 1 2. Public folder database 3. Private mailbox store 2 4. Temp mailbox database 5. Private mailbox store 3	Unchecked	 Unchecked Unchecked Unchecked Unchecked Unchecked	Unchecked
Ensure mailbox database cannot be overwritten 1. Private mailbox store 1 2. Public folder database 3. Private mailbox store 2 4. Temp mailbox database 5. Private mailbox store 3	Checked	 Unchecked Unchecked Unchecked Unchecked Unchecked	Unchecked
Verify default mailbox storage limits (issue warning at, prohibit send at, prohibit send and receive at) 1. Private mailbox store 1 3. Private mailbox store 2 4. Temp mailbox database 5. Private mailbox store 3	Custom	KB For 1, 3-5 1572864, 2097152, 2411520	Custom

Table 5.28 *The overall results of auditing and recommendations Mailbox server role of the council's email server (continued)*

References	**Defaults**	**Council B**	**Recommendations**
Ensure public folder database cannot be overwritten	Checked	Unchecked	Unchecked
Verify default public folder storage limits (issue warning, prohibit send and receive at (KB)	Custom	1991680KB - 10240KB	Custom
Audit public folder client access	Custom	Custom	Custom
Audit public folder administrative access	Custom	Custom	Custom
Verify proper permissions on public folder database	Custom	Custom	Custom
Mounting of public folder database at startup	Unchecked	Unchecked	Unchecked
Restrict email send size (mailbox identity, mail contact identity and distribution group identity)		Unlimited Unlimited Unlimited	10MB 10MB 10MB
Restrict mail receive size (mail box identity, mail contact identity and distribution group identity)		Unlimited Unlimited Unlimited	10MB 10MB 10MB
Restrict max recipients	5000	Unlimited	2000
Audit mailbox spam bypass settings	False	False	False
AntiSpam updates	Disabled	Disabled	Disabled
Zero out deleted database pages 1. Private mailbox store 1 2. Public folder database 3. Private mailbox store 2 4. Temp mailbox database 5. Private mailbox store 3	False	 False False False False False	True

- ***Risk 5***

Table 5.29 demonstrates overall results of auditing the Hub Transport server role of the council's email server including the mitigation recommendations based on the CIS suggestions.

Table 5.29 *The overall results of auditing and mitigation recommendations Hub Transport server role of the council's email server*

References	**Defaults**	**Council B**	**Recommendations**
Audit DNS lookup servers 1. Default CoB Gold 2. CoB Flourine 3. Client CoB Gold	None	 Custom Custom Custom	Custom
Restrict mail send size (max send size, max message size) 1. Default CoB Gold 2. CoB Flourine 3. Client CoB Gold	30MB 30MB	MB 20, 20 20, 20 20, 20	10MB 10MB
Restrict max recipients (max recipients per message) 1. Default CoB Gold 2. CoB Flourine 3. Client CoB Gold	5000	 5000 200 200	2000
Restrict mail receive size (max receive size, max message size, external dsn max message attach size and internal dsn max message attach size) 1. Default CoB Gold 2. CoB Flourine 3. Client CoB Gold	30MB 30MB 10MB 10MB	 20, 20, 10 ,10 20, 20, 10 ,10 20, 20, 10 ,10	10MB 10MB 10MB 10MB
Restrict IP range for receive connectors	None	None	Custom

- ***Risk 6***

Table 5.30 shows overall results of auditing CAS role of the council's email server including the mitigation recommendations based on the CIS suggestions.

Table 5.30 *The overall results of auditing and recommendations CAS role of the council's email server*

References	**Defaults**	**Council B**	**Recommendations**
Remove legacy web applications	Installed	Removed	Removed
Restrict web authentication methods*	See note	See note	See note
Require SSL for web applications	Checked Unchecked	Checked Checked	Checked Checked
Disable web anonymous access	Unchecked	Unchecked	Unchecked
Enable logging for default website	Checked	Checked	Checked

Table 5.30 *The overall results of auditing and recommendations CAS role of the council's email server (continued)*

References	Defaults	Council B	Recommendations
Enable policy for MS ActiveSync**	None	See note	See note
Forbid MS ActiveSync NonProvisionable devices 1. Default 2. Executive Nokia policy	Checked	 Checked Unchecked	Unchecked
Forbid MS ActiveSync simple device password 1. Default 2. Executive Nokia policy	Checked	 Unchecked Unchecked	Unchecked
Disable MS ActiveSync WSS/UNC access (windows file shares, sharepoint services) 1. Default 2. Executive Nokia policy	Checked Checked	Checked, Checked Unchecked, Unchecked	Unchecked Unchecked
Require MS ActiveSync password 1. Default 2. Executive Nokia policy	Unchecked	 Unchecked Unchecked	Checked
Require MS ActiveSync alphanumeric password 1. Default 2. Executive Nokia policy	Unchecked	 Unchecked Unchecked	Checked
Require MS ActiveSync minimum password length 1. Default 2. Executive Nokia policy	Checked, 4	 Unchecked, 3 Unchecked, 3	Checked, 8
Require MS ActiveSync password expiration 1. Default 2. Executive Nokia policy	Unchecked	 Unchecked Unchecked	60
Restrict MS ActiveSync attachment size 1. Default 2. Executive Nokia policy	Unchecked	For both 1 & 2 Unchecked, Unallocated	Unchecked 3MB
Require MS ActiveSync policy refresh 1. Default 2. Executive Nokia policy	None	 Unlimited 01:00:00	24.00:00:00
Restrict MS ActiveSync maximum password attempts 1. Default 2. Executive Nokia policy	8	Inactive Inactive	8
Require MS ActiveSync Certificate Based Authentication	Ignore Client Certs	Ignore Client Certs	Require Client Certs
Require MS ActiveSync inactivity lockout time	Enabled	Enabled	Disabled

Note:

Refers to restrict web authentication methods*

This task is to ensure that unneeded authentication methods for MS Exchange web applications are disabled. These measures will limit the possibility for unauthorised clients to access any unneeded services. Refer to CIS (2007, p. 76), MS Exchange 2007 recommendation "for web services and applications that cannot be disabled and removed from IIS ensure reasonable authentication methods are selected. These include Autodiscover, Exchange, EWS, Exadmin, Exchweb, MS-Exchange-ActiveSync, OAB, OWA, Public, and Unified Messaging". See more detail in Table 5.31.

Table 5.31 *The overall results and mitigation recommendations of auditing web authentication and access control of the council's email server*

Council B	**Integrate**	**Digest**	**Basic**	**Passport**
Autodiscover	X		X	
Exchange	X		X	
Exchange Web Services (EWS)	X			
Exadmin	X		X	
Exchweb	X		X	
MS-Exchange-ActiveSync			X	
Offline Address Book (OAB)	X			
Outlook Web Access (OWA)			X	
Public	X		X	
Unified Messaging (UM)	X			
Recommendations	**Integrate**	**Digest**	**Basic**	**Passport**
Autodiscover	X			
Exchange	X		X	
Exchange Web Services (EWS)	X			
Exadmin	X			
Exchweb	X			
MS-Exchange-ActiveSync			X*	
Offline Address Book (OAB)			X	
Outlook Web Access (OWA)			X	
Public	X		X	
Unified Messaging (UM)	X			

X represents enabled

X* represents only if not using Certificate

Refers to enable policy for MS ActiveSync**

This task creates and assigns policy for MS ActiveSync service. By enabling and configuring MS ActiveSync policy may assist to ensure that all corporate (Council B's) mobile devices are in line with its policy. This therefore may reduce the potential risks of the MS Exchange infrastructure in case of a mobile device disappearing (out of sync) from the network (CIS, 2007).

5.5.1.1.5 Testing stage 5: Possible mitigation

- ***Risks 1 and 2***

A technical policy relating to infrastructure devices (firewall, IDS/IPS, router and switch) as well as server (email) policies and procedures are recommended and should be implemented in order to provide better security of the council's email and related system.

5.5.1.2 Council B's online web system analysis – possible mitigations

As previously discussed, Council B's online web system consists of three sub systems which are the static web system, the CMS web system and the online payment system. The possible mitigation recommendations for the identified issues of Council B's online web system (all the three sub systems) are depicted in the following sections. Furthermore, each of the mitigations described relate to the identified risk issue number.

5.5.1.2.1 Testing stage 1: Possible mitigation

- ***Risk 1***

In the interests of general best practices, it is recommended that both the frontend and application features should be installed on different servers. The CoB-DMZ-Web server may still act as the frontend web server, whereas a new additional server should be installed to function as the application server. The new application server should be configured using a different subnetwork that is separated from the current frontend web server (the CoB-DMZ-Web). It should be located inside on the internal network.

The application of appropriate firewall rules to control the network traffic between both servers is also advisable in order to reduce any unwanted network traffic as well as potential risks to the new application server. The recommended application server can be just a VMware with appropriate Random Access Memory (RAM) and Small Computer System Interface (SCSI) hard disk spaces. Virus protection software should also be installed on this new application server to protect against virus and worm attacks. Table 5.32 summarises the recommended application server specifications.

Table 5.32 *A summary of the additional application server specifications*

Attributes	**Details**
Name	Anyname (anyname.cob.wa.gov.au)
Web server software	MS IIS web server 6.0 or 7.0 (preferred)
Other application software	Custom built application and virus protection software
OS	MS Windows 2003 Server service pack 2 or MS Windows 2008 (preferred)
Hardware	VMware C: 20 GB, E: 50 GB Hard Disk Drive (HDD) and virtual memory 4 GB
IP address	172.20.x.x/16

Additionally, it is recommended that the new application server should be separated from the backend database server (the CoB-Database). This separation can be done by placing the new application server on a different subnetwork or a VLAN from the backend database server. Moreover, appropriate ACLs should be configured to filter or control network traffic between both the subnets. These measures may prevent or mitigate any potential network security risks such as viruses, Trojans and DoS attacks infiltrating the database server from the new application server subnetwork.

5.5.1.2.2 Testing stage 2: Possible mitigation

- ***Risk 1***

It is recommended that Council B tighten its ACL settings, by creating each individual ACL for each individual service usage for both the HTTP and HTTPS protocols to only allow HTTP and HTTPS protocols from any source to the council's web server (A.B.C.121). This ACL configuration can restrict any unwanted access protocols as well as prevent potential risks such as DoS attacks to the web server.

- ***Risk 2***

The IDS/IPS software feature should be enabled on the Internet border router and a new IPS feature on the firewall may also be installed in order to inspect both the incoming and outgoing web network traffic. This can minimise any spoofing, scanning, malware, worm and DoS attacks from the incoming internetwork traffic.

However, this IPS feature is not capable of inspecting secured web (HTTPS) network traffic (Check Point Software Technologies Ltd., 2010). Refer to previous discussion on Section 5.5.1.1.2: Risk 6 for a third-party HTTPS inspection solution.

- ***Risk 3***

The aim of the frontend web server (CoB-DMZ-Web) is to only provide external access for Council B's residents. Allowing the frontend web server access to anywhere is unnecessary and can be a source of potential risk as mentioned earlier. This risk may be easily mitigated by changing the permit rule's destination from anywhere (any) which currently allows access to the DMZ, the internal and the external networks, to only access the external network (outside).

- ***Risk 4***

It was recommended that this rule should be removed. As per discussion with the web administrator, this firewall rule was inadvertent and was subsequently removed by the IT operational staff.

- ***Risk 5***

As per discussion with Council B's Web administrator, the CoB-Web server is not required to communicate with the CoB-DMZ-Web server via HTTP or HTTPS. Consequently, it is advisable to remove both these rules. Figure 5.10 illustrate the council's recommended static web system, including the network traffic protocols in a high level network diagram.

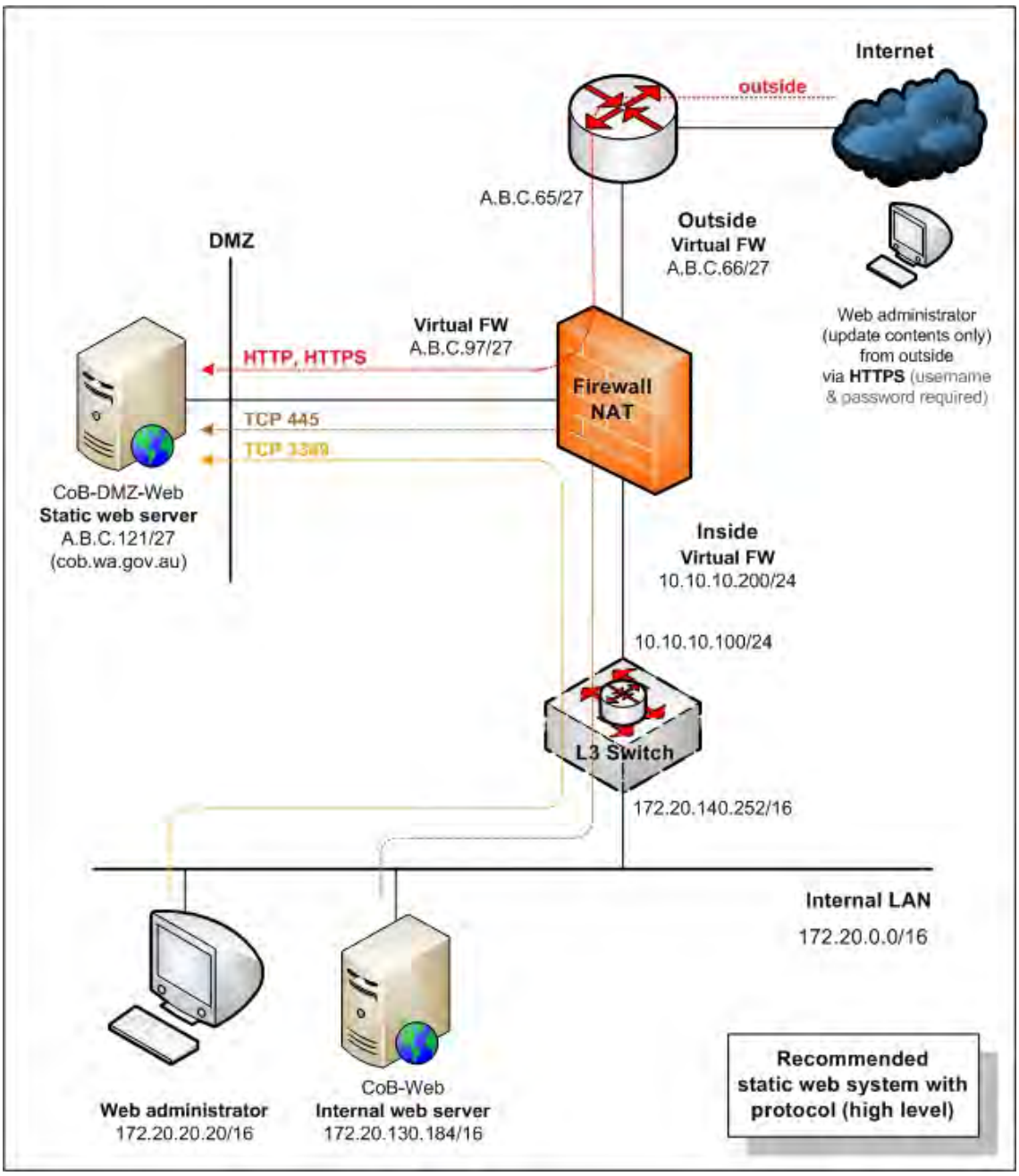

Figure 5.10. The recommended high level static web system including network traffic protocols for Council B

- ***Risk 6***

It was recommended that this rule should be removed. As per discussion with the web administrator of the council, this firewall rule was inadvertent and was subsequently deleted by the IT operational staff.

- ***Risk 7***

It was recommended that this rule should be removed. According to the web administrator, this firewall rule was inadvertent and was subsequently eliminated by the IT operational staff. Figure 5.11 display the council's recommended CMS static web system with network traffic protocols in a high level network diagram.

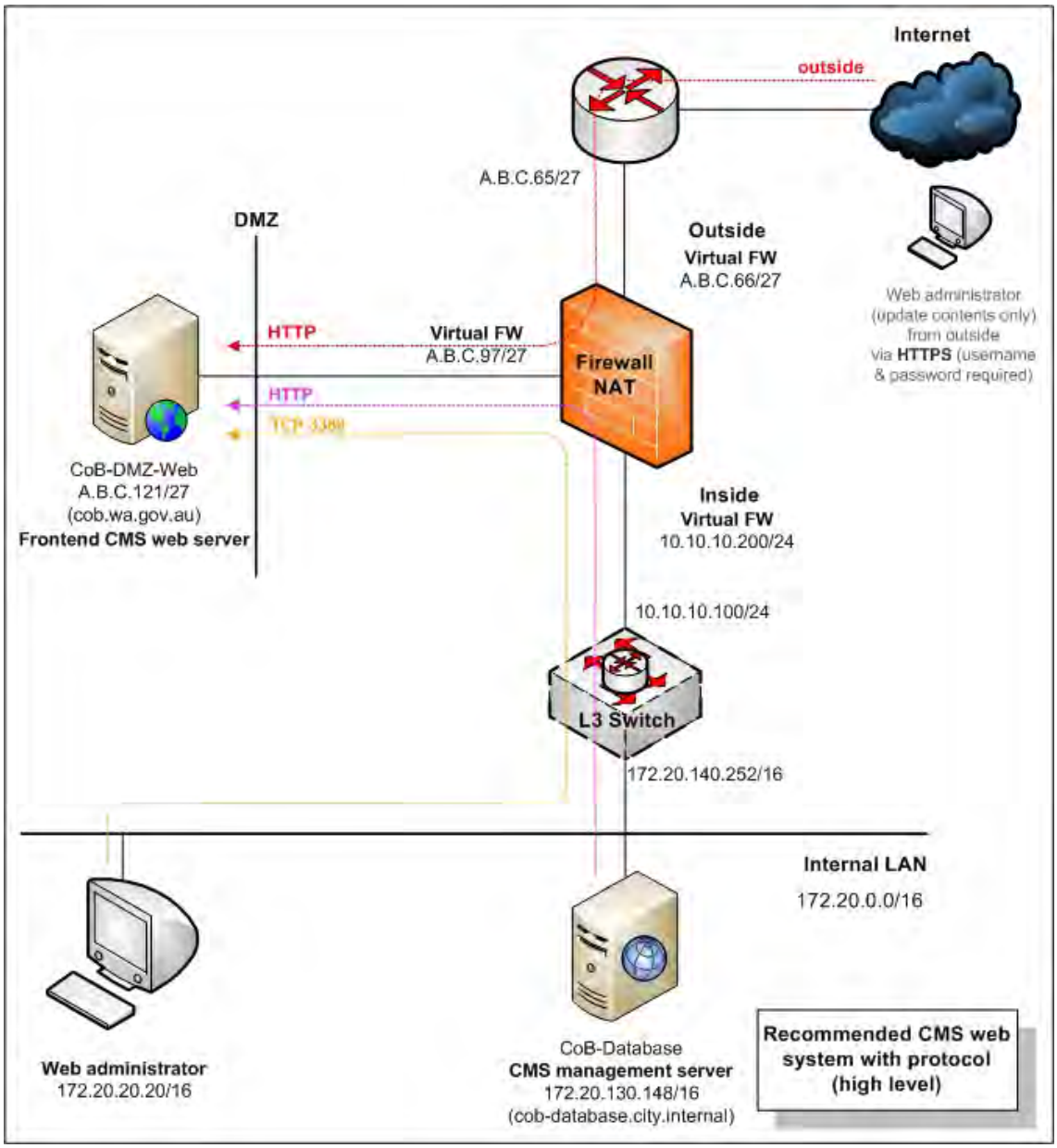

Figure 5.11. The recommended high level CMS web system with network traffic protocols for Council B

- ***Risk 8***

This rule may be enhanced in terms of security by adjusting the destination from anywhere (any) to outside or, this rule can be restricted to allow the CoB-DMZ-Web server access only to the external Online Gateway through TCP: HTTPS port

- ***Risk 9***

It was recommended that this rule should be removed. As per discussion with the web administrator, this firewall rule relating to the Sqlnet2 protocol was inadvertent and was subsequently removed by the IT operational staff. Figure 5.12 illustrates the recommended council's online payment system architecture with an additional application server including the network traffic protocols.

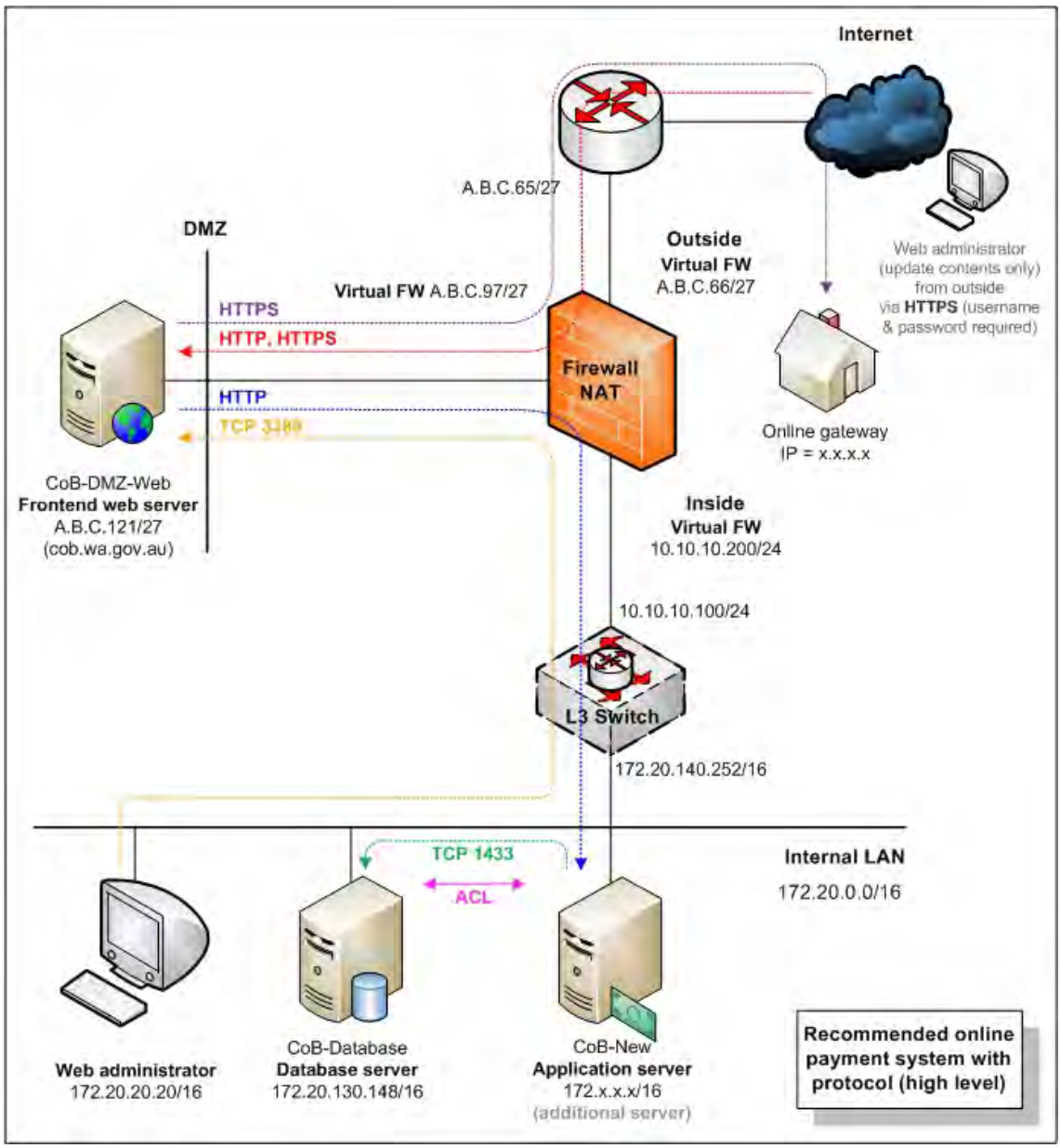

Figure 5.12. The recommended high level online payment system with an additional application server including network traffic protocols for Council B

- ***Risk 10***

In terms of the new switches detail recommendation, see previous discussion in Section 5.5.1.1.2 Risk 8. However, details on ports and VLANs, including possible connectivity of for the new switch recommendations for the council's online web system are provided in Figure 5.13.

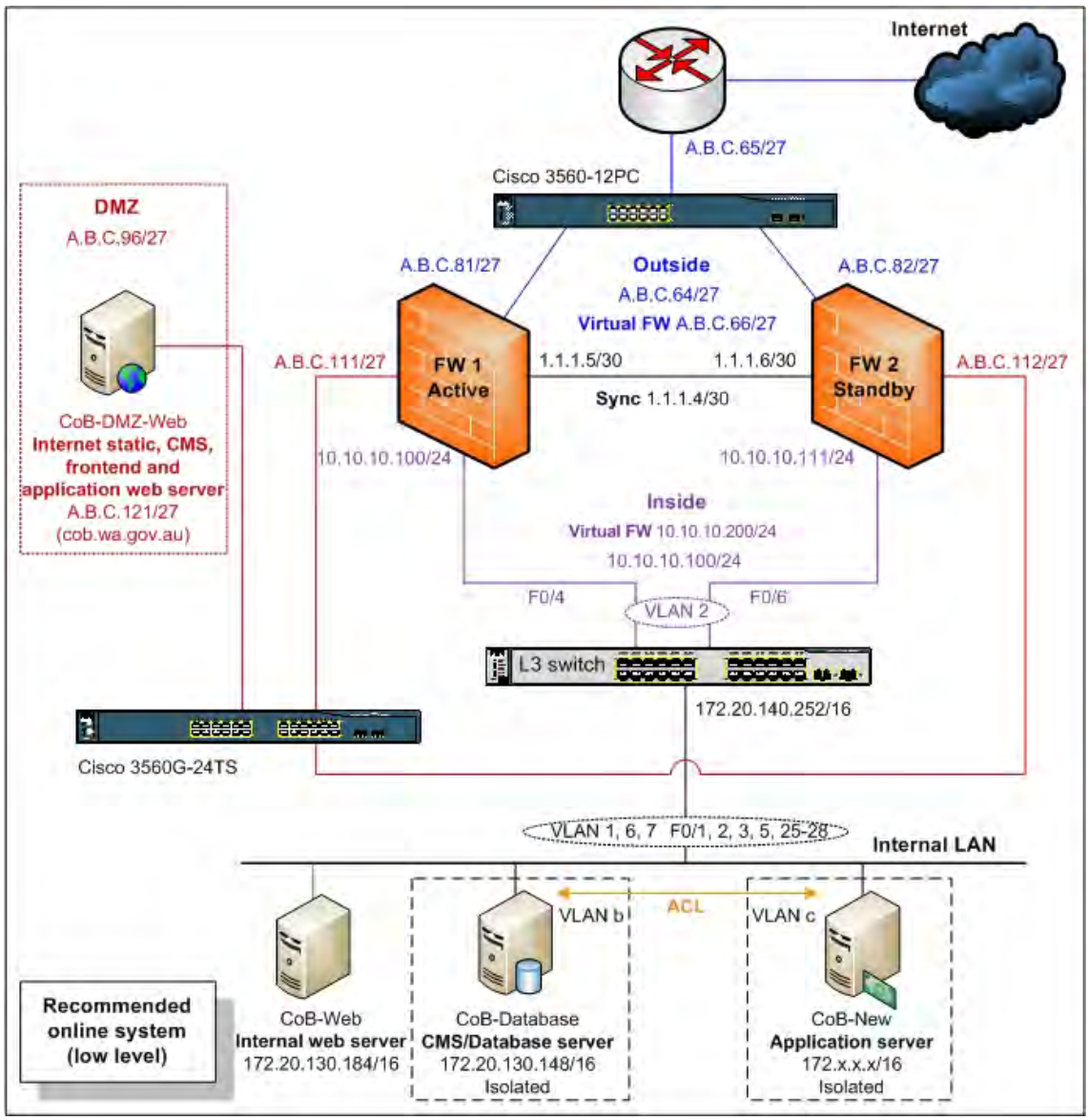

Figure 5.13. The recommended low level online web system network diagram (including the static, the CMS and the online payment web systems)

5.5.1.2.3 Testing stage 3: Possible mitigation

- ***Risk 1***

It is recommended to reconfigure the MS Windows password and revise the security auditing policies on all three council's online web servers (the CoB-DMZ-Web, the CoB-Web and the CoB-Database) in order to avoid any potential vulnerability that may occur. Furthermore, Appendices B11, B12 and B13 provide full details of the overall system information policy testing results and recommendations of the servers of Council B's online web systems.

- ***Risk 2***

There was one missing service pack and one missing critical patch on the CoB-Web server whereas the CoB-Database server had two missing service packs. In addition, the overall system patching testing analysis and the possible mitigation recommendations for the CoB-Web and the CoB-Database servers are presented in Appendices B14 and B15 respectively.s

- ***Risk 3***

Table 5.33 presents the total number of recommended open TCP and UDP ports on all the council's online payment servers.

Table 5.33 *The total number of recommended open TCP and UDP service ports on all Council B's online web servers*

Server names	**Recommended open TCP ports**	**Recommended open UDP ports**	**Comments**
CoB-DMZ-Web	3	2	Refer to Appendix B16
CoB-Web	4	2	Refer to Appendix B17
CoB-Database	5	3	Refer to Appendix B18

- ***Risk 4***

Refer to Appendices B19, B20 and B21 for full details of the identified risk issues and the possible mitigation recommendations.

5.5.1.2.4 Testing stage 4: Possible mitigation

- ***Risk 1***

See Appendices B22, B23, B24, B25, B26, B27, B28 and B29 for full details of all the results and findings including the possible mitigation recommendations based on the eight category groups respectively.

5.5.1.2.5 Testing stage 5: Possible mitigation

- ***Risks 1, 2 and 3***

As per general best practice recommendations, Council B may consider implementing general information security as well as related online technical policies and procedures such as web server, database server and infrastructure (firewall, IDS/IPS, router and switch) policies and procedures. The use of new and stringent technical policies and procedures will enhance the security of the council's online web system.

5.5.2 Discussion

The research activities conducted on Council B discovered that both the email and the online web system (the static web system, the CMS web system and the online payment system) did not meet either the national or the industry standards in terms of best practices. This can be a cause of potential risk of attacks to the council's email system, online web system as well as related ICT systems. Nevertheless, the mitigation recommendations have been presented in the analysis section of this thesis.

Similar to the results of Council A, both the recommended frameworks of email and online web systems can be utilised in order to audit any IT security systems with similar environments. See Chapter 8: Section 8.3 for examples and details of how to adapt the frameworks to similar environments.

There were seven main factors were found which can lead to the causes of potential risks in Council B's email and online web systems similar to Council A.

These factors include the lack of CIS and MS's IT security standards awareness, inadequate domain or service specific knowledge, inefficient communication between, limited IT training as a result of restricted training budget, insufficient time for task completion and reliance on external consultants for specific IT projects. These factors pose risks which may lead to interruption to both the email and online web systems services.

In addition, this may cause the council to lose its creditability. Full details of these factors are described in the following paragraphs.

Firstly, the lack of IT security standards awareness was examined. An audit which included several discussions with Council B's network and web administrators as well as testing analyses, was carried out over a period of several months. This investigation revealed a number of potential risks due to the lack of security awareness.

For example, both the email and online web systems' architectures were not following the IT security industry best practices. The email server architecture was also not in conformity to the MS Exchange 2007 architecture recommendation. Furthermore, there is currently no IT security policy pertaining to the email and online web systems used in Council B. Moreover, the architecture of the online payment system for Council B did not follow the good design recommendations of a multi-tiered (3) client-server architecture by Microsoft (Microsoft Corporation, 2010).

In addition, the interviews revealed that limited IT security standards of best practice were applied during the implementation on both the email and online web systems, according to the network and the web administrators. Table 5.34 summarises the findings related to the lack of IT security standards or industrial best practices by the staff of Council B.

Table 5.34 *The summary of the issues uncovered related to the lack of IT security standards awareness by the IT staff*

Results related to lack of IT security standards awareness by IT staff of the council	**Council B**
Internet border router redundancy/alternative Internet link deployed	No
IDS/IPS deployed and currently in use	No
Standalone external gateway switch deployed	No
Standalone DMZ switch deployed	No
Design of email server architecture based on the MS Exchange 2007 recommendations to best practices	No
Design of the online payment system conforming to recommendations of a multi-tiered client-server architecture	No

Secondly, the inadequate domain or service specific knowledge was outlined. This was evident from incorrect and inadequate configuration of the Internet border router's ACL, the DMZ switch's codes, the firewall rules, the unnecessary ports and the services installed on the email and online payment servers.

In addition, both the network and the web administrators were not formally trained in firewall and web security respectively (personal communications with Council B, 2010). Instead, they have kept abreast with technology through self-instruction mainly done after-hours. Consequently, there was a slow uptake and reduced enthusiasm by the IT operational staff to embrace new developments in firewall and web security. See the following table for more details.

Table 5.35 *The summary of results uncovered related to the inadequate specific knowledge*

Results related to inadequate domain or service specific knowledge by the IT staff of the council	**Council B**
Firewall configuration related to the email and online web systems	Insufficient
Switch configuration related to the email and online web systems	Insufficient
Setup and configuration of the email server application (MS Exchange 2007)	Incorrect
Setup and configuration of the online database application (MS SQL Server 2005)	Incorrect
Application of updated software patches on the email server	No
Application of updated software patches on the online web server	No
Application of updated software patches on the CMS server	No
Application of updated software patches on the online payment server	No
Internal email spoofing allowed	Yes
Unnecessarily opened or unused service ports on the email server	Yes
Unnecessarily opened or unused service ports on the online web server	Yes
Unnecessarily opened or unused service ports on the CMS server	Yes
Unnecessarily opened or unused service ports on the online payment server	Yes
Vulnerabilities uncovered on the email server	Yes
Vulnerabilities uncovered on the online web server	Yes
Vulnerabilities uncovered on the CMS server	Yes
Vulnerabilities uncovered on the online payment server	Yes

Thirdly, the inefficient communication was highlighted. It was apparent that there were incorrect configurations of the firewall for both the DMZ web server and the backend database server, such as wrong port numbers, as a result of verbal communication.

In addition, the lack of a change management process as well as IT recording auditing system may contribute to the inefficient communication between the IT operational staff. The use of a change management process will assist the council's IT manager and staff to manage, plan and track their system more efficiently.

Furthermore, a simple IT record auditing system such as a firewall log book would also helpful to the IT operational staff in terms of recording, reviewing and reporting. Additionally, the council has a total of 14 staff in its IT team which is further divided into separate groups such as the network and system administrations team, the web development team, the helpdesk team, the GIS and business software operation team and the IT management team. As a result, inter-staff communication may also be lacking due to poor interaction between the groups. Table 5.36 summarises the issues uncovered that can contribute to the inefficient communication between the council's IT operational staff.

Table 5.36 *The summary of results uncovered that can contribute to the inefficient communication between the IT operational staff*

Results uncovered that can contribute to the inefficient communication between the IT operational staff	**Council B**
Existence of change management procedures	No
Availability of simple specific technical log books	No
Updated documentation of the IT email system	No
Updated documentation of the IT online web system related	No

Fourthly, the limited IT training as a result of a restricted training budget was examined. There is a restricted IT training budget allocated by the council according to the IT managerial staff. This problem of specific training may be alleviated in the future should more money be allocated towards a training budget by the council. See details in Table 5.37.

Table 5.37 *The summary results related to the limited IT training as a result of limited training budget*

Issues uncovered in relation to the limited IT training budget	**Council B**
Formal industry or equivalent firewall training of the IT operational staff	No
Formal industry or equivalent training of the email application (MS Exchange 2007) of the IT operational staff	No
Formal industry or equivalent training of database application (MS SQL Server 2005 or equivalent) of the IT operational staff.	No
Formal IT Security training of the IT operational staff	No
IT training yearly budget allocation for each IT operational staff member	Partly
Support of the council for self-costed self study of IT operational staff	Yes

Fifthly, the matter of insufficient time for task completion was looked at. The 14 IT staff of Council B have to manage a daily routine covering a wide range of tasks in all areas including GIS, library, email, online payment, online website system, CMS, property management, communication and telephony systems.

As a consequence, some tasks are perpetually left incomplete which in turn exacerbates the problem of limited time for individual study or research. In addition, there is no time left for documentation. Table 5.38 summarised the insufficient time for task completion by the council IT operational staff.

Table 5.38 *Results uncovered related to the insufficient time for task completion*

Issues uncovered in relation to the insufficient time for task completion	**Council B**
The IT operational staff manages several complex IT systems task simultaneously	Yes
Use of enterprise information security policy	No
Use of technical (issue-specific and systems-specific) security policy	No
Updated documentation of the IT email system	No
Updated documentation of the IT online web system – static web system	No
Updated documentation of the IT online web system – CMS web system	No
Updated documentation of the IT online web system – online payment system	No

Sixthly, the factor of the reliance on external consultants for specific IT projects was analysed. The council's practice and reliance of outsourcing to solve the expertise problem has the disadvantage of a lack of knowledge transfer.

For example, there was no proper documentation that the firewall project was handed over to the council's IT operational staff apart from the notification of a simple ACL configuration rule (personal communications with Council B, 2010). This lack of handover procedures indicates poor contract management dealings with outsourcers. See Table 5.39 for more details.

Table 5.39 *Summary of issues uncovered relating to the reliance on external consultants for specific IT projects*

Issues in relation to the reliance on external consultants for specific IT projects	**Council B**
Implementation of the email spam blocker appliances by external consultants	Yes
Appropriate documentation for the email spam blocker appliances installation and management provided by the external consultants	Partly
Implementation of the firewall system by external consultants	Yes
Appropriate documentation for the firewall installation and management provided by the external consultants	No
Deployment of the email (MS Exchange 2007) application server by external consultants	Yes
Appropriate documentation for the email (MS Exchange 2007) installation and management provided by the external consultants	No

Finally, there was no valid testing environment in place at Council B. Council B's IT department has a testing VM server for pilot testing different kinds of servers. However, the council's IT department has no testing environment for network communication system.

Having both servers and network testing environments would provide enormous benefits to the council such as minimising potential risks, flexibility and opportunity to gain better understanding of the new system. The following table demonstrates more details of the summary of issues uncovered related to the lack of a valid testing environment.

Table 5.40 *Summary results uncovered related to no valid testing environment on place at the council*

Summary results related to the lack of a valid testing environment	**Council B**
Existence of a testing environment for the infrastructure	No
Existence of a testing environment for the email system	No
Existence of a testing environment for the online web system – static web system	No
Existence of a testing environment for the online web system – CMS web system	No
Existence of a testing environment for the online web system – online payment system	Partly

CHAPTER 6. EXPERIMENTAL EVALUATION AND ANALYSIS: A CASE STUDY OF COUNCIL C

The purpose of this chapter is to demonstrate the results and findings as uncovered from the examination of email and online web systems at Council C. The chapter is comprised of five subsections, including (1) background information; (2) methodology; (3) Council's C email system results; (4) Council's C online web system results; and (5) analysis and discussion.

6.1 Background information

Council C is a WA local government council which has its own IT section. The IT section provides IT support and services to the staff and residential clients of the council. These IT services cover a range of services including GIS, library, email, online web information and online payment systems, similar to Councils A and B. Council C's network infrastructure uses Ethernet network technology which currently connects its central and remote sites together in a star topology configuration. Council C connects to the outside world or the Internet via a leased fibre optic connection through an ISP. In addition, all the council's remote sites are interconnected to the council's central site via fibre optic, DSL and ADSL connections. Furthermore, the council owns licensed wireless connections which provide connectivity between the council's central site and the two associated libraries.

Similar to both Councils A and B's email systems, Council C also deploys MS Exchange Server 2007 as the prime email server software whereas the email client software uses MS Outlook 2007. This email system provides both traditional email and webmail features to its staff. The email server serves over 900 mailboxes and over 500 staff (personal communications with Council C, 2010).

In terms of the online web system, both Councils B and C's online web systems have their similarity in terms of the general static web, the CMS and the online payment systems. Council C's online web system provides both online general information and payment services to its residents.

Although both the email and online web systems are managed in-house by the council's IT staff, Council C does resort to external outsourcing in the case of unsolved problems or when implementing advanced ICT projects.

Ideally, advanced ICT projects would require advanced ICT technical skills to create, implement or deploy. The followings are some typically advanced ICT projects, but not limited to:

- Installation and/or upgrade of core switching and routing network system;
- Deployment of new redundancy firewall systems;
- Deployment or upgrade of Voice over IP systems;
- Deployment of fully secure wireless LAN systems;
- Upgrade of database and financial systems;
- Implementation of online payment systems;
- Deployment of Storage Area Network (SAN) systems; and
- Implementation of internet GIS mapping system (personal communications with Council C, 2008, 2009).

6.2 Methodology

This subsection aims to depict the overall methodology used in this research. It consists of pre-interview consultation, document review, interview investigation, existing architecture discovery, email system testing and online web system testing.

6.2.1 Pre-interview consultation

Council C's pre-interview consultation is similar to both the pre-interview consultation of Councils A and B. However, the participants of the initial open-ended meetings were the council's IT manager, the system administrator and the network administrator.

The overall risk analysis was discussed and it was agreed that the analysis was to be done in stages in order to minimise any potential risks or interruptions to the council's real-time Internet infrastructure, including the email and online web systems.

The time frame was set to five months for both the report deliverables which was the same time frame agreed upon by both Councils A and B.

In addition, the ethics and contract agreements were signed in the second meeting and the contents of the contract agreements were the same as for Councils A and B. For example, the project was to be done at no cost to the council with the two reports as deliverables as well as the provision for the council to discontinue the project at any time of its choosing.

6.2.2 Document review

The hardware and software specifications relating to both the council's email and online web systems documents were collected including specifications and records of configuration codes of the DMZ switch, the firewalls, the email server, the reverse proxy server, the static web server, the application server and the backend database server. In addition, a copy of the DMZ internetwork diagram was collected. However, there was no need for details of the Internet border router and IDS/IPS devices as both these devices were not deployed in the council's internetwork system.

From the interviews conducted with the IT manager and the system administrator, there was no ICT technical security policy on either the email or the online web systems in use, apart from an acceptable use of computing and communications facilities policy.

6.2.3 Interview investigation

Several interviews were carried out with the two main stakeholders as follows:

- The council's IT manager; and
- The council's IT Staff (the network and system administrators).

The purpose of the face-to-face interview and discussion with the council's IT manager was to obtain a general overview of the council's ICT computer and network system, in particular the council's email and online web systems. In addition, the specific project deliverables were discussed such as overall ICT system documentation, risk analysis

and feasible mitigation techniques of both the email and online web systems. Several interview techniques including face-to-face, telephone and email were used during the ongoing testing analysis interviews between the researcher, the network administrator and the system administrator. The interviews conducted with the network administrator were related to the council's network connectivity including the firewalls and the switches.

Furthermore, other related information such as the ACL configuration codes, the AD and the DNS were procured at this time. There were also a number of testing analysis interviews conducted with the system administrator that related to the configurations of the firewalls, the reverse proxy server, the email server, the backend database server, the CMS server, the static web server and the application server.

6.2.4 Existing architecture discovery

The existing architecture discovery of the email and online web systems of Council C is covered in this section in detail.

6.2.4.1 The existing email system architecture of Council C

The council's email system consists mainly of one Exchange 2007 VMware server, and one reverse proxy server. The email server is located in Council C's internal network whereas the reverse proxy server is situated in the DMZ area. Both devices are interconnected via the council's internetwork infrastructure. The infrastructure has two firewalls and one core switch as its component devices. The switch also provides internal network connectivity for Council C's network devices. In addition, only SMTP and HTTPS are allowed for email and webmail purposes similar to both Councils A and B. Furthermore, Council C uses 128-bit encryption with standard vailidation SSL certificate for thier webmail system (Limwiriyakul & Valli, 2011c).

In terms of the email system, the reverse proxy server communicates with the email Exchange server via HTTPS whereas the domain controller (10.1.1.210) server communicates via LDAP, radius and DNS ports. This communication mechanism allows the reverse proxy server to obtain email details and publish the associated webmail to the email users of Council C. More details are provided in Section 6.5.3 on

firewall rules and network port numbers. The mail exchanger record (MX record) of Council C is mail.coc.wa.gov.au and its corresponding Internet address is A.B.D.37. Figure 6.1 portrays all the devices connectivity, communication protocols and allowed email network traffic and related protocols in a high level network diagram.

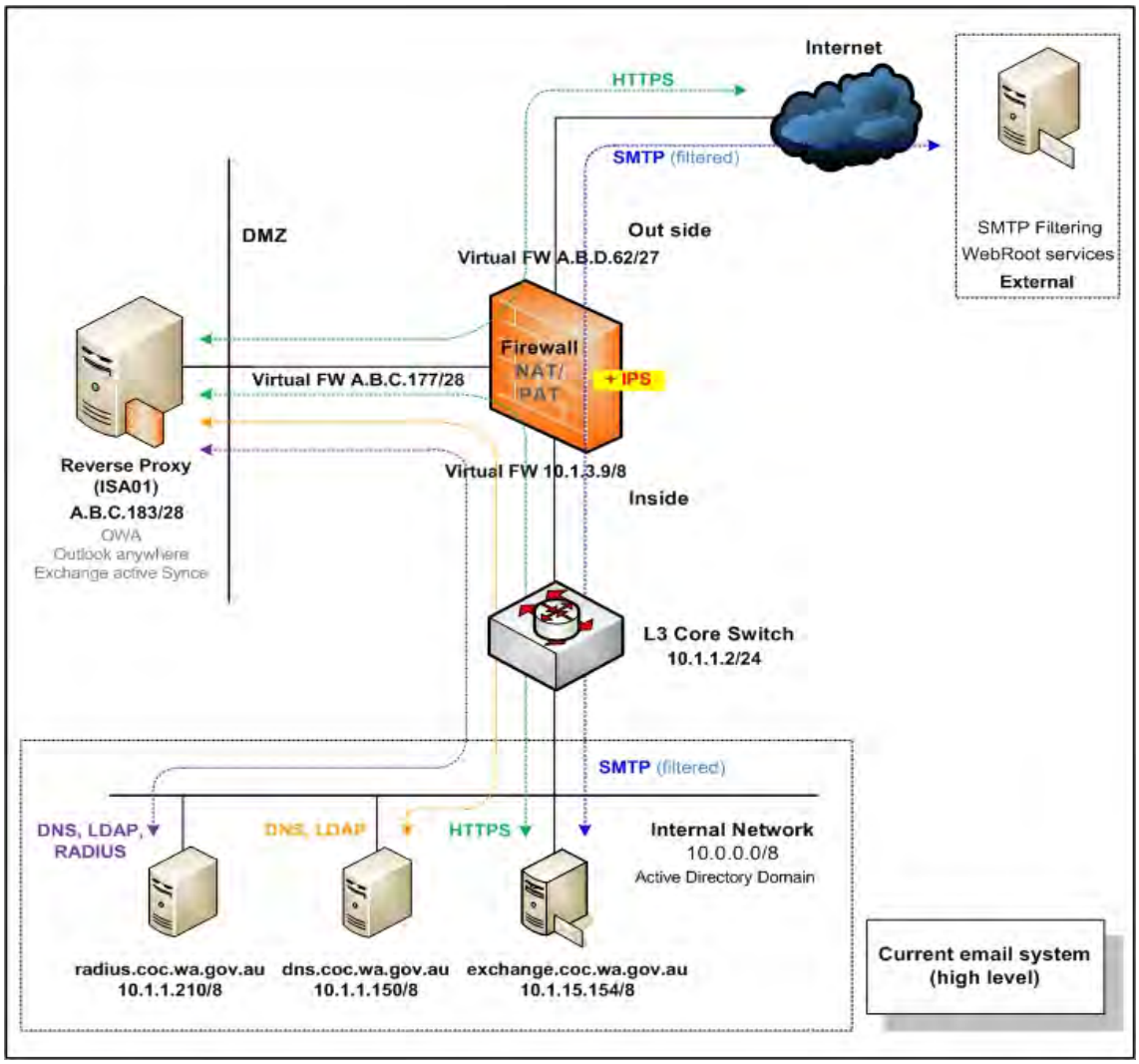

Figure 6.1. A current high level network diagram with allowed email network traffic and related protocols for the email system of Council C

6.2.4.2 The existing online web system's architecture of Council C

Council C's online web system provides the community services for the council's general information such as rates, libraries, events, facilities and jobs. At the time of the auditing, this online payment system was also used to provide online payment services to its residents for paying their rates, infringements and/or dog registrations.

The architecture of Council C's online web system can be categorised into three groups, namely the static web, the CMS web and the online payment systems.

6.2.4.2.1 The existing static web system architecture

The static web system has one web server (the CoC-DMZ-Web server) which is located in the council's DMZ network. The CoC-DMZ-Web server provides both simple/standard static and form based webpages. There were several UTP, TCP and IP network protocols that were being used for the static web system. Figure 6.2 depicts the council's current architecture on the static web system including the network traffic protocols in a high level network diagram.

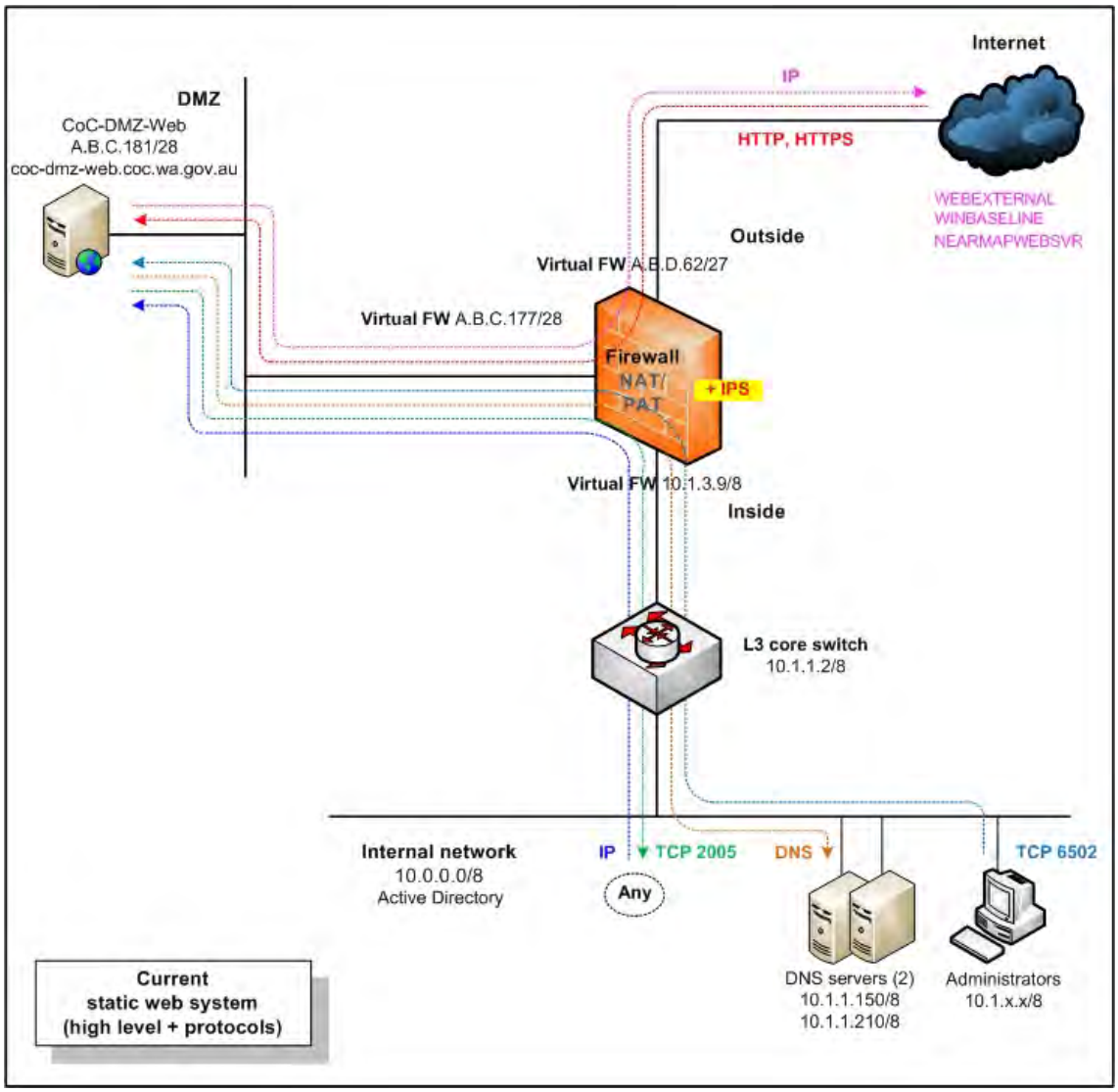

Figure 6.2. The high level static web system including network traffic protocols currently in use by Council C

6.2.4.2.2 The existing CMS web system architecture

The CMS web system (the CoC-DMZ-CMS and the CoC-CMS servers) provide simple/standard static and form based webpages. The CoC-DMZ-CMS server is located in the DMZ area in order to minimise any potential risks which may arise from attackers to Council C's CMS web system. On the other hand, the CoC-CMS server is located in the council's internal network.

Figure 6.3 illustrates Council C's current architecture on the CMS web server system including the network traffic protocols in a high level network diagram.

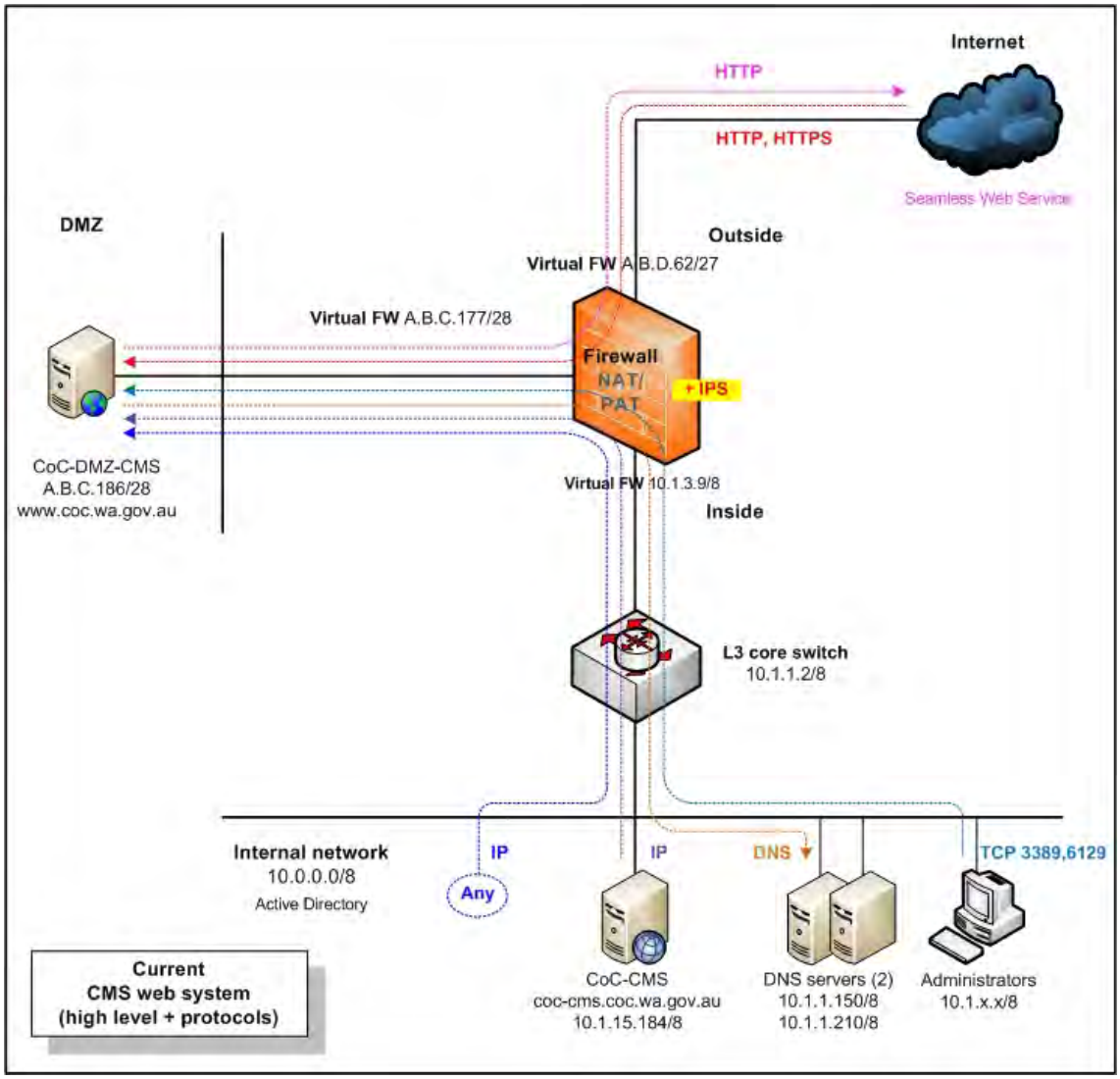

Figure 6.3. The high level CMS web system with network traffic protocols currently in use by Council C

Both the CoC-DMZ-CMS and the CoC-CMS servers interact with each other as part of a WCMS. The CoC-CMS server allows the council's IT operational staff to manage and update webpages information, before pushing the validated webpages from the CoC-CMS to the CoC-DMZ-CMS servers.

In addition, this connectivity provides better security as there is no direct connection between the client and the backend CMS server. The council's residents are able to access the CoC-DMZ-CMS server via http://www.coc.wa.gov.au to view or search for general information of the council

6.2.4.2.3 The existing online payment system architecture

Council C's current online payment system is multi-tiered (3-tier) client-server architecture. It consists mainly of the frontend web (Epathweb), the application (Epathway) and the backend database (Pathway) servers. The Epathweb and Epathway servers perform all of the application logic whereas the Pathway server performs the data logic.

In addition, the external gateway security payment service (Commweb01) is used by the council to provide secure payments such as rates and infringements for its residents. Council C's online payment system communicates with the external gateway security payment service via a HTTPS connection.

Furthermore, the SSL protocol is used to provide an encrypted communication channel between the client's web browser and the council's online payment system. Council C uses 128-bit encryption with extended validation SSL certificate (Limwiriyakul & Valli, 2011c). This method ensures secured private communications over the public Internet as well as it gives "high security web browsers information to clearly identify" (VeriSign Authentication Services, n.d., p. 1) the council website identity (Limwiriyakul & Valli, 2011c).

Figure 6.4 demonstrates the council's current online payment system architecture including network traffic protocols in a high level network diagram.

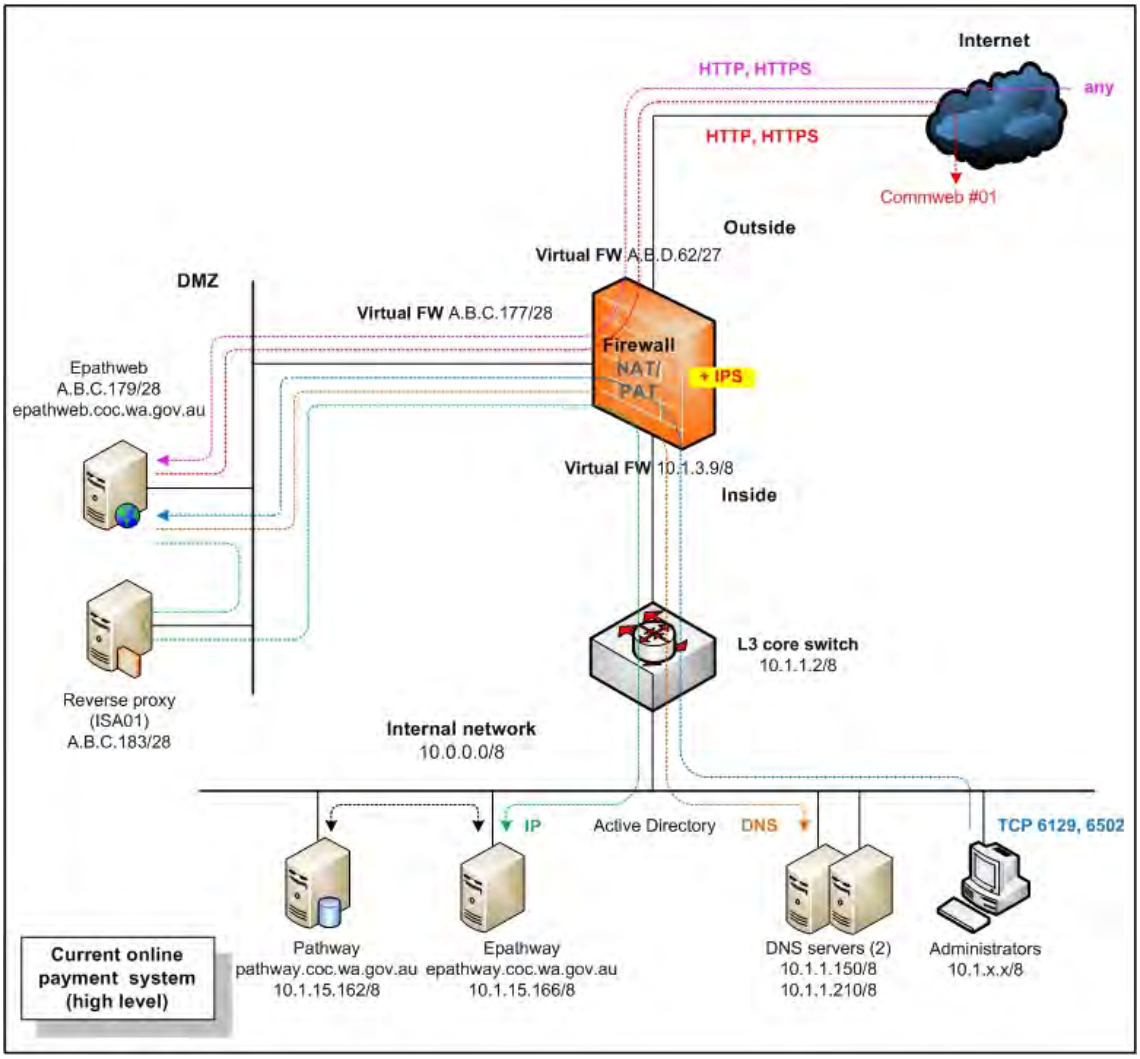

Figure 6.4. The high level diagram of the online payment system including network traffic protocols currently in use by Council C

6.2.5 Email system testing

Similar to both Councils A and B, the email system testing analysis consisted of five stages which are summarised as follows:

- Network surveying of Council C's email system, network architecture and network architecture recommendations;
- Auditing and reviewing the configuration codes of firewalls, switch and reverse proxy devices;
- Services and system identification, port scanning and vulnerability testing of the email server;

- Email spoofing testing and vendor security benchmark auditing on the email server; and
- Email system security policy review.

6.2.6 Online web system testing

The online web system testing analysis had five stages similar to Councils A and B, as follows:

- Network surveying, which included the current Council C's online web system's network architecture, identified risks and mitigation recommendations;
- Auditing, configuration codes review, identified risks and mitigation recommendations of the IDS/IPS, the firewalls and the switch devices related to Council C's online web system;
- Services and system identification, port scanning and vulnerability testing of the council's online web system's servers;
- Vendor security benchmark auditing on the online payment database server; and
- Online web system security policy review.

6.3 Council C's email system results

The review and testing results for the device configurations, the exposed vulnerabilities of all the email system servers, the email spoofing, the vendor security benchmark and the security policy for Council C are described in the following sections.

6.3.1 Testing stage 1: Network surveying

This first testing stage consisted of network surveying that collected information on the email system including the email server, the external spam blocker appliance, and the current Exchange email architecture and followed by the corresponding recommendations (same as Chapters 4 and 5). Information for the following components of Council C's email system was collected:

- Overall network diagram for Internet link, internal and DMZ infrastructure connectivity including the email system;
- The council's mail exchanger record (MX record);
- The firewall devices specification and related email configuration codes;
- The internal/DMZ switch specification and configuration codes;
- The council's reverse proxy and email servers specification summary; and
- The external spam blocker appliance to the council's specification summary.

6.3.1.1 The email system devices

Council C's email system consists of three specific devices. This includes the MS Exchange 2007 email server, the external spam blocker appliance and the reverse proxy server.

6.3.1.1.1 The email server

Current application software of the email server has MS Exchange Server 2007 with service pack 1 installed. The email server's operating software is running on MS Windows Server 2008 with service pack 1. Similar to both the email servers of Councils A and B, the current configuration of Council C's email server is configured as a single-server architecture in which two of the Exchange 2007 feature roles are not included which are the Edge Transport and the Unified Messaging server roles.

This was due to the fact that Council C uses the external spam filtering service and the Nortel PBX digital telephony systems. Both these systems perform the same functionality as the Edge Transport and the Unified Messaging server roles respectively. Summary details are presented in the Table 6.1.

Table 6.1 *A summary of the email server specifications*

Attributes	**Details**
Email application software	MS Exchange 2007 with service pack 1
Email scanning software	Sophos Anti-Virus
OS	MS Windows Server 2008 Enterprise Edition with service pack 1
Hardware	VMware server
IP address	10.1.15.154, 255.0.0.0
MS Exchange 2007 roles	Mailbox, Hub Transport, CAS combined
Email service protocols	SMTP and HTTPS
Other software	None

6.3.1.1.2 The spam blocker appliance

Webroot services is an external IT company which currently provides Internet filtering (email spam and web traffic) to Council C. Incoming SMTP email traffic is directly forwarded to Webroot services first, in order to remove viruses and block unwanted spam emails. Thereafter, only the desired email traffic is redirected to Council C's email server.

On the other hand, outgoing email traffic first arrives at the MS Exchange Server 2007, which then acts as a SMTP mail relay connector server. It forwards the email traffic to Webroot services which inspects and cleans any potential spam, prior to delivery of the emails to the recipients. The purpose of the external spam blocker appliance is to filter all incoming and outgoing SMTP emails to block malware, spyware and spam emails. More details for the external spam blocker appliance in terms of its current connectivity were provided in the high level network architecture diagram in Figure 6.1.

6.3.1.1.3 The reverse proxy server

Currently, there is a physical server which runs MS ISA 2006 which is being used as a reverse proxy server and is located in Council C's DMZ internetwork. The purpose of the reverse proxy server is that it is used as an intermediary by the council's Internet users who want to access the council's internal web database and webmail by sending its requests indirectly. In addition, the use of the reverse proxy server increases the security strength of the council's internal network.

Furthermore, in terms of the council's email system, both the reverse proxy and the MS Exchange (2007) servers communicate securely via TCP port 443 (HTTPS) in a server-to-server communication. The reverse proxy server is configured to publish a combination of popular methods including MS OWA, MS Exchange ActiveSync and MS Outlook Anywhere. Summary details of the reverse proxy server are provided in Table 6.2. Details of its current connectivity were provided in Figure 6.4.

Table 6.2 *A summary of the MS ISA server specifications*

Attributes	**Details**
Proxy application software	MS ISA 2006 standard version
OS	MS Windows Server 2003 Enterprise Edition with service pack 2
Hardware	HP 360 Generation 6
IP address	A.B.C.183 255.255.255.240
Interface	2 x Gigabit Ethernet (team)
MS Exchange 2007 roles	MS OWA, MS Exchange ActiveSync and MS Outlook Anywhere
Email service protocol	HTTPS
Other software	IIS version 7.0

6.3.1.2 Testing stage 1: Identified risk issues

The following sections explain the identified risk issues for the council's email system.

- ***Risk 1: Single point of failure***

The existing email architecture of Council C is made up of a simple single-server architecture similar to both Councils A and B. Council C's email system was considered to be a medium-sized deployment which may pose the potential risk of a single point of failure as the current system has only one email server.

The other potential risks to the email server are in the form of virus and malware attacks, which may allow attackers to steal the email credentials of the council's staff or interrupt the email services of the council.

- ***Risk 2: Same subnetwork***

The current email server is located in the same subnetwork as the other important servers of the council such as the application, file and database servers. This configuration may cause a potential risk to the other important servers in the event of the email server getting compromised due to the fact that there was no filtering mechanism in place to separate network traffic between the email and other servers.

- ***Risk 3: MS ActiveSync – Authentication***

The current email configuration for MS ActiveSync authentication was the same as the email system of Council B. Council C currently uses a basic authentication method together with a SSL connection.

In comparison to both certificate and token form authentication methods, basic authentication is considered as the simplest authentication method (Luckett et al., 2008). This is due to the fact that the passwords in basic authentication are sent in clear text or plain text format which may expose them to sniffing or eavesdropping attacks.

- ***Risk 4: MS Outlook Anywhere – Authentication***

Currently, Council C's email system supports MS Outlook Anywhere with basic authentication via SSL connection to its staff. The basic authentication is considered to provide the lowest security as compared to the other authentication option (NTLM) (Luckett et al., 2008).

6.3.2 Testing stage 2: The email system's infrastructure – Internet border router, IDS/IPS, firewalls and switch reviews

This second stage can be separated into a data collection and review of Internet border router, IDS/IPS, firewall and switch reviews of the council's email infrastructure.

6.3.2.1 Internet border router configuration codes data collection and reviews

Typically, an Internet border router acts as a gateway that permits the council's network to be able to communicate with the outside world. It forwards or routes the network traffics or protocols which serves the council's network services. However, Council C connects its internetwork directly via its firewall, which means that there is no existing Internet border router being deployed.

6.3.2.2 IDS/IPS configuration codes data collection and reviews

The existing firewalls (Juniper SSG-350M security appliances) have an annual licensed IPS engine and are available with an add-on feature called Juniper Networks Deep Inspection Firewall Signature Packs. This IPS engine provides deep inspection of the council's internetwork including protocol anomaly detection, stateful protocol signatures, IPS/Deep Inspection or DI attack pattern obfuscation and nightly updates of attack signatures (Juniper Networks, 2009).

6.3.2.3 Firewall configuration codes data collection and reviews

In the council's internetwork, the two firewalls act as a main filter for all incoming and outgoing network traffic. Furthermore, they perform NAT, Port Address Translation (PAT) as well as IPS functions. However, both the firewalls do not provide antivirus and antispam checking as both these antivirus and antispam features require additional annual licenses.

Nevertheless, both these features may not be required to be performed by the firewalls as the council uses the Sophos antivirus software to protect against virus attacks. However, one of the firewalls operates in the active mode and the other operates in a standby mode. More details of the firewall's connectivity are provided in Figure 6.5. Table 6.3 summarises the brief specifications of both the firewalls.

In addition, Appendix C1 shows the summary of the firewall codes with respect to the NAT/PAT of the council's email system. On the other hand, Appendix C2 shows the summary of the firewall codes with respect to Council C's email system.

Table 6.3 *A summary of the firewalls specifications*

Attributes	**Details**
Device type	Juniper firewall x 2
OS/model	SSG-350M series
Memory	256 MB (based memory)
Interfaces (fixed I/O)	4x10/100/1000
Physical Interface Module (PIM) Slots	5
Wide Area Network (WAN) interface options (PIMS)	Serial, T1, E1, ADSL/ADSL2/ADSL2+, G.SHDSL
LAN interface options (uPIMS)	8x10/100/1000, 16x10/100/1000, and 6xSFP

6.3.2.4 Switch configuration codes data collection and reviews

Council C's network is considered as an Ethernet network environment. The council has only one switch, which provides network communication and connectivity between the firewalls, the DMZ servers and the council's internal network. It is also a core switch, which interconnects all of Council C's Intermediate Distribution Frames (IDFs) and servers.

The current overall hardware and software details of the core switch are depicted in Table 6.4.

Table 6.4 *The email system – current switch hardware and software details*

Attributes	**Details**
Device name	C60175 (CoC-Core-Switch)
Device type	HP E5412 zl switch chassis (J8698A)
OS	K.14.41
Memory	256 MB
Switch port	12 open module slots; 1 RS-232C DB-9 console port; Supports a maximum of 48 10-GbE ports or 288 10/100/1000 ports or 288 mini-GBICs, or a combination
Operate at	Layer 2/3 OSI
VLANs	1, 2, 3, 10, 15, 17-19, 24-26, 29, 60, 80, 82, 100, 110-117, 200

Furthermore, details on ports and VLANs including its connectivity of the council's email system are presented in Figure 6.5.

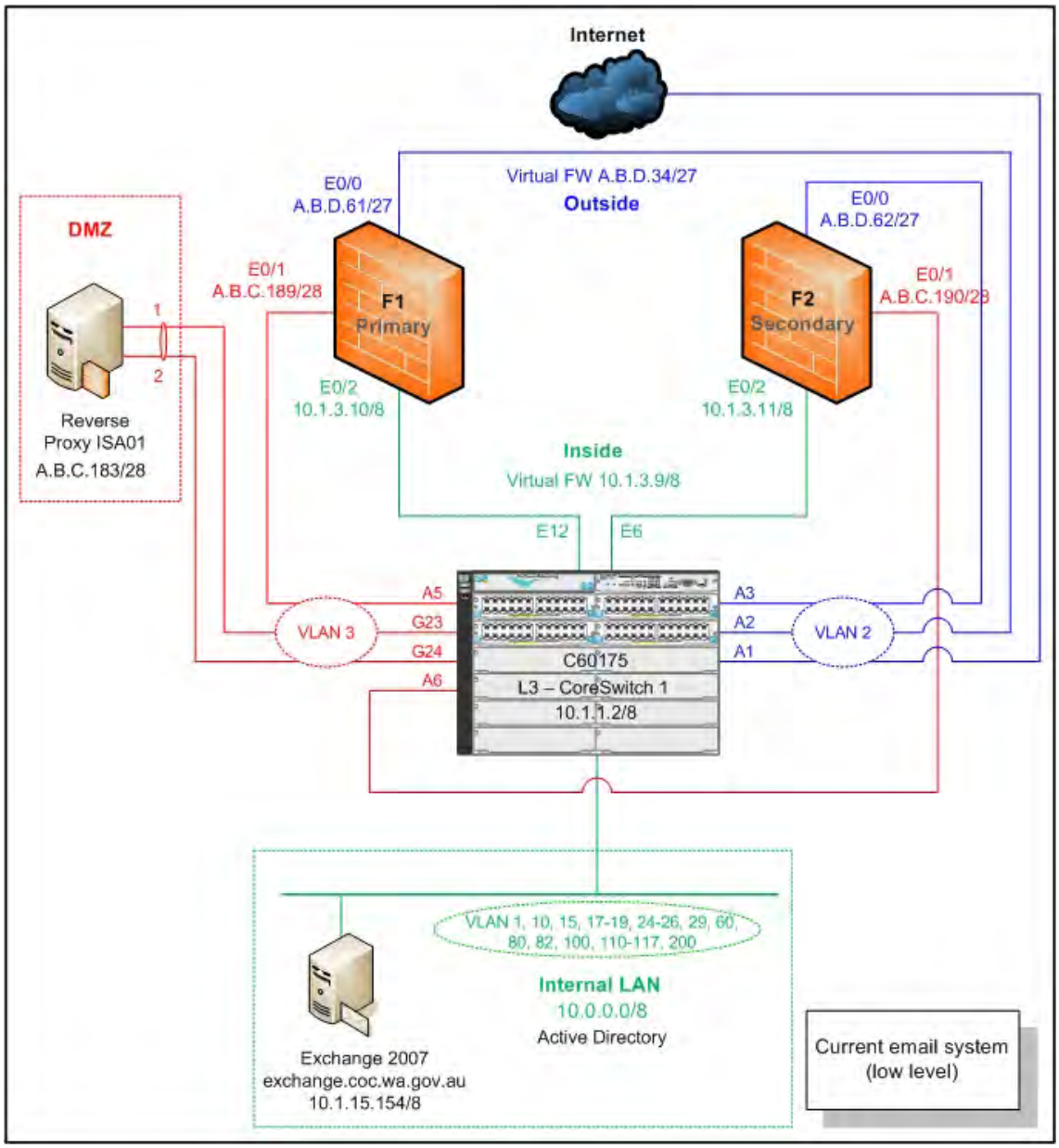

Figure 6.5. A current low level network diagram of the email system for Council C

6.3.2.5 Testing stage 2: Identified risk issues

The identified risk issues for Council C's email infrastructure system are detailed in the following sections.

- ***Risk 1: No Internet border router in place***

As mentioned earlier, there was no existing Internet border router deployed within the council's internetwork system. A missing Internet border router means that the council's internetwork system has only one layer of protection against any outside intrusion attacks such as spoofing and DoS.

The council used two firewalls (Juniper SSG-350M security appliances) to provide several features such as routing, VPN, filtering and inspecting incoming and outgoing network traffic for the council's internetwork system. This arrangement can be considered as a single point of failure for the several tasks that the firewalls serve.

- ***Risk 2: No IDS/IPS on the Internet border router***

As previously described, there was no Internet border router deployed at Council C. The future deployment of an Internet border router with IDS/IPS feature can provide a first layer of defence against intrusion attacks such as spoofing and scanning.

- ***Risk 3: Unnecessary ACL rule***

The firewall rule (see Appendix C1: Policy number 2) allows anyone to access the email server via the SMTP port. This accessibility to the email server is a potential risk to the email system of Council C, as unauthorised persons can potentially access the email server.

- ***Risk 4: Not in use ACL rule***

The current firewall rule (see Appendix C2: Policy number 5) translates the internal server (10.1.1.3) to the Exchange_gate2 name.

- ***Risk 5: Duplicated ACL rule***

There are duplicated firewall policy rules (see Appendix C2: Policy numbers 14 and 15).

- ***Risk 6: Duplicated ACL rule***

The current firewall rules allow anyone from the council's internal network to access the firewall via several methods including HTTPS, SSH, console and Telnet ports.

- ***Risk 7: Overall inadequate switch code security configurations***

On the current Council C's core switch (HP C60175), there were some inadequate switch code security configurations, which may lead to potential security risks such as ARP spoofing, ARP poisoning and sniffing attacks.

- ***Risk 8: Single point of failure***

Connectivity between the council's outside (external), the DMZ and the inside (internal) networks were served by only one core switch which can be considered as a single point of failure. In case of the core switch failure, serious interruptions may be caused to the council's core network, which includes downtime to the council's staff as well as the online systems to its residents.

6.3.3 Testing stage 3: Services and system identification, port scanning, vulnerability testing and results

Similar to testing steps conducted at Councils A and B, both NMAP and GFI LANguard network scanning tools were used to obtain information such as TCP, UDP ports, vulnerabilities, patches, services, software and hardware from the email system. NMAP with GUI standard (open source Zenmap version 5.0) for MS Windows XP version was run with slow comprehensive scan option.

On the other hand, GFI LANguard version 9.0 with full scan option was also utilised. Running intense comprehensive as well as full scan options on both the applications will maximise the collection of information

6.3.3.1 Services and system identification results

Appendices C3 and C4 summarise the results of the services and system identifications including system information and system patching status results for Council C's email server (MS Exchange 2007). However, the researcher did not test against the reverse proxy server (ISA01) as per recommendation of the system administrator in order to minimise any potential downtime which may have occurred due to the fact that the ISA01 server provides services to a wide range of Council C's computer systems.

6.3.3.2 Port scanning results

Similar techniques as carried out in Councils A and B were used for this purpose, in that both NMAP and GFI LANguard were used for port scanning on the email server. There was no unnecessarily opened UDP port found on the email server. However, there were some unnecessarily opened TCP ports found. Full details of the overall opened TCP and UDP ports are provided in Appendix C5.

6.3.3.3 Vulnerability testing results

In this testing stage, the vulnerability was categorised into four groups, which are high (H), medium (M), low (L) and potential (P) security vulnerabilities similar to Councils A and B. The vulnerability analysis was successfully conducted on the email server. Full details of the vulnerability testing results are provided in Appendix C6.

6.3.3.4 Testing stage 3: Identified risk issues

The identified risk issues of Testing stage 3 for the council's email system are described as follows.

- ***Risk 1: System information policy results for the email server***

The system information policy guidelines were not adhered to in parts, which can lead to a potential risk to the email server of Council C. The policy security measures not followed were the password, security auditing and services policies.

- ***Risk 2: System patching status results for the email server***

Both GFI LANguard and NMAP scanning tools were used to conduct the testing analysis of Council C's email server. There was one missing service pack and two missing patches which may create a security vulnerability to the council's email server. See Appendix C4 for full details.

- ***Risk 3: Unnecessary opened ports on the email server***

It was found that there were 24 opened TCP ports which include the unnecessarily opened ports identified on the email server. Some of these opened TCP ports can be a source of potential security risks to the email server.

See Table 6.5 for more a total numbers of opened TCP and UDP ports of the council's email server. Furthermore, Appendix C5 provides full details of the overall opened TCP and UDP ports as well as the possible mitigation recommendations.

Table 6.5 *List of the number of open TCP and UDP ports on the email server*

Server name	**Opened TCP ports**	**Opened UDP port**	**Comment**
Email server	24	1	Refer to Appendix C5

- ***Risk 4: Vulnerabilities found on the email server***

There were nine low and two potential risk category issues uncovered on the email server. For example, there were unnecessary TCP ports left opened such as POP3 and IMAP4 which may pose potential risks to the email server of the council.

Table 6.6 presents the total number of vulnerabilities found on the council's email server. See Appendix C6 for full details of the identified risk issues and the possible mitigation recommendations.

Table 6.6 *The overall of Council C's email server – vulnerabilities*

Server name	**H**	**M**	**L**	**P**	**Overall vulnerability level**	**Comment**
Email server	0	0	9	2	Medium (5/10)	Refer to Appendix C6

6.3.4 Testing stage 4: Spoofing testing and vendor security benchmark email server auditing

Two testing steps were undertaken; the email system spoofing testing and specific vendor security benchmark auditing of the MS Exchange 2007 on the council's email server are included in this stage.

6.3.4.1 Email system spoofing testing results

Both the OSSTMM and CIS templates were successfully used for the email system spoofing testing and specific vendor security benchmark auditing (MS Exchange 2007) respectively on Council C's email server. A number of identified risk issues were uncovered on the email server.

In addition, egression testing similar to Councils A and B was successfully carried out on the email system of Council C. The egression testing result and recommendation is detailed in Table 6.7.

Table 6.7 *Test egression result and recommendation – Council C's email server*

Testing technique	**Purpose**	**Result**	**Recommendation**
Sending an email from one internal address to both internal and external addresses using an external, a third-party POP server.	To test egression	Unsuccessful	Unsuccessful

6.3.4.2 Specific email security vendor auditing results

The auditing checklist in this section was adapted from the CIS – Exchange 2007 for Windows Server 2003 Version 1.0 in order to suit Council C's email system in the same manner as both Councils A and B.

Council C's email server was not configured for the Edge Transport server and the Unified Messaging server roles. Therefore, the Edge Transport server and the Unified Messaging server roles are not included in the overall modified checklist auditing tables.

6.3.4.3 Testing stage 4: Identified risk issues

The identified risk issues for the email spoofing, the Mailbox server, the Hub Transport server and the CAS roles of Council C's email server are explains as follows.

- ***Risk 1: The email server allowed relaying***

The email server may cause potential risks to spoofing attacks internally due to the fact that the email server allows emails to be sent from both internal and external addresses to any internal email addresses within Council C.

- ***Risk 2: The Mailbox server role***

Council C's Mailbox server role had one mailbox called GAIA which was stored at two different locations which were the Private Mailbox Store 1 and the Private Mailbox Store 2. A number of mis-configurations were uncovered on the Mailbox server role of the council's email server. For example the "restrict max recipients" option was set to unlimited. This particular configuration setting may cause the possibility of unnecessary network traffic which may affect the council's network performance. It may also be a potential risk to email flooding attacks. See Table 6.28 for more details.

- ***Risk 3: The Hub Transport server role***

Council C's Hub Transport server role has three groups which are the default GAIA, the application server using GAIA as a relay server and the client GAIA. As per industry best practice recommendations by CIS (2007), there were some misconfigurations or default configurations identified which should be reconfigured in order to increase the security of the email server. See Table 6.29 for more details.

- ***Risk 4: The CAS role***

The CAS role has one default group which has some mis-configurations, for example the "require ActiveSync password" and the "ActiveSync password expiration" options were disabled (unchecked). These particular mis-configurations may lead to the possibility of potential risk to the email server from authentication vulnerabilities. See Table 6.30 for more details.

6.3.5 Testing stage 5: The email system security policy review

There was no existing general and technical email policies apart from an acceptable use of computing and communications facilities policy (see Appendix C39) at Council C similar to both Councils A and B. Consequently, there were no policy and procedure guidelines for the council's IT operational staff.

6.3.5.1 Testing stage 5: Identified risk issues

The lack of a specific email system security policy can create a general cause of potential risk to the council's email and other ICT related systems. These potential risks are the possible interruption and misuse of the email services similar to both Councils A and B. See previous discussion in Section 4.3.5.1.

- ***Risk 1: Interruption of the email service***

Similarly to both Councils A and B, the lack of an email technical security policy may be a source of potential interruption to the council's email server as well as its related system.

- ***Risk 2: Misuse of the email service***

The lack of an email technical security guideline at the council may create a cause of potential risks such as allowing internal mail relaying and unauthorised access to the council's staff. See previous discussion in Chapter 4 for more details.

6.4 Council C's online web system results

Council C's online web system, including the static web, the CMS and the online payment systems, was audited and tested for the architecture, the intrusion detection, the device configurations, the vulnerabilities of all the online web system servers, the vendor security benchmark auditing on the backend database server and the online web system security policy review. The following sections depict all the results of these testings in detail.

6.4.1 Testing stage 1: Network surveying

This network surveying stage involved making an audit of the online web system architecture together with the networking devices such as the firewalls and the switch. The following network specifications and policy documents were collected:

- The overall network diagram for the Internet link, the DMZ infrastructure, the LAN and the WAN connectivity;
- The firewall device specification and the ACL codes related to Council C's online web system;
- The IDS/IPS, the DMZ switch specifications and configuration codes related to council's online web system; and
- The summary of online web system servers (the DMZ web server, the frontend CMS and the backend CMS servers) specifications and the online payment system servers (the frontend web, the application and the backend database servers) specifications summary.

The overall summary specifications of Council C's online web system devices (the static web system, the CMS web system and the payment system) are described in the following sections.

6.4.1.1 The static web system devices

As previously mentioned the static web system consists of a single web server which is the CoC-DMZ-Web server.

6.4.1.1.1 The CoC-DMZ-Web server

The CoC-DMZ-Web server is located in the DMZ area in order to reduce any potential risks that may arise from attackers. This web server presents Council C's specific information via static webpages to its residents and others.

The volunteer website (www.coc.volunteers.com.au) is an example of the council's specific information concerning its community. The CoC-DMZ-Web server specifications are summarised in Table 6.8.

Table 6.8 *A summary of the CoC-DMZ-Web server specifications*

Attributes	**Details**
Name	CoC-DMZ-Web (coc-dmz-web.coc.wa.gov.au)
Web server software	MS IIS web server 6.0
Application software	MS SQL Server 2000 8.00.194
OS	MS Windows Server 2003 with service pack 2
Hardware	HP physical server, 4GB Ram, hard disk size total 284 GB
IP address	A.B.C.181/28

6.4.1.2 The CMS web system devices

As previously discussed in Section 6.2.4.2.2 the CMS web system consists of two servers which are the CoC-DMZ-CMS and the CoC-CMS servers.

6.4.1.2.1 The frontend CMS server

The CoC-DMZ-CMS server served as a frontend CMS web server. The summary specifications of the server are described in the following table.

Table 6.9 *A summary of the frontend CMS web server specifications*

Attributes	**Details**
Name	CoC-DMZ-CMS (www.coc.wa.gov.au)
Web server software	MS IIS web server 7.0
Application software	Sophos
OS	MS Windows Server 2008 with service pack 2
Hardware	HP physical server
IP address	A.B.C.186/28

6.4.1.2.2 The CMS management server

The CoC-CMS server acts as the council's backend CMS management server. The summary specifications of the server are displayed in Table 6.10.

Table 6.10 *A summary of the backend CMS server specifications*

Attributes	**Details**
Name	CoC-CMS (CoC-CMS.coc.wa.gov.au)
Web server software	MS IIS web server 7.0
Application software	Sophos
OS	MS Windows Server 2008 x64
Hardware	VMware, virtual memory 7.5 GB, free virtual memory 5.85 GB
IP address	10.1.15.184/8

6.4.1.3 The online payment system devices

Council C's online payment servers (the frontend web, the application and the backend database servers) are summarised and briefly described as follows.

6.4.1.3.1 The frontend web server

The current frontend web server (the Epathweb) acts as application logic and is located in the DMZ area. It provides the frontline interface to the client web browser. Council C's residents or others can access the frontend web server via the website https://secure.coc.com/epathway using their registered usernames and passwords for applications. Either of or a combination of a valid assessment, invoice and payment numbers are required for rate, infringement, registration and application payments. Table 6.11 summarises the frontend web server specifications.

Table 6.11 *A summary of the frontend web server (the Epathweb) specifications*

Attributes	**Details**
Name	Epathweb (epathweb.coc.wa.gov.au)
Web server software	MS IIS web server 6.0
Application software	Epathweb, MS SQL Server 2005 9.00.4035 service pack 3, Sophos
OS	MS Windows Server 2003 service pack 2
Hardware	HP (H343LGP), 1.5 GB RAM
IP address	A.B.C.179

6.4.1.3.2 The application server

The application server (the Epathway) operates as a middle tier application server which interacts with both the frontend DMZ web server as well as the backend database server. It is located in the council's internal network and performs all necessary commands, calculations and SQL queries of the data from the backend database server. Table 6.12 summarises the council's application server specifications.

Table 6.12 *A summary of the application server (the Epathway) specifications*

Attributes	**Details**
Name	Epathway (epathway.coc.wa.gov.au)
Web server software	MS IIS web server 6.0
Application software	Epathway
OS	MS Windows Server 2003 service pack 2
Hardware	VMware, virtual memory 3.86 GB, free virtual memory 3.22 GB
IP address	10.1.15.166/8

6.4.1.3.3 The backend database server

The backend database server (the Pathway) is located within the council's internal network. It has the Pathway database application software running in conjunction with a MS SQL database Server 2005 application. The Pathway server operates as a backend database server which keeps all the necessary and important information such as usernames, passwords and street addresses.

However, any sensitive user information such as credit card numbers and expiry dates are not recorded in the database table. Table 6.13 presents more specification details of the council's backend database server.

Table 6.13 *A summary of the backend database server (the Pathway) specifications*

Attributes	**Details**
Name	Pathway (pathway.coc.wa.gov.au)
Web server software	MS IIS web server 6.0
Application software	Pathway, MS SQL Server 2005 9.00.4035 service pack 3, Sophos
OS	MS Windows Server 2003 service pack 2
Hardware	VMware, virtual memory 7.34 GB, free virtual memory 5.02 GB
IP address	10.1.15.162/8

6.4.1.4 Testing stage 1: Identified risk issues

The identified risk issues of testing stage 1 for Council C's online payment system are described in the following sections.

- ***Risk 1: The online payment system***

As previously mentioned the Epathway application server is located within the council's internal network and it has the same subnet or IP address range as the Pathway backend database server as well as other internal servers. This may be a potential risk to the council's backend database and other internal servers.

In case of the Epathweb frontend web server, which is located in the DMZ area being compromised, the attacks may carry on through the Epathway application server. This is due to the fact that the Epathway application server has direct communication (same subnet) with the Epathweb frontend web server.

6.4.2 Testing stage 2: The infrastructure of the online web system – Internet border router, IDS/IPS, firewalls and switch reviews

Testing stage 2 consists of the device and software configuration codes for the Internet border router, the switches, the firewalls, the IDS and the IPS.

6.4.2.1 Internet border router configuration codes data collection and reviews

As previously mentioned, there is no Internet border router being used at the council. The overall recommendations of an Internet border router were also previously discussed in Section 6.3.2.1. The emphasis in this section is on suggesting appropriate Internet border router's ACL codes which relate specifically to the online web system of the council.

6.4.2.2 IDS/IPS configuration codes data collection and reviews

Each of the two currently operating firewalls has a built-in IPS engine. This engine is being used to provide deep inspection of all Council C's internetwork traffic including protocol anomaly detection, stateful protocol signatures and IPS/DI attack pattern obfuscation as mentioned earlier in Section 6.5.2.2.

In addition, both HTTP and HTTPS protocols are inspected in real-time. However, several risk issues were uncovered related to the IPS during the review process for both the firewall devices. For example there was no IPS inspection of the DNS traffic.

6.4.2.3 Firewall configuration codes data collection and reviews

This section is separated into three groups which are the static web (the CoC-DMZ-Web server), the CMS web (the CoC-DMZ-CMS and CoC-CMS servers) and the online payment (the Epathweb, the Epathway and the Pathway servers) systems. For more details of the council's Internet firewalls specifications see Section 6.3.2.3.

A summary of all the firewall configuration codes related to the online static web system server (the CoC-DMZ-Web) is included in Appendix C7. The CoC-DMZ-Web server is used to communicate with the internal DNS server via a DNS port. It can also be used to communicate with any other device via the TCP port 2005. On the other hand, the firewall system allows any devices access to the CoC-DMZ-Web server via an IP (any) port. Currently, the IT operational staffs remotely manage the CoC-DMZ-Web server via TCP port 6502.

Council C's CMS web system consisted of the frontend web CMS (the CoC-DMZ-CMS) and the CMS management (the CoC-CMS) servers as previously mentioned. The summary of the firewall configuration codes with respect to both the CMS web servers are provided in Appendix C8. In addition, a related firewall configuration code setting of the CMS web system was uncovered, which can be a cause of potential risk to the council's CMS web system.

In terms of the online payment system, Pathway is the application software which is currently being used for Council C's online payment system similar to Council A. As previously mentioned in Section 6.2.4.2.3, Council C's online payment system consists of three servers which are the frontend web server (the Epathweb), the application server (the Epathway) and the backend database server (the Pathway).

The council's online payment system also uses the reverse proxy server (ISA01) as a network traffic screener to filter incoming protocol (all IP) which is forwarded from the Epathweb server to the Epathway server. The summary of the firewall codes with respect to the three online payment system servers are presented in Appendix C9.

6.4.2.4 Switch configuration codes data collection and reviews

Council C has only one switch which provides network communication and connectivity between the Internet connection (ISP), the firewalls, the DMZ servers and the council's internal network as previously mentioned in Section 6.3.2.4. The switch is also a core switch which interconnects all of Council C's Intermediate Distribution Frame (IDF) and servers. Accordingly, low level details on switch ports and VLANs including its connectivity for the council's online web system are presented in Figure 6.6.

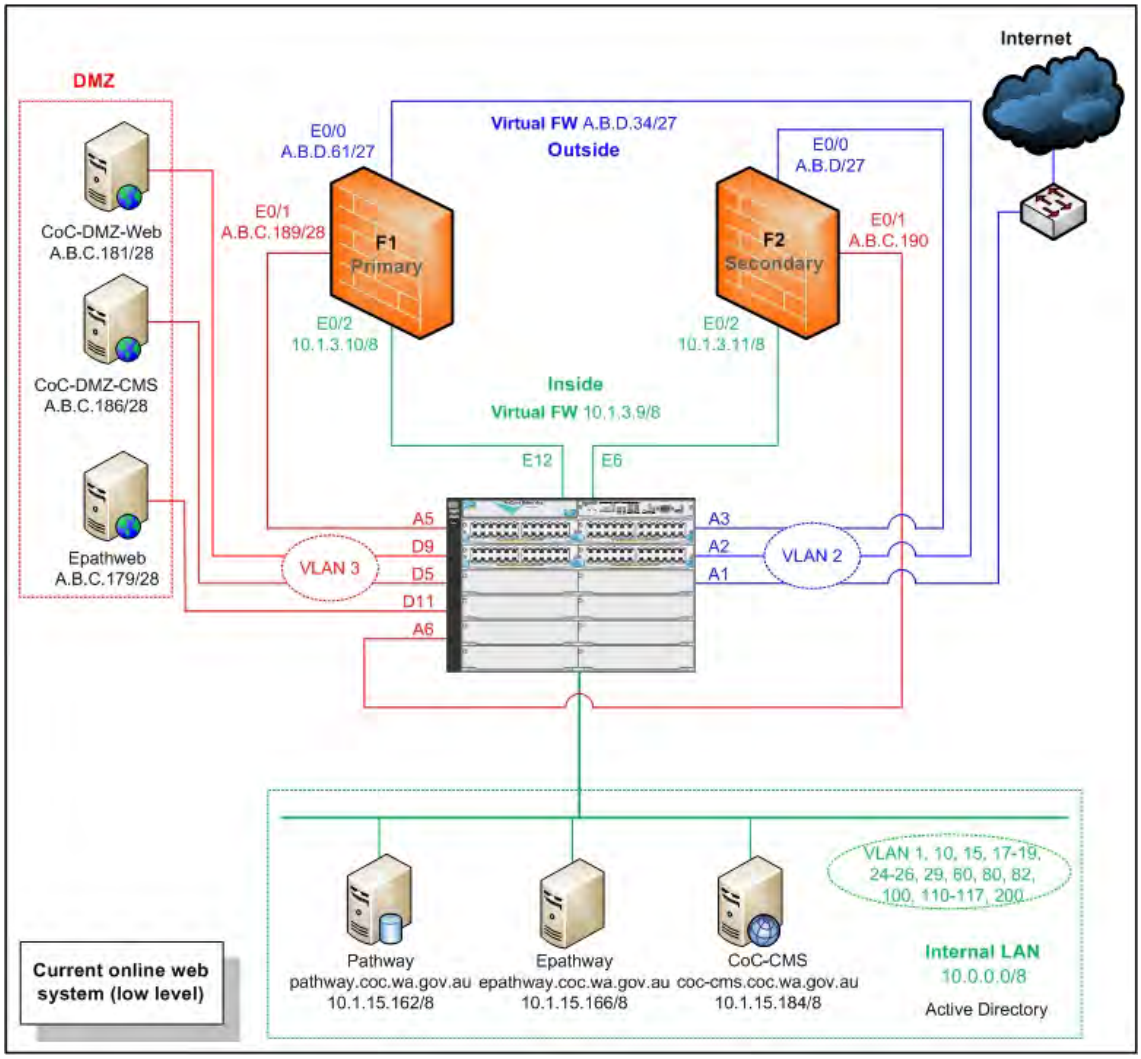

Figure 6.6. A current low level network diagram of the online web system for Council C

6.4.2.5 Testing stage 2: Identified risk issues

The identified risk issues for the infrastructure of the online web system (Internet border router, the IDS/IPS, the firewall and the switches) of Council C are detailed in the following sections.

- ***Risk 1: No Internet border router in place***

See Section 6.3.2.5 for more details.

- ***Risk 2: No IDS/IPS inspect on the DNS traffic***

Currently, the council's DMZ online web servers communicate with the council's internal DNS server via a DNS service port. This may be considered as a cause of potential risk to DNS spoofing and DNS cache poisoning attacks.

- ***Risk 3: The static web system: Unused firewall rules***

Currently, there are a number of unused firewall rules related to the council's static web system, which are TCP port 2005 as well as Appendix C7: Policy numbers 28 and 29. As per best practice recommendations to standard firewall configurations, these firewall rules should be removed.

- ***Risk 4: The static web system: Inadequate DNS traffic not inspected***

The current firewall rule (see Appendix C7: Policy number 27) permits UDP: DNS network traffic from the council's DMZ network to the two internal DNS servers which are located in the council's internal network. The two DNS servers also act as domain controllers (primary and secondary).

This can be a cause of potential risk to DNS attacks such as DNS cache poisoning, DNS amplification and reflection attacks which may lead to DoS or DDoS attack resulting in an interruption to the internal network of the council (Cisco, n.d.-a).

- ***Risk 5: The static web system: Permits IP from the CoC-DMZ-Web to the specific external network***

The current firewall rule (see Appendix C7: Policy number 30) allows the CoC-DMZ-Web server to access the specific external network (Webexternal) via IP port (any TCP or UDP ports).

This can be a cause of potential risk in the case of the static web server being compromised and controlled by an intruder to use as a proxy site from which attacks against the specific external network can be launched. This inadequate configuration can result in a bad reputation for the council as an easily compromisable site.

- ***Risk 6: The static web system: Allows IP from the CoC-DMZ-Web to the specific external network***

The current firewall rule (see Appendix C7: Policy number 31) permits the CoC-DMZ-Web server to access the specific external network (Nearmapserver) via IP port. This configuration can cause a potential risk to the specific external network.

- ***Risk 7: The static web system: Allows IP from the internal network to the DMZ network***

The existing firewall rule (see Appendix C7: Policy number 32) allows the council's internal network to access the DMZ network via any protocols (IP). This configuration can be a cause of potential risk as anyone from the council's internal (inside) network has the ability to access the council's DMZ network via any type of protocol. Therefore, internal attackers can utilise a variety of tools to compromise or gain knowledge of the council's DMZ network information.

- ***Risk 8: The CMS web system: DNS traffic not inspected***

Similar to the Risk 4, the current firewall rule permits UDP: DNS network traffic from the DMZ network to the two internal DNS servers. Furthermore, the CoC-DMZ-CMS server is required to obtain DNS information from the internal DNS servers via the UDP: DNS port. This basic configuration can cause a potential risk of DNS poisoning attacks.

- ***Risk 9: The CMS web system: Allows IP from the internal network to the DMZ network***

The firewall rule permits any devices on the council's internal network to access the DMZ network via any protocol ports (IP). This can be a cause of potential risk of unauthorised access from the internal network against all the DMZ resident devices.

- ***Risk 10: The online payment system: Mapping a whole destination subnet***

There was a firewall rule which mapped the whole class C subnet of the external A.B.C.0 network to the name "Commweb01" (see Appendix C9: Policy number 4). As per discussion with the system administrator, the requirement is specific to a few hosts.

- ***Risk 11: The online payment system: No logging on both HTTP and HTTPS traffics***

The current firewall rule (see Appendix C9: Policy number 5) allows both HTTP and HTTPS traffic without the logging feature from the external (outside) network to the frontend web server or the Epathweb (A.B.C.179) which is located in the council's DMZ network.

- ***Risk 12: The online payment system: Allows IP traffic from the Epathweb to the Epathway***

The current firewall rule (see Appendix C9: Policy number 6) allows all traffic protocols (IP) from the Epathweb frontend web server to the Epathway application server (10.1.15.166) via the council's reverse proxy server (ISA01). This configuration can cause a potential risk to the council's online payment system allowing an attacker direct access to the other DMZ servers of the council, should the Epathweb frontend web server get compromised.

- ***Risk 13: The online payment system: Allows HTTP traffic from the Epathweb to the external gateway payment service***

The current firewall rule (see Appendix C9: Policy number 7) allows both HTTP and HTTPS from the Epathweb frontend web server to the external gateway payment service (Commweb01). As per discussion with the system administrator, the permission to allow HTTP traffic was not required.

- ***Risk 14: The online payment system: DNS traffic not inspected***

The current firewall rule allows any device in the council's DMZ including the Epathweb frontend web server to communicate with the internal DNS server via the UDP: DNS port (see Appendix C9: Policy number 8). This rule can cause a potential risk to DNS poisoning attacks. See previously mentioned in Section 6.6.2.3 for more details.

- ***Risk 15: Overall inadequate switch code security configurations***

This point has been previously explained in Section 6.3.2.5: Risk 7.

6.4.3 Testing stage 3: Services and system identification, port scanning, vulnerability testing and results

The testing techniques in this Testing stage 3 were the same as carried out for Councils A and B. Both NMAP and GFI LANguard were used in all three testing steps (services and system identification, port scanning and vulnerability testings) for Council C's online web system (including the static, the CMS and the online payment web systems) network scanning.

6.4.3.1 Services and system identification results

The overall results of the services and system identifications of the six servers which were the CoC-DMZ-Web, the CoC-DMZ-CMS, the CoC-CMS, the Epathweb, the Epathway and the Pathway are summarised in Appendices C12, C13, C14, C15, C16, C17, C18 and C19. Furthermore, there were inadequate settings on password and security auditing policies on all the six servers.

6.4.3.2 Port scanning results

Similar to both Councils A and B, both NMAP and GFI LANguard network scanning tools were used to test the council's online web system servers. There were unnecessary TCP and UDP ports discovered in all the six servers. See the overall results in Appendices C20, C21, C22, C23, C24 and C25.

6.4.3.3 Vulnerability testing results

The same techniques as described in Section 6.3.3.3 were used in this vulnerability testing phase. There were vulnerabilities identified on all the six online web system servers which can lead to potential failures or interruptions to the council's online web system.

6.4.3.4 Testing stage 3: Identified risk issues

The identified risk issues of Testing stage 3 for Council C's online web system are explained as follows.

- ***Risk 1: System information policy results for all the six servers***

Council C's MS Windows current configuration settings for the six online web servers were lacking in that some services were missing and there were inadequate settings on password and security auditing policies. These inadequate settings can cause potential risks and create possible vulnerabilities to the council's online web system.

- ***Risk 2: System patching status results for all the six servers***

There were no missing service packs and patches on the CoC-CMS server. Furthermore, there were no service packs and system patching results for the CoC-DMZ-CMS as these were unobtainable due to the fact that access was denied to the server's system service and identification status.

In addition, there were a number of missing service packs and patches on the other four servers which can be a source of potential risks to the council, particularly to the Pathway server which holds the council's client database information.

- ***Risk 3: Unnecessary opened ports on all the six servers***

On the CoC-DMZ-CMS server, there were 24 TCP and two opened UDP ports which include unnecessary service ports such as FTP, MS-SQL and POP3 service ports which can cause a potential risk to the CoC-DMZ-CMS server.

Furthermore, both the CoC-DMZ-Web and the Epathweb servers had unnecessarily opened TCP ports over 500 and 600 respectively. These opened TCP ports on the Epathweb server include a majority number of unnecessarily opened TCP ports such as Edonkey, FTP, finger, login, shell, POP2, POP3, printer and whois. These opened ports can lead to possible unauthorised access to the Epathweb server, misuse of its services and create a potential risk to the council's internal network.

The overall opened TCP and UDP ports for all the six servers are provided in Table 6.14. Furthermore, Appendices C20, C21, C22, C23, C24 and C25 present all the opened TCP and UDP ports as well as the possible mitigation recommendations for the six servers respectively.

Table 6.14 *Overall opened TCP and UDP service ports of all the six servers*

Server name	**Opened TCP ports**	**Opened UDP ports**	**Comment**
CoC-DMZ-Web	528	12	Refer to Appendix C20
CoC-DMZ-CMS	24	2	Refer to Appendix C21
CoC-CMS	13	1	Refer to Appendix C22
Epathweb	653	10	Refer to Appendix C23
Epathway	22	6	Refer to Appendix C24
Pathway	21	7	Refer to Appendix C25

- ***Risk 4: Vulnerabilities found on all the six servers***

As previously mentioned, there were vulnerabilities identified on all the six online web system servers. For example, there were low and potential security vulnerabilities discovered on the CoC-DMZ-CMS and the CoC-CMS servers, such as the fact that FTP and POP3 services were enabled. The remote code execution vulnerability in MS DirectShow was uncovered on the Pathway server.

The overall vulnerability testing analysis and possible mitigation recommendations of the six servers are summarised in Table 6.15. See Appendices C26, C27, C28, C29, C30 and C31 for more details of the identified risk issues and the possible mitigation recommendations for all the six online web system servers respectively.

Table 6.15 *Overall vulnerability of the three servers of Council C's online web systems*

Server name	**H**	**M**	**L**	**P**	**Overall vulnerability level**	**Comment**
CoC-DMZ-Web	7	0	10	5	High (10/10)	Refer to Appendix C26
CoC-DMZ-CMS	0	0	3	3	Low (3/10)	Refer to Appendix C27
CoC-CMS	0	0	5	1	Low (3/10)	Refer to Appendix C28
Epathweb	8	1	8	4	High (10/10)	Refer to Appendix C29
Epathway	3	0	7	2	High (10/10)	Refer to Appendix C30
Pathway	3	0	6	3	High (10/10)	Refer to Appendix C31

6.4.4 Testing stage 4: Vendor security: Database security benchmark auditing

Similar to both Councils A and B, this fourth stage testing has one testing step which is the database security benchmark auditing on the council's online payment backend database server (the Pathway).

6.4.4.1 Database security benchmark results

Similar to both Councils A and B, Council C's online payment backend database server runs MS SQL Server 2005 as a database application. The database application is also running, together with the Pathway application. Both applications are currently running on the Epathway server. In this database security benchmark auditing stage, the Security Configuration Benchmark for Microsoft SQL Server 2005 version 1.2.0 January 12th, 2010 from CIS was used as a prime benchmark auditing tool.

As previously mentioned in Sections 4.4.4.1 and 5.4.4.1, the CIS benchmark auditing tool is categorised into nine groups. However, this database security audit was conducted on seven groups only, which were one to six and group nine. Group seven (replication) was not audited as there was no replication implemented in the council's database system. Furthermore, group eight (application development best practices) was also not audited as the council's IT operational staff has no responsibility for developing or editing the council's online webpage application.

6.4.4.2 Testing stage 4: Identified risk issues

The following sections describe the identified risk issues for the configuration of the MS SQL 2005 database on the council's backend server.

- ***Risk 1: Inadequate configuration for the database application of the backend database server***

There were some security issues uncovered from all the seven tested categories. These security issues can possibly cause interruptions to the council's Pathway backend database server. Table 6.16 displays the overall security issues uncovered (unsatisfactory) including risk rating of Council C's Pathway backend database server based on the seven category groups.

The overall details of all the findings (satisfactory and unsatisfactory) and the possible mitigation recommendations are provided in Appendices C32, C33, C34, C35, C36, C37 and C38.

Table 6.16 *The overall risks of the seven audited categories of the Pathway backend database server*

Category no.	**Risks (H)**	**Risks (M)**	**Risks (L)**	**Risks (P)**	**Comments**
1) OS and network specification configuration	1	4	9	4	Refers to Appendix C32
2) SQL server installation and patches	2	3	0	1	Refers to Appendix C33
3) SQL server settings	1	0	3	10	Refers to Appendix C34
4) Access controls	1	4	1		Refers to Appendix C35
5) Auditing and logging	0	0	0	43	Refers to Appendix C36
6) Backup and disaster recovery procedures	2	1	3	1	Refers to Appendix C37
9) Surface area configuration tool	0	0	2	0	Refers to Appendix C38

6.4.5 Testing stage 5: The online web system security policy review

This final testing stage consists of the review of the security policy for Council C's online web system which includes the static web, the CMS and the online payment systems. As previously discussed in Section 6.3.5, there were no existing general and technical information security policies at Council C, apart from an acceptable use of computing and communications facilities policy (see Appendix C39).

6.4.5.1 Testing stage 5: Identified risk issues

This lack of both general and technical information security policies can be considered as a cause of potential risks in terms of possible interruptions to Council C's online web services. Similar to both Councils A and B, the cause of these risks could be characterised as follows:

- Poor communication of risk; and
- Poor understanding of the risks that are in the system as a result of poor management/strategic oversight.

- ***Risk 1: Poor communication of risk***

There were some but not frequent enough discussions of ICT risk management in the weekly IT operational staff meetings (personal communications with Council C, 2010). This was due to the fact that the council's IT operational staff were often too busy managing their day to day operational tasks.

- ***Risk 2: Poor understanding of the risks that are in the system as a result of poor management/strategic oversight***

This was due to the fact that some of Council C's IT operational staff have a lack of technical knowledge of IT security. For example, there were some inadequate configurations on the firewalls and the core switch as a result of a lack of specific knowledge with regard to the device configuration.

6.5 Analysis and discussion

The details of analysis and discussion on both Council C's email and online web systems (the static web system, the CMS web system and the online payment system) are described in the following sections.

6.5.1 Analysis

The analyses of both Council C's email and online web systems are divided into two sections which are the email and the online web systems.

6.5.1.1 Council C's email system analysis – possible mitigations

The possible mitigation recommendations for the identified issues for Testing stages 1 to 5 of the council's email system are explained in the following sections.

6.5.1.1.1 Testing stage 1: Possible mitigation

- ***Risk 1***

In order to mitigate this type of potential risk, Council C should deploy an extra dedicated server to only perform a CAS role. This additional server would also reduce the load on the current MS Exchange server.

Similarly to both Councils A and B, a high-bandwidth (Gigabit) connection is strongly recommended for the connection between the CAS and the Mailbox server (Microsoft Exchange Documentation Team, 2009). Summary specifications of a new dedicated CAS are provided in Table 6.17.

Table 6.17 *A summary recommendations of the new CAS specifications*

Attributes	**Details**
Email application software	MS Exchange 2007 with service pack 1
OS	MS Windows Server 2008 Enterprise Edition with service pack 1
Hardware	VMware or equivalent 8 GB RAM, hard disks C: 20 GB, e: 100 GB
MS Exchange 2007 role	CAS
MS Exchange support	MS OWA, MS Outlook Anywhere, MS ActiveSync
TCP/IP protocols	HTTPS, RPC, LDAP
IP network	Different subnet with other email servers (isolate)
Network connection	Gigabit link between Client Access and Mailbox servers
ACL	Permits only allowed or required protocols
Other software	Virus protection software for server

- ***Risk 2***

The new dedicated CAS should be configured to a different subnetwork in order to further minimise and control any other potential risks that may occur. Any unwanted network traffic which allows communication between both the current email server and the new dedicated CAS should be filtered. An ACL is an example of a filtering technique that could be used to control the Exchange email related protocols.

Figure 6.7 illustrates all the devices connectivity including the recommended CAS in a high level network diagram.

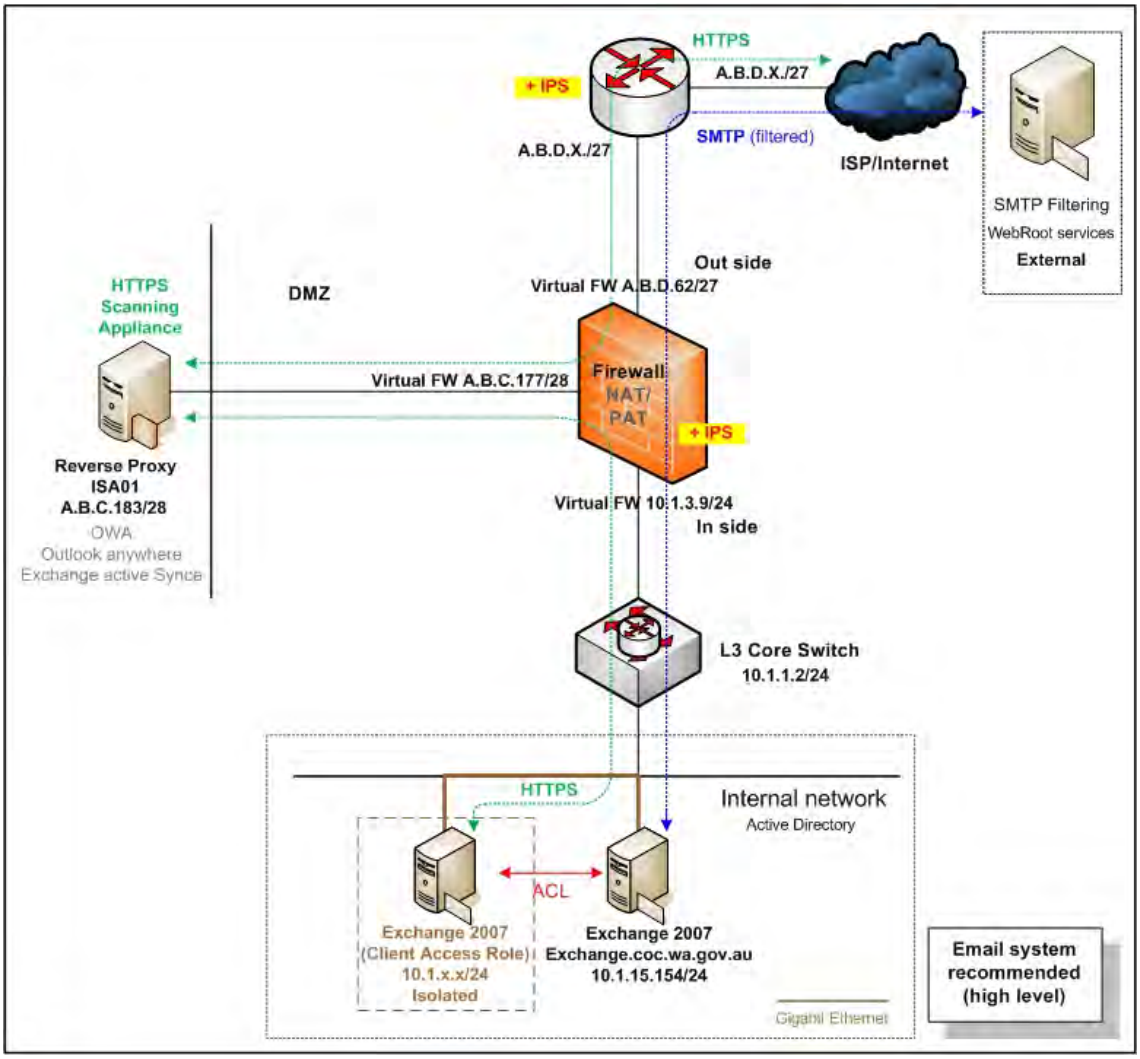

Figure 6.7. A recommended MS Exchange Server 2007 architecture with an extra MS Exchange 2007 server role (CAS role)

- ***Risk 3***

The use of either the certificate or token authentication methods will offer a better security mechanism than basic authentication. Token authentication is strongly recommended as the council already has an existing token authentication system in place. Therefore, the council should consider incorporating the email system authentication with the existing token authentication system. Although this option is a cost saving as opposed to purchasing a new server and application software, more tokens/dongles and software licenses will be required.

In addition, implementing the token authentication method may provide an additional layer of authentication to the email system of the council. Table 6.18 summarises the options and recommendations for improving the client access security authentication methods for Council C.

- ***Risk 4***

The mitigation recommendation is the same as for Council B, in that NTLM authentication may be considered for use with the current SSL connection in order to provide the best possible authentication method between the clients to the email server for the council's MS Outlook Anywhere application. See Table 6.18 for more details.

Table 6.18 *Overall current and recommendations client access security methods over SSL for the email system of Council C*

Client-to-server connections	**Authentication options**	**Council C current configurations**	**Recommended authentications for Council C**
MS OWA	Basic/form-based	Form-based	Form-based
MS ActiveSync	Basic/certificate/token	Basic	Token
MS Outlook Anywhere	Basic/NTLM	Basic	NTLM

Additionally, if the council wishes to manage the in-house spam blocker appliance, then MS Forefront Security may be taken into consideration as an example of spam blocker appliance technology. This spam blocker appliance may enhance the security capability when integrated with the council's current reverse proxy server (ISA 2006).

According to Microsoft Exchange Documentation Team (2006, p. 7), "Forefront Security for Exchange server delivers comprehensive on-premise antivirus protection for Exchange Edge Transport, Hub Transport and Mailbox roles. Using a multiple-scan engine with content-filtering capabilities, Forefront Security for Exchange server offers layered protection against virus-laden messages". See Figure 6.8 for more details.

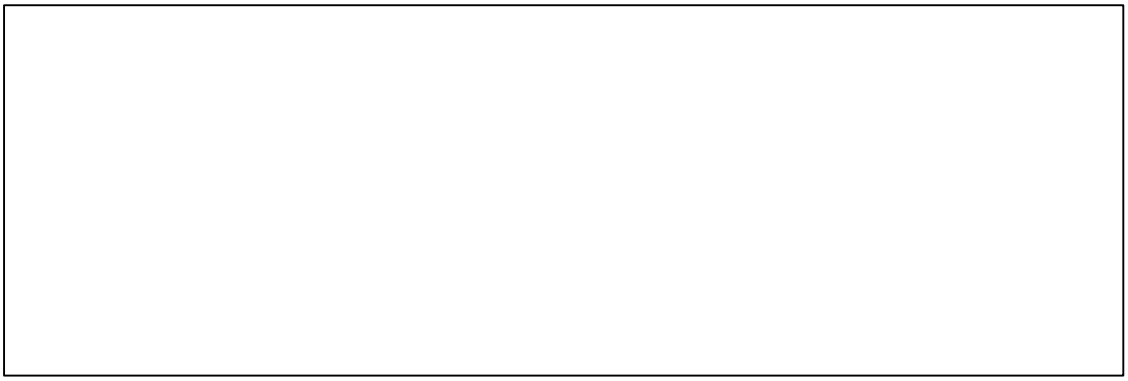

Figure 6.8. Using MS Forefront Security for MS Exchange Server 2007 for virus protection

(Source: Microsoft Exchange Documentation Team, 2006, p. 7)

6.5.1.1.2 Testing stage 2: Possible mitigation

- ***Risk 1***

Council C can enhance its internetwork performance and security by deploying an Internet border router. An Internet border router will provide a first layer of traffic filtering by only permitting addressed network traffic in and out of the council's network. This filtering function of the Internet border router can reduce the number of Internet-based worms prior to them reaching the firewall of Council C. It will also ease the load on the existing firewalls (Juniper SSG-350M security appliances).

Furthermore, the IPS feature of the Internet border router may more accurately identify, classify, and stop or block malicious traffic such as network spoofing and scanning in real-time. Table 6.19 summarises the specifications of the recommended Internet border router.

In addition, with these recommendations to the council's internetwork system structure, the council may further enhance efficiency in terms of redundancy and load balancing with the alternate Internet link using connections such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) technologies. However, more research may be required for this purpose in terms of protocols, equipment and costs.

Table 6.19 *A summary of the new Internet border router specifications*

Attributes	**Details**
Device type	Cisco 2911 or other equivalent vendor product
OS	12.4(15)T3 or later
Memory	Standard
Interfaces	3 integrated 10/100/1000 Ethernet ports (RJ-45 only)
IP addresses	A.B.D.x/27, A.B.D.x/27
Security and other features	Cisco IOS IPS, Authentication, Authorization and Accounting (AAA), IOS firewall, voice and video support

Finally, as mentioned earlier, in terms of filtering network traffic, Council C should consider tightening its ACLs when deploying an Internet border router, such as by blocking potential risky ports as well as private IP addresses.

In addition, creating each individual ACL for each individual service usage constitutes a recommended best practice for standard router configurations. Examples for the email service and the appropriate ACL recommendations are shown in Table 6.20.

Table 6.20 *Possible examples of the Internet border ACL for the email system*

Policy no.	**Rules**	**Protocol types**	**From (source)**	**To (destination)**	**Ports (service)**	**Recommendations**
1	Permit	TCP	Webroot services	The MS Exchange Server 2007	SMTP	Yes
2	Permit	TCP	Any	The ISA 2006 server	HTTPS	Yes

- ***Risk 2***

According to Juniper Networks (2009), IPS/DI features on the firewalls (Juniper SSG-350M security appliances) perform protocol anomaly detection, stateful protocol signatures and IPS/DI attack pattern obfuscation. Internet security can be increased significantly by simply enabling the IPS feature on both the existing firewalls (Juniper SSG-350M security appliances).

As previously discussed, the council's firewalls have enabled their IPS feature. Therefore, no further action is required in terms of network infrastructure for the email system. The summarised overall IDS/IPS details and possible mitigation recommendations for the council's internetwork are provided in Table 6.21.

Table 6.21 *A summary of the IDS/IPS of the council's internetwork system*

Products	**Currents**	**Recommendations**	**Descriptions**
IDS/IPS on the new Internet border router	Non-existent	Deploy an Internet border router with integrated with IPS	For blocking of any spoofing/scanning attacks and malicious traffic For reducing the load of the firewall's IPS
IPS on the firewall (DI)	Installed	No action is required	For real-time DI of all required important network traffic such as HTTPS for the purposes of blocking and preventing application-level attacks, any malicious or unwanted behaviour in real-time. See note below for more details.

- ***Risk 3***

As per discussion with the council's system administrator, Policy number 2 in Appendix C1 is unnecessary and may pose a potential risk to Council C's email system. According to the council's SMTP policy, the source of incoming SMTP traffic should only come from the Webroot services. Therefore, this rule should be removed as it is redundant.

- ***Risk 4***

As per discussion with the system administrator of Council C, the internal server (10.1.1.3) is no longer in use. Therefore, this rule can be safely removed. The removable of any unused firewall configuration codes can prevent any confusion which may arise in the future.

- ***Risk 5***

According to Appendix C2, the Policy number 14 is duplicated with the Policy number 15, and as such it can be safely removed.

- ***Risk 6***

Access to both the firewalls for administration purposes should be limited to an authorised staff member. Access to these devices via the Telnet port should be disabled as it poses a potential risk to sniffing attacks. Table 6.22 summarises the current and recommended access rules for both the firewalls.

Table 6.22 *A recommendation accessing methods summary of the firewalls*

Accessing types/from	**Current rules**	**Recommendations**	**Comments**
HTTP	Enable	Enable	Redirect to HTTPS
HTTPS	Enable	Enable	Secured web access
SSH	Disable	Enable	Provide more security as compared to Telnet
Telnet	Enable	Disable	Insecure, potential to sniffing attacks
Console	Enable	Enable	Recommended to create strong user name and password with MD5 (if applicable)
10.0.0.0 IP range	Allow	Limit IP range	Should only allow to the council's IT administrators access to the group's IP subnet

- ***Risk 7***

The council's switch codes review is presented in Table 6.23 along with the recommendations, which may feasibly mitigate such attacks against the council's core switch.

Table 6.23 *Council C's switch security audit details*

Security features	**Recommendations**
ACL applied to block unwanted devices	To do
Access to the device via HTTP is disabled	To do
Access to the device via Telnet is disabled	To do
Activate loop protection on all ports	To do
Apply appropriate log server	Satisfactory
Apply appropriate timestamps debug time	N/A
Apply appropriate timestamps log time	N/A
Apply appropriate time zone	Satisfactory

Table 6.23 *Council C's switch security audit details (continued)*

Security features	**Recommendations**
Appropriate SNMP in use	To do
Appropriate VLAN in use	Satisfactory
Best practice username and/or password in use	To do
Configure appropriate warning banner message	To do
Disable/shutdown unused switch ports	To do
Disable trunking on ports that do not need it	Satisfactory
Enable feature against ARP poisoning attacks	To do
Enable feature against ARP spoofing attacks	To do
Enable port broadcast storm control	Satisfactory
Enable port security limits MAC address to a port	To do
Ports connected to identified devices that do not support spanning-tree should be configured with BPDU filtering	To do
Ports not connected to anything yet should be configured with protection	To do
Set DTP on all ports not being used for trunking	N/A
Set strong password (MD5) for authenticating VTP message	To do
Strong password encryption (MD5) in use	To do
TFTP service is disabled	To do

- ***Risk 8***

Consequently, similar to Council B, it is recommended that two additional switches should be installed in the outside and the DMZ areas as follows:

- The outside area: A new switch to connect the two firewalls (Juniper SSG-350M security appliances) and the new Internet border router; and
- The DMZ area: A new switch to connect the two firewalls (Juniper SSG-350M security appliances) and the DMZ servers.

With this in place, the current core switch may be used solely to connect between the two firewalls (Juniper SSG-350M security appliances) and the council's internal network. The new switches recommendation details are provided in Table 6.24. Furthermore, Figure 6.9 illustrates the new switch recommendations, ports, VLANs including its connectivity.

Table 6.24 *New switches hardware and software recommendations for Council C*

Attributes	**Details**
Device location	The council's outside network area
Device type	HP 2610-24 (J9085A) OR HP 2810-24G (J9021A) switch
OS	Newest
Memory	Standard
Port	24 auto-sensing 10/100 ports (IEEE 802.3 type 10Base-T, IEEE 802.3u type 100Base-TX), 2 open mini-GBIC (SFP) slots
Operate at	Layer 2 OSI
Device location	The council's DMZ network area
Device type	HP 2810-24G (J9021A) switch
OS	Newest
Memory	Standard
Port	20 auto-sensing 10/100/1000 ports, 4 dual-personality ports - each port can be used as either an RJ-45 10/100/1000 port or an open mini-GBIC slot
Operate at	Layer 2 OSI

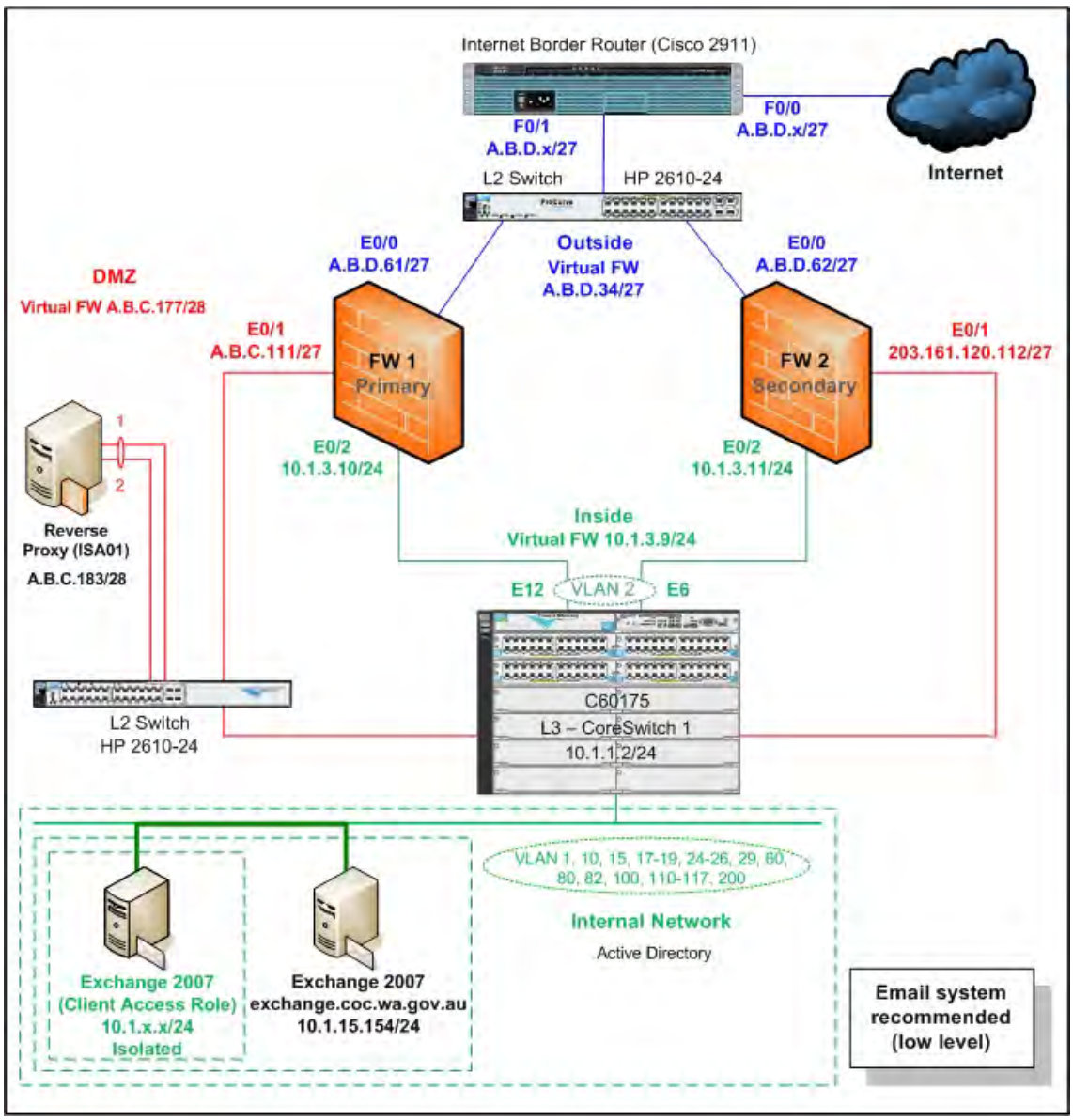

Figure 6.9. A low level network diagram of the email system for Council C with the new recommended switches

In addition, Figure 6.10 illustrates a recommended overall high level network diagram of the email system for Council C.

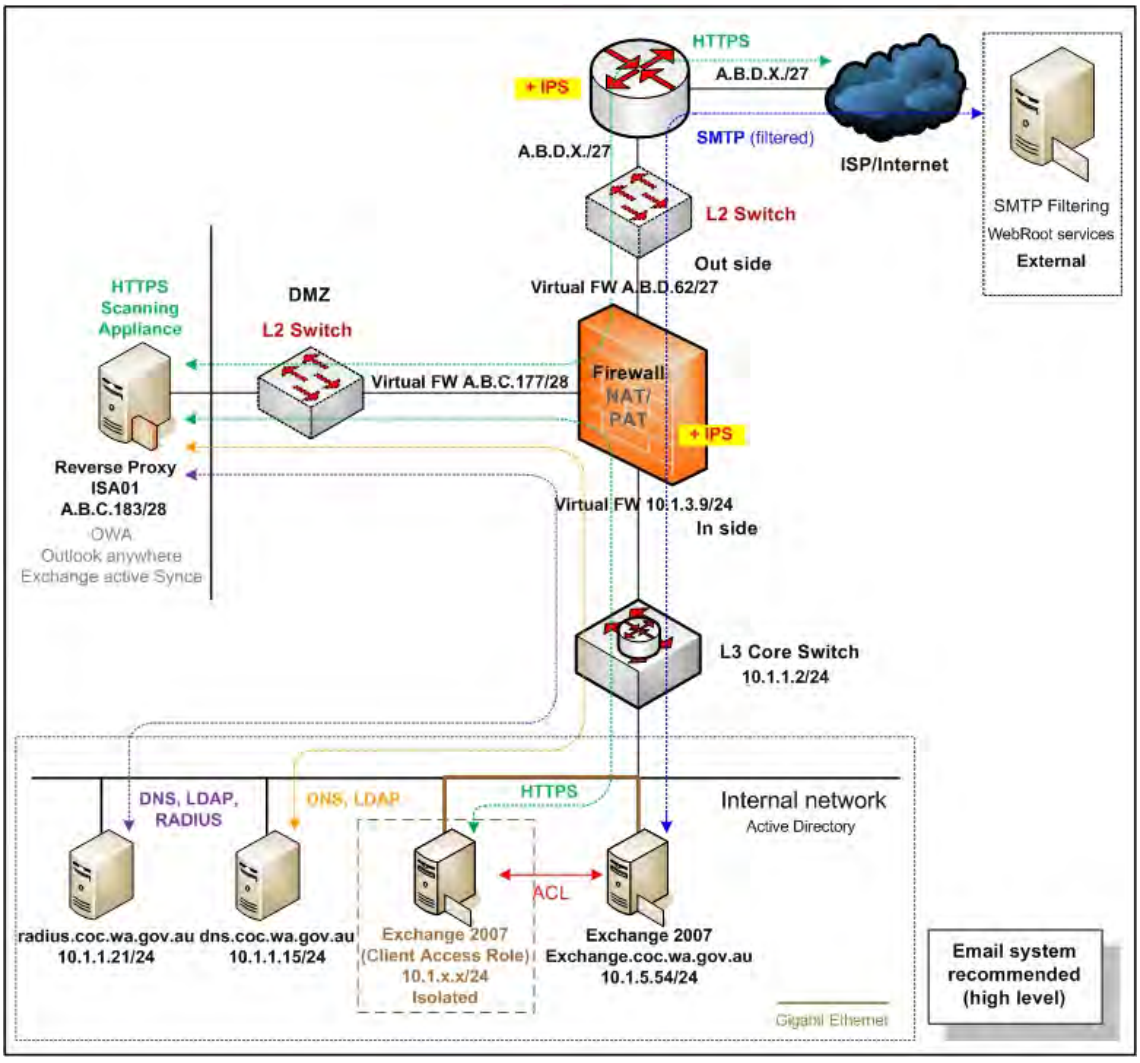

Figure 6.10. A recommended overall high level network diagram of the email system for Council C

6.5.1.1.3 Testing stage 3: Possible mitigation

- ***Risk 1***

The overall system information policy testing results of Council C's email system server are summarised in Table 6.25. Moreover, Appendix C3 provides full details of the overall system information policy testing results and recommendations of Council C's email system server.

Table 6.25 *the overall system information policy of the email server*

Server name	Password policy	Security audit policy	Comment
Email server	Unsatisfactory	Unsatisfactory	Refer to Appendix C3

- ***Risk 2***

Appendix C4 provides full details of the missing service pack and patches as well as possible mitigation recommendations for updating the email server.

- ***Risk 3***

As previously discussed, there were a total of 24 opened TCP ports including some unnecessarily opened ports. The total number of recommended open TCP ports on the email server is eight with only one open UDP port. Table 6.26 presents the total number of recommended open TCP and UDP ports on the email server.

Table 6.26 *The total number of recommended open TCP and UDP service ports on the email server*

Server name	Recommended open TCP ports	Recommended open UDP port	Comment
Email server	8	1	Refer to Appendix C5

- ***Risk 4***

Refer to Appendix C6 for full details of the identified risk issues and the possible mitigation recommendations.

6.5.1.1.4 Testing stage 4: Possible mitigation

- ***Risk 1***

Council C's email server allowed relaying of email messages for internal connectivity from both internal and external addresses to any internal email address. Table 6.27 presents the overall spoofing testing results and recommendations for the email server of Council C.

Table 6.27 *The spoofing testing results and recommendations for Council C's email server*

Testing techniques	**Purposes**	**Results**	**Recommendations**
Telnet to the email server and sending an email from one internal address to another internal address.	To test internal connectivity of the email server	Successful (allow relaying)	Should not allow email relaying See note
Sending an email from one external address to another external address using the target email server.	To test external relaying of the email server	Unsuccessful (do not allow relaying)	None
Sending an email from one internal address to an external address using the target email server.	To test internal relaying of the email server	Unsuccessful (do not allow relaying)	None
Sending an email from one external address to an internal address using the target email server.	To test email relaying of the email server	Successful (allow relaying)	Should not allow email relaying See note

Note:

Council C may block internal email relaying to the MS Exchange 2007 email server from unauthorised users by configuring the MS Exchange 2007 email server SMTP port to an alternative TCP port. The TCP port 587 is an alternative example which is recommended by Ganger (2007). This configuration will allow the Exchange client communicating with the Exchange server via TCP port 587 instead of typical SMTP port 25. Furthermore, Council C may configure both the firewalls to block their internal staff from directly accessing the email server via Telnet (TCP port 23) including SMTP (TCP port 25) ports.

- ***Risk 2***

Table 6.28 presents overall results of the auditing of the Mailbox server role of Council C's email server including the possible mitigation recommendations based on the CIS suggestions.

Table 6.28 *The overall results of auditing and recommendations for the Mailbox server role of Council C's email server*

References	**Defaults**	**Council C**	**Recommendations**
Restrict email deletion retention Private mailbox stores 1, 2	7 (days)	7, 7 (days)	7 (days)
Restrict mailbox deletion retention Private mailbox stores 1, 2	30 (days)	3, 3 (days)	30 (days)
Restrict deletion of emails or mailboxes until archival Private mailbox stores 1, 2	Unchecked	Unchecked Unchecked	Checked
Mounting of mailbox database at startup Private mailbox stores 1, 2	Unchecked	Unchecked Unchecked	Unchecked
Ensure mailbox database cannot be overwritten Private mailbox stores 1, 2	Checked	Unchecked Unchecked	Unchecked
Verify default mailbox storage limits (issue warning, prohibit send, prohibit send and receive at (KB)) Private mailbox stores 1, 2	Custom	Unassigned Unassigned	Custom
Ensure public folder database cannot be overwritten	Checked	Unchecked	Unchecked
Verify default public folder storage limits (issue warning, prohibit send, prohibit send and receive at (KB))	Custom	Unassigned	Custom
Audit public folder client access	Custom	Unassigned	Custom
Audit public folder administrative access	Custom	Unassigned	Custom
Verify proper permissions on public folder database	Custom	Unassigned	Custom
Mounting of public folder database at startup	Unchecked	Unchecked	Unchecked
Restrict deletion of emails or mailboxes until archival	Unchecked	Unchecked	Checked
Restrict email send size (mailbox identity, email contact identity, distribution group identity)		Unlimited Unlimited Unlimited	10MB 10MB 10MB
Restrict email receive size (mailbox identity, email contact identity, distribution group identity)		Unlimited Unlimited Unlimited	10MB 10MB 10MB
Restrict max recipients	5000	Unlimited	2000
Audit mailbox spam bypass settings	False	False	False
AntiSpam updates*	Disabled	Disabled	See note
Zero out deleted database pages Private mailbox stores 1, 2	False	False False	True

- ***Risk 3***

Table 6.29 presents overall results of auditing and recommendations for the Hub Transport server role of Council C's email server.

Table 6.29 *The overall results of auditing and recommendations for the Hub Transport server role of Council C's email server*

References	**Defaults**	**Council C**	**Recommendations**
Audit DNS lookup servers 1. Default GAIA 2. Relay server 3. Client GAIA	None	 Custom Custom Custom	Custom
Enable TLS for basic authentication	Unchecked	Unchecked	Checked
Restrict out of office responses	None	None	Internal only
Restrict email send size (max send size, max message size) 1. Default GAIA 2. Relay Server 3. Client GAIA	30MB 30MB	MB 30, 30 Unlimited 10, 10	10MB 10MB
Restrict email receive size (max receive size, max message size, external dsn max message attach size, internal dsn max message attach size) 1. Default GAIA 2. Relay server 3. Client GAIA	30MB 30MB 10MB 10MB	MB 30, 30, - ,- 30, 30, - ,- 30, 30, - ,-	10MB 10MB 10MB 10MB
Restrict max recipients (max recipients per message) 1. Default GAIA 2. Relay server 3. Client GAIA	5000	 5000 200 200	2000
Restrict IP range for receive connectors	None	None	Custom

- ***Risk 4***

The overall results of auditing CAS role of Council C's email server including the recommendations are presented in Table 6.30.

Table 6.30 *The overall results of auditing and recommendations for the CAS role of Council C's email server*

References	**Defaults**	**Council C**	**Recommendations**
Remove legacy web applications	Installed	Installed	Removed
Restrict web authentication methods**	See note	See note	See note
Require SSL for web applications	Checked Unchecked	Checked Checked	Checked Checked
Disable web anonymous access	Unchecked	Unchecked	Unchecked
Enable logging for default website	Checked	Checked	Checked
Enable policy for ActiveSync***	None	None	See note
Forbid ActiveSync NonProvisionable devices	Checked	Checked	Unchecked
Forbid ActiveSync simple device password	Checked	Checked	Unchecked
Disable ActiveSync WSS/UNC access (Windows file shares, sharepoint services)	Checked Checked	Checked Checked	Unchecked Unchecked
Require ActiveSync password	Unchecked	Unchecked	Checked
Require ActiveSync alphanumeric password	Unchecked	Unchecked	Checked
Require ActiveSync minimum password length	Checked, 4	Checked, 3	Checked, 8
Require ActiveSync password expiration	Unchecked	Unchecked	60
Require ActiveSync password history	0	0	5
Restrict ActiveSync attachment size	Unchecked	Unchecked Unallocated	Unchecked, 3MB
Require ActiveSync policy refresh	None	Unlimited	24.00:00:00
Restrict ActiveSync maximum password attempts	8	8	8
Require ActiveSync certificate based authentication	Ignore Client Certs	Ignore Client Certs	Require Client Certs
Require ActiveSync inactivity lockout time	Checked, 15	Checked, 15	Checked, 15
Disable Outlook Anywhere	Enabled	Enabled	Disabled

Note:

Refers to AntiSpam updates*

Council C is currently using an outside external antispam server as a combined email system. Therefore, this setting can remain as the default (disabled).

Refers to restrict web authentication methods**

As per best practice recommendations by CIS (2007), this task is to ensure that unneeded authentication methods for MS Exchange web applications should be disabled.

Refers to enable policy for ActiveSync***

The policy of ActiveSync should be enabled in order to reduce the potential risks to the MS Exchange infrastructure in case of a mobile device out of sync (failing) from the council's network (CIS, 2007). See Table 6.31 for more detail.

Table 6.31 *The overall results of auditing web authentication and access control of Council C's email server*

Council C	**Integrate**	**Digest**	**Basic**	**Passport**
Autodiscover	X		X	
Exchange			X	
Exchange Web Services (EWS)	X		X	
Exadmin			X	
Exchweb			X	
MS-Exchange-ActiveSync			X	
Offline Address Book (OAB)			X	
Outlook Web Access (OWA)			X	
Public			X	
Unified Messaging (UM)	X		X	
Recommendations	**Integrate**	**Digest**	**Basic**	**Passport**
Autodiscover	X			
Exchange	X		X	
Exchange Web Services (EWS)	X			
Exadmin	X			
Exchweb	X			
MS-Exchange-ActiveSync			X*	
Offline Address Book (OAB)			X	
Outlook Web Access (OWA)			X	
Public	X		X	
Unified Messaging (UM)	X			

6.5.1.1.5 Testing stage 5: Possible mitigation

- ***Risks 1 and 2***

In order to provide better security to the council's email system, it is strongly recommended that an ICT security policy be implemented to cover all of aspects of the council's network infrastructure, Internet border router, firewall, email and other ICT related systems.

6.5.1.2 Council C's online web system analysis – possible mitigations

Council C's online web system consists of three sub systems as previously discussed. The three sub systems are the static web system, the CMS web system and the online payment system. The following sections present the mitigation recommendations for the identified issues of all the three sub systems. Moreover, each of the mitigations described relate to the identified risk issue number.

6.5.1.2.1 Testing stage 1: Possible mitigation

- ***Risk 1***

In the interests of general best practices, it is recommended that both the application and the backend database servers be placed separately into different subnetworks or a VLAN. Furthermore, appropriate ACLs should be configured to filter or control network traffic between both the subnets. These measures can prevent or mitigate any potential network security risks such as viruses, trojans and DoS attacks.

6.5.1.2.2 Testing stage 2: Possible mitigation

- ***Risk 1***

It is recommended that an Internet border router be deployed as previously discussed on Section 6.5.1.1.2: Risk 1. Furthermore, it is also recommended to create an individual ACL for each service usage, such as permitting only HTTP traffic to the Epathweb server. Such ACL rules can restrict and allow only required access protocols to the web server. Therefore, it can minimise any potential vulnerability risks to the server.

- ***Risk 2***

Table 6.32 summarised overall IDS/IPS details and possible mitigation recommendations for Council C's internetwork system related to the online web system.

Table 6.32 *A summary of the IDS/IPS of the council's internetwork system for the online web system*

Products	**Settings**	**Recommendations**	**Descriptions**
IPS on the firewall (deep inspection) applied to HTTP and HTTPS protocols	Applied	No action is required	For real-time deep inspection of web network traffic (HTTP and HTTPS) for the purposes of blocking and preventing application-level attacks, any malicious or unwanted behaviour in real-time.
IPS on the firewall (deep inspection) applied to DNS protocol	Not applied	Apply deep inspection to DNS inbound protocol	For real-time deep inspection of DNS traffic particulary the DNS packet size from DMZ web servers to the council DNS server. This can prevent against DNS spoofing, cache poisoning, amplification or reflection attacks (Cisco, n.d.-c).

- ***Risk 3***

As per discussion with the system administrator, the TCP port 2005 and Appendix C7: Policy numbers 28 and 29 are no longer in use. Therefore, these firewall rules can be safely eliminated. The removal of unused firewall rules can prevent any potential confusion that may arise in the future to both the system and network administrators of the council.

- ***Risk 4***

This firewall rule should be incorporated with the DNS deep inspection (filter) and log feature in order to prevent any potential DNS attacks against the council's internal DNS servers (domain controllers). This DNS deep packet inspection will monitor the DNS packets (the message exchange) to ensure that both the IDS of the DNS queries and responses match (Cisco, n.d.-b). It also performs security checks on the size of the DNS packets such as checking that the maximum label length and the maximum domain name length are not longer than the DNS packet specifications (Cisco, n.d.-c).

- ***Risk 5***

As per discussion with the system administrator, this rule can be tightened by changing the allowed protocol from IP to TCP port 80 (HTTP) and TCP port 443 (HTTPS).

- ***Risk 6***

As per discussion with the system administrator, this rule can be tightened by adjusting the allowed protocol from IP to any other required TCP or UDP protocols which can be investigated by the system administrator in the future.

- ***Risk 7***

This rule opens all IP ports (all TCPs and UDPs) for the council's inside network to access its DMZ network. This can pose a potential risk to Council C's online web system. As per best practice recommendations to standard firewall configurations, this rule can be tightened by allowing the required TCP or UDP ports to specific user groups only, such as any ports for the IT administrator group, HTTP ports and HTTPS ports for normal Internet usage by the council's IT staff.

In addition, Figure 6.11 illustrates Council C's recommended static web server system including the network traffic protocols in a high level network diagram.

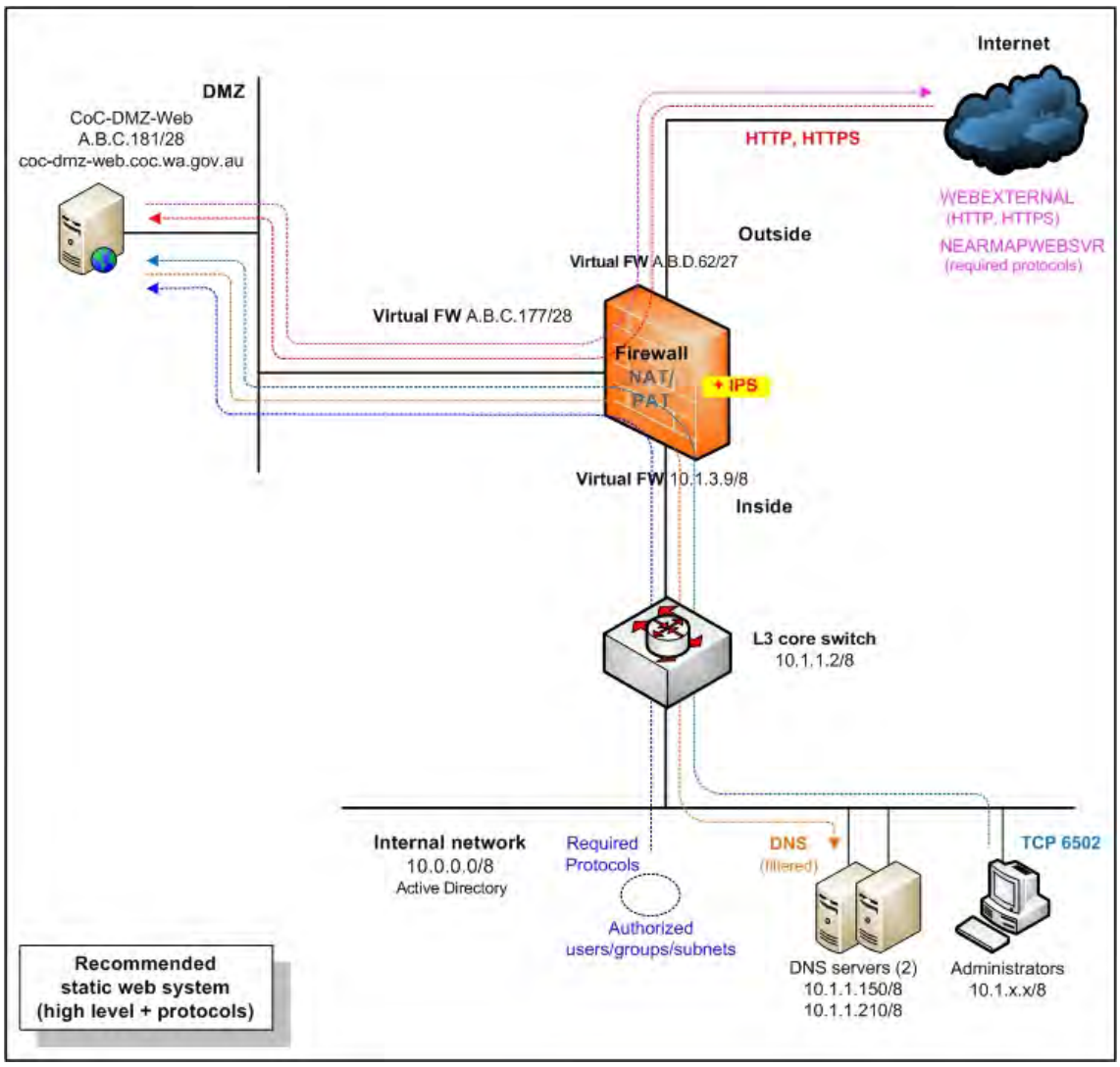

Figure 6.11. The recommended high level static web system including network traffic protocols for Council C

- ***Risk 8***

All DNS traffic which flow from the DMZ network to the council's internal network should be blocked or denied, otherwise this rule should be incorporated with the DNS deep inspection and log feature in order to prevent any potential DNS attacks against the council's internal DNS servers (domain controllers).

- ***Risk 9***

Only one-way communication is required from the CoC-DMZ-CMS server which is located in the council's internal network to push web content information through the firewall via a HTTP port to the CoC-DMZ-CMS server.

As per best practice recommendations to standard firewall configurations, this rule should be changed from permitting an IP to permitting only the HTTP (see Appendix C8: Policy number 6). This rule change will limit the CoC-CMS server to access the CoC-DMZ-CMS server via the HTTP port only.

In addition, this rule also allows the system administrator to manage the CoC-DMZ-CMS using the DameWare Mini Remote Control (via TCP port 6129) and MS Terminal Services (via TCP port 3389) software. A new firewall rule should be created in order to allow only the authorised devices (computers) to access the CoC-DMZ-CMS server via both TCP ports 3389 and 6129. Figure 6.12 illustrates the council's recommended CMS web system including network traffic protocols in a high level network diagram.

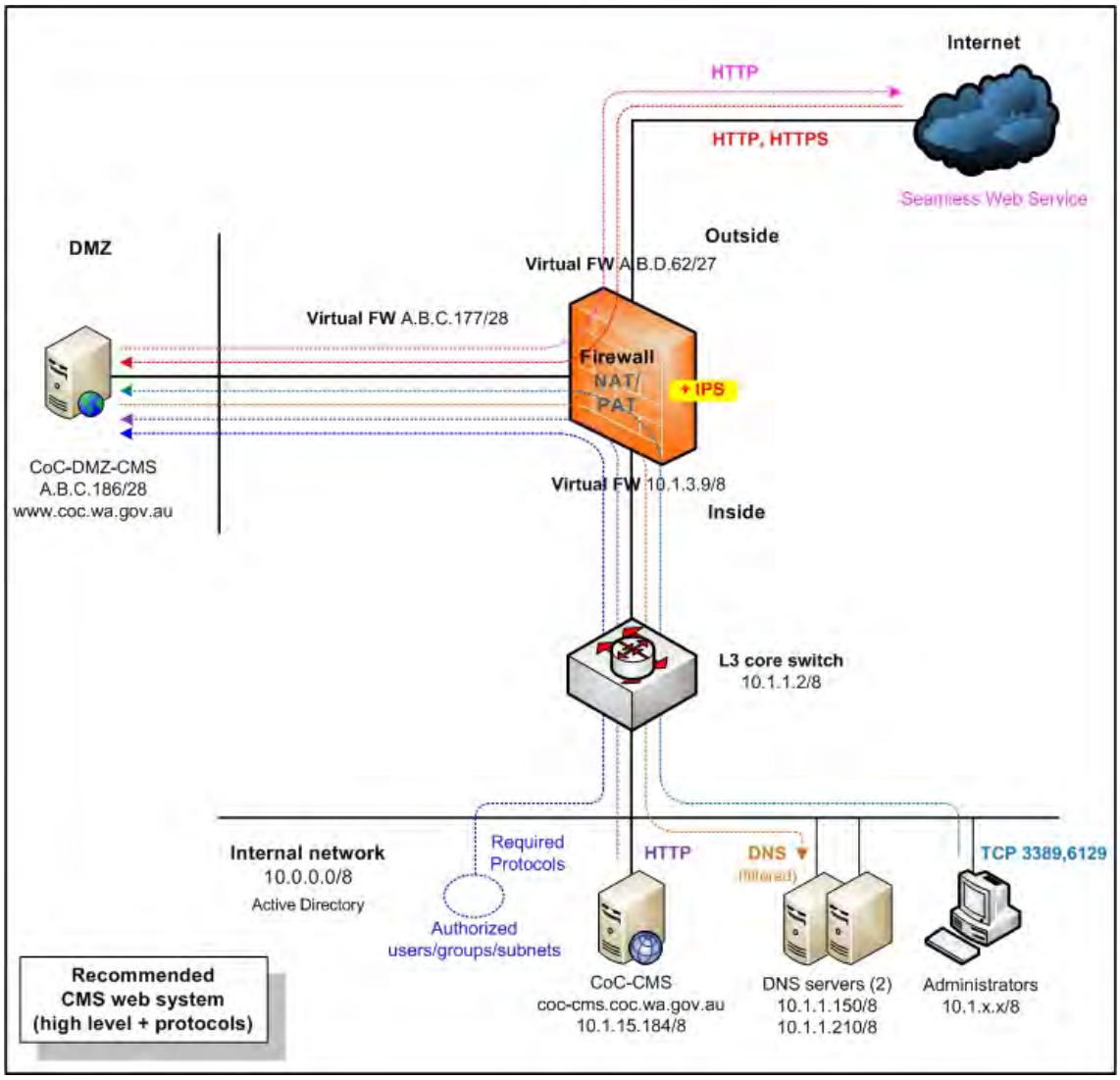

Figure 6.12. The recommended high level CMS web system with network traffic protocols for Council C

- ***Risk 10***

As per best practice recommendations to standard firewall configurations, the firewall rule can be tightened by mapping only the required IP addresses rather than the whole subnet.

- ***Risk 11***

Security can be enhanced using this rule by turning on the log feature of the firewalls.

- ***Risk 12***

As per best practice recommendations to standard firewall configurations, the port service should be changed from “any” (IP) protocol to the required protocol (TCP: HTTP). In addition, by activating both “IPS inspect (filter)” feature on the firewalls and “HTTP application layer inspect” on the reverse proxy server (ISA01), security can be enhanced and any potential risk related to its port service will be minimised.

- ***Risk 13***

HTTPS is only required for a one-way communication protocol from the Epathweb frontend web server to the external gateway payment service (Commweb01). Therefore, the setting for HTTP traffic can be safely removed.

- ***Risk 14***

In order to prevent any potential DNS attacks against the council’s online payment system, a new firewall rule should be created to allow only the Epathweb frontend web server to access both the internal DNS servers via the UDP: DNS port in conjunction with DNS deep inspection and enabling the log feature.

- ***Risk 15***

Refer to previous comments in Section 6.5.1.1.2: Risk 7 for details. In addition, this rule allows the system administrator to manage the Epathweb frontend web server using the DameWare Mini Remote Control (via TCP port 6129) and NetOp Remote Control software (via TCP port 6502).

Therefore, creating a new firewall rule which allows the system administrator to manage the Epathweb frontend web server via both TCP ports 6129 and 6502 is recommended. Figures 6.13 illustrate the council's recommended online payment system including network traffic protocols in a high level network diagram.

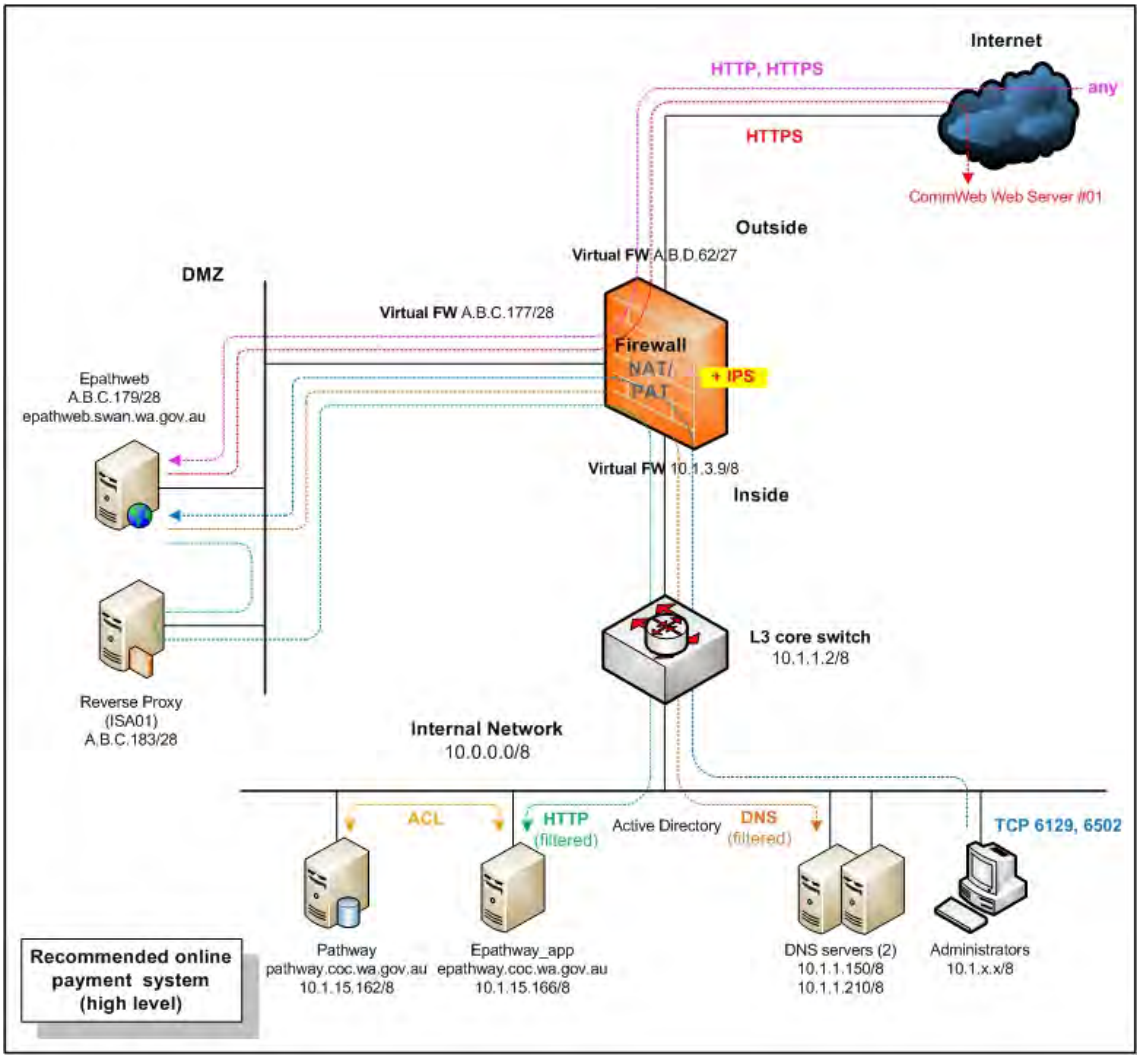

Figure 6.13. The recommended high level diagram of the online payment system including network traffic protocols for Council C

Note:

There were some critical firewall rules which were uncovered, that were not related to this thesis. Nevertheless, these firewall rules can be a source of potential risk against the council's internal network. Therefore, the identified risk issues and possible mitigation recommendations were discussed with the system administrator and provided in a separate submitted report.

- ***Risk 16***

Details of the new switch recommendations were previously discussed in Section 6.5.1.1.2: Risk 8. Furthermore, low level details on the new switch ports and VLANs including its connectivity for the council's online web system are presented Figure 6.14.

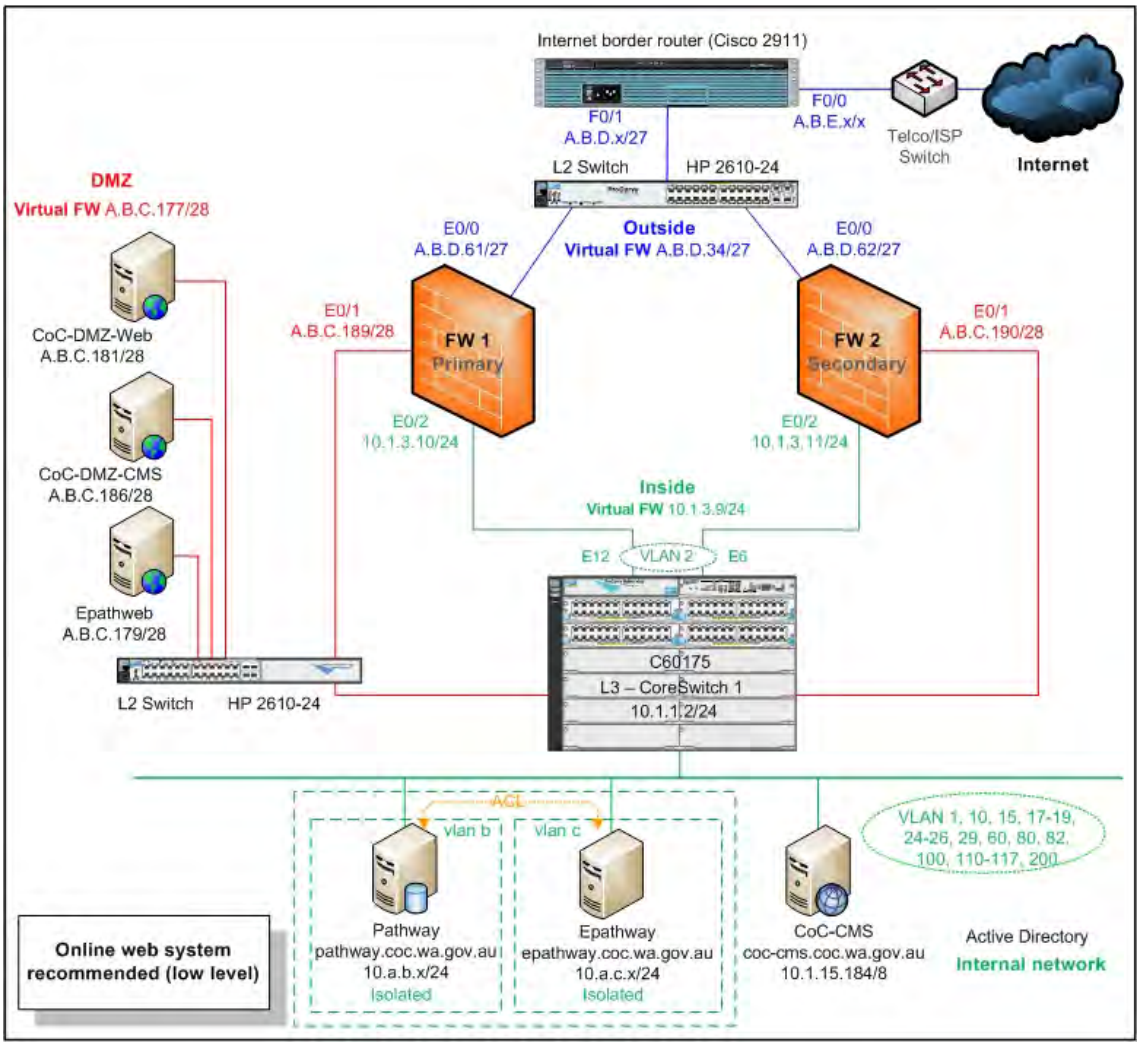

Figure 6.14. The recommended low level network diagram of the online web system for Council C with the two new recommended switches

6.5.1.2.3 Testing stage 3: Possible mitigation

- ***Risk 1***

There were poor Windows password configurations on the CoC-DMZ-Web, the CoC-DMZ-CMS, the CoC-CMS and the Pathway servers. The Windows password policy on these servers should be reconfigured in order to prevent any potential vulnerability. In addition, the security audit policy on the CoC-CMS, the Epathweb, the Epathway and the Pathway servers should be reviewed as indicated in Appendices C12, C13, C14 and C15.

- ***Risk 2***

It is recommended to install the missing service packs as well as patches to the four servers (the CoC-DMZ-Web, the Epathweb, the Epathway and the Pathway). Appendices C16, C17, C18 and C19 present the overall system patching testing analysis and the possible mitigation recommendations.

- ***Risk 3***

As previously discussed, there were unnecessary open TCP and UDP ports on all the six servers, particularly the CoC-DMZ-Web and the Epathweb servers. Table 6.33 presents the total number of recommended open TCP and UDP ports on all the council's online payment servers.

Table 6.33 *The total number of recommended open TCP and UDP service ports on all Council C's online web servers*

Server names	**Recommended open TCP ports**	**Recommended open UDP ports**	**Comments**
CoC-DMZ-Web	6	1	Refer to Appendix C20
CoC-DMZ-CMS	4	1	Refer to Appendix C21
CoC-CMS	7	1	Refer to Appendix C22
Epathweb	4	1	Refer to Appendix C23
Epathway	10	2	Refer to Appendix C24
Pathway	11	3	Refer to Appendix C25

- ***Risk 4***

See Appendices C26, C27, C28, C29, C30 and C31 for full details of the identified risk issues and the possible mitigation recommendations for all the six online web system servers respectively.

6.5.1.2.4 Testing stage 4: Possible mitigation

- ***Risk 1***

The overall details of all the findings (satisfactory and unsatisfactory) and the possible mitigation recommendations are provided in Appendices C32, C33, C34, C35, C36, C37 and C38 respectively.

6.5.1.2.5 Testing stage 5: Possible mitigation

- ***Risks 1 and 2***

As per recommendation to general best practices, the council may consider employing related online technical policies and procedures particularly for the online backend database as well as the web servers. In addition, policies and procedures for the council's infrastructure such as the firewall, the IDS/IPS and the switch may be considered, as the infrastructure provides internetwork connectivity to the database and the online web servers. This will enhance the security of Council C's online web system.

6.5.2 Discussion

In terms of general best practices, the research actions carried out on Council C identified that both the email and the online web system (the static web system, the CMS web system and the online payment system) did not meet the CIS and MS industry standards similar to both the results from Councils A and B. In addition, the recommended frameworks of email and online web systems were successfully utilised during the auditing period similar to both the results of Councils A and B. Chapter 8: Section 8.3 provides examples and details of how to use as well as adjust the recommended frameworks to other similar environments.

Six main factors were identified which can lead to the cause of potential risks and interruptions to the council's email, online web and other related systems. Similar to Council A and B, these factors include the lack of IT security standards awareness, inadequate specific knowledge, limited IT training as a result of restricted training budget, insufficient time for task completion, reliance on external consultants for specific IT projects and no valid testing environment in place. The full details of these factors are explained in the following paragraphs.

Firstly, the lack of IT security standards awareness was examined. There were several discussions with Council C's network administrator and system administrator in this audit testing analyses, which was conducted over a period of five months. This investigation uncovered a number of potential risks due to the lack of security awareness such as both the email and online web systems' architectures not following the CIS and MS IT security industry recommendations to best practices.

Similar to both Councils A and B, the email server architecture was not in conformity to the MS Exchange 2007 architecture recommendation. According to the network administrator and the system administrator, the MS Exchange email server was designed and deployed by the council's IT operational staff with some assistance from the external contractor.

Another lack of IT security standards awareness was that council's network architecture infrastructure did not have an Internet border router in place. Furthermore, the infrastructure used only one core switch to provide network connectivity for both the DMZ and the internal network areas. These factors can lead to be a cause of potential risks to the council's network infrastructure system in terms of a single point of failure.

Table 6.34 summarises the findings related to the lack of IT security standards or industrial best practices by the staff of Council C

Table 6.34 *The summary of the issues uncovered related to the lack of IT security standards awareness by the IT staff*

Results related to lack of IT security standards awareness by IT staff of the council	**Council C**
Internet border router deployed	No
Internet border router redundancy/alternative Internet link deployed	No
Standalone external gateway switch deployed	No
Standalone DMZ switch deployed	No
Design of email server architecture based on the MS Exchange 2007 recommendations to best practices	No

Secondly, the inadequate domain or service specific knowledge was outlined. Similar to both Councils A and B, this was evident from incorrect and inadequate configurations on the DMZ switch, the firewall rules, the unnecessary ports and services installed on the related servers. Furthermore, according to both the network administrator and the system administrator, they were not formally trained in specific email and online web system related courses, or even any other general ICT security related courses.

For example, system and network administrators did not attend any firewall, MS Exchange 2007 and MS SQL Server 2005 training courses. Instead, the IT operational staff have merely kept up-to-date with ICT developments through self instruction that was mainly done after working hours. See Table 6.35 for more details.

Table 6.35 *The summary of results uncovered related to the inadequate specific knowledge*

Results related to inadequate domain or service specific knowledge by the IT staff of the council	**Council C**
Firewall configuration related to the email and online web systems	Insufficient
Switch configuration related to the email and online web systems	Insufficient
Setup and configuration of the email server application (MS Exchange 2007)	Incorrect
Setup and configuration of the online database application (MS SQL Server 2005)	Incorrect
Application of updated software patches on the email server	No
Application of updated software patches on the online web server	No

Table 6.35 *The summary of results uncovered related to the inadequate specific knowledge (continued)*

Results related to inadequate domain or service specific knowledge by the IT staff of the council	**Council C**
Application of updated software patches on the CMS server	No
Application of updated software patches on the online payment server	No
Internal email spoofing allowed	Yes
Unnecessarily opened or unused service ports on the email server	Yes
Unnecessarily opened or unused service ports on the online web server	Yes
Unnecessarily opened or unused service ports on the CMS server	Yes
Unnecessarily opened or unused service ports on the online payment server	Yes
Vulnerabilities uncovered on the email server	Yes
Vulnerabilities uncovered on the online web server	Yes
Vulnerabilities uncovered on the CMS server	Yes
Vulnerabilities uncovered on the online payment server	Yes

Thirdly, the limited IT training as a result of a restricted training budget was examined. According to the council's IT manager, each year the IT operational staff received a very restricted training budget. Consequently, each of the IT operational staff had to take turns in training courses that occurred only every two or three years. See details in Table 6.36.

Table 6.36 *The summary results related to the limited IT training as a result of limited training budget*

Issues uncovered in relation to the limited IT training budget	**Council C**
Formal industry or equivalent routing training of the IT operational staff	No
Formal industry or equivalent firewall training of the IT operational staff	No
Formal industry or equivalent training of the email application (MS Exchange 2007) of the IT operational staff	No
Formal industry or equivalent training of database application (MS SQL Server 2005 or equivalent) of the IT operational staff.	No
Formal IT Security training of the IT operational staff	No
IT training yearly budget allocation for each IT operational staff member	Partly
Support of the council for self-costed self study of IT operational staff	Yes

Fourthly, the matter of insufficient time for task completion was looked at. Council C has eight IT operational staff including the IT manager. The IT operational staff have to manage a daily operation covering GIS, library, email, online payment, online website system, CMS, property management, communication and telephony systems.

In terms of infrastructure, the network administrator and the system administrator provide support for the infrastructure as well as all the ICT related servers. Therefore, some tasks were continually left incomplete, with little or no time for documentation and individual self study. Table 6.37 summarised the insufficient time for task completion by the council IT operational staff.

Table 6.37 *Results uncovered related to the insufficient time for task completion*

Issues uncovered in relation to the insufficient time for task completion	**Council C**
The IT operational staff manages several complex IT systems task simultaneously	Yes
Use of enterprise information security policy	No
Use of technical (issue-specific and systems-specific) security policy	No
Updated documentation of the IT email system	No
Updated documentation of the IT online web system – static web system	No
Updated documentation of the IT online web system – CMS web system	No
Updated documentation of the IT online web system – online payment system	No

Fifthly, the matter of the reliance on external consultants for specific IT projects was analysed. Council C also required external consultant to assist in implementing on some of their ICT projects such as wireless network, microwave link, email 2007 server and Pathway online payment server. However, they first tried to do as much as possible by themself before going to the external consultant (personal communications with Council C, 2010).

There was an evident lack of knowledge transfer in the implementation of email 2007 server such as partly email server installation documentation guide was given to the staff. This may point out that missed contract management by the council when dealing the project with the external consultant.

See Table 6.38 for more details relating to the reliance on external consultants for specific IT projects (related to both the email and online web systems) by Council C.

Table 6.38 *Summary of issues uncovered relating to the reliance on external consultants for specific IT projects*

Issues in relation to the reliance on external consultants for specific IT projects	**Council C**
Deployment of the email (MS Exchange 2007) application server by external consultants	Yes
Appropriate documentation for the email (MS Exchange 2007) installation and management provided by the external consultants	No
Deployment of the online payment system by external consultants	Partly
Appropriate documentation for the online payment system (Epathweb) installation and management provided by the external consultants	Partly

Finally, there was no valid testing environment in place at Council C. There is a testing VM server environment at the council's IT department for pilot testing on different kinds of servers such as email and online web servers.

Similar to both Councils A and B, there was no network communication system testing environment for the IT department at Council C. The installation of a network testing environment would provide benefits to all the of council such as minimising potential risks as well as providing flexibility to the council's IT operational staff during deployment of new devices. See the following table for more details.

Table 6.39 *Summary results uncovered related to no valid testing environment on place at the council*

Summary results related to the lack of a valid testing environment	**Council C**
Existence of a testing environment for the infrastructure	No
Existence of a testing environment for the email system	No
Existence of a testing environment for the online web system – static web system	No
Existence of a testing environment for the online web system – CMS web system	No
Existence of a testing environment for the online web system – online payment system	Partly

CHAPTER 7. DISCUSSION, FINDINGS AND LIMITATIONS

7.1 Discussion

The audit and analysis carried out at the three selected councils through the methodology described revealed several common security risks and deficiencies. It was identified that there was a prevalence of a lack of overall education, training and knowledge of security measures and issues, a lack of inter-staff communication and a lack of resources such as time and expertise.

The overall limitations of the research were in relation to limited time for conduction of testing and scheduling of meetings. Other limitations were due to changing conditions associated with real time systems as well as deficiencies in database knowledge (SQL 2005 Server).

7.2 Findings

This section is divided into two subsections, which include the seven common issues discovered as well as generic action plan checklist.

7.2.1 The seven common issues discovered

The following is list of the seven common factors uncovered during the email and online web systems testing process.

- Lack of IT security standards awareness;
- Inadequate domain or service specific knowledge;
- Inefficient communication;
- Limited IT training as a result of restricted training budget;
- Insufficient time for task completion;
- Reliance on external consultants for specific IT projects; and
- No valid testing environment in place at Council.

There were seven common security risk factors uncovered at both Councils A and B. However, there were six risk factors uncovered at Council C, the missing risk factor was the “Inefficient communication between the IT operational staff”.

The following sections describe the seven factors in detail.

1) *Lack of IT security standards awareness:* The two audits carried out included several discussions with the councils’ IT managerial and IT operational staff together with the email and online web testing analyses for each of the selected councils. The results of these audits indicated that there was a lack of IT security standards observance by the relevant IT operational staff.

   For example, the email server (MS Exchange 2007) architecture for all of the selected councils was not based on the MS Exchange 2007 best practice recommendations. Furthermore, the architecture of the online payment system for Council B did not follow the Microsoft best practice design recommendations of multi-tiered (3) client-server architecture (Microsoft Corporation, 2010). The following table describes the overall findings related to the lack of IT security standards awareness for generally accepted industrial best practice recommendations.

Table 7.1 *Overall findings related to the lack of IT security standards awareness for industrial best practices by the IT staff for the three selected councils*

Finding	**Council A**	**Council B**	**Council C**
Internet border router deployed	Yes	Yes	No
Internet border router redundancy/alternative Internet link deployed	No	No	No
IDS/IPS deployed and currently in use	No	No	Yes
Standalone external gateway switch deployed	Yes	No	No
Standalone DMZ switch deployed	Yes	No	No
Design of email server architecture based on the MS Exchange 2007 recommendations to best practices	No	No	No
Design of the online payment system conforming to recommendations of a multi-tiered client-server architecture	Yes	No	Yes

2) *Inadequate domain or service specific knowledge:* There was evidence of incorrect and insufficient configuration in all three selected councils' internetwork infrastructure (the firewalls, the switches and the Internet border routers) and the related servers. To some extent this was attributed to the lack of formal Internet and web server knowledge that was attributed to insufficient training, according to the different IT operational staff from each of the selected councils. The discussions with the IT management staff revealed that the IT operational staff was not well versed in the administration of the firewalls, the web servers' security, MS Exchange 2007 and MS SQL Server 2005. Table 7.2 below presents the overall evidence related to the factor of the inadequate specific knowledge at Councils A, B and C.

Table 7.2 *Overall results uncovered related to the inadequate specific knowledge*

Finding	**Council A**	**Council B**	**Council C**
Insufficient configuration on the Internet border router related to the email and online web systems	No	Yes	N/A
Insufficient configuration on the firewall related to the email and online web systems	Yes	Yes	Yes
Insufficient configuration on the switch related to the email and online web systems	No	Yes	Yes
Incorrect setup and configuration of the email server application (MS Exchange 2007)	Yes	Yes	Yes
Incorrect setup and configuration of the online database application (MS SQL Server 2005)	Yes	Yes	Yes
Application of updated software patches on the email server	No	No	No
Application of updated software patches on the online web server	N/A	No	No
Application of updated software patches on the CMS server	N/A	No	No
Application of updated software patches on the online payment server	No	No	No
Internal email spoofing allowed	Yes	Yes	Yes
Unnecessarily opened or unused service ports on the email server	Yes	Yes	Yes
Unnecessarily opened or unused service ports on the online web server	N/A	Yes	Yes
Unnecessarily opened or unused service ports on the CMS server	N/A	Yes	Yes
Unnecessarily opened or unused service ports on the online payment server	Yes	Yes	Yes

Table 7.2 *Overall results uncovered related to the inadequate specific knowledge (continued)*

Finding	**Council A**	**Council B**	**Council C**
Vulnerabilities uncovered on the email server	Yes	Yes	Yes
Vulnerabilities uncovered on the online web server	N/A	Yes	Yes
Vulnerabilities uncovered on the CMS server	N/A	Yes	Yes
Vulnerabilities uncovered on the online payment server	Yes	Yes	Yes

3) *Inefficient communication:* There was no evidence of a change management processes in place or any simple specific technical log books evident at any of the three selected councils. The absence of such guidelines and recording demonstrated inefficient communication and handover procedures between the IT operational staff. The lack of communication was also evidenced by the inadequate or non-existent IT documentation of both the email and online web systems. The lack of change management, documentation and communication contributed to a lack of knowledge transfer and knowledge sharing.

   For example, at Council A, there was a missed configuration on the firewall relating to the online payment application and database servers due to the Pathway application administrator not informing the network administrator to update the firewall rule. Similarly at Council B there was a missed configuration on the firewall rule related to the unnecessarily opened database ports as result of lack of communication between the network administrator and the web developer.

   It should be noted that, the mis-communication ceased following the email and online web system testings, which included several interviews with the network and system administrators of Council C. However, the evident inadequate or non-existent IT documentation of both email and online web systems will continue to contribute to a lack of knowledge transfer in the near future. Table 7.3 describes the overall findings that can contribute to the inefficient communication between the IT operational staff.

Table 7.3 *Overall issues uncovered that can contribute to the inefficient communication*

Finding	**Council A**	**Council B**	**Council C**
Existence of change management procedures	No	No	No
Availability of simple specific technical log books	No	No	No
Updated documentation of the IT email system	No	No	No
Updated documentation of the IT online web system related	No	No	No

4) *Limited IT training for the IT operational staff as a result of restricted training budget:* Several discussions with the IT operational staff at all three selected councils revealed that the IT training budget was limited. For example, each IT operational staff member was permitted to attend a maximum of one IT specific training course per year or every two years. This education policy contributed to insufficient specific knowledge for managing both the email and online web systems including the network infrastructure. The overall findings of the limited IT training for the IT operational staff as a result of restricted training budget are displayed in Table 7.4.

Table 7.4 *Overall findings related to the limited IT training for the IT operational staff as a result of limited training budget*

Finding	**Council A**	**Council B**	**Council C**
Formal industry or equivalent routing training of the IT operational staff	Yes	No	No
Formal industry or equivalent firewall training of the IT operational staff	No	No	No
The IT operational staff were formally industry or equivalent trained on the switching related course	Yes	No	No
Formal industry or equivalent training of the email application (MS Exchange 2007) of the IT operational staff	No	No	No
Formal industry or equivalent training of database application (MS SQL Server 2005 or equivalent) of the IT operational staff	No	No	No
Formal IT Security training of the IT operational staff	Partly	No	No
IT training yearly budget allocation for each IT operational staff member	Yes	Partly	Partly
Support of the council for self-costed self study of IT operational staff	Yes	Yes	Yes

5) *Insufficient time for documentation:* This was evident from the lack of proper IT documentation such as, no IT enterprise security and no technical policies and procedures in relation to both the email and online web systems at all three selected councils. The various discussions with the IT operational and management staff in all three selected councils revealed that there was insufficient time allocated for efficient and appropriate task completion, due to excessive workload as staff are required to manage several complex tasks simultaneously.

   For example, the network administrator of Council B was responsible for the entire network infrastructure, the telephony system, the virtual servers and the backup systems. Similarly, Council C's system administrator managed the database, the firewalls, the proxy, the email, the web, the applications and the virtual servers together with the backup systems.

   Table 7.5 provides the overall findings which related to the insufficient time for documentation.

Table 7.5 *Overall findings related to the insufficient time for documentation*

Finding	**Council A**	**Council B**	**Council C**
The IT operational staff manages several complex IT systems task simultaneously	Yes	Yes	Yes
Use of enterprise information security policy	No	No	No
Use of technical (issue-specific and systems-specific) security policy	No	No	No
Updated documentation of the IT email system	No	No	No
Updated documentation of the IT online web system – static web system	No	No	No
Updated documentation of the IT online web system – CMS system	N/A	No	No
Updated documentation of the IT online web system – payment system	No	No	No

6) *Reliance on external consultant for specific IT projects:* The reliance on external consultants was supported by the fact that the implementation of the email systems in all three selected councils was outsourced. The outsourced implementation of the email systems was exacerbated by the fact that no appropriate documentation was provided by the external consultants to be used as instruction manuals for the firewall, email installation and management. Consequently, this shortcoming in documentation and handover contributed to a lack of knowledge transfer in all three selected councils. The following table lists the overall findings which related to the reliance on external consultants for specific IT projects.

Table 7.6 *Overall findings related to the reliance on external consultants for specific IT projects*

Finding	**Council A**	**Council B**	**Council C**
Implementation of the firewall system by external consultants	Yes	Yes	No
Appropriate documentation for the firewall installation and management provided by the external consultants	Partly	Partly	N/A
Implementation of the email spam blocker appliances by external consultants	Yes	Yes	N/A
Appropriate documentation for the email spam blocker appliances installation and management provided by the external consultants	Yes	Yes	N/A
Deployment of the email (MS Exchange 2007) application server by external consultants	Yes	Yes	Yes
Appropriate documentation for the email (MS Exchange 2007) installation and management provided by the external consultants	No	No	No
Deployment of the online payment system by external consultants	Partly	No	Partly
Appropriate documentation for the online payment system (Epathweb) installation and management provided by the external consultants	Partly	N/A	Partly

In addition, in the case of all the three selected councils, no real costing and IT budgetary percentages either earmarked or allocated for external consultancy contracting were discussed or disclosed to the researcher. However, all of the three selected councils' IT managers made mention of allocated IT budgets for each advanced ICT project that required external consultancy (personal communications with the three selected WA councils, 2008, 2009).

Furthermore, it was found that all the three selected IT managers did prefer to use external consultants for their advanced ICT projects and only used their own IT staff to basic ICT projects (personal communications with the three selected WA councils, 2008, 2009).

The three selected councils' IT managers emphasised that the reasons and benefits of using external contractors were the confidence and trust in external professional expertise as well as to minimise any potential risk of project failure that may occur during the process (personal communications with the three selected WA councils, 2009). In addition, the use of external consultants was most likely provided that the projects were considered to be advanced ICT ventures, regardless of whether internal IT staff had undergone specific training courses for the same assigned projects (personal communications with the three selected WA councils, 2009).

7) *No valid testing environment in place:* All of the IT departments of the three selected councils did not have any mirrored live testing environments in place, apart from specific VM servers which were allocated as virtual testing servers for the database (Councils B and C only) and online payment servers (all three councils). The project also noted that there were no testing systems for the network communication equipment at all three selected councils. Table 7.7 displays more details of the summary of issues uncovered related to the lack of a valid testing environment.

Table 7.7 *Summary results uncovered related to the absence of a valid testing environment*

Findings	**Council A**	**Council B**	**Council C**
Existence of a testing environment for the infrastructure	No	No	No
Existence of a testing environment for the email system	Partly	Partly	Partly
Existence of a testing environment for the online payment system	Partly	Partly	Partly

In addition, there were a total of 32 t common findings based on the seven factors at all three selected WA councils (A, B and C). These most common factors are listed in Table 7.8.

Table 7.8 *Overall summary of the most common deficiencies uncovered at all three selected WA councils*

Total	**Factor number**	**Findings**
1	1	Internet border router redundancy/alternative Internet link deployed
2	1	Design of email server architecture based on the MS Exchange 2007 recommendations to best practices
3	1	Design of the online payment system conforming to recommendations of a multi-tiered client-server architecture
4	2	Insufficient configuration on the firewall related to the email and online web systems
5	2	Incorrect setup and configuration of the email server application (MS Exchange 2007)
6	2	Incorrect setup and configuration of the online database application (MS SQL Server 2005)
7	2	Application of updated software patches on the email server
8	2	Application of updated software patches on the online payment server
9	2	Internal email spoofing allowed
10	2	Unnecessarily opened or unused service ports on the email server
11	2	Unnecessarily opened or unused service ports on the online payment server
12	2	Vulnerabilities uncovered on the email server
13	2	Vulnerabilities uncovered on the online payment server
14	3	Existence of change management procedures
15	3	Availability of simple specific technical log books
16	3	Updated documentation of the IT email system
17	3	Updated documentation of the IT online web system related
18	4	Formal industry or equivalent firewall training of the IT operational staff
19	4	Formal industry or equivalent training of the email application (MS Exchange 2007) of the IT operational staff
20	4	Formal industry or equivalent training of database application (MS SQL Server 2005 or equivalent) of the IT operational staff
21	4	Support of the council for self-costed self study of IT operational staff
22	5	The IT operational staff manages several complex IT systems task simultaneously
23	5	Use of enterprise information security policy
24	5	Use of technical (issue-specific and systems-specific) security policy

Table 7.8 *Overall summary of the most common deficiencies uncovered at all three selected WA councils (continued)*

Total	Factor number	Findings
25	5	Updated documentation of the IT email system
26	5	Updated documentation of the IT online web system – static web system
27	5	Updated documentation of the IT online web system – payment system
28	6	Deployment of the email (MS Exchange 2007) application server by external consultants
29	6	Appropriate documentation for the email (MS Exchange 2007) installation and management provided by the external consultants
30	7	Existence of a testing environment for the infrastructure
31	7	Existence of a testing environment for the email system
32	7	Existence of a testing environment for the online payment system

7.2.2 Generic action plan and checklist

The outcome of this research was a generic action plan for any organisation interested in tightening its system and infrastructure security. This action plan was derived as a result of abstraction from the procedures carried out at the three selected WA councils. It emerged in the form of a checklist operating at three different levels that cover internetwork infrastructure, application services and documentation. At the infrastructure level, organisations should be concerned with the secure operation of devices such as the internet border router (outside communications), firewalls (screening) and switches (outside, DMZ and internal communications) as well as the general physical security of the whole installation. Within the application services level, organisations should be concerned with the security of their intranet and internet services such as email and online web services, whilst at the documentation level; the security focus should be on the general and specific ICT policy and procedures for standardisation and operational security.

This generic action plan is depicted in Tables 7.9, 7.10 and 7.11 in the form of quick checklist designed for use by ICT managers or system administrators to formulate their action plans if needed for their regular system audits. Ideally, this action plan should be revisited every six months or at each device or application service change as appropriate.

Table 7.9 *Recommended generic checklist 1: Internetworking*

Recommended generic checklist 1: Internetworking		**RT**	**FW**	**O-SW**	**D-SW**	**I-SW**	**Severity**
1	**Physical security**						
1.1	Place device in appropriate environment against dust, flood, etc.	✓	✓	✓	✓	✓	Important
1.2	Install temperature control system including air conditioner	✓	✓	✓	✓	✓	Important
1.3	Deploy appropriate uninterruptible power supply or alternative power supply	✓	✓	✓	✓	✓	Critical
1.4	Allow access to only authorised personnel	✓	✓	✓	✓	✓	Critical
1.5	Deploy surveillance system	✓	✓	✓	✓	✓	Low
2	**Infrastructure architecture**						
2.1	Redundancy or alternative link	✓					Low
2.2	Redundancy firewall architecture		✓				Low
2.3	Double firewall architecture		✓				Low
2.4	Deploy or enable IDS/IPS feature	✓	✓				Important
2.5	Deploy or enable logging server	✓	✓	✓	✓	✓	Important
2.6	Deploy standalone external gateway or outside switch			✓			Important
2.7	Deploy standalone DMZ gateway or outside switch				✓		Important
2.8	Create multiple DMZs (if applicable)				✓		Low
3	**Hardware and cabling**						
3.1	Redundancy hardware: Dual power supply (if applicable)	✓	✓	✓	✓	✓	Important
3.2	Space each device physically for air flow	✓	✓	✓	✓	✓	Low
3.3	All required cables should connect properly	✓	✓	✓	✓	✓	Important
4	**IOS/OS and application**						
4.1	IOS/OS up-to-date	✓	✓	✓	✓	✓	Critical
4.2	Up-to-date patch/hot fix	✓	✓	✓	✓	✓	Critical
4.3	Disable unused ports and interfaces	✓	✓	✓	✓	✓	Critical
4.4	Disable unnecessary services	✓	✓	✓	✓	✓	Critical
4.5	Application up-to-date (if applicable)	✓	✓				Critical
4.6	Install antivirus software (if applicable)	✓	✓				Critical
5	**Configuration of administrative, ACL and rules**						
5.1	Secure administrative control	✓	✓	✓	✓	✓	Critical
5.2	Appropriate privilege level or viewing access to different user groups	✓	✓	✓	✓	✓	Critical
5.3	Apply different login name and password to internal network infrastructure	✓	✓	✓	✓	✓	Important

Table 7.9 *Recommended generic checklist 1: Internetworking (continued)*

Recommended generic checklist 1: Internetworking		**RT**	**FW**	**O-SW**	**D-SW**	**I-SW**	**Severity**
5.4	Disable and restrict commonly configured management services, such as SNMP (if applicable use SNMP v.3)	✓	✓	✓	✓	✓	Important
5.5	Appropriate configure timekeeping which required encrypted authentication	✓	✓	✓	✓	✓	Important
5.6	Appropriate ACL rules to protect against IP spoofing, probing and scanning	✓					Critical
5.7	Appropriate ACL rules to specific required services such as DNS, email, FTP and web	✓	✓				Critical
5.8	Inspect critical external incoming network traffic such as HTTP and HTTPS		✓				Important
5.9	Screen unwanted and/or potential risk protocols such as IRC, Kazaa and MSN		✓				Important
5.10	Appropriate configuration of NAT and PAT		✓				Critical
5.11	Appropriate configuration to protect against ARP poisoning attacks			✓	✓	✓	Important
5.12	Apply appropriate VLAN setup and do not use vendor default VLAN setup			✓	✓	✓	Important
5.13	Appropriate configuration of switch port network and security control such as broadcast storm and port security (if applicable)			✓	✓	✓	Important
5.14	Appropriate configuration of trunking					✓	Important

RT represents Internet border router

FW represents firewall

O-SW represents outside switch

D-SW represents DMZ switch

I-SW represents inside switch

Table 7.10 *Recommended generic checklist 2: Application services*

Recommended generic checklist 2: Application services		**CMS**	**Email**	**Pay-ment**	**Static web**	**Severity**
1	**Physical security**					
1.1	Place device in appropriate environment to protect against dust, flood, etc.	✓	✓	✓	✓	Important
1.2	Install temperature control system including air conditioner	✓	✓	✓	✓	Important
1.3	Deploy appropriate UPS or alternative power supply	✓	✓	✓	✓	Critical
1.4	Allow access to only authorised personnel	✓	✓	✓	✓	Critical
1.5	Deploy surveillance system	✓	✓	✓	✓	Low
2	**Application architecture**					
2.1	Separate both frontend CMS and backend web servers by placing the frontend CMS server at DMZ area (if applicable) and placing the backend CMS server within the internal network with its own isolated network or VLAN (if applicable)	✓				Important
2.2	Separate both traditional email (SMTP) and webmail servers by placing the webmail server in the DMZ or internal network (depending on vendor email architecture recommendations to best practices) and the SMTP server within internal network		✓			Important
2.3	Deploy or install email spam blocker to filter incoming email traffic before forwarding to email (SMTP) server. The spam blocker should be located in the DMZ area (if applicable)		✓			Critical
2.4	Deploy online payment system conforming to recommendations of a multi-tiered client-server architecture by placing frontend online payment web server in DMZ area, and placing application server within the internal network with its own isolated network or VLAN			✓		Critical
2.5	Place static (or dynamic) web server in DMZ				✓	Critical
3	**Hardware and cabling**					
3.1	Redundancy hardware: Dual power supply, hard disk (if applicable)	✓				Important
3.2	All required cables should connect properly	✓				Important
3.3	Dedicate stand alone hardware and redundancy hard disks for critical servers such as database server			✓		Important
3.4	Appropriate assignment of high bandwidth/speed network to critical servers such as database, email client servers (if applicable)		✓	✓		Important

Table 7.10 *Recommended generic checklist 2: Application services (continued)*

Recommended generic checklist 2: Application services		**CMS**	**Email**	**Pay-ment**	**Static web**	**Severity**
4	**Secure operating system**					
4.1	OS up-to-date	✓	✓	✓	✓	Critical
4.2	Up-to-date patch/hot fix/service pack	✓	✓	✓	✓	Critical
4.3	Disable unused ports and services	✓	✓	✓	✓	Critical
4.4	Disable unnecessary user accounts (e.g. guest)	✓	✓	✓	✓	Important
4.5	Secure administrative control	✓	✓	✓	✓	Critical
4.6	Install antivirus software	✓	✓	✓	✓	Critical
5	**Secure application software and data**					
5.1	Applications update	✓	✓	✓	✓	Critical
5.2	Application of up-to-date patch/hot fixes	✓	✓	✓	✓	Critical
5.3	Disable default application login name and password (if applicable)	✓	✓	✓	✓	Important
5.4	Create appropriate levels of role based authorisation of users	✓	✓	✓	✓	Important
5.5	Apply appropriate alternative configuration port instead of default port such as SQL			✓		Important
5.6	Configure alternative internal email port to mitigate against email spoofing		✓			Important
5.7	Apply asymmetric encryption method to sensitive data such as customer credentials information			✓		Critical
5.8	Encrypt network traffic between servers (frontend, application and backend) if applicable			✓		Important
5.9	Limit access permission on all data folders	✓	✓	✓	✓	Important
5.10	Regularly backup and secure all the data	✓	✓	✓	✓	Critical
6	**Administrative, monitoring and logging**					
6.1	Allow only secure communication between server application and administrator terminal such as HTTPS, SSH	✓	✓	✓	✓	Critical
6.2	Appropriate application of logging feature to all servers	✓	✓	✓	✓	Important
6.3	Apply appropriate username and password for applications and operating systems	✓	✓	✓	✓	Important

Payment represents online web system – payment system

Static web represents online web system – static web system

Table 7.11 *Recommended generic checklist 3: Workflow and documentation*

Recommended generic checklist 3: Workflow and documentation		**Severity**
1	Create/apply appropriate change management procedures	Important
2	Create/apply appropriate simple specific technical log books such as for firewall and servers	Important
3	General or enterprise ICT security policies	Important
4	Technical ICT security (issue-specific and systems-specific) policies such as network, remote access policies	Important
5	End-user ICT policies such as login and email usage policies	Important
6	Standards, guidelines and procedures – circulation, updates and enforcement	Important
7	Regularly team meeting to minimise potential of lack of communication between ICT staff	Important
8	Allocate sufficient training budget to its ICT staff (if applicable)	Important
9	All external consultancy work carried out should be fully documented and available on site	Critical
10	Appropriate deployment of testing environment for network infrastructure	Important
11	Appropriate deployment of testing environment for server, particularly critical servers such as database server	Critical

7.3 Limitations of the research

There were a number of limitations of the research associated with the testing and analysis phases conducted at the three selected councils. They are presented below.

1) *Audit meetings cancelled or re-scheduled:* Meetings with each of the selected councils were sometimes postponed as a result of unforeseen circumstances. This meant that delays were incurred in the testing and analyses cycles. These were further complicated when the testing and analyses cycles were time critical in that there were performance time windows for when they could be carried out on the online web systems. The fact that this research was done on a non-payment basis may have contributed to this attitude of ascribing little importance to the meetings or the time set aside for the testings.

2) *Real-time data difficulties during the analysis*: As a result of data collection in real-time, several disruptions to data recordings occurred at all three selected councils. For instance, during the data collection and analysis process at Council A, the firewall configuration codes changed several times over a period of two weeks which meant that the reports had to be redone with the new configuration codes. In

addition, the email and online web systems at all three selected councils are real-time systems, requiring regular software updating such as patches and service packs. Any updates that occurred after the testing and analysis obfuscated the results and rendered the recommendations invalid.

3) *Limited time frame for data collection and reporting:* The data collection and reporting process, which included two reports per council, had a one year time frame in which both the email and online web systems at the three selected councils had to be completed. However, due to the unforeseen circumstances, the data collection and reporting process had to be extended from 12 months to 15 months.

4) *Requests for additional testing outside the scope of the research:* Two of the selected councils, Councils A and C, asked for additional testing analyses not covered by the parameters of the engagement.

   For example, Council A asked for security testing on their virtual servers, Citrix and remote access systems. Council C requested for in-depth security testing on their network infrastructure. These were not able to be carried out as they would have detracted from the main purpose of the research.

5) *Lack of specific database management skills in the selected councils:* There was a lack of database management skills in MS SQL Server 2005 for the IT operational staff in all three selected councils. These caused small interruptions during the online web system testing period at all three selected councils, as additional time had to be allocated to figure out the formulation of the benchmarking for the online web system testing.

As a consequence of the above mentioned difficulties, the research was limited to two systems only, viz. the email and online web systems. Online services such as the online library, online GIS and online GPS systems which normally form the suite of services, in addition to the email and online web systems, were outside the scope of this research.

Furthermore, time constraints prevented the web application security testing as denoted in Figure 8.3 in chapter 8 to be performed. This limitation meant that vulnerability testing specific to web application architecture to attack scenarios was not performed.

CHAPTER 8. CONCLUSION, RECOMMENDATIONS AND FUTURE RESEARCH DIRECTIONS

8.1 Conclusion

Three research questions were formulated in order to investigate feasible solutions to the problems that were exposed in the initial audit. These research questions were outlined in Chapter 1 and relate to the level of security of the email and online web systems deployed at the selected councils in terms of standards, usage and possible improvement.

The research activities carried out in this undertaking revolved around answering the three research questions postulated at the outset. The first question was to determine whether the current email and online web systems at the three selected councils (A, B and C) met with the relevant aforementioned IT security standards. The analyses that were conducted over a six-, 12- and 18-month period revealed that the implementation of these systems fell short of meeting these standards. Nevertheless, the research activity relating to this question provided recommendations to the selected councils to rectify the problems by implementing the proposed solutions so that those standards requirements could be met.

The second research question queried whether the processes could be formulated into a framework that could be used to improve the strength of the security of the email and online web systems at the selected councils. This was demonstrated in the form of a methodology and regime of implementation and maintenance at the selected councils that if followed consistently and repetitively with respect to the nature of the system (email, online static, dynamic and payment) under review would ensure the security strength of the systems for the future as all processes would be documented by check listing each phase of the frameworks as denoted in Figure x and Figure y for the email and online web systems respectively.

The third question was to determine whether other organisations with similar architecture and environments could utilise the proposed data analysis frameworks for both the email and online web systems to suit their own individual and specific needs. This question was answered in the first instance by the selection of the three separate entities of Councils A, B and C.

In the second instance, in as far as whether the frameworks are workable for other organisations are concerned, the frameworks have additional and generic stages which allow for substitutions of the parameters that uniquely characterise those systems under review. These substitutions have been already noted in the frameworks in Figure 8.1 and Figure 8.2.

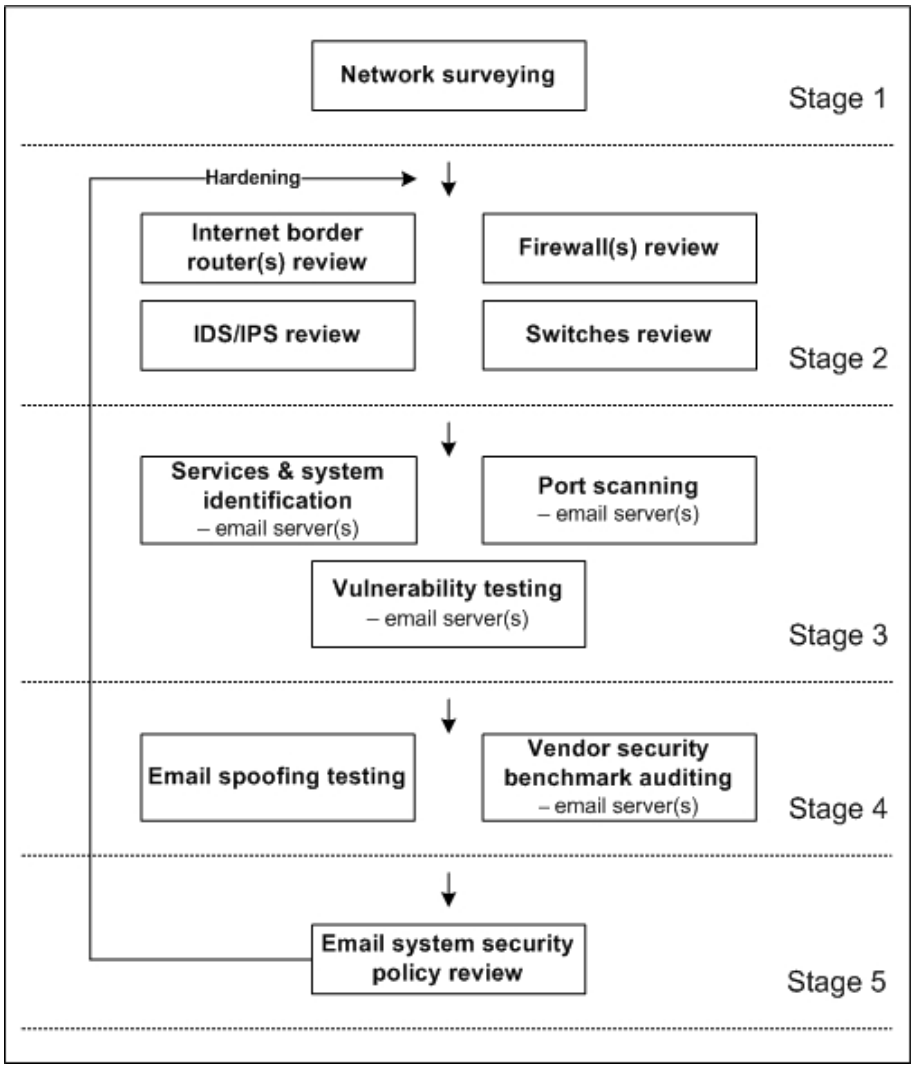

Figure 8.1. Data analysis framework for the analysis of the email system

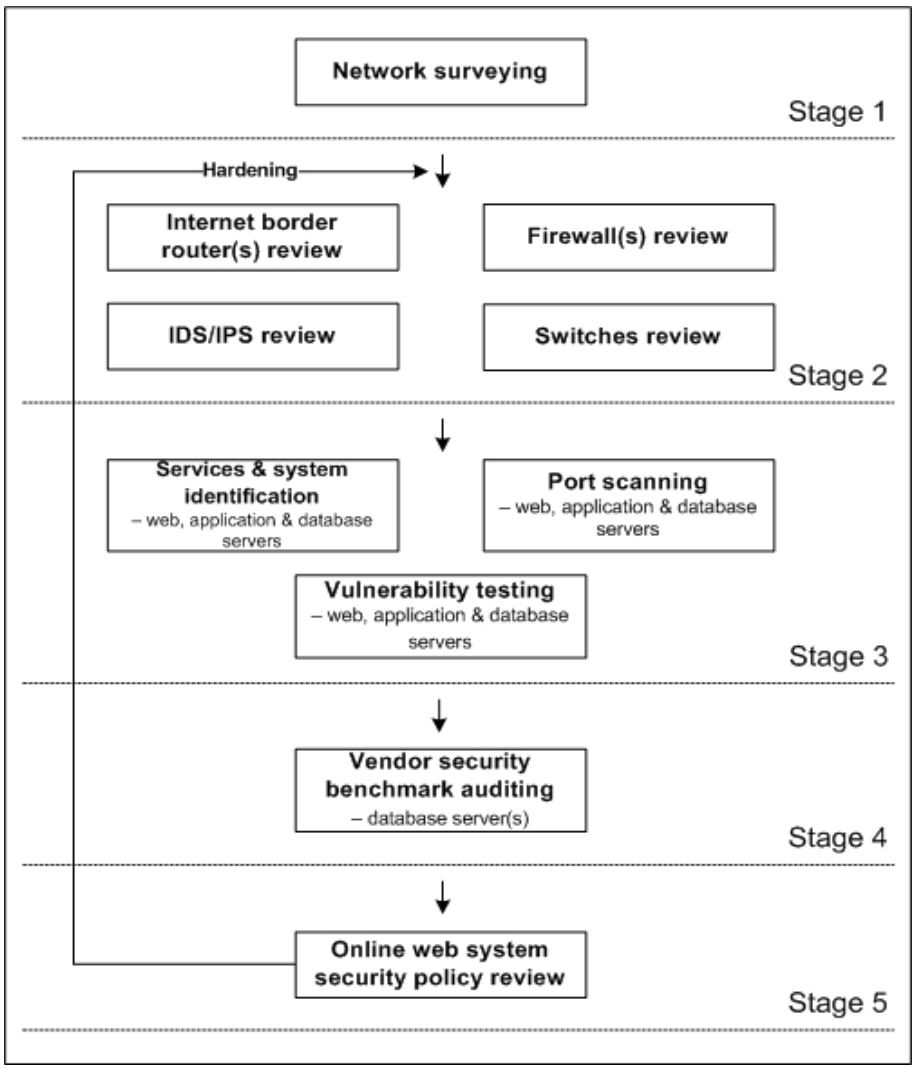

Figure 8.2. Data analysis framework for the analysis of the online web system

The provision of these examples of substitutions within the frameworks for the email and online web systems parameters peculiar to any other organisations, allow for generalisations and translatability fundamental to the concept of frameworks.

8.2 Recommendations

Given the findings from this research, a number of recommendations were proposed to the three selected councils in WA. The IT operational staff of the three selected councils were given the option to implement the solutions provided in Chapters 4, 5 and 6 for Councils A, B and C respectively. In addition, a more formal methodological framework solution, as outlined in Chapter 3 could be utilised to be implemented as a management solution at any council and/or organisation with similar architecture, with a view to enhancing network security as per individual requirements. For example, any other council wishing only to apply the developed information security framework for the online web system testing of their static online web systems without database servers auditing, may simply adjust the developed information security framework to suit their specific requirements. This modification to the online web system framework may be achieved by a simple removal of Testing stage 4: Vendor security benchmark auditing as depicted in Figure 8.3.

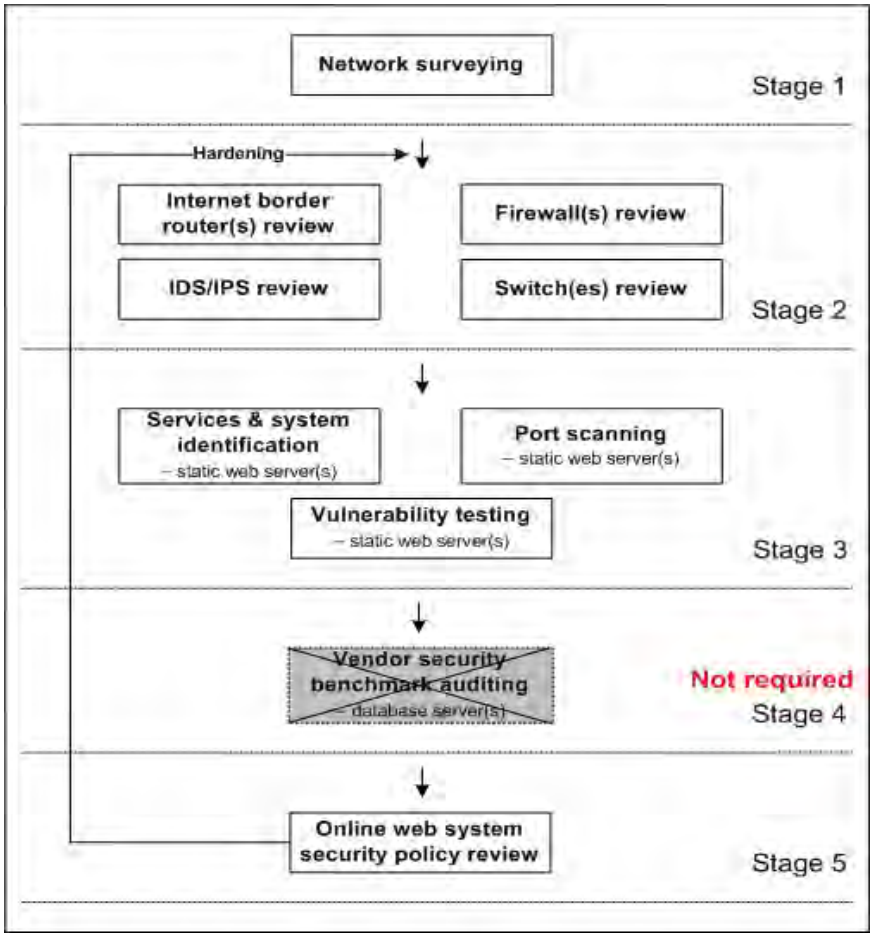

Figure 8.3. A sample of the modified framework of the static online web system

Another example in Figure 8.4 illustrates how the current email security auditing framework can be used at similar organisations which have the same or a different email application software.

For example, in case of an organisation using IBM Lotus Notes as their email application software, the only change to the framework is the vendor security benchmark auditing (on the email server) at stage 4. All other stages within the framework need not change. Specifically the only change would be in the auditing and best practices of IBM Lotus Notes instead of MS Exchange 2007 email applications in name only. The actual auditing steps would however, remain the same.

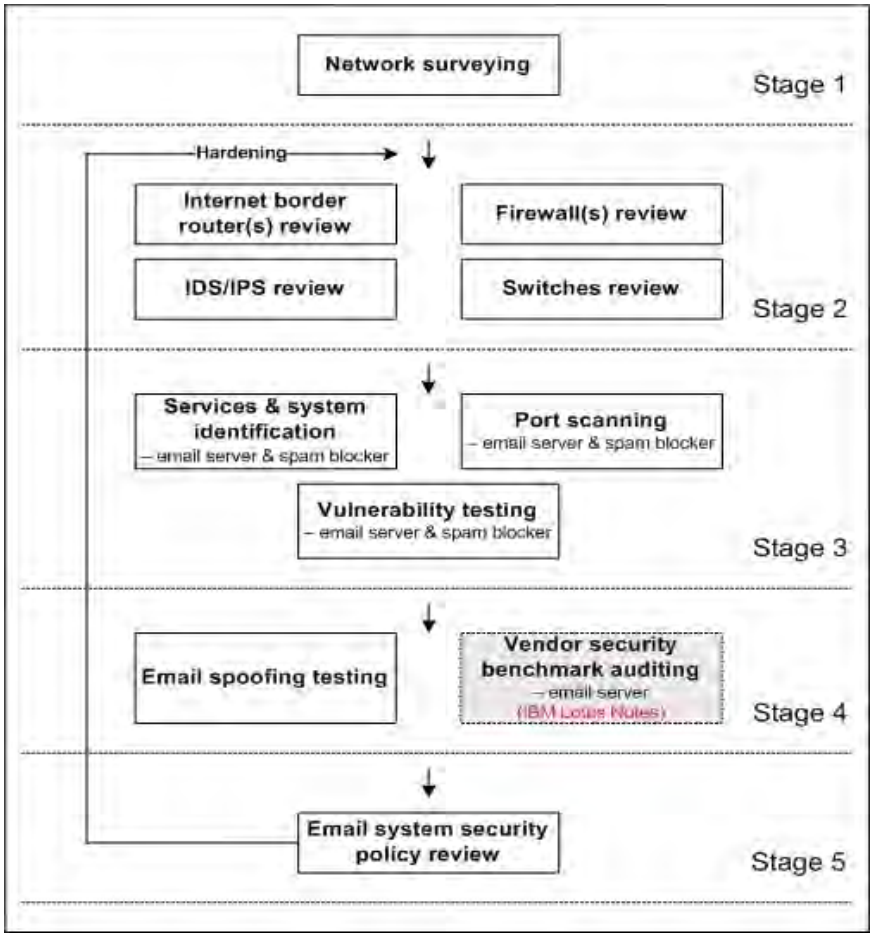

Figure 8.4. An example of the change required for a different email application

8.3 Future research directions

The methodology used in the analysis of the online web system was limited to the review and analysis of the internetwork, the vulnerability assessment of the web, the application and backend database servers, the vendor security benchmark auditing on the database server and the review of the related security policy due to constraints of this research study.

A future research direction would be to enhance the online web system framework by the addition of a web application security testing step in Testing stage 4 as denoted in Figure 8.5.

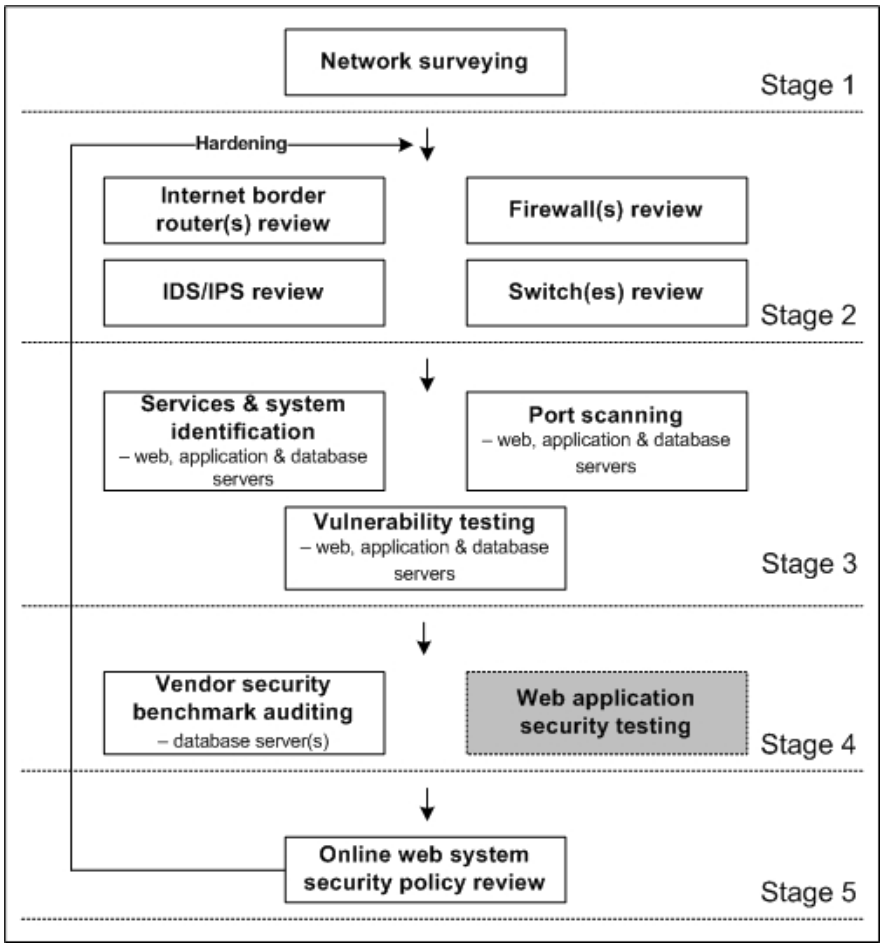

Figure 8.5. A diagram of the testing process framework of the online web system with the additional web application testing phase

The added web application security testing steps would incorporate testing the processes and applications for vulnerability against attacks on web platforms, web service (XML), input validation, web database, web authentication and authorisation (Scambray et al., 2006). See Figure 8.6 for more details.

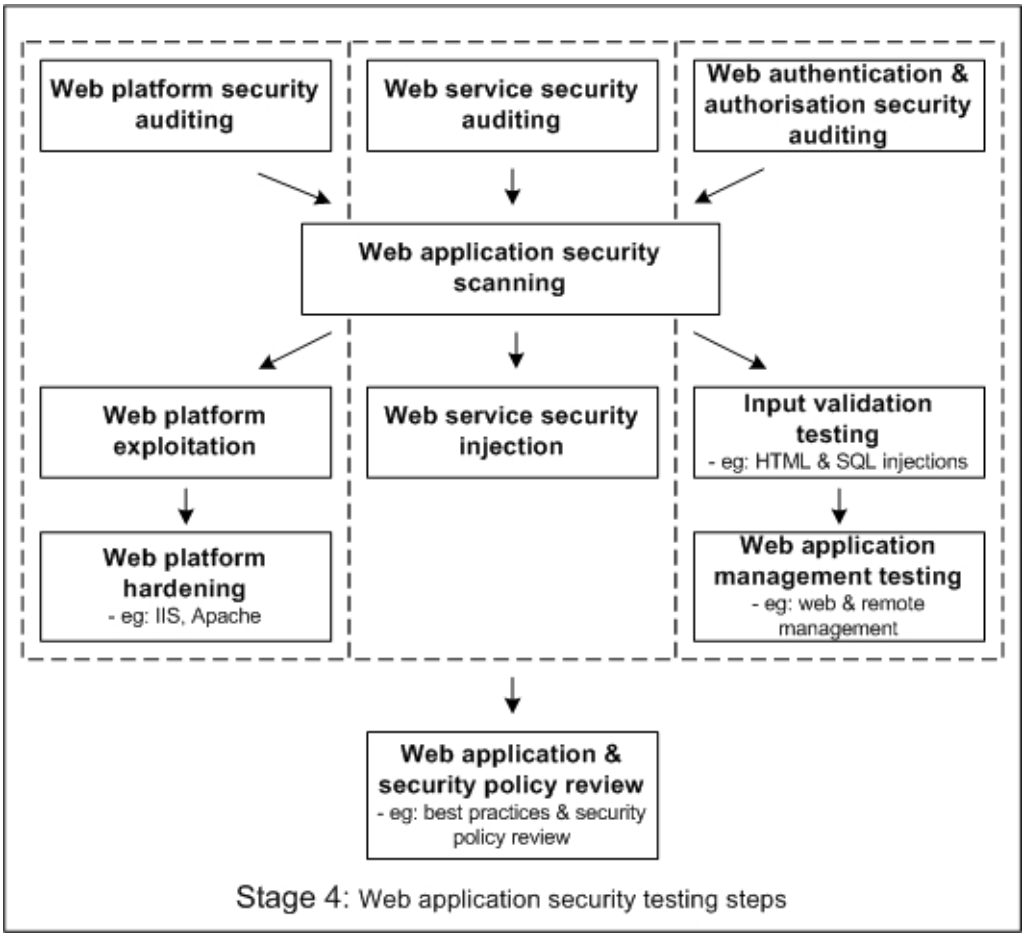

Figure 8.6. A diagram of detailing the extra web application security testing steps that would be included in the framework

This additional testing of the web application would cover the vulnerability issues related to a series of web threats and attack scenarios specific to the web application architecture deployed at each of the selected councils. In addition, the extra security testing in stage 4 would provide a defence strategy that could be deployed to mitigate any identified potential risks that the online web systems at these councils or other organsitions would be exposed to.

Another future direction would be to extend the security focus to the other online community services of the councils such as online library, online GIS and online GPS systems, in addition to the email and online web systems already covered in this research. These additions to the framework are outlined in the Figure 8.7.

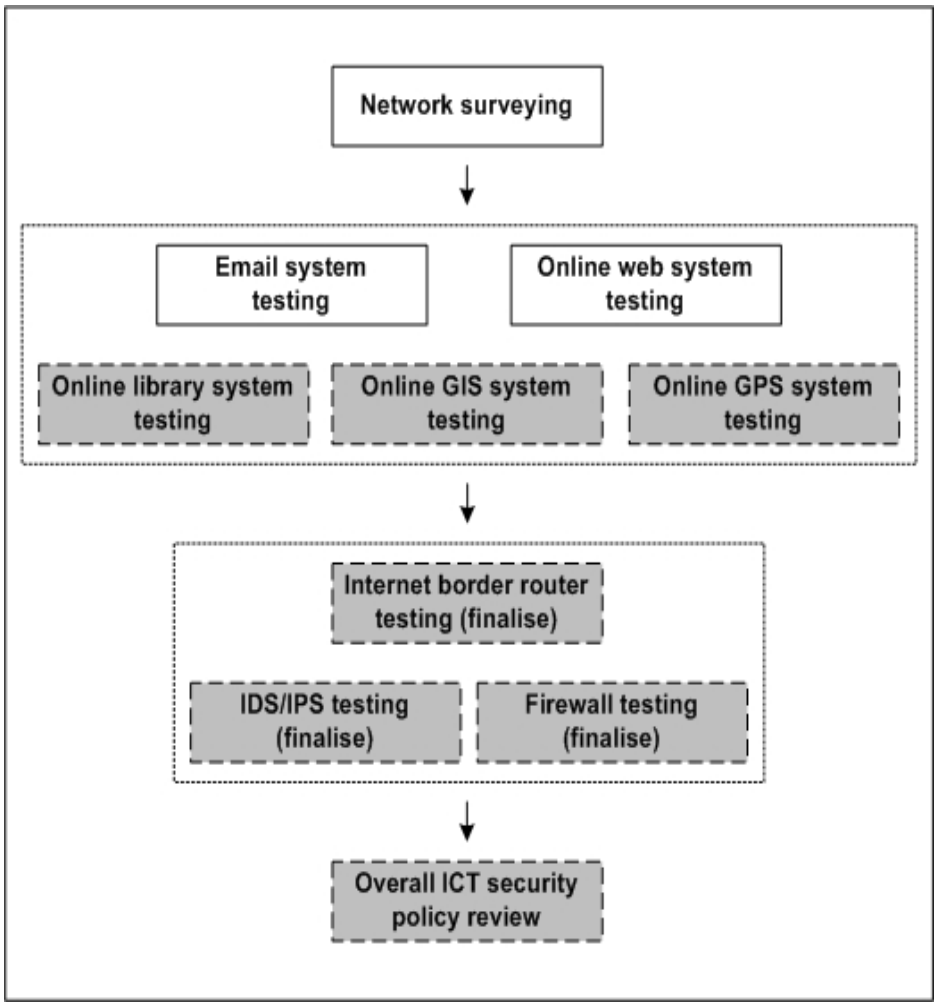

Figure 8.7. The stage module diagram incorporating all five online services for the further security enhancement of the councils

Figure 8.7 shows both the specific system testings as well as the finalised testings of the internetworking infrastructure devices and the policy review testing. The finalised testings would include services and system identification, port scanning, vulnerability and specific vendor assessment of the entire internetworking infrastructure devices such as the Internet border router, the DMZ switch(s), the firewall(s), the IDS/IPS and the reverse proxy server(s). Lastly, an overall ICT security policy review could also be included in any future undertaking.

This research has presented a multiple interpretive case based study of a method for security proofing an online communication service. This research was conducted through the extensive analysis of the email and online web systems of three selected councils. The analysis covered the details of network architecture, device configurations, port scanning, vulnerability testing, email and database auditing and related information security policy reviews. Data was gathered from stakeholders, organisation documents and network security audits (email and online web systems) in order to arrive at the conclusions put forward after the detailed analysis.

In conclusion, this research is the first step in a series of steps that provides a simple network auditing mechanism for both email and online (static, dynamic and payment) web systems. As such, the auditing mechanism could be extended to cover an audit of personal online banking websites for policy and information provided to existing and future customers based on the system of scrutiny utilised in this research. For example, the extension could commence with Australian banks and then be followed by similar audits to banks in other countries. Shifting the security focus in this way, could open up a myriad of other future research directions.

Furthermore, the extensions and future directions should further satisfy the seven principles of research expounded upon earlier. For example, porting this research and its principles to other contexts satisfy the principle of hermeneutics, contextualisation and abstraction and generalisation. Exploration of different contexts and environments also satisfy the principle of interaction between the researcher and the subjects.

REFERENCES

Abie, H., et al. (2004). The need for a digital rights management framework for the next generation of e-government services. Electronic Government, an International Journal 1(1), 8 - 28.

ABS. (2006). 8146.0: household use of information technology, Australia, 2005-06.Retrieved January, 2008, from http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/B1A7C67456AE9A09CA25724400780071/$File/81460_2005-06.pdf

ABS. (2009). 8146.0: household use of information technology, Australia, 2008-09.Retrieved November, 2010, from http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8146.02008-09?OpenDocument

Al-Ahmad, W., & Al-Kaabi, R. (2008). An extended security framework for e-government. Paper presented at the IEEE International Conference on Intelligence and Security Informatics (ISI 2008) Taipei, Taiwan.

Alavi, M., & Carlson, P. (1992). A review of MIS research and disciplinary development. Journal of Management Information Systems, 8(4), 45-62.

Allen, J., et al. (2007). Governing for enterprise security implementation guide. Retrieved January, 2008, from http://www.cert.org/governance/ges.html

Al-Mashari, M. (2007). A benchmarking study of experiences with electronic government. Benchmarking: An International Journal, 14(2), 172-185.

Australia Post. (n.d.). Postbillpay. Retrieved May, 2011, from http://www.postbillpay.com.au/

Australian Communications and Media Auhtority. (2008). Telecommunications today: Report 6 - Internet activity and content Retrieved September, 2011, from http://www.acma.gov.au/WEB/STANDARD/pc=PC_9058

Australian Government: Attorney-General's Department. (2006). Wireless security – Information for CIO's. Retrieved September, 2011, from http://www.ag.gov.au /agd/WWW/rwpattach.nsf/VAP/(7A188806B7893EBA0402BC1472412E58)~ Wirel

Basta, A., & Halton, W. (2008). Computer security and penetration testing (1st ed.). Boston: Thompson.

Benbasat, I., et al. (1987). The case research strategy in studies of information systems. MIS Quarterly, 11(3), 369-386.

Benbasat, I., & Weber, R. (1996). Research commentary: Rethinking "Diversity" in information systems research. Information systems research, 7(4), 389-399.

Berger, P. L., & Kellner, H. (1981). Sociology reinterpreted: An essay on method and vocation. Garden City, NY: Anchor Press/Doubleday.

Cacho-Elizondo, S., & Loussaïef, L. (2009). The impact of sustainable development initiatives on consumers' relationship with retailers: An exploratory study of French food retailers. Retrieved March, 2010, from www.marketing-trends-congress.com/2009.../CachoElizondo_Loussaief.pdf

Cavaye, A. L. M. (1996). Case study research: A multi-faceted research approach for IS. Information Systems Journal, 6(3), 227-242.

Check Point Software Technologies Ltd. (2010). Check Point datasheet: UTM-1 appliances. Retrieved November, 2010, from http://www.64bit.eu/soubory /3187/check-point-utm-1-datasheet.pdf?ms=3

CIS. (2007). Center for internet security benchmark for Exchange 2007 for Windows Server 2003 version 1.0. Retrieved March, 2008, from http://www. cisecurity.org/tools2/exchange/CIS_Benchmark_Exchange2007_1.0.pdf

CIS. (2010). Security configuration benchmark for Microsoft SQL Server 2005 version 1.2.0 January 12th, 2010. Retrieved March, 2010, from https://www.cisecurity.org/.../sqlserver/CIS_SQL2005_Benchmark_v1.2.0.pdf

Cisco. (2002). Action steps to improving information security. Retrieved January, 2008, from http://www.cisco.com/warp/public/cc/so/neso/sqso/roi5_wp.pdf

Cisco. (n.d.-a). Cisco IronPort S-Series web security appliances. Retrieved September, 2011, from http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/ironport_s_series_datasheet.pdf

Cisco. (n.d.-b). DNS best practices, network protections, and attack identification. Retrieved August, 2011, from http://www.cisco.com/web/about/security/intelligence/dns-bcp.html

Cisco. (n.d.-c). Configuring application protocol inspection. Retrieved August, 2011, from http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/security/guide/appinsp.html#wp1063720

Commonwealth Bank of Australia. (n.d.). BPOINT. Retrieved May, 2011, from http://www.commbank.com.au/xpos/bpoint/bpoint.asp

Dave, P. (2008). Introduction to SQL Server encryption and symmetric key encryption tutorial. Retrieved October, 2010, from http://dotnetslackers.com/articles/sql/IntroductionToSQLServerEncryptionAndSymmetricKeyEncryptionTutorial.aspx

Davis, G. B., et al. (1992). Diagnosis of an information system failure: A framework and interpretive process Information & Management, 23(5), 293-318.

DMS. (n.d.). IntraMaps. Retrieved May, 2011, from http://www.mapsolutions.com.au/intramaps.aspx

Economic Commission for Africa. (2003). E-strategies: National, sectoral and regional ICT policies, plans and strategies. Retrieved October, 2010, from http:// www. uneca.org/aisi/docs/e-strategies.pdf

Fadia, A. (2006). The unofficial guide to ethical hacking (2nd ed.). USA: Thomson Course Technology.

Farahmand, F., et al. (2003). Managing vulnerabilities of information systems to security incidents. Paper presented at the ICEC '03 Proceedings of the 5th International Conference on Electronic Commerce, New York, USA.

Farahmand, F., et al. (2005). A management perspective on risk of security threats to information systems. Information Technology and Management, 6(2-3), 203-225.

Fontana, J. (2007). DNS hole puts e-mail, directory services at risk. Retrieved January, 2008, from http://www.pcworld.idg.com.au/article/180325/dns_hole_puts_e-mail_directory_services_risk/

Ganger, D. L. (2007). Top 5 Exchange Server 2007 security best practices. Retrieved March, 2011, from http://technet.microsoft.com/en-us/library/cc512685.aspx

GFI. (2009). Network security scanning and patch management. Retrieved November, 2009, from http://www.gfi.com/lannetscan/

Gillett, S. E., et al. (2004). Local government broadband initiatives. Telecommunica tions Policy, 28(7-8), 537-558.

Glanz, L. (2003). Expatriate stories: A vehicle of professional development abroad? Journal of Managerial Psychology, 18(3), 259-274.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In K. Denzin & Y. S. Lincoln (Eds.), Handbook of qualitative research (pp. 105-117). Thousand Oaks, CA: SAGE.

Hamel, J., et al. (1993). Case study methods. Newbury Park, CA: SAGE.

Herzog, P. (2006). OSSTMM 2.2: Open-source security testing methodology manual. Retrieved January, 2008, from http://isecom.securenetltd.com/osstmm.en.2.2.pdf

Hirwade, M. A. (2010). Responding to information needs of the citizens through e-government portals and online services in India. The International Information & Library Review 42(3), 154-163.

Hwang, M.-S., et al. (2004). Challenges in e-government and security of information. Information & Security, 15(1), 9-20.

Infor. (2009). ePathway. Retrieved May, 2011, from http://www.infor.com/content /brochures/epathway.pdf/

Intel Corporation. (2005a). Core technologies for developing a digital community framework: Solutions for transforming government. Retrieved January, 2008, from http://download.intel.com/pressroom/kits/digitalcommunities/DCFramework_Whitepaper_5_081405.pdf

Intel Corporation. (2005b). Digital community best practices: Solutions for transforming government. Retrieved January, 2008, from http://www.intel. com/business/bss/industry/government/digital-community-best-practices.pdf

Intel Corporation. (2005c). The wireless city: Solutions for transforming government. Retrieved January, 2008, from http://www.intel.com/business/bss/industry/ government/wireless_city.pdf

Ishida, T., (Ed). (2003). Understanding digital cities: Cross-cultural perspectives. Cambridge, MA: MIT Press.

Joshi, S. (2011). SQL injection attack and defense. Retrieved June, 2011, from http:// www.securitydocs.com/library/3587/

Juniper Networks. (2009). Datasheet: SSG320M and SSG350M secure services gateways. Retrieved March, 2010, from http://www.juniper.net/us/en/local/pdf/datasheets/1000203-en.pdf

Kambalyal, C. (n.d.). 3-Tier architecture. Retrieved October, 2010, from http://channukambalyal.tripod.com/NTierArchitecture.pdf

Kaplan, B., & Maxwell, J. A. (1994). Qualitative research methods for evaluating computer information systems. In J. G. Anderson, C. E. Aydin & S. J. Jay (Eds.), Evaluating health care information systems: Methods and applications (pp. 45-68). Thousand Oaks, CA: SAGE.

Kiely, D. (2006). Microsoft SQL Server 2005: Protect sensitive data using encryption in SQL Server 2005. Retrieved October, 2010, from http://download.microsoft.com/download/4/7/a/47a548b9.../sqlencryption.doc

Kim, J.-W., et al. (2006). Securing e-government services. Computer, 39(11), 111-112.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Quarterly, 23(1), 67-88.

Klein, H. K., & Myers, M. D. (2001). A classification scheme for interpretive research in information systems. In E. M. Trauth (Ed.), Qualitative research in IS: Issues and trends (pp. 218-239). Hershey, PA, USA: IGI Global.

Lee, A. S. (1989). A scientific methodology for MIS case studies. MIS Quarterly 13(1), 33-52.

Limwiriyakul, S. (2009). Method for securing online community service: A study of selected Western Australian councils. Paper presented at the 7th Australian Information Security Management Conference, Perth, Western Australia.

Limwiriyakul, S., & Valli, C. (2011a). An IT security investigation into the email systems of selected local government councils in WA. Paper presented at the

International Conference on Information and Electronics Engineering (ICIEE 2011), Bangkok, Thailand.

Limwiriyakul, S., & Valli, C. (2011b). Results from the deployment of a targeted security testing framework for the testing of email systems in local government in Western Australia. International Journal of Information and Electronics Engineering (IJIEE), 1(1).

Limwiriyakul, S., & Valli, C. (2011c). An IT security investigation into the online payment systems of selected local government councils in WA. Paper presented at the 2011 International Conference on Security and Management (SAM'11), Las Vegas, Nevada, USA.

Luckett, R., et al. (2008). Microsoft Exchange Server 2007: The complete reference (2nd ed.). Berkshire, UK: McGraw-Hill Education.

Lyon, G. (2009). Nmap security scanner. Retrieved November, 2009, from http:// nmap.org

Mayo, E. (1933). The human problems of an industrial civilization. New York: MacMillan.

McDonald, D., et al. (2009). Delphi technique: Dialogue methods for understanding a problem broadly: integrating judgments. Retrieved June, 2012, from http://epress.anu.edu.au/dialogue_methods/mobile_devices/ch03s04.html

Microsoft Corporation. (2005). Improving data security by using SQL Server 2005. Retrieved October, 2010, from http://www.itsecure.hu/library/file/Biztons%C3%A1gi%20%C3%BAtmutat%C3%B3k/Adatb%C3%A1zis%20szerverek/Microsoft%20IT%20Showcase%20Improving%20Data%20Security%20by%20Using%20SQL%20Server%202005.pdf

Microsoft Corporation. (2010). N-Tier data applications overview. Retrieved November, 2010, from http://msdn.microsoft.com/en-us/library/bb384398.aspx

Microsoft Exchange Documentation Team. (2006). An overview of Microsoft Exchange Server 2007. Retrieved October, 2009, from http://www.priasoft.com/.../Exchange2007_Overview_WhitePaper.pdf

Microsoft Exchange Documentation Team. (2009). Exchange Server 2007 planning. Retrieved March, 2010, from http://www.microsoft.com/downloads/en/details.aspx?FamilyID=1A6EFDD6-D80E-489D-9A1D-8F3E01BAA3C5&displaylang=en

Microsoft TechNet. (2004). Securing Exchange communications Retrieved March, 2008, from http://technet.microsoft.com/en-us/library/dd277366.aspx

Microsoft TechNet. (2005a). Telnet Client concepts. Retrieved March, 2008, from http://technet.microsoft.com/en-us/library/cc740241(WS.10).aspx

Microsoft TechNet. (2005b). Telnet Client overview. Retrieved March, 2008, from http://technet.microsoft.com/en-us/library/cc757343(WS.10).aspx

Microsoft TechNet. (2007a). IT showcase: Exchange Server 2007 design and architecture at Microsoft. Retrieved March, 2008, from http://www.microsoft.com/downloads/en/details.aspx?FamilyID=98C522BC-814A-421A-99C0-D964ED119C0D&displaylang=en&displaylang=en

Microsoft TechNet. (2007b). Overview of Outlook Anywhere. Retrieved March, 2008, from http://technet.microsoft.com/en-us/library/bb123741(EXCHG.80).aspx

Microsoft TechNet. (2007c). Recommendations for Outlook Anywhere. Retrieved March, 2008, from http://technet.microsoft.com/en-us/library/aa997703(EXCHG.80).aspx

Microsoft TechNet. (2009). Planning for Client Access Servers. Retrieved January, 2010, from http://technet.microsoft.com/en-us/library/bb232184(v=exchg.140).aspx

Miles, M. B., & Huberman, A. M. (1984). Qualitative data analysis: A source book of new methods. Beverly Hills, CA: SAGE.

Myers, M. (2000). Qualitative research and the generalizability question: Standing firm with Proteus [Electronic Version]. The Qualitative Report, 4. Retrieved February 2011 from http://www.nova.edu/ssss/QR/QR4-3/myers.html.

Myers, M. D. (1997). Qualitative research in information systems. MIS Quarterly 21(2), 241-242.

Myers, M. D. (2009). Qualitative research in business & management. London: Sage Publications.

Myers, M. D., & Walsham, G. (1998). Exemplifying interpretive research in information systems: An overview Journal of Information Technology, 13(4), 233-234.

Neuman, W. L. (1997). Social research methods: Qualitative and quantitative approaches (3rd ed.). Boston, USA: Allyn & Bacon.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. Information System Research, 2(1), 1-28.

Ortiz, J. A., & Tapia, A. H. (2008a). Keeping promises: Municipal communities struggle to fulfill promises to narrow the digital divide with municipal-community wireless networks. The Journal of Community Informatics – Special issue on wireless networking for communities, citizens and the public interest, 4(1).

Ortiz, J. A., & Tapia, A. H. (2008b). On democracy, public participation, and ethics, municipal wireless networks: Toward justice for all? Sociological Focus Journal, 41(3), 256-275.

OWASP. (2009). Buffer overflow. Retrieved March, 2009, from http://www.owasp.org/index.php/Buffer_Overflow

Paul, S., et al. (2011). Architectures for the future networks and the next generation internet: A survey Computer Communications, 34(1), 2-42.

Pazalos, K., et al. (2010). A structured methodology for assessing and improving e-services in digital cities. Telematics and Informatics, 1-14.

Phiri, J., & Agbinya, J. I. (2006). Modelling and information fusion in digital identity management systems. Paper presented at the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06), Morne, Mauritius.

Pinto, J. K., & Slevin, D. P. (1989). The project champion: Key to implementation success. Project Management Journal, 20(4), 15-20.

Rathore, B., et al. (2006). Information systems security assessment framework (ISSAF) draft 0.2.1. Retrieved January, 2009, from http://www.oissg.org/downloads/issaf-0.2/index.php

Reddick, C. G. (2005). Citizen interaction with e-government: From the streets to servers? Government Information Quarterly, 22(1), 38–57.

Robey, D. (1979). User attitudes and management information system use. Academy of Management Journal, 22(3), 527-538.

Scambray, J., et al. (2001). Hacking exposed: Network security secrets & solutions (2nd ed.). Osborne: McGraw-Hill.

Scambray, J., et al. (2006). Hacking exposed web applications (2nd ed.): McGraw-Hill Osborne Media.

Secure Computing Corporation. (2006). Eliminating your SSL blind spot: The solution to managing—and securing—HTTPS traffic. Retrieved February, 2011, from http://www.silicon.com/i/s/wp/spnsr/securecomputing/WW-SSL-WP-Aug06vF1.pdf

Shan, S., & Wang, J. (2009). A study on the evaluation model for development of local eGovernment in China. Paper presented at the Management and Service Science, 2009. MASS '09. International Conference on, Wuhan.

Speed Guide. (n.d.-a). Port 9 details. Retrieved October, 2010, from http://www.speedguide.net/port.php?port=9

Speed Guide. (n.d.-b). Port 19 details. Retrieved October, 2010, from http://www.speedguide.net/port.php?port=19

Speed Guide. (n.d.-c). Port 79 details. Retrieved October, 2010, from http://www.speedguide.net/port.php?port=79

Speed Guide. (n.d.-d). Port 666 details. Retrieved October, 2010, from http://www.speedguide.net/port.php?port=666

Speed Guide. (n.d.-e). Port 999 details Retrieved October, 2010, from http://www.speedguide.net/port.php?port=999

Speed Guide. (n.d.-f). Port 1080 details. Retrieved October, 2010, from http://www.speedguide.net/port.php?port=1080

Speed Guide. (n.d.-g). Port 1900 details. Retrieved October, 2010, from http://www.speedguide.net/port.php?port=1900

Speed Guide. (n.d.-h). Port 1999 details. Retrieved October, 2010, from http://www.speedguide.net/port.php?port=1999

Speed Guide. (n.d.-i). Port 2049 details. Retrieved October, 2010, from http://www.speedguide.net/port.php?port=2049

Speed Guide. (n.d.-j). Port 6969 details. Retrieved October, 2010, from http://www.speedguide.net/port.php?port=6969

Stanford University. Residential Computing. (2007). Information & news: Wireless in the residences: What to buy and how to configure it. Retrieved February, 2011, from http://rescomp.stanford.edu/info/wireless/recommendation.html

Stanton, D. (2004). Local e-government in Western Australia: How prepared are councils to deliver services and interact with communities in an electronic environment? Retrieved January, 2008, from http://www.finance.gov.au/publications/future-challenges-for-egovernment/docs/AGIMO-FC-no1.pdf

Stewart, J. (2003). Third-party mail relay (open relay) and Microsoft Exchange Server. Retrieved January, 2008, from http://www.sans.org/reading_room/ whitepapers/email/third-party-mail-relay-open-relay-microsoft-exchange-server_963

Steyaert, J. (2000). Local government online and the role of the resident. Social Science Computer Review, 18(1), 3-16.

Tanabe, M., et al. (2002). Digital cities In LNCS 2362 (pp. 101–109). Berlin, Heidelberg: Springer-Verlag.

Tapia, A., et al. (2006). Making IT work for municipalities: Building municipal wireless networks Government Information Quarterly, 23(3-4), 359-380.

Teece, D. J. (2010). Business models, business strategy and innovation Long Range Planning, 43(2-3), 172-194.

Tellis, W. (1997). Introduction to case study The Qualitative Report, 3(2).

Torres, L., et al. (2005). E-government developments on delivering public services among EU cities Government Information Quarterly, 22(2), 217-238.

Tracy, M., et al. (2007). Guidelines on securing public web servers: Recommendations of the National Institute of Standards and Technology. Retrieved January, 2008, from http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP80044v2.pdf

VeriSign Authentication Services. (n.d.). FAQ: Extended validation SSL. Retrieved May, 2011, from http://www.verisign.com.au/ssl/ssl-information-center/extended-validation-ssl-certificates/

Wack, J., et al. (2003). Guideline on network security testing. Retrieved January, 2008, from http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf

WALGA. (2007). Local government: Council websites. Retrieved January, 2008, from http://www.walga.asn.au/careers/council_websites

WALGA. (2010a). ICT online services. Retrieved November, 2010, from http://www.walga.asn.au/products_services/documents/directory/ict_online_services.pdf

WALGA. (2010b). Local government: Council websites. Retrieved November, 2010, from http://www.walga.asn.au/careers/council_websites

Walsham, G. (1993). Interpreting information systems in organizations. Chichester: Wiley

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. European Journal of Information Systems 4(2), 74–81.

Websense. (2010). Websense content gateway HTTPS configuration. Retrieved February, 2011, from http://kb.websense.com/pf/12/webfiles/Webinars/webinar_pdf/February 202010_WebinarSlides.pdf

Whitman, M. E., & Mattord, H. J. (2006). Principles of incident response and disaster recovery (1st ed.). USA: Thomson Course Technology.

Williamson, K., et al. (2002). Research methods for students, academics and professionals: Information management and systems (2nd ed.). Wagga Wagga, NSW: Centre for Information Studies, Charles Sturt University.

Yin, R. (1984). Case study research: Design and method (1st ed.). Beverly Hills, CA: SAGE.

Yin, R. (1993). Applications of case study research. Beverly Hills, CA: SAGE.

Yin, R. (1994). Case study research: Design and method (2nd ed.). Beverly Hills, CA: SAGE.

APPENDICES

Appendix A: Additional results for Chapter 4

Appendix A1: A summary of the firewall configuration codes (email-NAT) of Council A's firewall

Policy no.	Rules	From (source)	To (destination)
1	Translate	A.B.C.82	192.168.1.92
2	Translate	A.B.C.89	172.16.25.251

Appendix A2: A summary of the firewall configuration codes of Council A's email system

Policy no.	Rules	Protocol types	Interface	From (source)	To (destination)	Ports (service)
1	Permit	TCP	Outside	Any	192.168.1.92	SMTP
2	Permit	TCP	Inside	172.16.25.251	192.168.1.92	SMTP
3	Permit	TCP	Inside	172.16.25.251	192.168.1.92	SSH
4	Permit	TCP	Inside	172.16.25.70	192.168.1.92	MS-DS
5	Permit	UDP	DMZ	192.168.1.92	Any	DNS
6	Permit	TCP	DMZ	192.168.1.92	Any	HTTP
7	Permit	TCP	DMZ	192.168.1.92	Any	HTTPS
8	Permit	TCP	DMZ	192.168.1.92	172.16.5.70	MS-DS
9	Permit	TCP	DMZ	192.168.1.92	172.16.5.70	LDAP
10	Permit	TCP	DMZ	192.168.1.92	172.16.25.251	SMTP
11	Permit	TCP	DMZ	192.168.1.92	Any	SMTP
12	Permit	TCP	Inside	172.16.25.251	192.168.1.93	SMTP
13	Permit	TCP	DMZ	192.168.1.93	172.16.25.251	SMTP
14	Permit	TCP	DMZ	192.168.1.93	Any	SMTP
15	Permit	TCP	Inside	172.16.25.251	Any	SMTP
16	Permit	TCP	Inside	172.16.25.251	192.168.1.89	ms-wbt-server
17	Permit	TCP	Inside	172.16.25.251	Any	HTTPS

Appendix A3: A full details of system information policy results of Council A's email server

System information policy – CoA-email server (172.16.25.251)				
Services				
116				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length:	6 chars		At least 8 chars	
Maximum password age:	30 days		30 days	
Minimum password age:	0 day		0 day	
Force logoff:	Never force		Force	
Password history:	3 passwords		N/A	
Security auditing policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	No	Yes	Yes
Audit account management	No	No	Yes	Yes
Audit directory service access	No	No	Yes	Yes
Audit logon events	Yes	No	Yes	Yes
Audit object access	No	No	Yes	Yes
Audit policy change	No	No	Yes	Yes
Audit privilege use	No	No	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	No	No	Yes	Yes

Appendix A4: A summary of both missing service packs and patches information of Council A's email server

Missing service pack (0) – email server (172.16.25.251)				
Product	**Severity**	**Description**	**Vulnerability issue**	**Recommendation**
N/A	NA/	N/A	N/A	N/A
Missing patches (9) – email server (172.16.25.251)				
Products	**Severities**	**Descriptions**	**Vulnerability issues**	**Recommendations**
Windows	Moderate	KB961501	in Windows print spooler could allow remote code execution	Deploy/patch
Windows	Important	KB968537	in Windows kernel could allow elevation of privilege	Deploy/patch asap
Windows	Important	KB970238	in RPC could allow elevation of privilege	Deploy/patch asap
Windows	Important	KB970483	in IIS could allow elevation of privilege	Deploy/patch asap
Windows	Important	KB956803	in the MS Ancillary function driver could allow elevation of privilege	Deploy/patch asap
Windows	N/A	KB951072	cumulative time zone update for MS Windows OS	Deploy/patch
Exchange	N/A	KB960384	many vulnerabilities based on update rollup 7 for MS Exchange Server 2007 service pack 1	Deploy an update rollup 7 for MS Exchange Server 2007 service pack 1 asap.
Exchange	Critical	KB959241	many vulnerabilities based on update rollup 6 for MS Exchange Server 2007 service pack 1	Deploy an update rollup 6 for MS Exchange Server 2007 service pack 1 immediately.
Exchange	Important	KB949870	many vulnerabilities based on update rollup 3 for MS Exchange Server 2007 service pack 1	Deploy update rollup 3 for MS Exchange Server 2007 service pack 1 asap.

Appendix A5: The overall opened TCP and UDP service ports, and the possible mitigation recommendation on Council A's email server

The overall opened TCP service ports (31) – email server (172.16.25.251)				
Port no.	**Services**	**Descriptions**	**Products**	**Recommendations**
25	SMTP	Simple Mail Transfer Protocol	MS ESMTP	Open
80	HTTP	Hyper Text Transfer Protocol	MS IIS webserver 6.0	Open
110	POP3-proxy	Post Office Protocol 3	AVG POP3 proxy 8.5.373/8.5.374	Close
135	MSRPC	MS Remote Procedure Call	MS Windows RPC	Open
139	NetBIOS-ssn	NetBIOS session service	NetBIOS session service	Open
143	imap	Internet message access protocol	MS Exchange 2007 imapd	Close
443	HTTPS	HTTP over TLS/SSL	MS IIS webserver 6.0	Open
445	microsoft-ds	MS-DS active directory, Windows shares	MS Windows 2003	Open
587	MS ESMTP	email message submission	MS ESMTP	Close
593	ncacn_http_ epmap	HTTP RPC Ep Map	MS Windows RPC over HTTP 1.0	Close
993	Imaps	Internet message access protocol over SSL	MS Exchange 2007 imapd	Close
995	POP3S	Post office protocol 3 over TLS/SSL	MS Exchange 2007 POP3d	Close
1046	msrpc	MS Windows RPC		Close
1052	ddt	Dynamic DNS tools		Close
1098	rmiactivation	RMI activation		Close
1114	mini-sql	Mini SQL		Close
1124	hpvmmcontrol	HP VMM control		Close
1127	kwdb-commn	KWDB remote communication		Close
1149	bvtsonar	BVT sonar service		Close
1192	caids-sensor	caids sensors channel		Close
1232	msrpc	MS Windows RPC	MS Windows RPC	Close
1239	nmsd	NMSD		Close
1283	productinfo	Product information		Close
3128	ndl-aas	Active API server port		Close
3389	microsoft-rdp		MS terminal service	Open
6001-6002, 6004	ncacn_http	MS Windows RPC	MS Windows RPC over HTTP 1.0	Close
8080	http-alt	HTTP alternate		Open

The overall opened TCP service ports (31) – email server (172.16.25.251) (continued)				
Port no.	**Services**	**Descriptions**	**Products**	**Recommendations**
8400	cvp	Commvault unified data management		Close
8402	galaxy		Galaxy client event manager	Close
The overall opened UDP service ports (5) – email server (172.16.25.251)				
Port no	**Services**	**Descriptions**	**Products**	**Recommendations**
137	netbios-ns	NETBIOS Name Service	MS Windows NT netbios-ssn	Open
138	netbios-dgm	NETBIOS datagram service		Close
445	microsoft-ds	Microsoft-DS SMB file sharing		Close if not required
500	isakmp	Internet Security Association and Key Management Protocol		Close
4500	nat-t-ike	IPsec NAT-Traversal (RFC 3947)		Close

Appendix A6: A summary of Council A's email server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of Council A's email server (172.16.25.251)	
High security vulnerabilities (2)	
Section: Types	**Recommendations**
Miscellaneous: AutoRun is enabled	It is a virtual server, no action is required.
Services: TCP port 110 (POP3) open	Should be disabled
Low security vulnerabilities (7)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Services: FTP	Should be disabled
Services: HTTP	Should be disabled if not required
Services: HTTPS	Satisfactory
Services: IMAP	Should be disabled
Services: POP3	Should be disabled
Services: SMTP	Satisfactory
Potential vulnerabilities (3)	
Section: Types	**Recommendations**
Information: Administrator account exists	Rename the administrator account.
Information: Some IMAP4 server banners providing information to attacker	The service POP3 server should be turned off.
Information: Some POP3 server banners providing information to attacker	The service POP3 server should be turned off.

Appendix A7: A summary of the firewall configuration codes for Council A's online payment system

Policy no.	**Rules**	**Protocol types**	**From (source)**	**To (destination)**	**Ports (service)**
1	Translate	N/A	A.B.C.84	192.168.1.84	N/A
2	Permit	TCP	Any	A.B.C.84	https (443)
3	Permit	TCP	172.16.25.73	192.168.1.84	www (80)
4	Permit	TCP	172.16.25.75	192.168.1.84	www (80)
5	Permit	IP	172.16.21.21 (admin)	192.168.1.84	Any
6	Permit	IP	172.16.21.22 (admin)	192.168.1.84	Any
8	Permit	TCP	172.16.25.40	192.168.1.84	ms-wbt-server (3389)
9	Permit	TCP	172.16.25.227	192.168.1.84	avenue (2134)
10	Permit	TCP	192.168.1.84	172.16.25.173	www (80)
11	Permit	TCP	192.168.1.84	172.16.25.175	www (80)
12	Permit	TCP	192.168.1.84	Any	www (80)
13	Permit	TCP	192.168.1.84	Any	https (443)
14	Permit	UDP	192.168.1.84	Any	domain (53)
15	Permit	TCP	192.168.1.84	172.16.25.68	m-sql-s (1433)
16	Permit	TCP	192.168.1.84	172.16.25.214	bb (1984)
17	Permit	TCP	192.168.1.84	172.16.25.214	www (80)
18	Permit	TCP	192.168.1.84	172.16.25.64	m-sql-s (1433)
19	Permit	TCP	192.168.1.84	172.16.25.194	www (80)
20	Permit	TCP	192.168.1.84	172.16.25.193	www (80)
21	Permit	TCP	192.168.1.84	172.16.25.227	avenue (2134)

Appendix A8: A full details of system information policy results and recommendations of Council A's CoA-DMZ-Epathway server

System information policy – CoA-DMZ-Epathway server (192.168.1.84)				
Services				
102				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	0 char		At least 8 chars	
Maximum password age	42 days		30 days	
Minimum password age	0 day		0 day	
Force logoff	Never force		Force	
Password history	No history		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	No	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	No	Yes	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	Yes	Yes	Yes	Yes

Appendix A9: A full details of system information policy results and recommendations of Council A's CoA-Pathway server

System information policy – CoA-Pathway server (172.16.25.173)				
Services				
N/A (could not obtained the services information; access denied)				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	6 chars		At least 8 chars	
Maximum password age	45 days		30 days	
Minimum password age	2 days		0 day	
Force logoff	Never force		Force	
Password history	6 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	Yes	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	No	Yes	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	Yes	No	Yes	Yes

Appendix A10: A full details of system information policy results and recommendations of Council A's CoA-SQL server

System information policy – CoA-SQL server (172.16.25.227)				
Services				
N/A (due to error connecting to WMI server: Access was denied)				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	6 chars		At least 8 chars	
Maximum password age	45 days		30 days	
Minimum password age	2 days		0 day	
Force logoff	Never force		Force	
Password history	6 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	Yes	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	No	Yes	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	Yes	No	Yes	Yes

Appendix A11: A summary of missing service pack and patches, and the possible mitigation recommendations for the CoA-Pathway server

Missing service pack (1) – CoA-Pathway server (172.16.25.173)				
Product	**Filename**	**Knowledge base**	**Vulnerability issue**	**Recommendation**
Virtual Studio	VS80sp1-KB926601-X86-ENU.exe	N/A	Virtual studio 2005 service pack 1	Deploy/patch
Missing patches (2) – CoA-Pathway server (172.16.25.173)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
Windows	Low	N/A	Windows IE 7 for MS Windows Server 2003	Deploy/patch
SDK components	Critical	KB931906	MS07-028 security update for CAPICOM	Deploy/patch asap

Appendix A12: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the CoA-DMZ-Epathweb server

The overall opened TCP service ports (22) – CoA-DMZ-Epathweb server (192.168.1.84)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
21	FTP	File Transfer Protocol	Close
80	HTTP	Hyper Text Transfer Protocol, MS IIS webserver 6.0	Close if not required
110	POP3	Post Office Protocol 3	Close
135	MSRPC	MS Remote Procedure Call, MS Windows RPC	Close if not required
139	NetBIOS-ssn	NetBIOS session service	Close if not required
443	HTTPS	Hypertext Transfer Protocol over TLS/SSL MS IIS webserver 6.0	Open
445	Microsoft-ds	MS-DS active directory, Windows shares MS Windows 2003	Close
1025	MSRPC	MS Windows RPC	Close if not required
1038	MTQP	Message Tracking Query Protocol	Close
1049	Flexlm	FlexLM license manage	Close
3128	NDL-AAS	Active API server port	Close
3389	Microsoft-rdp	MS WBT server, MS terminal service	Open
5168	MSRPC	MS Remote Procedure Call, MS Windows RPC	Close
5169	MSRPC	MS Remote Procedure Call, MS Windows RPC	Close
5555	Omiback	HP open view omniback	Close
5988	Tcpwrapped	Tcpwrapped	Close
5989	SSL/TCPwrapped	SSL/TCPwrapped	Close
8080	HTTP alternate	Alternate HTTP port	Open
8400	CVP	Commvault unified data management	Close
8402	Galaxy	Galaxy client event manager	Close
8600	Asterix	Surveillance data	Close
14247	Unassigned	Unassigned	Close
The overall opened UDP service ports (11) – CoA-DMZ-Epathweb server (192.168.1.84)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
1	Sockets des Troie	Remote access/ICQ Trojan	Close
53	Domain	Domain name server	Open
69	TFTP	Trivial File Transfer	Close
137	NetBIOS-ns	NetBIOS name service MS Windows NT NetBIOS-ssn	Close if not required

The overall opened UDP service ports (11) – CoA-DMZ-Epathweb server (192.168.1.84) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
138	NetBIOS-dgm	NetBIOS datagram service	Close if not required
445	ms-ds	Microsoft-DS SMB file sharing	Close
500	Isakmp	Internet security association and key management protocol	Close if not required
1755	WMS	Microsoft Media Services (MMS, ms-streaming)	Close
4500	Nat-t-ike	IPSec NAT-traversal (RFC 3947)	Close if not required
8012	Ptakks	Backdoor.Ptakks, remote access/keylogger	Close
61747	KiLo	Remote access	Close

Appendix A13: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the CoA-Pathway server

The overall opened TCP service ports (22) – CoA-Pathway server (172.16.25.173)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
21	FTP	File Transfer Protocol	Close
80	HTTP	Hyper Text Transfer Protocol, MS IIS webserver 6.0	Open
110	POP3	Post Office Protocol 3	Close
135	MSRPC	MS Remote Procedure Call, MS Windows RPC	Open
139	NetBIOS-ssn	NetBIOS session service	Open
445	Microsoft-ds	MS-DS active directory, Windows shares MS Windows 2003	Open
1025	MSRPC	MS Windows RPC	Close if not required
1049	Flexlm	FlexLM license manage	Close
1068	Instl_bootc	instl_bootc, installation bootstrap proto. Cli.	Close
3104	Autocuelog	Autocue logger protocol	Close
3128	NDL-AAS	Active API server port	Close
3389	Microsoft-rdp	MS WBT server, MS terminal service	Open
4105	Ca-mq	CA message queuing server	Close
4728	Capmux	CA port multiplexer	Close
5988	Tcpwrapped	Tcpwrapped	Close
5989	SSL/TCPwrapped	SSL/TCPwrapped	Close
7166	aruba-server/Flexlm	Aruba eDiscovery Server	Close if not required
7188	Unassigned	Unassigned	Close
8080	HTTP alternate	Alternate HTTP port	Open
8400	CVP	Commvault unified data management	Close
8402	Galaxy	Galaxy client event manager	Close
14247	Unassigned	Unassigned	Close
The overall opened UDP service ports (9) – CoA-Pathway server (172.16.25.173)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
5	RJE	Remote job entry	Close
13	Daytime	Daytime (RFC 867)	Close
18	MSP	Message send protocol	Close
137	NetBIOS-ns	NetBIOS name service MS Windows NT NetBIOS-ssn	Open/ Close if not required
138	NetBIOS-dgm	NetBIOS datagram service	Open/ Close if not required

The overall opened UDP service ports (9) – CoA-Pathway server (172.16.25.173) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
445	Microsoft-ds	MS-DS SMB file sharing	Open
500	Isakmp	Internet security association and key management protocol	Close
1051	Optima-vnet	Optima VNET	Close
4500	Nat-t-ike	IPSec NAT-traversal (RFC 3947)	Close

Appendix A14: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the CoA-SQL server

The overall opened TCP service ports (23) – CoA-SQL server (172.16.25.227)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
21	FTP	File Transfer Protocol	Close
80	HTTP	Hyper Text Transfer Protocol, MS IIS webserver 6.0	Open
110	POP3	Post Office Protocol 3	Close
111	Rpcbind	SUN Remote Procedure Call	Close
135	MSRPC	MS Remote Procedure Call, MS Windows RPC	Open
139	NetBIOS-ssn	NetBIOS session service	Open
445	Microsoft-ds	MS-DS active directory, Windows shares MS Windows 2003	Open
775	Rpcbind	Entomb	Close
1042	MSRPC	MS Windows RPC	Open
1050	Java-or-OTGfileshare	J2EE nameserver, also OTG, also called Disk/Application extender. Could also be MiniCommand backdoor OTGlicenseserv	Close
1215	MSRPC	MS remote procedure call, MS Windows RPC	Close if not required
1433	MS-SQL-S	MS-SQL-server	Open
1518	MSRPC	MS remote procedure call, MS Windows RPC	
2134	Assigned	Council A's assigned port	Open
3104	Autocuelog	Autocue logger protocol	Close
3128	NDL-AAS	Active API server port	Close
3389	Microsoft-rdp	MS WBT server, MS terminal service	Open
4105	CA-MQ	CA Message Queuing server	Close
4443	MSRPC	MS remote procedure call, MS Windows RPC	Close
4728	Capmux	CA port multiplexer	Close
8080	HTTP alternate	Alternate HTTP port	Open
8400	CVP	Commvault unified data management	Close
8402	Galaxy	Galaxy client event manager	Close
The overall opened UDP service ports (14) – CoA-SQL server (172.16.25.227)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
111	Rpcbind	SUN remote procedure call	Close
123	NTP	Network time protocol	Close
135	MSRPC	MS remote procedure call, MS Windows RPC	Open/Close if not required

The overall opened UDP service ports (14) – CoA-SQL server (172.16.25.227) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
137	NetBIOS-ns	NetBIOS name service MS Windows NT NetBIOS-ssn	Open/Close if not required
138	NetBIOS-dgm	NetBIOS datagram service	Open/Close if not required
161	SNMP	SNMP	Close
445	Microsoft-ds	Microsoft-DS SMB file sharing	Open
500	Isakmp	Internet security association and key management protocol	Close
753	RRH	Reverse Routing Header	Close
1025	MSRPC	MS remote procedure call, MS Windows RPC	Close if not required
1026	Winrpc	Windows RPC	Close
1069	Cognex-insight	COGNEX-INSIGHT	Close
1434	MS-SQL-M	Microsoft-SQL-monitor	Open
4500	Nat-t-ike	IPSec NAT-traversal (RFC 3947)	Close

Appendix A15: A summary of Council A's CoA-DMZ-Epathweb server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of Council A's CoA-DMZ-Epathweb server	
High security vulnerabilities (6)	
Section: Types	**Recommendations**
Backdoor – open ports commonly used by Trojans: Sockets des Troie (1)	Disable port 1
Backdoor – open ports commonly used by Trojans: NetControle (1772)	Disable port 1772
Backdoor – open ports commonly used by Trojans: Ptakks (8012)	Disable port 8012
Backdoor – open ports commonly used by Trojans: KiLo (61747)	Disable port 61747
Miscellaneous: AutoRun is enabled	Disable AutoRun both for CD/DVD drives and also other removable drives
Services: POP3	Disable POP3 port
Low security vulnerabilities (7)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Registry: Last logged-on username visible	Should be disabled
Registry: Windows AutoUpdate is enabled but requires user intervention for both patch download and installation	No further action is required
Services: FTP	Disable FTP service port
Services: HTTP	No further action is required
Services: HTTPS	No further action is required
Potential vulnerabilities (2)	
Section: Types	**Recommendations**
Information: Administrator account exists	It is recommended to rename this account.
Information: Some POP3 server banners providing information to attacker	Disable POP3 service port

Appendix A16: A summary of Council A's CoA-Pathway server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of the Council A's CoA-Pathway server	
High security vulnerability (1)	
Section: Type	**Recommendation**
Services: POP3	Disable POP3 port
Low security vulnerabilities (2)	
Section: Types	**Recommendations**
Services: HTTP	No further action is required
Services: FTP	Disable FTP service port

Appendix A17: A summary of Council A's CoA-SQL server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of the Council A's CoA-SQL server	
High security vulnerabilities (2)	
Section: Types	**Recommendations**
Backdoor – open ports commonly used by Trojans: Force (1215)	Disable port 1215
Services: POP3	Disable POP3 port
Low security vulnerabilities (2)	
Section: Types	**Recommendations**
Services: HTTP	No further action is required
Services: FTP	Disable FTP service port
Potential vulnerabilities (2)	
Section: Types	**Recommendations**
Information: MS SQL server	
Information: Some POP3 server banners providing information to attacker	Disable POP3 service port

Appendix A18: OS and network specification configuration

OS and network specification configuration				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
1.1	Physical security	Place the SQL server in an area where it will be physically secure.	Satisfactory	H
1.2	Domain environment	If the SQL Server is in a domain that is trusted by other domains, document the access granted by the trust.	Satisfactory; only IT administrator groups are allowed to access the online backend database server.	H
1.3	SQL servers accessed via Internet	If the SQL server is being accessed via the Internet, place the SQL Server inside a DMZ with the Web Server.	Satisfactory; there is a frontend web (CoA-DMZ-Epathweb) server located in the DMZ.	H
1.4	SQL servers accessed via Internet	Put a firewall between your server and the Internet. Block TCP port 1433 and UDP port 1434 on your perimeter firewall. If named instances are listening on additional ports, block those too. In a multi-tier environment, use multiple firewalls to create more secure screened subnets	Satisfactory; the SQL server is located be hide the Internet firewall, and both TCP port 1433 and 1434 are blocked from external access.	H
1.5	Encryption	Implement SSL. Use the fully-qualified DNS name of the frontend web server in the certificate to help prevent masquerading.	Satisfactory; the Epathway frontend server uses SSL and fully qualified DNS name.	H
1.6	Test and development servers	Maintain test and development servers on a separate network segment from the production servers.	Not satisfactory (the test and development servers are on the same class C network).	H
1.7	Dedicated server	Install SQL server on a computer that does not provide additional services, e.g., Web or mail services.	Satisfactory; the SQL server is only for SQL database operation.	M
1.8	OS benchmark configuration	Configure Windows 2003 server level I benchmark settings with the following modifications:		
1.8.1	Windows accounts	Make sure the Windows guest account is disabled.	Satisfactory	M
1.8.2	Disk subsystem	Use RAID for critical data files.	Satisfactory; raid level 10: database and temp drives raid level 5: backup drive.	M

OS and network specification configuration (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
1.8.3	Separate partitions	Create separate partitions for OS/SQL program files, SQL data files, and SQL transaction logs.	Satisfactory	M
1.8.4	Volume / partition type	Format all volumes with NTFS	Satisfactory	H
1.9	Services	Disable the following services on a SQL server machine		
1.9.1		Alerter	Not satisfactory; currently set to Started Automatic.	P
1.9.2		Clipbook server	Not satisfactory; currently set to Started Automatic.	P
1.9.3		Computer browser	Not satisfactory; currently set to Started Automatic.	L
1.9.4		DHCP client	Not satisfactory; currently set to Started Automatic.	L
1.9.5		Distributed file system	Not satisfactory; currently set to Started Manual.	L
1.9.6		Distributed transaction coordinator	Not satisfactory; currently set to Started Automatic.	L
1.9.7		Fax service	Satisfactory; (disabled).	P
1.9.8		Internet connection sharing	Satisfactory; (disabled).	L
1.9.9		IPSec policy agent	Satisfactory; (disabled).	L
1.9.10		License logging	Satisfactory; (disabled).	L
1.9.11		Logical disk manager administrative service	Not satisfactory; currently set to Started Automatic (this service is needed by the system administrator).	L
1.9.12		Messenger	Satisfactory; (disabled).	P
1.9.13		NetMeeting remote desktop sharing	Satisfactory; (disabled).	P
1.9.14		Network DDE	Satisfactory; (disabled).	L
1.9.15		Network DDE DSDM	Satisfactory; (disabled).	L
1.9.16		Print spooler	Satisfactory; (disabled).	L
1.9.17		Remote access connection manager	Satisfactory; (disabled).	L
1.9.18		Remote registry	Not satisfactory; currently set to Started Automatic	L
1.9.19		Removable storage	Satisfactory; (disabled).	P
1.9.20		RunAs service	Satisfactory; (disabled)	M
1.9.21		Smart card	Satisfactory; (disabled).	P
1.9.22		Smart card helper	Satisfactory; (disabled)	P

OS and network specification configuration (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
1.9.23		Task scheduler	Not satisfactory; currently set to Started Automatic.	P
1.9.24		Telephony	Satisfactory; (disabled).	P
1.9.25		Telnet	Satisfactory; (disabled).	L
1.9.26		Windows installer	Satisfactory; (disabled).	L
1.10	MSSQL server service account	Use a low-privileged local or Domain account for the MS SQL server service.	Satisfactory	M
1.11	SQL server agent service account	Use a low-privileged domain account for SQL server agent if replication, DTS, or other inter-server connection is required.	Satisfactory	M
1.12	Local users group membership	Assign the local service account as a member of only the users group.	Satisfactory	M
1.13	Domain service account group membership	Make a domain service account a member of only non-privileged groups.	N/A; the current configuration does not use the domain service account group.	M
1.14	SQL server service account rights	Grant the SQL server service account(s) the following rights:	N/A; there is no SQL service account assigned.	
		Log on as a service		M
		Act as part of the OS.		L
		Log on as a batch job		L
		Replace a process-level token		L
		Bypass traverse checking		L
		Adjust memory quotas for a process		M
		Permission to start SQL server active directory helper		L
		Permission to start SQL writer		M
1.15	SQL server agent service account rights	Grant the SQL server agent service account(s) the following rights:	N/A; there is no SQL service account assigned.	
		Log on as a service		M
		Act as part of the OS		L
		Log on as a batch job		L
		Replace a process-level token		L
		Bypass traverse checking		L
		Adjust memory quotas for a process		M

OS and network specification configuration (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
1.16	Integration service account rights	Grant the integration service account(s) the following rights:	N/A; there is no SQL service account assigned.	
		Log on as a service		M
		Permission to write to the application event log		L
		Bypass traverse checking		L
		Create global objects		M
		Impersonate a client after authentication		L
1.17	SQL server services account rights	Deny the service account the “Log on locally” right.	Satisfactory	M
1.18	SQL server services account rights	If a service account is a domain account, configure the account to have the Windows permission “Log on To” the database server only.	Satisfactory	M
1.19.1	SQL server proxy accounts	Create dedicated user accounts specifically for proxies, and only use these proxy user accounts for running job steps.	N/A; there is no proxy account assigned.	M
1.19.2	SQL server proxy accounts	Only grant the necessary permissions to proxy user accounts. Grant only those permissions actually required to run the job steps that are assigned to a given proxy account.	N/A; there is no proxy account assigned.	M
1.19.3	SQL server proxy accounts	Do not run the SQL server agent service under a MS Windows account that is a member of the Windows administrators group.	N/A; there is no proxy account assigned.	M

Appendix A19: MS SQL server installation and patches audit details

MS SQL server installation and patches audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
2.1	SQL server install platform	Avoid installing SQL server on a domain controller.	Satisfactory	M
2.2	Patches and hotfixes	Ensure the current SQL server service pack and hotfixes are installed.	Satisfactory; currently updating both service pack and critical hotfixes every three months	H
2.3	SQL server ports	Change SQL server default ports from 1433 and 1434.	Satisfactory	H
2.4	Naming conventions	In naming SQL Server instances, limit the instance name to less than 16 characters with no reference to a version number or other sensitive information.	Satisfactory; currently the name is less than 16 characters (11).	L
2.5	SQL server instances	Keep an inventory of all versions, editions and languages of SQL Server.	Not satisfactory; there is no inventory process.	P
2.6	Authentication mode	Select Windows authentication mode.	Not satisfactory (currently the council uses both Windows and SQL server authentication modes).	M
2.7	Rename sa account	The “sa” account should be renamed to something that is not easily identifiable as the “sa” account. ALTER LOGIN sa WITH NAME = <new name>	Not satisfactory; the council uses the default account (sa).	M
2.8	Strong password	Use a strong password for the “sa” login account.	Satisfactory	M
2.9	Sample databases	Do not install the sample databases. Delete all sample databases if they already exist.	Satisfactory; there is no sample database installed.	L
2.10	Initialisation parameter	C2 Audit Mode– set to 1 if no custom defined audit trace is enabled	Satisfactory; the current setup is 1.	P
2.11	Initialisation parameter	Remote Access– set to 0 unless replication is being used or the requirement is justified	Satisfactory; the current setup is 0.	M
2.12	Initialisation parameter	Scan for Startup Procedures– set to 0 unless justified	Satisfactory; the current setup is 0.	L

Appendix A20: MS SQL server setting audit details

MS SQL server setting audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
3.1	SQL server configuration manager	Disable the “Named Pipes” network protocol.	Not satisfactory	L
3.2	SQL server properties	The following settings are recommended:		
3.2.1	Auto restart SQL server	Set the SQL server service start mode to “Automatic”	Satisfactory	L
3.2.2	Auto restart SQL server agent	If the SQL server agent is required, set the “SQL server agent” start mode to “Automatic”.	Satisfactory	L
3.2.3	Distributed transaction coordinator	Set the “distributed transaction coordinator” service start mode to “Disabled” if this service is not required.	N/A	L
3.2.4	Cross database-ownership chaining	Disable the cross_db_ownership_chaining option.	Satisfactory	M
3.2.5	Advanced server settings	Do not enable direct modifications to the system catalogs.	N/A	M
3.2.6	Backup/restore from tape timeout	Set the backup/restore from tape timeout period to “Try for 5 minutes”	Not satisfactory; (currently set to “Wait Indefinitely”)	L
3.2.7	Media retention	Set the default backup media retention to the minimum number of days needed to retain a full backup of the database. Ideally, this should be as high as your resources permit.	Satisfactory	L
3.3	Data directory	The default data directory should be a dedicated data partition	Not satisfactory; (c:\programfiles\microsoft SQL server\mssql\data)	M
3.4	Data directory	The default log directory should be a dedicated partition separate from all programs and data	Not satisfactory; (c:\programfiles\microsoft SQL server\mssql\logs)	M
3.5	Replication	Do not enable replication.	N/A	L
3.6	Other SQL server configuration options	Set the number of logs retained based on the maximum number of restarts and log cyclings which may occur within your desired log retention window. The default value of 6 may be too low for many installations.	Satisfactory; the default is 6.	P

MS SQL server setting audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
3.7	Database mail	Disable database mail where messaging is not required.	Satisfactory	L
3.8	Trace messages	Error log/include execution trace messages = off	Satisfactory	P
3.9	User-defined stored procedures	Ensure that all user-defined stored procedures are stored in encrypted format.	Not satisfactory; stored in unencrypted format.	H
3.10	User-defined extended stored procedures	Avoid using user-defined extended stored procedures. If extended functionality is required, use Common Language Runtime (CLR) assemblies instead.	Not installed	L
3.11	Extended stored procedures	Disable access to the following extended stored procedures:		
3.11.1		xp_available media	Satisfactory	L
3.11.2		xp_cmdshell	Satisfactory	L
3.11.3		xp_dirtree	Not satisfactory; (enabled).	P
3.11.4		xp_dsninfo	Satisfactory	P
3.11.5		xp_enumdsn	Satisfactory	P
3.11.6		xp_enumerrorlogs	Satisfactory	P
3.11.7		xp_enumgroups	Satisfactory	P
3.11.8		xp_eventlog	Satisfactory	P
3.11.9		xp_fixeddrives	Not satisfactory; (enabled).	P
3.11.10		xp_getfiledetails	Satisfactory	P
3.11.11		xp_getnetname	Satisfactory	P
3.11.12		xp_logevent	Satisfactory	P
3.11.13		xp_loginconfig	Satisfactory	P
3.11.14		xp_msver	Satisfactory	P
3.11.15		xp_readerrorlog	Satisfactory	P
3.11.16		xp_servicecontrol	Satisfactory	P
3.11.17		xp_sprintf	Satisfactory	P
3.11.18		xp_sscanf	Satisfactory	P
3.11.19		xp_subdirs	Satisfactory	P
3.12	SQLmail extended stored procedures	Disable access to the following SQLMail extended stored procedures:		
3.12.1		xp_deletemail	Satisfactory	P
3.12.2		xp_findnextmsg	Satisfactory	P

MS SQL server setting audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
3.12.3		xp_get_mapi_default_profile	Satisfactory	P
3.12.4		xp_get_mapi_profiles	Satisfactory	P
3.12.5		xp_readmail	Satisfactory	P
3.12.6		xp_sendmail	Satisfactory	P
3.12.7		xp_startmail	Satisfactory	P
3.12.8		xp_stopmail	Satisfactory	P
3.13	WebTask extended stored procedures	Disable access to the following WebTask extended stored procedures. Delete the xpweb70.dll file that implements the following WebTask extended stored procedures:		
3.13.1		xp_cleanupwebtask	Satisfactory	P
3.13.2		xp_convertwebtask	Satisfactory	P
3.13.3		xp_dropwebtask	Satisfactory	P
3.13.4		xp_enumcodepages	Satisfactory	P
3.13.5		xp_makewebtask	Satisfactory	P
3.13.6		xp_readwebtask	Satisfactory	P
3.13.7		xp_runwebtask	Satisfactory	P
3.14	OLE automation stored procedures	Disable access to the following OLE automation stored procedures:		
3.14.1		sp_OACreate	Satisfactory	L
3.14.2		sp_OADestroy	Satisfactory	L
3.14.3		sp_OAGetErrorInfo	Satisfactory	L
3.14.4		sp_OAGetProperty	Satisfactory	L
3.14.5		sp_OAMethod	Satisfactory	L
3.14.6		sp_OASetProperty	Satisfactory	L
3.14.7		sp_OAStop	Satisfactory	L
3.15	Registry access extended stored procedures	Disable access to the following registry access extended stored procedures:		
3.15.1		xp_regaddmultistring	Not satisfactory; (enabled).	P
3.15.2		xp_regdeletekey	Not satisfactory; (enabled).	P
3.15.3		xp_regdeletevalue	Not satisfactory; (enabled).	P
3.15.4		xp_regenumvalues	Not satisfactory; (enabled).	P

MS SQL server setting audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
3.15.5		xp_regremovemultistring	Not satisfactory; (enabled).	P
3.15.6		xp_regwrite	Not satisfactory; (enabled).	P
3.16	Advanced setting	SQL server event forwarding/forward events to a different server = off	Satisfactory; (off).	L
3.17	SQL server browser service	Disable SQL server browser service	Not satisfactory; (enabled).	L

Appendix A21: MS SQL server access controls audit details

MS SQL server access controls audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
4.1	Permissions on OS tools	Restrict access to the executables in the System32 directory e.g. Explorer.exe and cmd.exe.	Not satisfactory (administrator has full control, Power users set to modify, and user group set to execute).	H
4.2	SQL server install directory permissions	Modify the permissions to the [Drive]:\Program Files\Microsoft SQL server directory.	Satisfactory; remove the Users group's permission to run executables.	H
4.3	SQL server database instance directory permissions	Delete or secure old setup files. Protect files in the <system drive>:\Program Files\Microsoft SQL Server\MSSQL.X\MSSQL\Install, e.g., sqlstp.log, sqlsp.log and setup.iss. "X" represents the installations of various SQL server installs due to the fact that multiple instances of SQL server or SQL express can be installed.	Satisfactory; access to the current install folder is allowed for the system administrator groups only.	M
4.4	Assigning system administrators role	When assigning database administrators to the system administrators role, map their Windows accounts to SQL logins, and then assign them to the role.	Satisfactory	M
4.5	SQL logins	Remove the default BUILTIN\administrators SQL login.	Not satisfactory; the BUILTIN\administrators SQL login is still exits.	M
4.6	SQL logins	Ensure that all SQL logins have strong passwords.	Satisfactory	M
4.7	OS guests access	Deny database login for the guests OS group.	Satisfactory	H
4.8	Fixed server roles	Only use the fixed server roles sysadmin, server admin, setup admin etc, to support DBA activity.	Satisfactory	L
4.9	SQL server database users and roles	Remove the guest user from all databases except master and tempdb.	Not satisfactory; (the guest user stills exist).	M
4.10	Statement permissions	Grant DDL statement permissions to only the database and schema owner, not individual users.	Satisfactory	M
4.11	Database owners permissions	Ensure dbo owns all user-created database schemas	Not satisfactory	L

MS SQL server access controls audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
4.12	Low-privileged users	Do not grant object permissions to PUBLIC or GUEST.	N/A	M
4.13	Stored procedure permissions	Grant executes permissions on stored procedures to database roles (not users).	Satisfactory	M
4.14	Using the GRANT option	Do not assign the GRANT option of object permission to a user or role.	N/A	M
4.15	SQL server agent subsystem privileges	Restrict proxy access to required/approved subsystems.	N/A; no proxy access.	M
4.16	User-defined database roles	Create user-defined database roles to assign permissions to objects in the database when a pre-defined database role does not supply the appropriate permissions to a group of users.	N/A; no user defined database roles.	M
4.17	Database roles	Avoid nesting database roles.	Satisfactory	M
4.18	Users and roles	Ensure that the members of the roles (users/groups/other roles) in the target database actually exist.	Satisfactory	L
4.19	Application roles	Use application roles to limit access to data to users of specific applications. Use encryption to protect the role name and password in the connection string. Use “EXECUTE AS WITH NO REVERT” or “WITH COOKIE” to allow individuals to access the application without knowing the password.	N/A	M
4.20	Use of predefined roles	Avoid assigning predefined roles to PUBLIC or GUEST.	N/A; no predefined roles created.	L
4.21	Linked or remote servers	Use linked servers rather than remote servers where required. Remove any unused linked servers or disable this feature.	N/A	L
4.22	Linked or remote servers	Configure linked or remote servers to use Windows authentication where required. Disable linked servers otherwise.	Not satisfactory; (currently the council uses both windows and SQL authentications).	M
4.23	Linked server logins	Allow linked server access only to those logins that need it. Disable linked servers otherwise.	Satisfactory	M
4.24	Ad Hoc data access	Disable ad hoc data access on all providers for all users except members of the sysadmin fixed role.	N/A	L

Appendix A22: MS SQL server auditing and logging audit details

MS SQL server auditing and logging audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
5.1	Auditing – general	Prepare a schedule for reviewing audit information regularly.	**Not satisfactory;** currently there is no auditing schedule.	P
5.2	SQL server properties – security tab	Through the SQL server management studio, enable auditing for SQL server.	Satisfactory	P
5.3	SQL server logs	SQL server audit data must be protected from loss. The SQL server and SQL server agent logs must be backed up before they are overwritten.	Satisfactory; the default setup is 6.	P
5.4	SQL profiler	Use SQL profiler to generate and manage audit trails.	Satisfactory	P
5.5	Profiler events	Capture the following events using SQL profiler		
		Event		
5.5.1		Audit add DB user event	Not satisfactory	P
5.5.2		Audit add login to server Role	Not satisfactory	P
5.5.3		Audit add member to DB role	Not satisfactory	P
5.5.4		Audit add role event	Not satisfactory	P
5.5.5		Audit addlogin event	Not satisfactory	P
5.5.6		Audit app role change password	Not satisfactory	P
5.5.7		Audit backup/restore	Not satisfactory	P
5.5.8		Audit broker conversation	Not satisfactory	P
5.5.9		Audit broker login	Not satisfactory	P
5.5.10		Audit change audit	Not satisfactory	P
5.5.11		Audit change database owner	Not satisfactory	P
5.5.12		Audit DBCC	Not satisfactory	P
5.5.13		Audit database management	Not satisfactory	P
5.5.14		Audit database object access	Not satisfactory	P
5.5.15		Audit database object GDR	Not satisfactory	P
5.5.16		Audit database object management	Not satisfactory	P
5.5.17		Audit database object take ownership	Not satisfactory	P
5.5.18		Audit database operation	Not satisfactory	P

MS SQL server auditing and logging audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council A**	**Risk levels**
5.5.19		Audit database principal impersonation	Not satisfactory	P
5.5.20		Audit database principal management	Not satisfactory	P
5.5.21		Audit database scope GDR	Not satisfactory	P
5.5.22		Audit login change password	Not satisfactory	P
5.5.23		Audit login change property	Not satisfactory	P
5.5.24		Audit login	Not satisfactory	P
5.5.25		Audit login failed	Not satisfactory	P
5.5.26		Audit login GDR event	Not satisfactory	P
5.5.27		Audit logout	Not satisfactory	P
5.5.28		Audit object derived permission event	Not satisfactory	P
5.5.29		Audit schema object access	Not satisfactory	P
5.5.30		Audit schema object GDR	Not satisfactory	P
5.5.31		Audit schema object management	Not satisfactory	P
5.5.32		Audit schema object take ownership	Not satisfactory	P
5.5.33		Audit server alter trace	Not satisfactory	P
5.5.34		Audit server object GDR	Not satisfactory	P
5.5.35		Audit server object management	Not satisfactory	P
5.5.36		Audit server object take ownership	Not satisfactory	P
5.5.37		Audit server operation	Not satisfactory	P
5.5.38		Audit server principal impersonation	Not satisfactory	P
5.5.39		Audit server principal management	Not satisfactory	P
5.5.40		Audit server scope GDR	Not satisfactory	P
5.5.41		Audit server starts and stops	Not satisfactory	P
5.5.42		Audit statement permission event	Not satisfactory	P

Appendix A23: MS SQL server backup and disaster recovery procedures audit details

MS SQL server backup and disaster recovery procedures audit details				
Item no.	**Configuration items**	**Action / recommended Parameters**	**Council A**	**Risk levels**
6.1	Backups – general	Use full database backups combined with differential or transaction log backups to restore the database to a specific point in time.	Satisfactory; currently the council's backup is done nightly.	M
6.2	System databases	It is important to include the system databases in your backup plan i.e. the master, msdb and model databases.	Satisfactory	M
6.3	Backing up master database	Backup the master database when any of the following events occur: ▪ A database is created or deleted ▪ Login accounts are created, deleted or modified Server-wide or database settings are modified	Satisfactory	M
6.4	Backing up MSDB database	Backup the msdb database when any of the following events occur: Alerts, jobs, schedules or operators are created, deleted or modified	Satisfactory	M
6.5	Backup media	Password protects the backup media.	Satisfactory	H
6.6	Access to backup files	Restrict access to the backup files to system administrators.	Satisfactory	H
6.7	Access to backup files	Restrict restore permissions to DBAs	Satisfactory; currently, only the system administrator group can restore the backup files.	H
6.8	Recommended periodic administrative procedures	Run the MS baseline security analyser weekly and follow the security recommendations as closely as possible to secure the OS.	Not satisfactory; the MS baseline security analyser not in use.	L
6.9	Recommended periodic administrative procedures	Run the SQL best practices analyser regularly and note any changes to the environment.	Not satisfactory; the SQL best practices analyser not in use.	L

MS SQL server backup and disaster recovery procedures audit details (continued)				
Item no.	**Configuration items**	**Action / recommended Parameters**	**Council A**	**Risk levels**
6.10	Enable password policy enforcement	When a password change mechanism is introduced into clients and applications; enable password expiration. Always specify MUST_CHANGE when specifying a password on behalf of another principal.	Not satisfactory; no enforce password policy	M
6.11	Periodic scan of role members	Periodically scan fixed server and database roles to ensure that only trusted individuals are members.	Not satisfactory; currently, there are only a few users. Periodic scan may is recommended when number of users increases.	L
6.12	Periodic scan of stored procedures	Verify stored procedures that have been set to AutoStart are secure.	Not satisfactory; no AutoStart enabled.	P

Appendix A24: Council A's information security policy

A97/7041 – Council A community access to the Internet policy
Recommendation

1. That the following libraries policy (4) - community access to the Internet - be adopted:

Libraries Policy (4)

Subject: Community access to the Internet

Objective

To ensure our community has access to a local gateway of knowledge and information necessary to enhance lifelong learning, literacy, education, independent decision making and cultural, business or personal development.

The policy aims to clarify the conditions of use for community access to the Internet.

Policy statement

The Council A library and information service provides community access to the Internet through its public library system which includes:

- AH Bracks library.
- Bull Creek library.
- Canning Bridge library.
- Civic Square library.
- Willagee library.

Community access to the Internet through the Council A public library system is based on the following:

A) Conditions of use.

B) Management of use.

C) The principles of equity and access.

1. Conditions of use

   A) Community access to the Internet will be available during the normal library hours of operation;

   B) The maximum length of any one session will be limited to thirty (30) minutes. Any change to this condition will be at the discretion of the branch librarian;

   C) Search and read facilities only are available for public use;

   D) Facilities such as e-mail and file transfer are not available for public use;

   E) Print facilities will be available and charged at a rate of 20¢ per page which will be subject to an annual review; and

   F) The Council A does not guarantee or accept any liability for the accuracy, authoritativeness, timeliness or usefulness of any information retrieved from the Internet.

2. Management of use

   A) The staff of the Council A libraries under the direction of the manager library and information services and the respective branch librarian, will be responsible for managing the use of community access to the Internet;

   B) Prospective users of the Internet will be encouraged to book their session in advance to avoid unnecessary delays;

   C) Booking in advance may not be necessary if the Internet is not being used. It should be noted a pre booked session will take precedence over casual use; and

   D) Library users are expected to comply with all local, state, and federal laws while using the Internet. Users found to have violated any laws, (including but not limited to those

concerning copyright, fraud, privacy, or obscenity) or who access information that is considered unacceptable according to common community standards and that would not be included in the normal print collection while using library facilities or equipment will have their privileges revoked.

3. Equity and access

The principle that all members of the community are entitled to have access to library services and resources and that such person should not be discriminated against on the grounds of age, sex, race, religion, national origin, disability, economic conditions, individual lifestyle or political or social views are recognised and will be upheld where possible within this policy.

Appendix B: Additional results for Chapter 5

Appendix B1: A summary of the Internet border access list code for the email system of Council B

Policy no.	Rule	Protocol type	From (source)	To (destination)	Port (service)
1	Permit	IP	Any	Any	Any

Appendix B2: A summary of the firewall configuration codes (email-NAT) of Council B's firewall

Policy no.	**Rule**	**From (source)**	**To (destination)**
1	Translate	A.B.C.89	172.20.130.224

Appendix B3: A summary of the firewall configuration codes of Council B's email system

Policy no.	Rules	Protocol types	From (source)	To (destination)	Ports (service)
1	Permit	TCP	CoB Internal LAN	A.B.C.99 A.B.C.101	SMTP
2	Permit	TCP	Any	A.B.C.98 A.B.C.100	SMTP
3	Permit	TCP	CoB Internal LAN	A.B.C.98 A.B.C.100	HTTP,HTTPS, Telnet, IronPort_quarantine
4	Permit	TCP	A.B.C.98 A.B.C.100	Any	HTTP,HTTPS, SMTP, Global_Catalogue

Appendix B4: A full details of system information policy results and recommendations of Council B's email server

System information policy– CoB-email server (172.20.130.224)				
Services				
135				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length:	6 chars		At least 8 chars	
Maximum password age:	45 days		30 days	
Minimum password age:	2 days		0 day	
Force logoff:	Never force		Force	
Password history:	6 passwords		N/A	
Security auditing policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	Yes	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	No	Yes	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	Yes	No	Yes	Yes

Appendix B5: A summary of missing patches information of Council B's email server

Missing patches (5) – email server (172.20.130.224)				
Products	**Severities**	**Descriptions**	**Vulnerabilities**	**Recommendations**
MS Windows	N/A	KB890830	It helps remove specific prevalent malicious software from computers that are running MS Windows Server 2003, and other Windows OS.	Deploy/patch
MS Windows	Critical	KB938464	MS08-052 - addresses a vulnerability in MS Windows vulnerabilities in GDI+ could allow remote code execution (954593)	Deploy/patch asap
MS Exchange	N/A	KB960384	Many vulnerabilities based on update rollup 7 for MS Exchange Server 2007 service pack 1	Deploy an update rollup 7 for MS Exchange Server 2007 service pack 1 asap
MS Exchange	Critical	KB959241	Many vulnerabilities based on update rollup 6 for MS Exchange Server 2007 service pack 1	Deploy an update rollup 6 for MS Exchange Server 2007 service pack 1 immediately.
MS Exchange	Important	KB949870	Many vulnerabilities based on update rollup 3 for MS Exchange Server 2007 service pack 1	Deploy update rollup 3 for MS Exchange Server 2007 service pack 1 asap

Appendix B6: The overall opened TCP and UDP service ports, and the possible mitigation recommendation on Council B's email server

The overall opened TCP service ports (21) – email server (172.20.130.224)				
Port no.	**Services**	**Descriptions**	**Products**	**Recommendations**
25	SMTP	SMTP	MS ESMTP	Open
80	HTTP	HTTP	MS IIS webserver 6.0	Open
110	POP3	POP3	MS Exchange Server 2007 POP3	Close
135	MSRPC	MS RPC	MS Windows RPC	Open
139	NetBIOS - ssn	NetBIOS Session Service	NetBIOS Session Service	Open
443	HTTPS	Hypertext Transfer Protocol over TLS/SSL	MS IIS webserver 6.0	Open
445	MS-ds	MS-DS Active Directory, Windows shares	MS Windows 2003	Open
587	email message submission	email message submission (SMTP)	MS ESMTP	Close
593	ncacn_http_ epmap	HTTP RPC Ep Map	MS Windows RPC over HTTP 1.0	Close
1075	MSRPC	MS Windows RPC	MS Windows RPC	Close
1091	MSRPC	MS Windows RPC	MS Windows RPC	Close
1123	MSRPC	MS Windows RPC	MS Windows RPC	Close
1163	MSRPC	MS Windows RPC	MS Windows RPC	Close
1165	MSRPC	MS Windows RPC	MS Windows RPC	Close
1248	MSRPC	MS Windows RPC	MS Windows RPC	Close
3389	MS-RDP	MS Remote Session	MS Terminal Service	Open
6001	ncacn_http	MS RPC for MS Exchange (information store)	MS Windows RPC over HTTP 1.0	Close
6002	ncacn_http	MS RPC (directory referral)	MS Windows RPC over HTTP 1.0	Close
6004	ncacn_http	MS RPC (DSProxy/NSPI)	MS Windows RPC over HTTP 1.0	Close
8400	cvp	Commvault Unified Data Management		Close
8402	galaxy		Galaxy Client Event Manager	Close

The overall opened UDP service ports (8) - email server (172.20.130.224)				
Port no.	**Services**	**Descriptions**	**Products**	**Recommendations**
123	NTP	Network Time Protocol		Close
137	NetBIOS -ns	NetBIOS Name Service	MS Windows NT netbios-ssn	Open
138	NetBIOS -dgm	NetBIOS Datagram Service	MS Windows	Close
161	SNMP	Simple Network Management Protocol	SNMP v1 server (public)	Close
445	MS-ds	MS-DS SMB file sharing	MS Windows	Close if not required
500	isakmp	Internet Security Association and Key Management Protocol	MS Windows	Close
1434	ms-sql-m	MS SQL Server	MS SQL Server 9.00.4035.00	Close if not required
4500	nat-t-ike	IPsec NAT-Traversal (RFC 3947)	MS Windows	Close

Appendix B7: A summary of Council B's email server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of the email server (172.20.130.224)	
High security vulnerabilities (2)	
Section: Types	**Recommendations**
Miscellaneous: AutoRun is enabled	It is a virtual server, no action is required.
Services: TCP port 110 (POP3) open	Should be disabled
Medium security vulnerability (1)	
Section: Type	**Recommendation**
SNMP	Should be disabled if not required
Low security vulnerabilities (7)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Services: Alter service enabled	Should be disabled if not required
Services: HTTP	Should be disabled if not required
Services: SMTP	Satisfactory
Services: HTTPS	Satisfactory
Services: POP3 open	Should be disabled
Potential vulnerabilities (2)	
Section: Types	**Recommendations**
Information: Administrator account exists	Rename the administrator account.
Information: Some POP3 server banners providing information to attacker	The service POP3 server should be turned off.

Appendix B8: A summary of the firewall configuration codes for Council B's static web system with respect to the CoB-DMZ-Web and the CoB-Web servers

Policy no.	Rules	Protocol types	From (source)	To (destination)	Ports (service)
1	MIP	Address	CoB-DMZ-Web	A.B.C.121/27	N/A
2	MIP	Address	CoB-Web	172.20.130.184/16	N/A
3	Permit	TCP	Any	CoB-DMZ-Web	HTTP
4	Permit	TCP	CoB-DMZ-Web	Any	HTTP
5	Permit	TCP	CoB-DMZ-Web	CoB-Web	HTTP
6	Permit	TCP	CoB-Web	CoB-DMZ-Web	HTTP
7	Permit	TCP	CoB-Web	CoB-DMZ-Web	HTTPS
8	Permit	TCP	CoB-Web	CoB-DMZ-Web	445
9	Permit	TCP	172.20.20.20/16	CoB-DMZ-Web	3389

Appendix B9: A summary of the firewall configuration codes for Council B's CMS web system with respect to the CoB-DMZ-Web and the CoB-Database servers

Policy no.	Rules	Protocol types	From (source)	To (destination)	Ports (service)
1	MIP	Address	CoB-DMZ-Web	A.B.C.121/27	N/A
2	MIP	Address	CoB-Database	172.20.130.148/16	N/A
3	Permit	TCP	Any	CoB-DMZ-Web	HTTP
4	Permit	TCP	CoB-DMZ-Web	Any	HTTP
5	Permit	TCP	CoB-DMZ-Web	CoB-Database	HTTP
6	Permit	TCP	CoB-DMZ-Web	CoB-Database	HTTPS
7	Permit	TCP	CoB-Database	CoB-DMZ-Web	HTTP
8	Permit	TCP	CoB-Database	CoB-DMZ-Web	HTTPS
9	Permit	TCP	172.20.20.20/16	CoB-DMZ-Web	3389

Appendix B10: A summary of the firewall configuration codes for Council B's online payment system

Policy no.	Rules	Protocol types	From (source)	To (destination)	Ports (service)
1	MIP	Address	Online Gateway	x.x.x.x	N/A
2	Permit	TCP	Any	CoB-DMZ-Web	HTTP
3	Permit	TCP	Any	CoB-Database	HTTPS
4	Permit	TCP	CoB-DMZ-Web	Any	HTTP
5	Permit	TCP	CoB-DMZ-Web	Any	HTTPS
6	Permit	TCP	CoB-DMZ-Web	CoB-Database	Sqlnet2
7	Permit	TCP	CoB-DMZ-Web	CoB-Database	1443

Appendix B11: A full details of system information policy results and recommendations of Council B's CoB-DMZ-Web server

System information policy– CoB-DMZ-Web server (A.B.C.121)				
Services				
115				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	6 chars		At least 8 chars	
Maximum password age	45 days		30 days	
Minimum password age	2 days		0 day	
Force logoff	Never force		Force	
Password history	6 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	Yes	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	No	Yes	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	Yes	No	Yes	Yes

Appendix B12: A full details of system information policy results and recommendations of Council B's CoB -Web server

System information policy – CoB-Web server (172.20.130.184)				
Services				
111				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	6 chars		At least 8 chars	
Maximum password age	45 days		30 days	
Minimum password age	2 days		0 day	
Force logoff	Never force		Force	
Password history	6 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	Yes	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	No	Yes	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	Yes	No	Yes	Yes

Appendix B13: A full details of system information policy results and recommendations of Council B's CoB –Database server

System information policy– CoB-Database server (172.20.130.148)				
Services				
117				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	6 chars		At least 8 chars	
Maximum password age	45 days		30 days	
Minimum password age	2 days		0 day	
Force logoff	Never force		Force	
Password history	6 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	Yes	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	No	Yes	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	Yes	No	Yes	Yes

Appendix B14: A summary of missing service pack and patches, and the possible mitigation recommendations for the CoB-Web server

Missing service pack (1) – CoB-Web server (172.20.130.184)				
Product	**Filename**	**Knowledge base**	**Vulnerability issue**	**Recommendation**
Virtual Studio	VS80sp1-KB926601-X86-ENU.exe	N/A	Virtual Studio 2005 service pack 1	Deploy/patch
Missing patches (3) – CoB-Web server (172.20.130.184)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS Windows	N/A	KB890830	MS Windows malicious software removal tool - April 2009	Deploy/patch
MS Windows	N/A	N/A	MS Windows IE 7 for MS Windows Server 2003	Deploy/patch
SDK components	Critical	KB931906	MS07-028 security update for CAPICOM	Deploy/patch asap

Appendix B15: A summary of missing service packs and patch, and the possible mitigation recommendations for the CoB-Database server

Missing service packs (2) – CoB-Database server (172.20.130.148)				
Products	**Filenames**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
Visual Studio	VS80sp1-KB926601-X86-ENU.exe	N/A	Visual Studio 2005 service pack 1	Deploy/patch
Office	OWC11SP3.CAB	N/A	MS Office 2003 service pack 3	Deploy/patch
Missing patch (1) – CoB-Database server (172.20.130.148)				
Product	**Severity**	**Knowledge base**	**Vulnerability issue**	**Recommendation**
MS Windows	N/A	KB890830	MS Windows malicious software removal tool x64 - April 2009	Deploy/patch

Appendix B16: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the CoB-DMZ-Web server

The overall opened TCP service ports (20) – CoB-DMZ-Web server (A.B.C.121)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
25	SMTP	Simple Mail Transfer Protocol, MS ESMTP 6.0.3790.1830	Close
80	HTTP	Hyper Text Transfer Protocol, MS IIS webserver 6.0	Open
135	MSRPC	MS Remote Procedure Call, MS Windows RPC	Open/close if not required
139	NetBIOS-ssn	NetBIOS Session Service	Close if not required
443	HTTPS	MS IIS webserver 6.0	Open
445	MS-DS	MS-DS Active Directory, Windows shares, MS Windows 2003	Open/close if not required
554	RTSP	Real-Time Streaming Protocol, MS Windows Media Server 9.1.1.5001	Close if not required
1025	MSRPC	MS Remote Procedure Call, MS Windows RPC	Close if not required
1040	NETSAINT	Netsaint status daemon, If this service is not installed beware could be Trojan	Close if not required
1047	TROJAN	remoteNC, If this service is not installed beware could be Trojan	Close if not required
1052	MSRPC	MSMQ, If this service is not installed beware could be Trojan: Fire HacKer, Slapper	Close if not required
1056	MSRPC	MS Remote Procedure Call, MS Windows RPC	Close if not required
1057	MSRPC	MS Remote Procedure Call, MS Windows RPC	Close if not required
1080	MSRPC	MS Remote Procedure Call, MS Windows RPC	Close if not required
1720	H.323/Q.931	Interactive media	Close if not required
1755	WMS	Windows media service	Close if not required
3389	MS-rdp	MS WBT Server, MS Terminal Service	Open
8400	CVP	Commvault Unified Data Management	Close if not required
8402	Galaxy	Galaxy Client Event Manager	Close if not required
8600	Asterix	Surveillance Data	Close if not required
The overall opened UDP service ports (9) – CoB-DMZ-Web server (A.B.C.121)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
67	DHCPs	Bootstrap Protocol (BOOTP) Server; also used by Dynamic Host Configuration Protocol (DHCP)	Close
123	NTP	Network Time Protocol	Close
137	NetBIOS -ns	NetBIOS Name Service MS Windows NT netbios-ssn	Open/Close if not required
138	NetBIOS -dgm	NetBIOS Datagram Service	Close if not required

The overall opened UDP service ports (9) – CoB-DMZ-Web server (A.B.C.121) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
161	SNMP	Simple Network Management Protocol	Close if not required
445	MS-ds	MS-DS SMB file sharing	Open/close if not required
500	isakmp	Internet Security Association and Key Management Protocol	Close
1755	WMS	MS Media Services (MMS, ms-streaming)	Close
4500	nat-t-ike	IPSec NAT-Traversal (RFC 3947)	Close

Appendix B17: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the CoB-Web server

The overall opened TCP service ports (9) – CoB-Web server (172.20.130.184)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
25	SMTP	Simple Mail Transfer Protocol, MS ESMTP 6.0.3790.1830	Close
80	HTTP	Hyper Text Transfer Protocol, MS IIS webserver 6.0	Open
135	MSRPC	MS Remote Procedure Call; MS Windows RPC	Open
139	NetBIOS - ssn	NetBIOS Session Service for MS File and Printer Sharing	Open
445	MS-DS	MS-DS Active Directory, Windows shares	Open/close if not required
1025	MSRPC	MS Remote Procedure Call, MS Windows RPC	Close if not required
3389	MS-RDP	MS WBT Server, MS Terminal Service	Open
8400	CVP	Commvault Unified Data Management	Close if not required
8402	Galaxy	Galaxy Client Event Manager	Close if not required
The overall opened UDP service ports (9) – CoB-Web server (172.20.130.184)			
Port no.	**Services**	**Descriptions, Actions and products**	**Recommendations**
123	NTP	Network Time Protocol	Close
137	NetBIOS -ns	NetBIOS Name Service MS Windows NT	Open/ Close if not required
138	NetBIOS - dgm	NetBIOS Datagram Service	Close
161	SNMP	Simple Network Management Protocol	Close if not required
445	MS-DS	MS-DS SMB file sharing	Open
500	ISAKMP	Internet Security Association and Key Management Protocol	Close
3456	IISrpc-or-vat	Also VAT default data; If this service is not installed beware could be Trojan	Close if not required
4128	RedShad	If this service is not installed beware could be Trojan	Close if not required
4500	Nat-t-ike	IPsec NAT-Traversal (RFC 3947)	Close

Appendix B18: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the CoB-Database server

The overall opened TCP service ports (10) – CoB-Database server (172.20.130.148)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
80	HTTP	Hyper Text Transfer Protocol, MS IIS webserver 6.0	Close if not required
135	MSRPC	MS Remote Procedure Call; MS Windows RPC	Open
139	NetBIOS - SSN	NetBIOS Session Service for MS File and Printer Sharing	Open
445	MS-DS	MS-DS Active Directory, Windows shares	Open
1037	MSRPC	MS Remote Procedure Call, MS Windows RPC; If this service is not installed beware could be Trojan: Arctic , Dosh, KWM, MoSucker	Close if not required
1433	MS-SQL-S	MS SQL Server 2005	Open
2383	MS-OLAP-4	MS OLAP	Close if not required
3389	MS-RDP	MS WBT Server, MS Terminal Service	Open
8400	CVP	Commvault Unified Data Management	Close if not required
8402	Galaxy	Galaxy Client Event Manager	Close if not required
The overall opened UDP service ports (9) – CoB-Database server (172.20.130.148)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
123	NTP	Network Time Protocol	Close
137	NetBIOS -NS	NetBIOS Name Service MS Windows NT netbios-ssn (workgroup: CoB-SHIRE)	Open/Close if not required
138	NetBIOS - DGM	NetBIOS Datagram Service	Close
161	SNMP	Simple network management protocol	Close if not required
162	SNMP TRAP	Simple network management protocol trap	Close if not required
445	MS-DS	MS-DS SMB file sharing	Open
500	ISAKMP	Internet Security Association and Key Management Protocol	Close
1434	MS-SQL-M	MS SQL Server database management system Monitor; MS SQL Server 9.00.4035.00	Open
4500	NAT-T-IKE	IPsec NAT-Traversal (RFC 3947)	Close

Appendix B19: A summary of Council B's CoB-DMZ-Web server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of the council's CoB-DMZ-Web server	
High security vulnerability (1)	
Section: Type	**Recommendation**
Miscellaneous: AutoRun is enabled	Disable AutoRun both for CD/DVD drives and also other removable drives.
Medium security vulnerabilities (3)	
Section: Types	**Recommendations**
Registry: Guest users have access to the application log	Disable guest access by creating a DWORD key named "RestrictGuestAccess" with value of "1" (HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLog/Application)
Registry: Guest users have access to the security log	Disable guest access by creating a DWORD key named "RestrictGuestAccess" with value of "1" (HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLog/Security).
Registry: Guest users have access to the system log	Disable guest access by creating a DWORD key named "RestrictGuestAccess" with value of "1" (HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLog/System)
Low security vulnerabilities (7)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Registry: Last logged-on username visible	Should be disabled
Services: Alerter service enabled	Should be disabled
Services: HTTP	No further action is required
Services: SMTP	Disable SMTP service port
Services: HTTPS	No further action is required
Potential vulnerabilities (2)	
Section: Types	**Recommendations**
Information: Administrator account exists	It is recommended to rename this account.
Information: User WMUS_COB-MANGANESE never logged on	It is recommended to remove this account if not used.

Appendix B20: A summary of Council B's CoB-Web server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of the council's CoB-Web server	
High security vulnerability (1)	
Section: Type	**Recommendation**
Miscellaneous: AutoRun is enabled	Disable AutoRun both for CD/DVD drives and also other removable drives.
Medium security vulnerability (0)	
Section: Type	**Recommendation**
None	None
Low security vulnerabilities (6)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Services: Alerter service enabled	Should be disabled
Services: HTTP	No further action is required
Services: SMTP	Disable SMTP service port
Web: IIS: Frontpage check	Disable the Frontpage extensions which currently are installed on this computer.
Potential vulnerability (1)	
Section: Type	**Recommendation**
Information: Administrator account exists	It is recommended to rename this account.

Appendix B21: A summary of Council B's CoB-Database server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of the council's CoB-Database server	
High security vulnerability (1)	
Section: Type	**Recommendation**
Miscellaneous: AutoRun is enabled	Disable AutoRun both for CD/DVD drives and also other removable drives.
Medium security vulnerabilities (0)	
Section: Type	**Recommendation**
None	None
Low security vulnerabilities (4)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Services: Alerter service enabled	Should be disabled
Services: HTTP	No further action is required
Potential vulnerabilities (2)	
Section: Types	**Recommendations**
Information: Administrator account exists	It is recommended to rename this account.
Information: MS SQL Server	No further action is required

Appendix B22: OS and network specification configuration

OS and network specification configuration				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
1.1	Physical security	Place the SQL server in an area where it will be physically secure.	Satisfactory	H
1.2	Domain environment	If the SQL Server is in a domain that is trusted by other domains, document the access granted by the trust.	Satisfactory; only IT administrator groups are allowed to access the online backend database server.	H
1.3	SQL servers accessed via Internet	If the SQL server is being accessed via the Internet, place the SQL Server inside a DMZ with the Web Server.	Satisfactory; there is a frontend web (CoB-DMZ-Web) server located in the DMZ.	H
1.4	SQL servers accessed via Internet	Put a firewall between your server and the Internet. Block TCP port 1433 and UDP port 1434 on your perimeter firewall. If named instances are listening on additional ports, block those too. In a multi-tier environment, use multiple firewalls to create more secure screened subnets	Satisfactory; the SQL server is located be hide the Internet firewall, and both TCP port 1433 and 1434 are blocked from external access.	H
1.5	Encryption	Implement SSL. Use the fully-qualified DNS name of the frontend web server in the certificate to help prevent masquerading.	Satisfactory; the frontend server uses SSL and fully qualified DNS name.	H
1.6	Test and development servers	Maintain test and development servers on a separate network segment from the production servers.	**Not satisfactory**; the test and development servers are on the same class B network.	H
1.7	Dedicated server	Install SQL server on a computer that does not provide additional services, e.g., Web or mail services.	Satisfactory; the SQL server is only for SQL database operation.	M
1.8	OS benchmark configuration	Configure Windows 2003 server level I benchmark settings with the following modifications:		
1.8.1	Windows accounts	Make sure the Windows guest account is disabled.	Satisfactory	M
1.8.2	Disk subsystem	Use RAID for critical data files.	**Not satisfactory;** VMware with SCSI hard disks.	M

OS and network specification configuration (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
1.8.3	Separate partitions	Create separate partitions for OS/SQL program files, SQL data files, and SQL transaction logs.	**Not satisfactory;** both SQL data files and transaction logs are located in different folders but in the same drive partition.	M
1.8.4	Volume / partition type	Format all volumes with NTFS	Satisfactory	H
1.9	Services	Disable the following services on a SQL server machine		
1.9.1		Alerter	**Not satisfactory**; currently set to Started Automatic.	P
1.9.2		Clipbook server	Satisfactory; (disabled).	P
1.9.3		Computer browser	Satisfactory; (disabled).	L
1.9.4		DHCP client	**Not satisfactory;** currently set to Started Automatic.	L
1.9.5		Distributed file system	**Not satisfactory;** currently set to Started Manual.	L
1.9.6		Distributed transaction coordinator	**Not satisfactory;** currently set to Started Automatic.	L
1.9.7		Fax service	Satisfactory; (disabled).	P
1.9.8		Internet connection sharing	Satisfactory; (disabled).	L
1.9.9		IPSec policy agent	**Not satisfactory;** currently set to Started Automatic.	L
1.9.10		License logging	Satisfactory; (disabled).	L
1.9.11		Logical disk manager administrative service	**Not satisfactory;** currently set to Started Automatic (this service is needed by the system administrator).	L
1.9.12		Messenger	Satisfactory; (disabled).	P
1.9.13		NetMeeting remote desktop sharing	Satisfactory; (disabled).	P
1.9.14		Network DDE	Satisfactory; (disabled).	L
1.9.15		Network DDE DSDM	Satisfactory; (disabled).	L
1.9.16		Print spooler	**Not satisfactory;** currently set to Started Automatic.	L
1.9.17		Remote access connection manager	**Not satisfactory;** currently set to Started Automatic.	L
1.9.18		Remote registry	**Not satisfactory;** currently set to Started Automatic.	L
1.9.19		Removable storage	Satisfactory; (disabled).	P
1.9.20		RunAs service	Satisfactory; (disabled)	M
1.9.21		Smart card	Satisfactory; (disabled).	P
1.9.22		Smart card helper	Satisfactory; (disabled)	P

OS and network specification configuration (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
1.9.23		Task scheduler	**Not satisfactory;** currently set to Started Automatic.	P
1.9.24		Telephony	**Not satisfactory;** currently set to Started Automatic.	P
1.9.25		Telnet	Satisfactory; (disabled).	L
1.9.26		Windows installer	**Not satisfactory;** currently set to Started Automatic.	L
1.10	MSSQL server service account	Use a low-privileged local or Domain account for the MS SQL server service.	Satisfactory	M
1.11	SQL server agent service account	Use a low-privileged domain account for SQL server agent if replication, DTS, or other inter-server connection is required.	Satisfactory	M
1.12	Local users group membership	Assign the local service account as a member of only the users group.	**Not satisfactory**; there is no assigned user in the “Users” group.	M
1.13	Domain service account group membership	Make a domain service account a member of only non-privileged groups.	N/A; the current configuration does not use the domain service account group.	M
1.14	SQL server service account rights	Grant the SQL server service account(s) the following rights:	N/A; there is no SQL service account assigned.	
		Log on as a service		M
		Act as part of the OS.		L
		Log on as a batch job		L
		Replace a process-level token		L
		Bypass traverse checking		L
		Adjust memory quotas for a process		M
		Permission to start SQL server active directory helper		L
		Permission to start SQL writer		M
1.15	SQL server agent service account rights	Grant the SQL server agent service account(s) the following rights:	N/A; there is no SQL service account assigned.	
		Log on as a service		M
		Act as part of the OS		L
		Log on as a batch job		L
		Replace a process-level token		L
		Bypass traverse checking		L

OS and network specification configuration (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
		Adjust memory quotas for a process		M
1.16	Integration service account rights	Grant the integration service account(s) the following rights:	N/A; there is no SQL service account assigned.	
		Log on as a service		M
		Permission to write to the application event log		L
		Bypass traverse checking		L
		Create global objects		M
		Impersonate a client after authentication		L
1.17	SQL server services account rights	Deny the service account the “Log on locally” right.	Satisfactory	M
1.18	SQL server services account rights	If a service account is a domain account, configure the account to have the Windows permission “Log on To” the database server only.	**Not satisfactory**; currently the domain/sqladmin account can log on to all computers.	M
1.19.1	SQL server proxy accounts	Create dedicated user accounts specifically for proxies, and only use these proxy user accounts for running job steps.	N/A; there is no proxy account assigned.	M
1.19.2	SQL server proxy accounts	Only grant the necessary permissions to proxy user accounts. Grant only those permissions actually required to run the job steps that are assigned to a given proxy account.	N/A; there is no proxy account assigned.	M
1.19.3	SQL server proxy accounts	Do not run the SQL server agent service under a MS Windows account that is a member of the Windows administrators group.	N/A; there is no proxy account assigned.	M

Appendix B23: MS SQL server installation and patches audit details

MS SQL server installation and patches audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
2.1	SQL server install platform	Avoid installing SQL server on a domain controller.	Satisfactory	M
2.2	Patches and hotfixes	Ensure the current SQL server service pack and hotfixes are installed.	Satisfactory; currently updating both service pack and critical hotfixes every three months	H
2.3	SQL server ports	Change SQL server default ports from 1433 and 1434.	Satisfactory	H
2.4	Naming conventions	In naming SQL Server instances, limit the instance name to less than 16 characters with no reference to a version number or other sensitive information.	Satisfactory; currently the name is less than 16 characters (11).	L
2.5	SQL server instances	Keep an inventory of all versions, editions and languages of SQL Server.	**Not satisfactory;** there is no inventory process.	P
2.6	Authentication mode	Select Windows authentication mode.	**Not satisfactory**; currently the council uses both Windows and SQL server authentication modes.	M
2.7	Rename sa account	The “sa” account should be renamed to something that is not easily identifiable as the “sa” account. ALTER LOGIN sa WITH NAME = <new name>	**Not satisfactory;** the council uses the default account (sa).	M
2.8	Strong password	Use a strong password for the “sa” login account.	Satisfactory	M
2.9	Sample databases	Do not install the sample databases. Delete all sample databases if they already exist.	Satisfactory; there is no sample database installed.	L
2.10	Initialisation parameter	C2 Audit Mode– set to 1 if no custom defined audit trace is enabled	Satisfactory; the current setup is 1.	P
2.11	Initialisation parameter	Remote Access– set to 0 unless replication is being used or the requirement is justified	**Not satisfactory** (the current setup is 1).	M
2.12	Initialisation parameter	Scan for Startup Procedures– set to 0 unless justified	Satisfactory; the current setup is 0.	L

Appendix B24: MS SQL server setting audit details

MS SQL server setting audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
3.1	SQL server configuration manager	Disable the “Named Pipes” network protocol.	**Not satisfactory**	L
3.2	SQL server properties	The following settings are recommended:		
3.2.1	Auto restart SQL server	Set the SQL server service start mode to “Automatic”	Satisfactory	L
3.2.2	Auto restart SQL server agent	If the SQL server agent is required, set the “SQL server agent” start mode to “Automatic”.	Satisfactory	L
3.2.3	Distributed transaction coordinator	Set the “distributed transaction coordinator” service start mode to “Disabled” if this service is not required.	N/A	L
3.2.4	Cross database-ownership chaining	Disable the cross_db_ownership_chaining option.	Satisfactory	M
3.2.5	Advanced server settings	Do not enable direct modifications to the system catalogs.	N/A	M
3.2.6	Backup/restore from tape timeout	Set the backup/restore from tape timeout period to “Try for 5 minutes”	**Not satisfactory;** currently set to “Wait Indefinitely”	L
3.2.7	Media retention	Set the default backup media retention to the minimum number of days needed to retain a full backup of the database. Ideally, this should be as high as your resources permit.	Not satisfactory (currently set to 0.)	L
3.3	Data directory	The default data directory should be a dedicated data partition	**Not satisfactory;** (c:\programfiles\microsoft SQL server\mssql\data)	M
3.4	Data directory	The default log directory should be a dedicated partition separate from all programs and data	**Not satisfactory;** (c:\programfiles\microsoft SQL server\mssql\logs)	M
3.5	Replication	Do not enable replication.	N/A	L
3.6	Other SQL server configuration options	Set the number of logs retained based on the maximum number of restarts and log cyclings which may occur within your desired log retention window. The default value of 6 may be too low for many installations.	Satisfactory; the default is 6.	P

MS SQL server setting audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
3.7	Database mail	Disable database mail where messaging is not required.	Satisfactory	L
3.8	Trace messages	Error log/include execution trace messages = off	Satisfactory	P
3.9	User-defined stored procedures	Ensure that all user-defined stored procedures are stored in encrypted format.	**Not satisfactory**; stored in unencrypted format.	H
3.10	User-defined extended stored procedures	Avoid using user-defined extended stored procedures. If extended functionality is required, use Common Language Runtime (CLR) assemblies instead.	Not installed	L
3.11	Extended stored procedures	Disable access to the following extended stored procedures:		
3.11.1		xp_available media	Satisfactory	L
3.11.2		xp_cmdshell	Satisfactory	L
3.11.3		xp_dirtree	**Not satisfactory;** (enabled).	P
3.11.4		xp_dsninfo	Satisfactory	P
3.11.5		xp_enumdsn	Satisfactory	P
3.11.6		xp_enumerrorlogs	Satisfactory	P
3.11.7		xp_enumgroups	Satisfactory	P
3.11.8		xp_eventlog	Satisfactory	P
3.11.9		xp_fixeddrives	**Not satisfactory;** (enabled).	P
3.11.10		xp_getfiledetails	Satisfactory	P
3.11.11		xp_getnetname	**Not satisfactory;** (enabled).	P
3.11.12		xp_logevent	Satisfactory	P
3.11.13		xp_loginconfig	Satisfactory	P
3.11.14		xp_msver	Satisfactory	P
3.11.15		xp_readerrorlog	Satisfactory	P
3.11.16		xp_servicecontrol	Satisfactory	P
3.11.17		xp_sprintf	Satisfactory	P
3.11.18		xp_sscanf	**Not satisfactory;** (enabled).	P
3.11.19		xp_subdirs	Satisfactory	P
3.12	SQLmail extended stored procedures	Disable access to the following SQLMail extended stored procedures:		
3.12.1		xp_deletemail	Satisfactory	P

MS SQL server setting audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
3.12.2		xp_findnextmsg	Satisfactory	P
3.12.3		xp_get_mapi_default_profile	Satisfactory	P
3.12.4		xp_get_mapi_profiles	Satisfactory	P
3.12.5		xp_readmail	Satisfactory	P
3.12.6		xp_sendmail	Satisfactory	P
3.12.7		xp_startmail	Satisfactory	P
3.12.8		xp_stopmail	Satisfactory	P
3.13	WebTask extended stored procedures	Disable access to the following WebTask extended stored procedures. Delete the xpweb70.dll file that implements the following WebTask extended stored procedures:		
3.13.1		xp_cleanupwebtask	Satisfactory	P
3.13.2		xp_convertwebtask	Satisfactory	P
3.13.3		xp_dropwebtask	Satisfactory	P
3.13.4		xp_enumcodepages	Satisfactory	P
3.13.5		xp_makewebtask	Satisfactory	P
3.13.6		xp_readwebtask	Satisfactory	P
3.13.7		xp_runwebtask	Satisfactory	P
3.14	OLE automation stored procedures	Disable access to the following OLE automation stored procedures:		
3.14.1		sp_OACreate	Satisfactory	L
3.14.2		sp_OADestroy	Satisfactory	L
3.14.3		sp_OAGetErrorInfo	Satisfactory	L
3.14.4		sp_OAGetProperty	Satisfactory	L
3.14.5		sp_OAMethod	Satisfactory	L
3.14.6		sp_OASetProperty	Satisfactory	L
3.14.7		sp_OAStop	Satisfactory	L
3.15	Registry access extended stored procedures	Disable access to the following registry access extended stored procedures:		
3.15.1		xp_regaddmultistring	**Not satisfactory;** (enabled).	P
3.15.2		xp_regdeletekey	**Not satisfactory;** (enabled).	P
3.15.3		xp_regdeletevalue	**Not satisfactory;** (enabled).	P
3.15.4		xp_regenumvalues	**Not satisfactory;** (enabled).	P

MS SQL server setting audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
3.15.5		xp_regremovemultistring	**Not satisfactory;** (enabled).	P
3.15.6		xp_regwrite	**Not satisfactory;** (enabled).	P
3.16	Advanced setting	SQL server event forwarding/forward events to a different server = off	Satisfactory; (off).	L
3.17	SQL server browser service	Disable SQL server browser service	**Not satisfactory;** (enabled).	L

Appendix B25: MS SQL server access controls audit details

MS SQL server access controls audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
4.1	Permissions on OS tools	Restrict access to the executables in the System32 directory e.g. Explorer.exe and cmd.exe.	**Not satisfactory**; administrator has full control, Power users set to modify, and user group set to execute.	H
4.2	SQL server install directory permissions	Modify the permissions to the [Drive]:\Program Files\Microsoft SQL server directory.	**Not satisfactory**; currently the council's local administrator and user groups and is allowed.	H
4.3	SQL server database instance directory permissions	Delete or secure old setup files. Protect files in the <system drive>:\Program Files\Microsoft SQL Server\MSSQL.X\MSSQL\Install, e.g., sqlstp.log, sqlsp.log and setup.iss. "X" represents the installations of various SQL server installs due to the fact that multiple instances of SQL server or SQL express can be installed.	Satisfactory; access to the current install folder is allowed for the system administrator groups only.	M
4.4	Assigning system administrators role	When assigning database administrators to the system administrators role, map their Windows accounts to SQL logins, and then assign them to the role.	Satisfactory	M
4.5	SQL logins	Remove the default BUILTIN\administrators SQL login.	**Not satisfactory;** the BUILTIN\administrators SQL login is still exits.	M
4.6	SQL logins	Ensure that all SQL logins have strong passwords.	Satisfactory	M
4.7	OS guests access	Deny database login for the guests OS group.	Satisfactory	H
4.8	Fixed server roles	Only use the fixed server roles sysadmin, server admin, setup admin etc, to support DBA activity.	Satisfactory	L
4.9	SQL server database users and roles	Remove the guest user from all databases except master and tempdb.	**Not satisfactory;** the guest user stills exist.	M
4.10	Statement permissions	Grant DDL statement permissions to only the database and schema owner, not individual users.	Satisfactory	M
4.11	Database owners permissions	Ensure dbo owns all user-created database schemas	Not satisfactory	L

MS SQL server access controls audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
4.12	Low-privileged users	Do not grant object permissions to PUBLIC or GUEST.	N/A	M
4.13	Stored procedure permissions	Grant executes permissions on stored procedures to database roles (not users).	Satisfactory	M
4.14	Using the GRANT option	Do not assign the GRANT option of object permission to a user or role.	N/A	M
4.15	SQL server agent subsystem privileges	Restrict proxy access to required/approved subsystems.	N/A; no proxy access.	M
4.16	User-defined database roles	Create user-defined database roles to assign permissions to objects in the database when a pre-defined database role does not supply the appropriate permissions to a group of users.	N/A; no user defined database roles.	M
4.17	Database roles	Avoid nesting database roles.	Satisfactory	M
4.18	Users and roles	Ensure that the members of the roles (users/groups/other roles) in the target database actually exist.	Satisfactory	L
4.19	Application roles	Use application roles to limit access to data to users of specific applications. Use encryption to protect the role name and password in the connection string. Use “EXECUTE AS WITH NO REVERT” or “WITH COOKIE” to allow individuals to access the application without knowing the password.	N/A	M
4.20	Use of predefined roles	Avoid assigning predefined roles to PUBLIC or GUEST.	N/A; no predefined roles created.	L
4.21	Linked or remote servers	Use linked servers rather than remote servers where required. Remove any unused linked servers or disable this feature.	N/A	L
4.22	Linked or remote servers	Configure linked or remote servers to use Windows authentication where required. Disable linked servers otherwise.	**Not satisfactory;** currently the council uses both windows and SQL authentications.	M
4.23	Linked server logins	Allow linked server access only to those logins that need it. Disable linked servers otherwise.	Satisfactory	M
4.24	Ad Hoc data access	Disable ad hoc data access on all providers for all users except members of the sysadmin fixed role.	N/A	L

Appendix B26: MS SQL server auditing and logging audit details

MS SQL server auditing and logging audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
5.1	Auditing – general	Prepare a schedule for reviewing audit information regularly.	**Not satisfactory;** currently there is no auditing schedule.	P
5.2	SQL server properties – security tab	Through the SQL server management studio, enable auditing for SQL server.	Satisfactory	P
5.3	SQL server logs	SQL server audit data must be protected from loss. The SQL server and SQL server agent logs must be backed up before they are overwritten.	Satisfactory; the default setup is 6.	P
5.4	SQL profiler	Use SQL profiler to generate and manage audit trails.	Satisfactory	P
5.5	Profiler events	Capture the following events using SQL profiler		
		Event		
5.5.1		Audit add DB user event	**Not satisfactory**	P
5.5.2		Audit add login to server Role	**Not satisfactory**	P
5.5.3		Audit add member to DB role	**Not satisfactory**	P
5.5.4		Audit add role event	**Not satisfactory**	P
5.5.5		Audit addlogin event	**Not satisfactory**	P
5.5.6		Audit app role change password	**Not satisfactory**	P
5.5.7		Audit backup/restore	**Not satisfactory**	P
5.5.8		Audit broker conversation	**Not satisfactory**	P
5.5.9		Audit broker login	**Not satisfactory**	P
5.5.10		Audit change audit	**Not satisfactory**	P
5.5.11		Audit change database owner	**Not satisfactory**	P
5.5.12		Audit DBCC	**Not satisfactory**	P
5.5.13		Audit database management	**Not satisfactory**	P
5.5.14		Audit database object access	**Not satisfactory**	P
5.5.15		Audit database object GDR	**Not satisfactory**	P
5.5.16		Audit database object management	**Not satisfactory**	P
5.5.17		Audit database object take ownership	**Not satisfactory**	P
5.5.18		Audit database operation	**Not satisfactory**	P

MS SQL server auditing and logging audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
5.5.19		Audit database principal impersonation	**Not satisfactory**	P
5.5.20		Audit database principal management	**Not satisfactory**	P
5.5.21		Audit database scope GDR	**Not satisfactory**	P
5.5.22		Audit login change password	**Not satisfactory**	P
5.5.23		Audit login change property	**Not satisfactory**	P
5.5.24		Audit login	**Not satisfactory**	P
5.5.25		Audit login failed	**Not satisfactory**	P
5.5.26		Audit login GDR event	**Not satisfactory**	P
5.5.27		Audit logout	**Not satisfactory**	P
5.5.28		Audit object derived permission event	**Not satisfactory**	P
5.5.29		Audit schema object access	**Not satisfactory**	P
5.5.30		Audit schema object GDR	**Not satisfactory**	P
5.5.31		Audit schema object management	**Not satisfactory**	P
5.5.32		Audit schema object take ownership	**Not satisfactory**	P
5.5.33		Audit server alter trace	**Not satisfactory**	P
5.5.34		Audit server object GDR	**Not satisfactory**	P
5.5.35		Audit server object management	**Not satisfactory**	P
5.5.36		Audit server object take ownership	**Not satisfactory**	P
5.5.37		Audit server operation	**Not satisfactory**	P
5.5.38		Audit server principal impersonation	**Not satisfactory**	P
5.5.39		Audit server principal management	**Not satisfactory**	P
5.5.40		Audit server scope GDR	**Not satisfactory**	P
5.5.41		Audit server starts and stops	**Not satisfactory**	P
5.5.42		Audit statement permission event	**Not satisfactory**	P

Appendix B27: MS SQL server backup and disaster recovery procedures audit details

MS SQL server backup and disaster recovery procedures audit details				
Item no.	**Configuration items**	**Action / recommended Parameters**	**Council B**	**Risk levels**
6.1	Backups – general	Use full database backups combined with differential or transaction log backups to restore the database to a specific point in time.	Satisfactory; currently the council's backup is done nightly.	M
6.2	System databases	It is important to include the system databases in your backup plan i.e. the master, msdb and model databases.	Satisfactory	M
6.3	Backing up master database	Backup the master database when any of the following events occur: ▪ A database is created or deleted ▪ Login accounts are created, deleted or modified Server-wide or database settings are modified	Satisfactory	M
6.4	Backing up MSDB database	Backup the msdb database when any of the following events occur: Alerts, jobs, schedules or operators are created, deleted or modified	Satisfactory	M
6.5	Backup media	Password protects the backup media.	Satisfactory	H
6.6	Access to backup files	Restrict access to the backup files to system administrators.	Satisfactory	H
6.7	Access to backup files	Restrict restore permissions to DBAs	Satisfactory; currently, only the system administrator group can restore the backup files.	H
6.8	Recommended periodic administrative procedures	Run the MS baseline security analyser weekly and follow the security recommendations as closely as possible to secure the OS.	**Satisfactory;** the MS baseline security analyser is in use.	L
6.9	Recommended periodic administrative procedures	Run the SQL best practices analyser regularly and note any changes to the environment.	**Satisfactory;** the SQL best practices analyser is in use.	L

MS SQL server backup and disaster recovery procedures audit details (continued)				
Item no.	**Configuration items**	**Action / recommended Parameters**	**Council B**	**Risk levels**
6.10	Enable password policy enforcement	When a password change mechanism is introduced into clients and applications; enable password expiration. Always specify MUST_CHANGE when specifying a password on behalf of another principal.	**Not satisfactory;** no enforce password policy	M
6.11	Periodic scan of role members	Periodically scan fixed server and database roles to ensure that only trusted individuals are members.	**Not satisfactory;** currently, there are only a few users. Periodic scan may is recommended when number of users increases.	L
6.12	Periodic scan of stored procedures	Verify stored procedures that have been set to AutoStart are secure.	**Not satisfactory;** no AutoStart enabled.	P

Appendix B28: Application development best practices

Application development best practices				
Item no.	**Configuration items**	**Action/recommended Parameters**	**Council B**	**Risk levels**
8.1	Ownership chaining	Use ownership chaining within a single database to simplify permissions management.	**Not satisfactory**	M
8.2	Role assignments	Assign permissions to roles rather than users. The principle of “Least Privilege” applies, thus users should not be given access to roles they do not need for their job function.	Satisfactory	M
8.3	Encrypted connections	Enable encrypted connections between the user and the database server.	**Not satisfactory;** no encrypted connections between the user and the CoB-Database server.	H
8.4	Error handling	Do not propagate errors back to the user.	Satisfactory	P
8.5	User input	Prevent SQL injection by validating all user input before transmitting it to the database server.	Satisfactory	H
8.6	Developer awareness	Increase awareness of issues such as cross-site scripting, buffer overflows, SQL injection and dangerous APIs.	Satisfactory	L
8.7	Developer awareness	Identify categories of threats that apply to your application, such as denial of service, escalation of privileges, spoofing, data tampering, information disclosure and repudiation.	Satisfactory	L
8.8	Security reviews	Add security reviews to all stages of the application development lifecycle (from design to testing).	Satisfactory	L
8.9	Distributing SQLEXPRESS	If you distribute SQLEXPRESS, install SQLEXPRESS using Windows security mode as the default.	N/A	L
8.10	Net-Libraries	If SQLEXPRESS will operate as a local data store, disable any unnecessary client protocols.	N/A	L
8.11	Customer awareness	Let your customers know that your product includes SQLEXPRESS so that they can be prepared to install or accept SQLEXPRESS -specific software updates.	N/A	L

Appendix B29: Surface area configuration tool audit details

Surface area configuration tool audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council B**	**Risk levels**
9.1	Ad Hoc Remote Queries	Disable Ad Hoc Remote Queries where not required.	Satisfactory	L
9.2	CLR integration	Disable CLR integration where not required.	Satisfactory	L
9.3	DAC	Disable the remote dedicated administrator connection where not required.	Satisfactory	L
9.4	Database mail	Disable database mail where messaging is not required.	Satisfactory	L
9.5	Native XML web services	Do not configure XML web services endpoints where not required.	Satisfactory	L
9.6	OLE automation	Disable OLE automation where not required.	Satisfactory	L
9.7	Service broker	Do not configure service broker endpoints where not required.	Satisfactory	L
9.8	SQL mail	Do not enable SQL mail where not required or where database mail could be used instead.	Satisfactory	L
9.9	Web assistant	Disable web assistant where not required.	Satisfactory	P
9.10	xp_cmdshell	Disable the xp_cmdshell stored procedure where not required.	Satisfactory	L
9.11	Ad Hoc data mining	Disable ad hoc data mining queries where not required.	Satisfactory	L
9.12	Anonymous connections	Disable anonymous connections to the analysis services where not required.	Satisfactory	M
9.13	Linked objects	“Enable links to other instances” should be disabled where not required.	**Not satisfactory**	L
9.14	Linked objects	“Enable links from other instances” should be disabled. where not required.	**Not satisfactory**	L
9.15	User-defined functions	Disable loading of user-defined COM functions where not required.	Satisfactory	L
9.16	Scheduled events and report delivery	Disable scheduled events and report delivery where not required.	**Not satisfactory**	P
9.17	Web service and HTTP access	Disable web service and HTTP access where not required.	Satisfactory	L
9.18	Windows integrated security	Enable Windows integrated security for report data source connections.	**Not satisfactory**	M

Appendix B30: Council B's information security policy

Protocol Name: Online Services Usage Protocol	
Keywords	Acceptable use, prohibited use, email and Internet, data confidentiality, logon accounts, passwords, electronic fax
Protocol	This Protocol provides guidance on the acceptable business use and incidental personal use when using the City's online services to ensure that the services are used in an appropriate and professional manner. It also provides guidance on the use of logon accounts, passwords and email etiquette. The purpose of this Protocol is to safeguard the City as well as individuals from the misuse of the City's email, Internet and electronic fax communications systems. Any queries regarding this Protocol should be directed to the Manager IT on Ext xxxx.
Related policies (Council/City)	Code of Conduct Policy 4-1 Records Management Policy 8-4
Related documentation (Plans/Legislative Authority)	Your Record Keeping Responsibilities State and Commonwealth legislation including but not limited to: State Records Act – 2000 Freedom of Information Act 1992 Copyright Amendment (Digital Agenda) Act 2000 Copyright Act 1968 Public Service Regulations 1968 Criminal Code – Section 85
Protocol/procedure owner	Manager IT
Last reviewed	September 2009
Flowchart	

PROTOCOL PROCEDURE

Protocol name: Online Services Usage Protocol

Objectives

This Protocol has been developed to:

- Maintain and protect the availability, reliability, confidentiality, integrity and security of all networked systems and related data from risk or inappropriate use;
- To ensure the City's internal computer network and related systems are used in an appropriate manner consistent with business needs and best practice;
- To define acceptable and unacceptable use of the City's online services; and
- To educate users about their responsibilities.

Scope

The Online Services Usage Protocol applies to:

- All employees of the City; and
- The use of the Council network and related systems, including Internet, email and electronic fax.

Employee responsibilities

When using City information systems, officers are expected to be aware of their responsibilities to:

- Comply with all legislative and administrative requirements;
- Ensure any action taken serves to enhance the services of the City and will not bring the City into disrepute;

- Be informed of all security requirements and risks related to the use of Internet and email facilities and ensure that the facilities are not compromised by their actions; and
- Seek advice if they are unsure of what is required.

Non-compliance with the Online Services Usage Protocol

Non-compliance with this protocol may result in loss of access privileges or disciplinary action and will be subject to the provisions of Policy 4-1 - Code of Conduct and the Corporate Protocol – Managing Employee Relations Issues or provisions of other relevant State or Commonwealth legislation. Directors and Managers are responsible for Business Unit compliance with this protocol.

Acceptable use

The City's network and related systems are provided primarily for conducting the City's business or directly related to the mission, charter or work tasks of the City. Users are expected to treat systems with due care and ensure that all communications are professional and respectful to others.

New employees agree to the Online Services Usage Protocol at Induction when they sign a copy of this document and all employees agree to the Protocol on each occasion they log in.

Prohibited uses

Prohibited uses include:

- A use which is in breach of the law;
- A use which is in breach of the City's Code of Conduct;
- Personal gain or for profit, including private business, commercial activity, advertising or gambling;
- Unauthorised copy or transmission of copyright material;

- Accessing or distributing material or emails which may be illegal, offensive, threatening or harassing to others or discriminatory on the basis of race, religion, political beliefs, sexual orientation, physical features or age;
- Deliberately accessing material perceived as indecent, obscene or pornographic;
- Misrepresentation of persons without the expressed consent of those other persons;
- Breaching confidentiality;
- Political lobbying;
- Unauthorised use, release or destruction of corporate records;
- Unauthorised access to or use of systems;
- Downloading unauthorised software;
- Downloading large files containing picture images, live pictures or graphics which increases the load on the network or slows down the system for other uses. This includes:
    - Computer games
    - Music files
    - Radio or television stations broadcasting via the Internet;
- Non-compliance with or deliberate avoidance of the City's procedures for filtering of viruses, malware or otherwise filtered content;
- Use of Internet services to interfere with or disrupt network users, services or equipment;
- Use of Internet services to develop programs designed to harass other users or infiltrate a computer system, and/or damage or alter the software components, e.g. implant viruses;
- Use for fundraising or public relations activities not specifically related to the City's activities;
- Subscriptions to electronic newsletters that are not related to work or professional development;
- Spending excessive time on personal usage which impacts on completion of an employee's work; and

- Distributing chain letters or spam.

Where a genuine reason exists to access sites that would normally be regarded as inappropriate, Managers are required to nominate the staff members requiring access and written authorisation by the relevant Director is required before access will be given.

Personal use

Incidental personal use of online services, including email, Internet and electronic faxes, is permitted so long as it does not interfere with work, is not detrimental to the City's business, does not involve unethical behaviour and does not involve any of the prohibited uses listed above. Communications relating to professional development are permitted.

All Internet use, whether on City business or personal use, is subject to content filtering that restricts access to illegal or otherwise undesirable or unapproved content. Personal use is entirely at the risk of the individual staff member.

Monitoring of emails, Internet use, electronic faxes and business records

All activities on the network may be monitored or recorded to protect the City from potential consequences that may occur through misuse. Users consent to monitoring when they agree to the Online Services Usage Protocol. The City maintains a log of Internet and email access transactions for all users and examines unusual usage patterns. The City is able to determine the sites visited and the times they were accessed. The City has the right to review, audit, intercept, access and disclose all activities received or sent via the Internet or email.

All incoming and outgoing email is retained in an archive, which is separate from the Record Keeping system. All archived email is potentially subject to a legal discovery order (providing records for court proceedings) or similar forms of legal process.

The CEO, Directors and Managers may determine what is regarded as appropriate use of the Internet or email and may restrict, suspend or close a user at any time.

Access to business records

The City respects the rights of employees to privacy, however, reserves the right to access business records created by all employees and to investigate any suspected improper conduct on the part of an employee. Officers authorised by the CEO may investigate alleged breaches of the City's Code of Conduct.

Mailbox privacy

Access to another user's email account without the user's permission or the authorisation of a Manager is not permitted. Only officers from IT are permitted to access individual email boxes and only if:

- A request is formally logged via the IT Service Desk Request;
- The mailbox owner makes the request; or
- The written request is signed by a Manager, Director or the CEO stating the reason for the request. Each request will be judged on its merits and further justification may be requested by the Manager IT if there are any doubts to the validity of the request.

Where the requests for access arise from statutory obligations, legal discovery orders or similar legal obligations, the request will be complied with. Access by IT staff will be for the duration of the requested task only.

Confidentiality

Information on the City's systems is for the purposes of conducting the City's business and must not be disclosed to third parties. (See the Protocol on Data Privacy).

Corporate records

Email and electronic fax communications are subject to the same legal, privacy, records management and Freedom of Information obligations as a letter, memo or report. Users should:

- Ensure that all content in emails and faxes is expressed in a professional manner; and
- Ensure that emails and electronic faxes which are considered corporate records are stored to the City's Records Management System. Refer to Your Record Keeping Responsibilities.

Other legal obligations

There is a range of legislation which applies to users of information systems, designed to promote compliance with record keeping and copyright provisions, and to restrict illegal practices and the availability of inappropriate material. These include but are not restricted to the:

- State Records Act – 2000;
- Freedom of Information Act 1992;
- Copyright Amendment (Digital Agenda) Act 2000;
- Copyright Act 1968;
- Public Service Regulations 1968; and
- Criminal Code – Section 85.

The Council and the user can be held liable for illegal activities, such as breaches of copyright or licensing agreements, disclosing confidential information, sending libellous, defamatory, offensive or racist content in emails and accessing inappropriate material. Staff members must at all times comply with their legal obligations under relevant legislation. Any unauthorised access or attempted access of any Commonwealth or state computing and/or network system or violation of Australian Commonwealth or State laws is subject to criminal prosecution.

SCHEDULE 1 – ELECTRONIC MAIL ETIQUETTE

Schedule 1 presents some general guidelines for electronic mail etiquette.

- Check emails regularly, at least daily;
- Reply to emails promptly in accordance with the Customer Service Charter;
- Check the calendar function of Outlook daily;
- Maintain the Inbox, Sent Items and Deleted Items. Delete unwanted items regularly to maintain available system space;
- Store emails which contain corporate records to the Records Management System;
- Ensure that an Out of Office message is set up for periods of absence or leave. Under exceptional circumstances a Business Unit Manager may request IT to activate an Out of Office message if a staff member has unplanned leave for a significant period of time, e.g. sickness;
- Staff are responsible for managing delegated access to their mailbox by other users;
- Avoid sending emails to the group CoB All Staff. If the matter relates to City business it is recommended that a News Item on the intranet is published. This reduces email traffic;
- Avoid sending internal emails with large attachments as this may slow down the network. It is better to place the attachment on the Intranet and use a link in an email or in a News Item;
- Emails which exceed 20 megabytes in size will be blocked from being transmitted to external recipients. Consult the IT Service Desk for assistance in these instances. Note that an external email recipient’s system may not necessarily be able to receive large emails;
- Do not use emails instead of formal contracts or agreements because of the potential for forgery or misrepresentation. Note that emails are considered written records and are legally binding; and

- Ensure that emails have a confidentiality note in the signature block as set out below.

Email signatures

All email text should be black with no backgrounds or wallpapers. The signature block should be set in your email options so that it will be used by default on all emails. (Refer to the Intranet - How do I?)

GivenName FamilyName	**- 10 point Arial, bold**
Position or Title	- 10 point Arial, normal
Council B	- 10 point Arial, normal
Tel: 08 9xxx xxxx	- 8 point Arial, normal
Mobile: 0xxx xxx xxx	- 8 point Arial, normal
Fax: 08 9xxx xxxx	- 8 point Arial, normal
Email:givenname.familyname@CouncilB.wa.gov.au	- 8 point Arial, normal
Council B	
The information contained in this communication may be confidential or commercially sensitive. If you are not the intended recipient you must not copy this communication, disclose its contents to any other party, or take any action in reliance on it. Please delete and destroy all copies and immediately notify the sender on 9xxx xxxx, or by reply message.	

Logon accounts and passwords

- A logon and password is created following an authorised New User Request (See How Do I – Forms.) Users are provided with a secure temporary password which they are forced to change immediately upon next login;
- Expired accounts require an authorised New User Request before they will be reactivated;
- Each user requires his/her own log on and password to use the City's network and all systems. This is to prevent unauthorised access and to facilitate confidentiality and security of all networked systems and related data;
- Logon accounts are the means to validate a user's identity to access the City's network or application systems;
- Logon accounts are derived from a unique combination of the user's first name and initial characters of their surname;
- Shared workstations, e.g. workstation used for the issuing of books in libraries or handling customer enquiries are given a generic logon which reflects the

function. Access through generic logons to fileservers, email and corporate applications are restricted to functions that do not require user accountability or security network security;

- Users maintain their own passwords;
- Avoid keeping a paper copy of passwords;
- Temporary passwords provided when users forget or lock their password account will only be supplied following positive identification of the user;
- Passwords are not to be divulged to third parties and details are not to be provided to other users to enable their use of a specific application;
- Change passwords when there is an indication of possible system or password compromise; and
- Passwords must comply with system enforced password rules.These rules are displayed when prompted by the system to change your password.

Closing down and locking the workstation

- The PC automatically locks following a period of inactivity;
- It is the responsibility of all system users to ensure that they activate the workstation locking mechanism before leaving their desks using the CTRL+Alt+Delete keys to ensure the PC is secure while unattended; and
- Users should shut down the PC at the close of each business day.

Appendix C: Additional results for Chapter 6

Appendix C1: A summary of the firewall configuration codes (email-NAT) of Council C's firewall

Policy no.	Rules	Protocol types	From (source)	To (destination)	Ports (service)
1	MIP (mapped IP)	TCP	Webrootservices	A.B.C.37	SMTP
2	MIP	TCP	Any	A.B.C.37	SMTP

Appendix C2: A summary of the firewall configuration codes of Council C's email system

Policy no.	Rules	Protocol types	From (source)	To (destination)	Ports (service)
1	Translate	Address	ISA-Exchange	A.B.C.184	N/A
2	Translate	Address	BDC-1	10.1.1.150	N/A
3	Translate	Address	BDC-2	10.1.1.210	N/A
4	Translate	Address	Exchange-gate1	10.1.15.154	N/A
5	Translate	Address	Exchange-gate2	10.1.1.3	N/A
6	Add	Address	BDC-1	Domaincon	N/A
7	Add	Address	BDC-2	Domaincon	N/A
8	Permit	TCP	Exchange-gate1	Any	SMTP
9	Permit	TCP	ISA-Exchange	Exchange-gate1	HTTPS
10	Permit	TCP	Any	ISA-Exchange	HTTPS
11	Inspect	TCP	Any	ISA-Exchange	HTTPS
12	Permit	TCP/UDP	ISA-Exchange	Domaincon	DNS
13	Permit	TCP	ISA-Exchange	Domaincon	LDAP (389)
14	Permit	UDP	ISA_Exchange	Domaincontrollers	Radius (1812, 1813)
15	Permit	UDP	ISA_Exchange	Domaincontrollers	Radius (1812, 1813)

Appendix C3: A full details of system information policy results of Council C's email server

System information policy – exchange.coc.wa.gov.au (10.1.15.154)				
Services				
157				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length:	6 chars		At least 8 chars	
Maximum password age:	91 days		30 days	
Minimum password age:	0 day		0 day	
Force logoff:	Never force		Force	
Password history:	8 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	No	No	Yes	Yes
Audit directory service access	No	No	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	No	No	Yes	Yes
Audit policy change	No	No	Yes	Yes
Audit privilege use	No	No	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	No	No	Yes	Yes

Appendix C4: A summary of both missing service pack and patches information of Council C's email server

Missing service pack (1) – email server (10.1.15.154)				
Product	**Severity**	**Description**	**Vulnerability issue**	**Recommendation**
MS Windows	N/A	MS Windows Server 2008 service pack 2 standalone x64-based systems (KB948465)	Service pack 2 for MS Windows Server 2008 is an update to MS Windows Server 2008 that supports new kinds of hardware and emerging hardware standards, and includes all updates delivered since service pack 1.	Deploy/patch
Missing patches (2) – email server (10.1.15.154)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS Windows	Moderate	KB969897	MS09-019 cumulative security update for MS Internet Explorer 7 for MS Windows Server 2008 x64 edition	Deploy/patch
MS Windows	N/A	KB951072	Update for MS Windows Server 2008 x64 edition	Deploy/patch

Appendix C5: The overall opened TCP and UDP service ports, and the possible mitigation recommendation on Council C's email server

The overall opened TCP service ports (24) – email server (10.1.15.154)				
Port no.	**Services**	**Descriptions**	**Products**	**Recommendations**
21	FTP	File Transfer Protocol		Close
25	SMTP	Simple Mail Transfer Protocol	MS ESMTP	Open
80	HTTP	Hyper Text Transfer Protocol	MS IIS webserver 7.0	Open
110	POP3	Post Office Protocol 3	MS Exchange Server 2007 POP3	Close
135	MSRPC	Microsoft Remote Procedure Call	MS Windows RPC	Open
139	NetBIOS-ssn	NetBIOS session service	NetBIOS session service	Open
143	IMAP4	Internet Message Access Protocol 4	MS Exchange 2007 imapd	Close
443	HTTPS	Hypertext Transfer Protocol over TLS/SSL	MS IIS webserver 6.0	Open
445	MS-DS	MS-DS Active Directory, Windows shares	MS Windows 2003	Open
587	Email message submission	Email message submission (SMTP)	MS ESMTP	Close
593	Ncacn_http_ epmap	HTTP RPC Ep Map	MS Windows RPC over HTTP 1.0	Close
993	Imaps	Internet Message Access Protocol over SSL	MS Exchange 2007 imapd	Close
1028	MSRPC	LSASS	MS Windows RPC, Possibility of a Trojan attack if not installed	Close
1029	MSRPC	InetInfo	MS Windows RPC, Possibility of a Trojan attack if not installed	Close
1058	MSRPC	MS Windows RPC	MS Windows RPC	Close
3389	Microsoft-rdp	MS terminal service	MS terminal service	Open to authorised users only
5357	HTTP	MS HTTPAPI	MS HTTPAPI httpd 2.0 (SSDP/UPnP)	Close
6001	Ncacn_http	MS Windows RPC	MS Windows RPC over HTTP 1.0	Close
6002	Ncacn_http	MS Windows RPC	MS Windows RPC over HTTP 1.0	Close
6004	Ncacn_http	MS Windows RPC	MS Windows RPC over HTTP 1.0	Close

The overall opened TCP service ports (24) – email server (10.1.15.154) (continued)				
Port no.	**Services**	**Descriptions**	**Products**	**Recommendations**
6129	Damewaremr	DameWare mini remote control	DameWare mini remote control	Close if not required
6969	Tcpwrapped			Close
8080	HTTP-ALT	HTTP alternate		Open
10000	Snet-sensor-mgmt	Webmin and Oracle	Possibility of a Trojan attack if not installed	Close
The overall opened UDP service port (1) – email server (10.1.15.154)				
Port no.	**Service**	**Description**	**Product**	**Recommendation**
137	NetBIOS-ns	NetBIOS name service, (workgroup: COCSHIRE)	Microsoft Windows NT NetBIOS-ssn	Open

Appendix C6: A summary of Council C's email server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of Council C's email server (10.1.15.154)	
Low security vulnerabilities (9)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Registry: Last logged-on username visible	Should be disabled
Services: HTTP	Should be disabled if not required
Services: FTP	Should be disabled
Services: SMTP	Satisfactory
Services: HTTPS	Satisfactory
Services: TCP port 110 (POP3) open	Should be disabled
Services: IMAP4	Should be disabled
Potential vulnerabilities (2)	
Section: Types	**Recommendations**
Information: Administrator account exists	Rename the administrator account
Information: IMAP4 server banner provides information to attacker	IMAP banners should be omitted or changed to something more generic

Appendix C7: A summary of the firewall configuration codes for Council C's static web system with respect to the CoC-DMZ-Web server

Policy no.	Rules	Protocol types	From (source)	To (destination)	Ports (service)
1	MIP	Address	A.B.C.181	CoC-DMZ-Web	N/A
2	MIP	Address	HeadOffice	10.0.0.0/8	N/A
3	MIP	Address	BDC-1	10.1.1.210	N/A
4	MIP	Address	BDC-2	10.1.1.150	N/A
5	MIP	Address	Wbaseline1	X.X.X.101	N/A
6	MIP	Address	Wbaseline2	X.X.X.11	N/A
7	MIP	Address	Wbaseline3	X.X.X.157	N/A
8	MIP	Address	NearMap #01	Y.Y.X.0/24	N/A
9	MIP	Address	NearMap #02	Y.Y.Y.0/24	N/A
10	MIP	Address	NearMap #03	Y.Y.Z.0/24	N/A
11	MIP	Address	Busgov	V.V.V.122	N/A
12	Set	Group	Domaincon	N/A	N/A
13	Set	Group	Winbaseline	N/A	N/A
14	Set	Group	Webexternal	N/A	N/A
15	Set	Group	Nearmapserver	N/A	N/A
16	Add	Address	BDC-1	Domaincon	N/A
17	Add	Address	BDC-1	Domaincon	N/A
18	Add	Address	Wbaseline1	Winbaseline	N/A
19	Add	Address	Wbaseline2	Winbaseline	N/A
20	Add	Address	Wbaseline3	Winbaseline	N/A
21	Add	Address	Busgov	Webexternal	N/A
22	Add	Address	NearMap#01	Nearmapserver	N/A
23	Add	Address	NearMap #02	Nearmapserver	N/A
24	Add	Address	NearMap #03	Nearmapserver	N/A
25	Set	TCP	src-port 2005	des-port 0-65535	2005
26	Permit, inspect	TCP	Any (outside/untrust)	CoC-DMZ-Web	HTTP, HTTPS
27	Permit	UDP	Any (DMZ)	Domaincon	DNS
28	Permit	TCP	CoC-DMZ-Web	HeadOffice	2005
29	Permit	IP	CoC-DMZ-Web	Winbaseline	Any
30	Permit	IP	CoC-DMZ-Web	Webexternal	Any
31	Permit	IP	CoC-DMZ-Web	Nearmapserver	Any
32	Permit	IP	Any (inside/trust)	Any (DMZ)	Any

Appendix C8: A summary of the firewall configuration codes for Council C's CMS web system with respect to the CoC-DMZ-CMS and the CoC-CMS servers

Policy no.	**Rules**	**Protocol types**	**From (source)**	**To (destination)**	**Ports (service)**
1	MIP	Address	A.B.C.186	CoC-DMZ-CMS	N/A
2	MIP	Address	F.F.F.169	Seamless web service	N/A
3	Permit, inspect, log	TCP	Any (outside)	CoC-DMZ-CMS	HTTP, HTTPS
4	Permit, log	TCP	CoC-DMZ-CMS	Seamless web service	HTTP
5	Permit	UDP	Any (DMZ)	Domaincon	DNS
6	Permit	IP	Any (inside/trust)	Any (DMZ)	Any

Appendix C9: A summary of the firewall configuration codes for Council C's online payment system

Policy no.	Rules	Protocol types	From (source)	To (destination)	Ports (service)
1	MIP	Address	A.B.C.179	Pathway-server	N/A
2	MIP	Address	10.1.15.166	Pathway-app	N/A
3	MIP	Address	A.B.C.183	ISA01	N/A
4	MIP	Address	N.N.N.0/24	Commweb01	N/A
5	Permit, inspect	TCP	Any (outside)	Pathway-server	HTTP, HTTPS
6	Permit, log	IP	ISA01 (DMZ) source address Pathway-server	Pathway-app	Any
7	Permit, log	TCP	Pathway-server	Commweb01	HTTP, HTTPS
8	Permit	UDP	Any (DMZ)	Domaincon	DNS
9	Permit	IP	Any (inside/trust)	Any (DMZ)	Any

Appendix C10: A full details of system information policy results and recommendations of Council C's CoC-DMZ-Web server

System information policy – CoC-DMZ-Web server (A.B.C.181)				
Services				
140				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	0 char		At least 8 chars	
Maximum password age	42 days		30 days	
Minimum password age	0 day		0 day	
Force logoff	Never force		Force	
Password history	No history		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	Yes	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	Yes	Yes	Yes	Yes
Audit process tracking	Yes	Yes	Yes	Yes
Audit system events	Yes	Yes	Yes	Yes

Appendix C11: A full details of system information policy results and recommendations of Council C's CoC-DMZ-CMS server

System information policy – CoC-DMZ-CMS server (A.B.C.186)				
Services				
N/A – could not obtained (access denied)				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	0 char		At least 8 chars	
Maximum password age	42 days		30 days	
Minimum password age	0 day		0 day	
Force logoff	Never force		Force	
Password history	No history		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	N/A	N/A	Yes	Yes
Audit account management	N/A	N/A	Yes	Yes
Audit directory service access	N/A	N/A	Yes	Yes
Audit logon events	N/A	N/A	Yes	Yes
Audit object access	N/A	N/A	Yes	Yes
Audit policy change	N/A	N/A	Yes	Yes
Audit privilege use	N/A	N/A	Yes	Yes
Audit process tracking	N/A	N/A	Yes	Yes
Audit system events	N/A	N/A	Yes	Yes

Appendix C12: A full details of system information policy results and recommendations of Council C's CoC-CMS server

System information policy – CoC-CMS server (10.1.15.184)				
Services				
145				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	6 chars		At least 8 chars	
Maximum password age	91 days		30 days	
Minimum password age	0 day		0 day	
Force logoff	Never force		Force	
Password history	8 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	No	No	Yes	Yes
Audit directory service access	No	No	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	No	No	Yes	Yes
Audit policy change	No	No	Yes	Yes
Audit privilege use	No	No	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	No	No	Yes	Yes

Appendix C13: A full details of system information policy results and recommendations of Council C's Epathweb server

System information policy – Epathweb server (A.B.C.179)				
Services				
126				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	10 chars		No action required	
Maximum password age	30 days		No action required	
Minimum password age	0 day		0 day	
Force logoff	Never force		Force	
Password history	10 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	No	No	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	No	No	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	No	Yes	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	Yes	No	Yes	Yes

Appendix C14: A full details of system information policy results and recommendations of Council C's Epathway server

System information policy – Epathway server (10.1.15.166)				
Services				
124				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	6 chars		No action required	
Maximum password age	91 days		No action required	
Minimum password age	0 day		0 day	
Force logoff	Never force		Force	
Password history	8 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes
Audit object access	No	No	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes
Audit privilege use	No	Yes	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	Yes	No	Yes	Yes

Appendix C15: A full details of system information policy results and recommendations of Council C's Pathway server

System information policy – Pathway server (10.1.15.162)				
Services				
118				
Password policy				
Types	**Current settings**		**Recommendations**	
Minimum password length	6 chars		No action required	
Maximum password age	91 days		No action required	
Minimum password age	0 day		0 day	
Force logoff	Never force		Force	
Password history	8 passwords		N/A	
Security audit policy				
Auditing policies	**Success (current settings)**	**Failure (current settings)**	**Success (recommendations)**	**Failure (recommendations)**
Audit account logon events	Yes	Yes	Yes	Yes
Audit account management	No	No	Yes	Yes
Audit directory service access	No	No	Yes	Yes
Audit logon events	No	No	Yes	Yes
Audit object access	No	No	Yes	Yes
Audit policy change	No	No	Yes	Yes
Audit privilege use	No	No	Yes	Yes
Audit process tracking	No	No	Yes	Yes
Audit system events	No	No	Yes	Yes

Appendix C16: A summary of missing service packs and patch, and the possible mitigation recommendations for the CoC-DMZ-Web server

Missing service packs (2) – CoC-DMZ-Web server (A.B.C.181)				
Products	**Filenames**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
Office	MAINSP3ff.cab	N/A	Office XP service pack 3	Deploy/patch
SQL server	SQL2000-KB884525-SP4-x86-ENU.EXE	N/A	2000 service pack 4 for database components	Deploy/patch
Missing patch (0) – CoC-DMZ-Web (A.B.C.181)				
Product	**Severity**	**Knowledge base**	**Vulnerability issue**	**Recommendation**
Not available	Not available	Not available	Not available	Not available

Appendix C17: A summary of missing service packs and patches, and the possible mitigation recommendations for the Epathweb server

Missing service packs (5) – Epathweb server (A.B.C.179)				
Products	**Filenames**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
Visual Studio	VS80sp1-KB926601-X86-ENU.exe	N/A	Visual Studio 2005 service pack 1	Deploy/patch
MS Windows	dotnetfx35.exe	KB951847	MS.NET framework 3.5 service pack 1 and .NET framework 3.5 family update x86	Deploy/patch
MS Windows	NDP20SP2-KB958481-x86.exe	KB951847	MS.NET framework 3.5 service pack 1 and .NET framework 3.5 family update x86	Deploy/patch
MS Windows	NDP30SP2-KB958483-x86.exe	KB951847	MS.NET framework 3.5 service pack 1 and .NET framework 3.5 family update x86	Deploy/patch
MS Windows	NDP35SP1-KB958484-x86.exe	KB951847	MS.NET framework 3.5 service pack 1 and .NET framework 3.5 family update x86	Deploy/patch
Missing patches (37) – Epathweb server (A.B.C.179)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS09-024	Important	KB957646	Security update for MS Office XP	Deploy/patch
MS09-021	Important	KB969680	Security update for MS Excel 2002	Deploy/patch
MS09-027	Important	KB969602	Security update for MS Word 2002	Deploy/patch
MS09-017	Important	KB957781	Security update for MS PowerPoint 2002	Deploy/patch
MS09-010	Important	KB933399	Security update for MS Office XP	Deploy/patch
MS08-056	Moderate	KB956464	Security update for MS Office 2002	Deploy/patch
MS08-052	Important	KB953405	Security update for MS Office XP	Deploy/patch
MS08-044	Important	KB921596	Security update for MS Office XP	Deploy/patch
MS08-041	Critical	KB955440	Security update for Access Snapshot Viewer 2002	Deploy/patch asap
MS08-027	Important	KB950129	Security update for MS Publisher 2002	Deploy/patch

Missing patches (37) – Epathweb server (A.B.C.179) (continued)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS08-017	Critical	KB932031	Security update for MS Office Web Components 2000 for MS Office XP	Deploy/patch asap
MS08-015	Critical	KB946985	Security update for MS Outlook 2002	Deploy/patch asap
MS08-013	Important	KB944423	Security update for MS Office XP	Deploy/patch
MS07-013	Important	KB920816	Security update for MS Office XP	Deploy/patch
MS09-020	Important	KB970483	Security update for MS Windows Server 2003	Deploy/patch
MS09-019	Moderate	KB969897	Cumulative security update for MS Internet Explorer 7 for MS Windows Server 2003	Deploy/patch
MS09-026	Important	KB970238	Security update for MS Windows Server 2003	Deploy/patch
MS09-025	Important	KB968537	Security update for MS Windows Server 2003	Deploy/patch
MS09-022	Moderate	KB961501	Security update for MS Windows Server 2003	Deploy/patch
MS09-011	Critical	KB961373	Security update for MS Windows Server 2003	Deploy/patch asap
MS09-012	Important	KB956572	Security update for MS Windows Server 2003	Deploy/patch
MS09-012	Important	KB952004	Security update for MS Windows Server 2003	Deploy/patch
MS09-013	Critical	KB960803	Security update for MS Windows Server 2003	Deploy/patch asap
MS09-015	Important	KB959426	Security update for MS Windows Server 2003	Deploy/patch
MS09-010	Important	KB923561	Security update for MS Windows Server 2003	Deploy/patch
N/A	Important	KB890830	MS Windows Malicious Software Removal Tool - April 2009	Deploy/patch
MS09-007	Important	KB960225	Security update for MS Windows Server 2003	Deploy/patch
N/A	Important	KB960715	Update Rollup for ActiveX Killbits for MS Windows Server 2003	Deploy/patch
MS09-001	Critical	KB958687	Security update for MS Windows Server 2003	Deploy/patch asap
MS08-071	Critical	KB956802	Security update for MS Windows Server 2003	Deploy/patch asap

Missing patches (37) – Epathweb server (A.B.C.179) (continued)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS08-076	Important	KB954600	Security update for MS Windows Server 2003	Deploy/patch
MS08-076	Important	KB952069	Security update for MS Windows Server 2003	Deploy/patch
MS08-068	Important	KB957097	Security update for MS Windows Server 2003	Deploy/patch
MS08-069	Important	KB954459	Security Update for MS Microsoft XML Core Services 6.0 service pack 2	Deploy/patch
MS08-069	Critical	KB955069	Security update for MS Windows Server 2003	Deploy/patch asap
MS07-040	Critical	KB928365	Security update for Microsoft .NET framework, version 2.0	Deploy/patch asap
MS07-050	Critical	KB938127	Security update for MS Internet Explorer 7 for MS Windows Server 2003	Deploy/patch asap

Appendix C18: A summary of missing service packs and patches, and the possible mitigation recommendations for the Epathway server

Missing service packs (4) – Epathway server (10.1.15.166)				
Products	**Filenames**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS Windows	dotnetfx35.exe	KB951847	Microsoft .NET framework 3.5 service pack 1 and .NET framework 3.5 family update	Deploy/patch
MS Windows	DP20SP2-KB958481-x86.exe	KB951847	Microsoft .NET framework 3.5 service pack 1 and .NET framework 3.5 family update	Deploy/patch
MS Windows	NDP30SP2-KB958483-x86.ex	KB951847	Microsoft .NET framework 3.5 service pack 1 and .NET framework 3.5 family update	Deploy/patch
MS Windows	NDP35SP1-KB958484-x86.exe	KB951847	Microsoft .NET framework 3.5 service pack 1 and .NET framework 3.5 family update	Deploy/patch
Missing patches (22) – Epathway server (10.1.15.166)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS Office	Important	KB969559	MS09-024 security update for the 2007 MS Office system	Deploy/patch
MS Office	Important	KB969613	MS09-027 security update for the 2007 MS Office system	Deploy/patch
MS Office	Important	KB969604	MS09-027 security update for MS Word 2007	Deploy/patch
MS Office	Important	KB969682	MS09-021 security update for MS Excel 2007	Deploy/patch
MS Office	Important	KB969679	MS09-021 security update for the 2007 MS Office system	Deploy/patch
MS Office	Important	KB957789	MS09-017 security update for MS PowerPoint 2007	Deploy/patch
MS Windows	Important	KB970483	MS09-020 security update for MS Windows Server 2003	Deploy/patch

Missing patches (22) – Epathway server (10.1.15.166) (continued)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS Windows	Important	KB970238	MS09-026 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Important	KB956803	MS08-066 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Important	KB954459	MS08-069 security update for MS XML core services 6.0 SP 2	Deploy/patch
MS Windows	N/A	N/A	MS Windows Internet Explorer 7 for Windows Server 2003	Deploy/patch
MS Windows	Important	KB944653	MS07-067 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Critical	KB941569	MS07-068 security update for MS Windows Server 2003	Deploy/patch asap
MS Windows	Critical	KB933854	MS07-040 security update for Microsoft .NET framework, version 1.1 service pack 1	Deploy/patch asap
MS Windows	Critical	KB938127	MS07-050 security update for MS Windows Server 2003	Deploy/patch asap
MS Windows	Important	KB926122	MS07-039 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Critical	KB925398	MS06-078 security update for MS Windows Media Player 6.4	Deploy/patch asap
MS Windows	Low	KB929123	MS07-034 cumulative security update for MS Outlook Express for MS Windows Server 2003	Deploy/patch
MS Windows	Important	KB924667	MS07-012 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Moderate	KB932168	MS07-020 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Critical	KB930178	MS07-021 security update for MS Windows Server 2003	Deploy/patch asap
MS SQL server	Critical	925673	MS06-061 MS XML 6.0 RTM security update	Deploy/patch asap

Appendix C19: A summary of missing service packs and patches, and the possible mitigation recommendations for the Pathway server

Missing service packs (5) – Pathway server (10.1.15.162)				
Products	**Filenames**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS Windows	dotnetfx35.exe	KB951847	Microsoft .NET framework 3.5 service pack 1 and .NET framework 3.5 family update	Deploy/patch
MS Windows	NDP20SP2-KB958481-x86.exe	KB951847	Microsoft .NET framework 3.5 service pack 1 and .NET framework 3.5 family update	Deploy/patch
MS Windows	NDP30SP2-KB958483-x86.exe	KB951847	Microsoft .NET framework 3.5 service pack 1 and .NET framework 3.5 family update	Deploy/patch
MS Windows	NDP35SP1-KB958484-x86.exe	KB951847	Microsoft .NET framework 3.5 service pack 1 and .NET framework 3.5 family update	Deploy/patch
MS Office	OWC11SP3.CAB	N/A	MS Office 2003 service pack 3	Deploy/patch
Missing patches (15) – Pathway server (10.1.15.162)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS Windows	Important	KB970238	MS09-026 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Important	KB970483	MS09-020 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Important	KB956803	MS08-066 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Important	KB954459	MS08-069 security update for MS XML core services 6.0 service pack 2	Deploy/patch
MS Windows	Important	N/A	MS Internet Explorer 7 for MS Windows Server 2003	Deploy/patch
MS Windows	Important	KB944653	MS07-067 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Critical	KB941569	MS07-068 security update for MS Windows Server 2003	Deploy/patch asap

Missing patches (15) – Pathway server (10.1.15.162) (continued)				
Products	**Severities**	**Knowledge base**	**Vulnerability issues**	**Recommendations**
MS Windows	Critical	KB933854	MS07-040 security update for Microsoft .NET framework, version 1.1 service pack 1	Deploy/patch asap
MS Windows	Critical	KB938127	MS07-050 security update for MS Windows Server 2003	Deploy/patch asap
MS Windows	Critical	KB925398	MS06-078 security update for MS Windows media player 6.4	Deploy/patch asap
MS Windows	Important	KB926122	MS07-039 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Important	KB924667	MS07-012 security update for MS Windows Server 2003	Deploy/patch
MS Windows	Low	KB929123	MS07-034 cumulative security update for MS Outlook Express for MS Windows Server 2003	Deploy/patch
MS Windows	Critical	KB930178	MS07-021 security update for MS Windows Server 2003	Deploy/patch asap
MS Windows	Moderate	KB932168	MS07-020 security update for MS Windows Server 2003	Deploy/patch

Appendix C20: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the CoC-DMZ-Web server

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
6	N/A	Unassigned	Close
7	echo	echo	Close
21	FTP	File Transfer Protocol; MS FTP service	Close
22	SSH	Secure Shell Open; SSH_3.8	Close if not required
24	Priv-mail	Any private mail system	Close
25	SMTP	Simple Mail Transfer Protocol; MS ESMTP 6.0.3790.3959	Close
30	N/A	Unassigned	Close
32	N/A	Unassigned	Close
80	HTTP	Hyper Text Transfer Protocol; MS IIS webserver 6.0	**Open**
81	hosts2-ns	HOSTS2 Name Server	Close
82	xfer	XFER Utility	Close
83	mit-ml-dev	MIT ML device	Close
85	mit-ml-dev	MIT ML device	Close
88	Kerberos-sec	Kerberos	Close if not required
90	dnsix	DNSIX security attribute token map	Close
99	metagram	Metagram relay	Close
106	POP3pw		Close
110	POP3	Post Office Protocol 3	Close
125	locus-map	Locus PC-Interface Net Map Ser	Close
135	MSRPC	MS Remote Procedure Call; MS Windows RPC	Close if not required
139	NetBIOS-ssn	NetBIOS Session Service for MS File and printer sharing	Close if not required
144	news	NeWS window system	Close
146	iso-tp0	ISO-IP0	Close
161	snmp	SNMP	Close if not required
163	cmip-man	CMIP/TCP manager	Close
211	914c/g	Texas instruments 914C/G terminal	Close
212	anet	ATEXSSTR	Close
222	rsh-spx	Berkeley rshd with SPX auth	Close
259	esro-gen	Efficient short remote operations	Close
280	http-mgmt	http-mgmt	Close
301	N/A	Unassigned	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
389	ldap	Lightweight Directory Access Protocol	Close if not required
406	imsp	Interactive Mail Support Protocol	Close
417	onmux	Onmux	Close
443	HTTPS	Hypertext Transfer Protocol over TLS/SSL; MS IIS webserver 6.0	Open
445	MS-ds	MS-DS Active Directory, Windows shares MS Windows 2003	Close if not required
464	kpasswd	kpasswd	Close
465	SMTPS	SMTP secure	Close
481	dvs	DVS	Close
500	isakmp	Security association and key management protocol	Close if not required
512	exec	Remote Execution-- Allows remote execution of commands without logon.	Close
513	login	Remote Login-- Remote term service that operates via telnet process- but with automatic auth performed based on trust. If no trust- will prompt for username/password logon similar to telnet.	Close
524	NPC	NCP	Close
544	kshell	krcmd	Close
625	apple-xsvr-admin	Apple	Close
636	ldapssl	ldap protocol over TLS/SSL (was sldap)	Close if not required
648	RRP	Registry Registrar Protocol (RRP)	Close
667	disclose	Campaign contribution disclosures - SDR Technologies	Close
668	mecomm	MeComm	Close
691	resvc	MS Exchange routing engine	Close
700	epp	Extensible Provisioning Protocol	Close
714	iris-xpcs	IRIS over XPCS	Close
722	unknown	Unassigned	Close
726	unknown	Unassigned	Close
765	webster	Webster	Close
777	multiling-http	Multiling HTTP	Close
783	spamassasin	Apache SpamAssassin spamd	Close
787	qsc	QSC	Close
800	mdbs_daemon	Mdbs_daemon	Close
801	device	Device	Close
808	ccproxy-http	CCProxy HTTP/Gopher/FTP (over HTTP) proxy	Close
873	rsync	rsync	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
888	accessbuilder	AccessBuilder	Close
898	sun-manageconsole	Solaris Management Console Java listener (Solaris 8 & 9)	Close
900	unknown	unknown	Close
901	samba-swat	Samba SWAT tool	Close
903	iss-console-mgr	ISS Console Manager	Close
912	apex-mesh	APEX relay-relay service	Close
990	FTPs	FTP protocol, control, over TLS/SSL	Close if not required
992	Telnets	Telnet protocol over TLS/SSL	Close if not required
1007	unknown	unknown	Close
1009	unknown	Unassigned	Close
1010	surf	surf or possibility Doly Trojan	Close
1025	MSRPC	MS Windows RPC	Close if not required
1026	LSA-or-nterm	nterm remote_login network_terminal	Close
1029	ms-lsa	Ms-lsa	Close
1031	iad2	BBN IAD	Close
1034	zincite-a	Zincite.A backdoor	Close
1035	multidropper	A Multidropper Adware, or PhoneFree	Close
1036, 1037	unknown	unknown	Close
1038	mtqp	Message Tracking Query Protocol	Close
1039	MSRPC	MS Windows RPC	Close if not required
1040	netsaint	Netsaint status daemon	Close
1041	danf-ak2, Trojan	AK2 Product , Dosh, RemoteNC; , If these services are not installed beware could be Trojan	Close
1042	Unknown; bla Trojan	BLA Trojan; If these services are not installed beware could be Trojan	Close
1043	boinc	BOINC client control	Close
1044-1049	unknown	unknown	Close
1050	java-or-OTGfileshare	J2EE nameserver, also OTG, also called Disk/Application extender. Could also be MiniCommand backdoor OTGlicenseserv	Close
1051	optima-vnet	Optima VNET	Close
1052	ddt	Dynamic DNS tools	Close
1053, 1056, 1057	unknown	unknown	Close
1059	nimreg	Nimreg	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
1061, 1064-1065	unknown	unknown	Close
1066	fpo-fns	FPO-FNS	Close
1067	instl_boots	Installation bootstrap protocol serv.	Close
1070-1072, 1077	unknown	unknown	Close
1081	unknown	unknown	Close
1083	ansoft-lm-1	Anasoft license manager	Close
1084	ansoft-lm-2	Anasoft license manager	Close
1087, 1088, 1090, 1097-1100, 1104-1107	unknown	unknown	Close
1112	msql	mini-sql server	Close if not required
1114, 1117, 1121, 1122, 1124, 1126, 1130-1132, 1137, 1147, 1148, 1152, 1163, 1165, 1174	unknown	unknown	Close
1185, 1186, 1192, 1213, 1217	unknown	unknown	Close
1218	aeroflight-ads	AeroFlight-ADs	Close
1234	hotline	If these services are not installed beware could be Trojan	Close
1248	hermes	hermes	Close
1259, 1271, 1272, 1287, 1301, 1309	unknown	unknown	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
1311	rxmon	RxMon	Close
1322, 1328, 1334	unknown	unknown	Close
1352	lotusnotes	Lotusnotes	Close
1433	ms-sql-s	MS-SQL-Server	Close if not required
1434	ms-sql-m	MS-SQL-Server	Close if not required
1443	Ies-lm	Integrated engineering software	Close
1455	Ies-lm	Integrated engineering software	Close
1461	Ibm_wrless_lan	IBM Wireless LAN	Close
1503	imtc-mcs	Databeam	Close
1521	oracle	oracle	Close
1556, 1580, 1594, 1641, 1658	unknown	unknown	Close
1666	netview-aix-6	netview-aix-6	Close
1700	mps-raft	mps-raft	Close
1718	h323gatedisc	h323gatedisc	Close
1755	wms	Windows media service	Close
1761	landesk-rc	LANDesk Remote Control	Close
1782	hp-hcip	hp-hcip	Close
1783, 1812, 1840	unknown	unknown	Close
1863	MSNP	MSNP	Close
1864	paradym-31	Paradym 31 Port	Close
1935	RTMP	Adobe Flash media server connection port, Real Time Messaging Protocol (RTMP)	Close
1971, 1972	unknown	unknown	Close
1998	x25-svc-port	cisco X.25 service (XOT)	Close
2000	callbook	"RemoteAnywhere" installs a webserver on this port. NeWS/OpenWin (Sun's older variation of X-Windows) uses this port.	Close
2001	dc	dc or nfr20 web queries; If these services are not installed beware could be Trojan	Close
2003	finger	GNU finger (cfingerd)	Close
2005	deslogin	encrypted symmetric telnet/login	Close
2008	conf	conf	Close
2009	news	news	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
2013	raid-am	raid-am	Close
2020	xinupageserver	Xinupageserver	Close
2021	servexec	Servexec	Close
2040	lam	Lam	Close
2045	cdfunc	Cdfunc	Close
2047	dls	Dls	Close
2048	dls-monitor	Dls-monitor	Close
2103	zephyr-clt	Zephyr serv-hm connection	Close
2105	eklogin	Kerberos (v4) encrypted rlogin	Close
2106	ekshell	Kerberos (v4) encrypted rshell	Close
2111	kx	X over kerberos	Close
2121	ccproxy-ftp	CCProxy FTP Proxy	Close
2160	unknown	unknown	Close
2161	apc-agent	APC 2161	Close
2190, 2191, 2222, 2251, 2260, 2288	unknown	unknown	Close
2301	HTTP	HP Proliant System Management 2.0.1.104 (CompaqHTTPServer 9.9)	Close
2323	unknown	unknown	Close
2381	HTTP	Compaq insight manager HTTP server 5.7	Close
2382	unknown	unknown	Close
2383	ms-olap4	MS OLAP 4	Close
2393, 2394, 2399	unknown	unknown	Close
2601	zebra	zebra vty	Close
2605	bgpod	BGPd vty	Close
2607	unknown	unknown	Close
2701	sms-rcinfo	SMS remote control (control) SMS remote control agent	Close if not required
2702	sms-xfer	SMS XFER	Close if not required
2710, 2717, 2800	unknown	unknown	Close
2809	corbaloc	CORBA LOC	Close
2869	UPnP Framework	Allows a computer to receive UPnP discovery requests from other computers and devices.	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
2909, 2910, 2968	unknown	unknown	Close
2998	iss-release	ISS RealSecure IDS Remote Console Admin port	Close
3001	nessus	Nessus Security Scanner Daemon	Close
3017, 3050, 3071	unknown	unknown	Close
3128	tcpwrapped	Proxy/socks, If these services are not installed beware could be Trojan	Close
3211	unknown	unknown	Close
3260	iscsi	iSCSI port	Close
3261	unknown	unknown	Close
3268	globalcatLDAP	MS global catalogue	Close
3269	globalcatLDAPssl	MS global catalogue with LDAP/SSL	Close
3301, 3323, 3324	unknown	unknown	Close
3333	dec-notes	DEC Notes	Close
3351, 3367, 3371	unknown	unknown	Close
3389	MS-rdp	MS terminal service	Open
3390, 3404, 3476, 3493, 3517, 3527, 3546, 3551, 3659	unknown	unknown	Close
3690	svn	Subversion	Close
3809, 3814, 3851, 3869, 3871, 3889, 3914, 3918	unknown	unknown	Close
3986	mapper-ws-ethd	MAPPER workstation server	Close
3995	unknown	unknown	Close
4000	remoteanything	If these services are not installed beware could be Trojan	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
4001, 4003, 4005, 4011	unknown	unknown	Close
4125	rww	Remote Web Workplace for MS Windows Small Business Server	Close
4126	unknown	unknown	Close
4224	xtell	Xtell messenging server	Close
4343	unicall	UNICALL	Close
4446, 4567	unknown	unknown	Close
4899	radmin	RAdmin Port	Close
4900	unknown	unknown	Close
4998	maybe-veritas	maybe-veritas	Close
5000	upnp	Universal plug and play service, If these services are not installed beware could be Trojan	Close
5001	complex-link	Yahoo messenger chat, If these services are not installed beware could be Trojan	Close
5003	filemaker	FileMaker, Inc. - Proprietary transport	Close
5009	airport-admin	Apple AirPort WAP administration	Close
5050	mmcc	multimedia conference control tool	Close
5051	ida-agent	ITA Agent, Symantec Intruder Alert	Close
5054	unknown	unknown	Close
5060	sip	SIP (Session Initiation Protocol)	Close
5080	unknown	unknown	Close
5101	admdog	chili!soft asp	Close
5200, 5222, 5225, 5226, 5280, 5357	unknown	unknown	Close
5431	park-agent	PARK AGENT	Close
5440	unknown	unknown	Close
5500	hotline	Hotline file sharing client/server	Close
5510	secureidprop	secureidprop-ace/server services	Close
5544	unknown	unknown	Close
5550	sdadmind	ACE Server services	Close
5555	freeciv	Freeciv gameplay	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
5560	isqlplus	Oracle web enabled SQL interface (version 10g+)	Close
5566, 5633, 5730	unknown	unknown	Close
5800	vnc-http	VNC (Virtual Network Computing) HTTP Access	Close
5801	vnc-http-1	VNC (Virtual Network Computing) HTTP Access	Close
5802	vnc-http-2	VNC (Virtual Network Computing) HTTP Access	Close if not required
5811, 5815, 5877	unknown	unknown	Close
5901	vnc-1	VNC display 1	Close
5904, 5907, 5910, 5915, 5922, 5925, 5950, 5962, 5963, 5987, 5988	unknown	unknown	Close
5998	ncd-diag	NCD Diagnostics Telnet	Close
5999	ncd-conf	NCD Configuration Telnet	Close
6000	X11	X Window System	Close
6001	X11:1	X Window Server	Close
6003	X11:3	X Window Server	Close
6004	X11:4	X Window Server	Close
6005	X11:5	X Window Server	Close
6006	X11:6	X Window Server	Close
6059	X11:59	X Window Server	Close
6101	backupexec	Veritas BackupExec	Close
6106	isdninfo	isdninfo	Close
6129	damewaremr	DameWare Mini Remote Control	Open
6156	unknown	unknown	Close
6346	gnutella	gnutella-svc (Gnutella P2P file-sharing system)	Close
6502	netop-rc	NetOp Remote Control (by Danware Data A/S)	Open
6547	powerchuteplus	Powerchuteplus	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
6566, 6567, 6580, 6646	unknown	unknown	Close
6666, 6668, 6669	irc	IRC (Internet Relay Chat), many Trojans/backdoors also use this port	Close
6692	unknown	unknown	Close
6699	napster	Napster File (MP3) sharing software	Close
6788	unknown	unknown	Close
6881	bittorrent-tracker	BitTorrent	Close
6901	unknown	unknown	Close
6969	tcpwrapped	NMAP tcpwrapped	Close
7001	afs3-callback	callbacks to cache managers	Close
7007	afs3-bos	basic overseer process	Close
7025	unknown	unknown	Close
7200	fodms	FODMS FLIP	Close
7443, 7496, 7512, 7676, 7741, 7777, 7778, 7800, 7911, 7921	unknown	unknown	Close
7937	nsrexecd	Legato NetWorker	Close
7999	unknown	unknown	Close
8000	http-alt	HTTP Alternate (official) for Apache	Close if not required
8001	unknown	If these services are not installed beware could be Trojan	Close
8002	teradataordbms	Teradata ORDBMS	Close
8007	ajp12	Apache JServ Protocol 1.x	Close
8008	HTTP	HTTP alternate (official)	Close
8009	ajp13	Default configuration Tomcat	Close
8010	xmpp	Extensible Messaging and Presence Protocol (XMPP) (formerly named Jabber) file transfers	Close
8021	ftp-proxy	Common FTP proxy port	Close
8022, 8031, 8042, 8045	unknown	unknown	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
8082	blackice-alerts	Blackice alerts sent to this port	Close
8085-8090, 8093, 8099, 8181	unknown	unknown	Close
8194	sophos	Sophos Remote Management System	Open
8291, 8292, 8400	unknown	unknown	Close
8443	https-alt	HTTPS alternate (official) for Apache	Close if not required
8600, 8649, 8651, 8654, 8800, 8873, 9003, 9010, 9011	unknown	unknown	Close
9040	tor-tans	Tor TransPort, www.torproject.org	Close
9080, 9081	unknown	unknown	Close
9090	zeus-admin	Zeus admin server	Close
9099	unknown	unknown	Close
9101, 9102	jetdirect	Port numbers 9101 and 9102 are for parallel ports 2 and 3 on the three-port HP Jetdirect external print servers	Close
9111	DragonIDSConsole	Dragon IDS Console	Close
9207, 9415, 9418, 9503	unknown	unknown	Close
9594	msgsys	Message system	Close
9595	pds	Ping Discovery Service	Close
9666	unknown	unknown	Close
9876	sd	Session Director	Close
9877, 9878, 9898	unknown	unknown	Close
9900	iua	IUA	Close
9968	unknown	unknown	Close
9999	abyss	Abyss web server remote web management interface	Close
10000	snet-sensor-mgmt	SecureNet Pro Sensor https management server or apple airport admin	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
10003, 10004, 10009, 10010, 10012, 10024, 10025, 10215, 10617, 10628, 11111, 12174	unknown	unknown	Close
13783	netbackup	VERITAS NetBackup - One-time password user authentication daemon	Close if not required
14000, 14238, 14441, 15660, 16000, 16001, 16012, 16992 16993, 18040, 19350, 19780	unknown	unknown	Close
20005	btx	xcept4 (Interacts with German Telekom's CEPT videotext service)	Close
20031, 20221, 20222, 20828, 25734, 27352	Unknown	unknown	Close
31038, 32768	unknown	unknown	Close
32774	Sometimes-rpc11	Sometimes an RPC port on Solaris box	Close
32775	Sometimes-rpc13	Sometimes an RPC port on Solaris box	Close
32776	Sometimes-rpc15	Sometimes an RPC port on Solaris box	Close
32780	Sometimes-rpc23	Sometimes an RPC port on Solaris box	Close
32781-32783, 34572, 40911, 41511	unknown	unknown	Close
44442, 44443	coldfusion-auth	ColdFusion advanced security/siteminder authentication port	Close
45100, 48080	unknown	unknown	Close

The overall opened TCP service ports (528) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
49153, 49154, 49157, 49158, 49160, 49161, 49163, 4965	unknown	unknown	Close
50000	iiimsf	Internet/Intranet input method server framework	Close
50003, 50006, 50300, 50389, 50800, 51493, 52822, 52848, 54328, 55056, 55555, 55600, 56737, 56738, 57797, 58080, 60020, 60443, 61532	unknown	unknown	Close
62078	iphone-sync	Apparently used by iPhone while synchronising	Close
63331, 64623, 64680, 65129, 65389	unknown	unknown	Close
The overall opened UDP service ports (12) – CoC-DMZ-Web server (A.B.C.181)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
53	Domain	Domain Name Server	Open
123	NTP	Network Time Protocol	Close
137	NetBIOS-ns	NetBIOS Name Service, MS File and printer sharing	Close if not required
138	NetBIOS-dgm	NetBIOS Datagram Service, MS File and printer sharing	Close if not required
161	SNMP	Simple Network Management Protocol	Close
445	ms-ds	MS-DS SMB file sharing, MS Common Internet File System (CIFS) for file sharing	Close if not required
1434	ms-sql-m	MS SQL Server 8.00.194	Close if not required

The overall opened UDP service ports (12) – CoC-DMZ-Web server (A.B.C.181) (continued)			
Port no.	**Services**	**Descriptions, actions and products**	**Recommendations**
1719	H323gatestat	H.323 Gatestat	Close
2427	MGCP	Cisco Media Gateway Control Protocol	Close
3456	IISrpc-or-vat	IIS RPC or VAT default data	Close
5060	SIP	Session Initiation Protocol	Close
34125	unknown	unknown	Close

Appendix C21: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the CoC-DMZ-CMS server

The overall opened TCP service ports (24) – CoC-DMZ-CMS server (A.B.C.186)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
21	FTP	File Transfer Protocol	Close
80	HTTP	Hyper Text Transfer Protocol, MS IIS webserver 6.0	Open
110	POP3	Post Office Protocol 3	Close
135	MSRPC	MS Remote Procedure Call, MS Wins RPC	Close if not required
139	NetBIOS-ssn	NetBIOS Session Service	Close if not required
445	ms-ds	MS-DS Active Directory, Windows shares, MS Windows 2003	Close if not required
1021, 1077, 1093	unknown	unknown	Close if not required
1433	ms-sql-s	Microsoft-SQL-Server	Close
2161	apc-agent	APC 2161	Close if not required
2500	rtsserv	Resource Tracking System Server	Close if not required
2701	sms-rcinfo	SMS Remote Control (control) SMS Remote Control Agent	Close if not required
3128	ndl-aas	Active API Server Port, If these services are not installed beware could be Trojan	Close if not required
3389	microsoft-rdp	MS WBT Server, MS Terminal Service	Open
5550	sdadmind	ACE Server services	Close if not required
6129	damewaremr	DameWare Mini Remote Control	Open
6792, 7911,	unknown	unknown	Close if not required
8080	HTTP alternate	Hyper Text Transfer Protocol (HTTP) - alternative ports used for web traffic.	Open
9943	unknown	unknown	Close if not required
10000	snet-sensor-mgmt	SecureNet Pro Sensor https management server or apple airport admin, If these services are not installed beware could be Trojan, TCP Door, XHX	Close if not required
12000	cce4x	ClearCommerce Engine 4.x	Close
49155	MSRPC	MS Remote Procedure Call, MS Wins RPC	Close if not required
The overall opened UDP service ports (2) – CoC-DMZ-CMS server (A.B.C.186)			
Port no.	**Services**	**Descriptionss, actions and products**	**Recommendations**
53	UDP	domain	Open
137	NetBIOS-ns	NetBIOS Name Service MS Windows NT NetBIOS-ssn (workgroup: CMSWORKGROUP)	Close if not required

Appendix C22: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the CoC-CMS server

The overall opened TCP service ports (13) – CoC-CMS server (10.1.15.184)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
21	FTP	File Transfer Protocol; MS FTP service	Close
80	HTTP	MS HTTPAPI httpd 2.0 (SSDP/UPnP)	Open
110	POP3	Post Office Protocol 3	Close
135	MSRPC	MS Remote Procedure Call; MS Windows RPC	Open
139	NetBIOS-ssn	NetBIOS Session Service for MS File and Printer Sharing	Open
445	microsoft-ds	Microsoft-DS Active Directory, Windows shares	Open
3128	tcpwrapped	Proxy/socks, If these services are not installed beware could be Trojan	Close if not required
3389	microsoft-rdp	MS WBT Server, MS Terminal Service	Open
6129	damewaremr	DameWare Mini Remote Control	Open
6969	acmsoda	"Backdoor.Assasin.D Trojan - opens a backdoor on one of the following ports: 5695,6595,6969,27589. Backdoor.Assasin opens port 27589, Backdoor.Assasin.B opens port 6969, Backdoor.Assasin.C opens port 6595, and Backdoor.Assasin.D opens port 5695 to listen for commands from the attacker. Other Trojans that use this port: GateCrasher, IRC 3/IRC Hack, Net Controller, Priority, Danton, 2000Cracks." (Speed Guide, n.d.-j, p. 1)	Close
8080	http_alt	HTTP alternate	Open
10000	snet-sensor-mgmt	SecureNet Pro Sensor https management server or apple airport admin	Close if not required
49155	MSRPC	MS Remote Procedure Call; MS Windows RPC	Close if not required
The overall opened UDP service port (1) – CoC-CMS server (10.1.15.184)			
Port no.	**Service**	**Description, action or product**	**Recommendation**
137	NetBIOS-ns	NetBIOS Name Service MS Windows NT NetBIOS-ssn (workgroup: COCGROUP)	Open

Appendix C23: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the Epathweb server

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
1	tcpmux	TCP Port Service Multiplexer	Close
3	compressnet	Compression process	Close
9	discard	"Discard server - this protocol is only installed on machines for test purposes. The service listening at this port (both TCP and UDP) simply discards any input." (Speed Guide, n.d.-a, p. 1)	Close
13	daytime	Daytime service [RFC 867] - responds with the current time of day. Different machines respond with slightly different date/time format, so port can be used to fingerprint machines.	Close
17	qotd	Responds with Quote of the Day. See [RFC 865]; Skun Trojan also uses this port.	Close
19	chargen	"Generates and replies with a stream of characters (TCP) or a packet containing characters (UDP). Should be disabled if there is no specific need for it, source for potential attacks. [RFC 864]; Skun Trojan also uses this port." (Speed Guide, n.d.-b, p. 1)	Close
21	FTP	File Transfer Protocol; MS FTP service	Close
24	priv-mail	Any private mail system	Close
30	unknown	unknown	Close
43	whois	WHOIS protocol (official)	Close
79	finger	"Finger protocol (official); Finger Security Concerns: Provides key host info to attacker; Trojans that also use this port: ADM worm, Back Orifice 2000 (BO2K), CDK Trojan (ports 79, 15858), Firehotcker (ports 79, 5321)." (Speed Guide, n.d.-c, p. 1)	Close
80	HTTP	MS HTTP webserver 6.0	Open
81	hosts2-ns	HOSTS2 Name Server	Close
82	xfer	XFER utility	Close
83	mit-ml-dev	MIT ML device	Close
85	mit-ml-dev	MIT ML device	Close
89	su-mit-tg	SU MIT Telnet gateway	Close
90	metagram	Metagram relay	Close
99	metagram	Metagram relay	Close
100	newacct	unauthorised use	Close
106	POP3pw	Eudora compatible PW changer	Close
109	POP2	Post Office Protocol - version 2	Close
110	POP3	Post Office Protocol 3	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
119	NNTP	Network News Transfer Protocol (NNTP) - used for retrieving newsgroup messages (official)	Close
135	MSRPC	MS Remote Procedure Call; MS Windows RPC	Close
139	NetBIOS-ssn	NetBIOS Session Service for MS File and printer sharing	Close
146	iso-tp0	ISO-IP0	Close
161	SNMP	SNMP	Close
179	bgp	Border Gateway Protocol	Close
211	914c/g	Texas instruments 914C/G terminal	Close
212	anet	ATEXSSTR	Close
254, 255	unknown	unknown	Close
259	esro-gen	Efficient short remote operations	Close
280	http-mgmt	http-mgmt	Close
301, 306	unknown	Unassigned	Close
311	asip-webadmin	Mac OS X Server admin (officially AppleShare IP Web administration)	Close
406	imsp	Interactive Mail Support Protocol	Close
416	silverplatter	Silverplatter	Close
417	onmux	Onmux	Close
427	svrloc	Server location	Close
443	HTTPS	Hypertext Transfer Protocol over TLS/SSL; MS IIS webserver 6.0	Open
445	MS-ds	MS-DS Active Directory, Windows shares MS Windows 2003	Close
458	appleqtc	Apple quick time	Close
464	kpasswd	kpasswd	Close
465	SMTPS	SMTP Secure	Close
481	dvs/ph	Dvs or PH service	Close
500	isakmp	Security Association and Key Management Protocol	Close
512	exec	Remote execution-- Allows remote execution of commands without logon.	Close
513	login	Remote login-- Remote term service that operates via telnet process- but with automatic auth performed based on trust. If no trust- will prompt for username/password logon similar to telnet.	Close
514	shell	Used by rsh and (also rcp), interactive shell without any logging; Some vulnerabilities of this port: RPC Backdoor, Whacky, ADM worm	Close
515	printer	Printing services, listening for incoming connections; Trojans using this port: MscanWorm, lpdw0rm, Ramen.	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
543	klogin	Kerberos login	Close
544	kshell	Kerberos remote shell	Close
545	ekshell	Kerberos encrypted remote shell	Close
555	dsf	dsf; Trojans that use this port: 711 Trojan (Seven Eleven), Ini-Killer, Net Administrator (NeTadmin), Phase Zero, Stealth Spy	Close
593	http-rpc-epmap	HTTP RPC Ep Map	Close
616	unknown	unknown	Close
617	sco-dtmgr	SCO Desktop Administration Server or Arkeia (www.akriea.com) backup software	Close
625	apple-xsvr-admin	Apple	Close
631	ipp	Internet Printing Protocol	Close
636	ldapssl	ldap protocol over TLS/SSL (was sldap)	Close
646	ldp	Label Distribution Protocol, a routing protocol used in MPLS networks (official)	Close
648	RRP	Registry Registrar Protocol (RRP)	Close
666	doom	“Used by the game Doom (ID Software), however, because of the cool connotations, this port is also used by numerous Trojan horses/backdoors. Here is a list: Attack FTP, Back Construction, BLA Trojan, Cain & Abel, NokNok, Satans Back Door - SBD, ServU, Shadow Phyre, th3r1pp3rz (the rippers), lpdw0rm, Backdoor.FTP_Ana.C - backdoor Trojan, 03.2003. Affects all current Windows versions.” (Speed Guide, n.d.-d, p. 1)	Close
667	disclose	Campaign contribution disclosures - SDR Technologies	Close
668	mecomm	MeComm	Close
683	corba-iiop	Corba-iiop	Close
687, 705, 711	unknown	unknown	Close
714	iris-xpcs	IRIS over XPCS	Close
720, 722, 726	unknown	unknown	Close
749	kerberos-adm	Kerberos administration	Close
777	multiling-http	Multiling HTTP, Trojans that use this port: AimSpy (AIM trojan), Un-Detected (a.k.a. Backdoor.TDS, 4Fuk, Trojan.Win32.TrojanRunner.Levil, U4).	Close
783	spamassasin	Apache SpamAssassin spamd	Close
800	mdbs_daemon	Mdbs_daemon	Close
801	device	Device	Close
808	ccproxy-http	CCProxy HTTP/Gopher/FTP (over HTTP) proxy	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
873	rsync	rsync	Close
880	unknown	unknown	Close
898	sun-manageconsole	Solaris Management Console Java listener (Solaris 8 & 9)	Close
911, 987	unknown	unknown	Close
990	FTPs	FTP protocol, control, over TLS/SSL	Close
992	Telnets	telnet protocol over TLS/SSL	Close
999	garcon	"Port used by ScimoreDB database system; Trojans that run on this port: DeepThroat (a.k.a. DTV2, DTV3, BackDoor-J), F0replay (a.k.a. WiNNUke eXtreame), WinSatan." (Speed Guide, n.d.-e, p. 1)	Close
1000	cadlock	cadlock	Close
1001	unknown	unknown	Close
1002	window-icfw	Windows Internet connection firewall or Internet locator server for NetMeeting.	Close
1009, 1011, 1022	unknown	unknown	Close
1023	netvenuechat	Nortel NetVenue Notification, Chat, Intercom	Close
1026	LSA-or-nterm	Nterm remote_login network_terminal	Close
1027	IIS	IIS	Close
1029	ms-lsa	Ms-lsa	Close
1030	iad1	BBN IAD	Close
1031	iad2	BBN IAD	Close
1032	Iad3	BBN IAD	Close
1035	multidropper	A Multidropper Adware, or PhoneFree	Close
1036, 1037	unknown	unknown	Close
1038	mtqp	Message Tracking Query Protocol	Close
1039	msrpc	MS Windows RPC	Close
1041	danf-ak2, Trojan	AK2 Product , Dosh, RemoteNC; , If these services are not installed beware could be Trojan	Close
1042	unknown, bla Trojan	BLA Trojan; If these services are not installed beware could be Trojan	Close
1043	boinc	BOINC Client Control	Close
1044-1047, 1049	unknown	unknown	Close
1051	optima-vnet	Optima VNET	Close
1053	unknown	unknown	Close
1055	ansyslmd	ANSYS - license manager	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
1056, 1057	unknown	unknown	Close
1058	nim	nimreg, IBM AIX Network installation manager (NIM) (official)	Close
1059	nimreg		Close
1060	polestar	POLESTAR	Close
1062	veracity	Veracity	Close
1064	unknown	unknown	Close
1069	cognex-insight		Close
1070, 1072, 1074, 1075	unknown	unknown	Close
1077	unknown	unknown	Close
1080	socks	"Socks Proxy is an Internet proxy service, potential spam relay point. Common programs using this port: Wingate Trojans/worms that use this port as well: Bugbear.xx - wide-spread mass-mailing worm, many variants. SubSeven - remote access Trojan, 03.2001. Afects all current Windows versions. WinHole - remote access Trojan, 01.2000 (a.k.a. WinGate, Backdoor.WLF, BackGate). Affects Windows 9x. Trojan.Webus.C - remote access Trojan, 10.12.2004. Affects all current Windows versions. Connects to an IRC server (on port 8080) and opens a backdoor on TCP port 10888 or 1080." (Speed Guide, n.d.-f, p. 1)	Close
1082	unknown	unknown	Close
1083	ansoft-lm-1	Anasoft License Manager	Close
1084	ansoft-lm-2	Anasoft License Manager	Close
1085-1092, 1095	unknown	unknown	Close
1096, 1099, 1100, 1105, 1108, 1111	unknown	unknown	Close
1112	msql	mini-sql server	Close
1113, 1117, 1119, 1121	Unknown	unknown	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
1123, 1131, 1132, 1141, 1145, 1147, 1148, 1152, 1154, 1165, 1166, 1169, 1174, 1183, 1185, 1187, 1192	unknown	unknown	Close
1199, 1201, 1216	unknown	unknown	Close
1234	hotline	If these services are not installed beware could be Trojan	Close
1236, 1244	unknown	unknown	Close
1248	hermes	hermes	Close
1271, 1277, 1287, 1296, 1300, 1309, 1310	unknown	unknown	Close
1311	rxmon	RxMon	Close
1417	timbuktu-srv1	Timbuktu Service 1 Port	Close
1433	ms-sql-s	MS-SQL-Server 2005 9.00.4035; SP3	Close if not required
1434	ms-sql-m	MS-SQL-Server	Close if not required
1443	Ies-lm	Integrated engineering software	Close
1455	Ies-lm	Integrated engineering software	Close
1461	Ibm_wrless_lan	IBM Wireless LAN	Close
1494	citrix-ica	Citrix XenApp Independent Computing Architecture (ICA) thin client protocol	Close
1500	vlsi-lm	VLSI License Manager	Close
1501	sas-3	Satellite-data Acquisition System 3	Close
1503	imtc-mcs	Databeam	Close
1524	ingreslock	Ingres; If these services are not installed beware could be Trojan	Close
1533	virtual-places	Virtual Places software	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
1580, 1583, 1594	unknown	unknown	Close
1600	issd	Issd	Close
1641	unknown	unknown	Close
1658	unknown	unknown	Close
1666	netview-aix-6	netview-aix-6	Close
1717	fj-hdnet	fj-hdnet	Close
1718	h323gatedisc	h323gatedisc	Close
1755	wms	Windows media service	Close
1782	hp-hcip	hp-hcip	Close
1783, 1801, 1839, 1840	unknown	unknown	Close
1864	paradym-31	Paradym 31 Port	Close
1875	unknown	unknown	Close
1900	upnp	“UPnP discovery/SSDP is a service that runs by default on WinXP, and creates immediately exploitable security vulnerability for any network-connected system. Filtering this port proactively prevents XP systems from being remotely compromised by malicious worms or intruders.” (Speed Guide, n.d.-g, p. 1)	Close
1914	unknown	unknown	Close
1935	RTMP	Adobe Flash Media Server connection port, Real Time Messaging Protocol (RTMP)	Close
1947, 1971, 1972, 1974	unknown	unknown	Close
1998	x25-svc-port	Cisco X.25 over TCP (XOT) service	Close
1999	tcp-id-port	“Cisco identification port. Some Trojans also use this port: Back Door, SubSeven, TransScout Backdoor.Bifrose.C (05.19.2005) - Trojan that opens a backdoor on port 1999/tcp, and sends information to a remote server.” (Speed Guide, n.d.-h, p. 1)	Close
2000	callbook	Callbook; If these services are not installed beware could be Trojan	Close
2001	dc	dc or nfr20 web queries; If these services are not installed beware could be Trojan	Close
2002	globe	Globe; If these services are not installed beware could be Trojan	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
2003	finger	GNU finger (cfingerd)	Close
2005	deslogin	encrypted symmetric telnet/login	Close
2006	invokator	invokator	Close
2007	dectalk	dectalk	Close
2008	conf	conf	Close
2013	raid-am	raid-am	Close
2021	servexec	servexec	Close
2022	down	down	Close
2033	glogger	glogger	Close
2038	objectmanager	objectmanager	Close
2040	lam	lam	Close
2042	isis	isis	Close
2045	cdfunc	Cdfunc	Close
2049	NFS	“Network File System (NFS) - remote filesystem access. (RFC 1813). A commonly scanned and exploited attack vector. Normally, access to portmapper is needed to find which port this service runs on, but since most installations run NFS on this port, hackers/crackers can bypass portmapper and try this port directly.” (Speed Guide, n.d.-i, p. 1)	Close
2065	dlsrpn	Data Link Switch Read Port Number	Close
2068	advocentkvm	Advocent KVM Server	Close
2100	unknown	unknown	Close
2105	eklogin	Kerberos (v4) encrypted rlogin	Close
2107, 2119	unknown	unknown	Close
2121	ccproxy-ftp	CCProxy FTP Proxy	Close
2144	unknown	unknown	Close
2161	apc-agent	APC 2161	Close
2170, 2190, 2196, 2200, 2222, 2260	unknown	unknown	Close
2301	HTTP	HP Proliant System Management 2.0.1.104 (CompaqHTTPServer 9.9)	Close
2323	unknown	unknown	Close
2381	HTTP	Compaq Insight Manager HTTP server 5.7	Close
2382	unknown	unknown	Close
2383	ms-olap4	MS OLAP 4	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
2399	unknown	unknown	Close
2401	cvspserver	CVS network server	Close
2492	unknown	unknown	Close
2500	rtsserv	Resource Tracking system server	Close
2522, 2525	unknown	unknown	Close
2601	zebra	zebra vty	Close
2602	ripd	RIPd vty	Close
2605	bgpod	BGPd vty	Close
2607, 2608	unknown	unknown	Close
2638	sybase	Sybase database	Close
2701	sms-rcinfo	SMS Remote Control (control) SMS Remote Control Agent	Close
2710, 2717, 2725, 2811, 2875, 2910, 2920	unknown	unknown	Close
2967	symantec-av	Symantec AntiVirus (rtvscan.exe)	Close
2968	unknown	unknown	Close
2998	iss-release	ISS RealSecure IDS Remote Console Admin port	Close
3000	ppp	User-level ppp daemon, or chili!soft asp	Close
3001	nessus	Nessus Security Scanner Daemon	Close
3005	deslogin	encrypted symmetric telnet/login	Close
3006	deslogind	deslogind	Close
3013, 3017, 3030, 3031, 3050, 3071	unknown	unknown	Close
3128	tcpwrapped	Proxy/socks, If these services are not installed beware could be Trojan	Close
3168, 3211, 3221	unknown	unknown	Close
3260	iscsi	iSCSI port	Close
3261	unknown	unknown	Close
3268	globalcatLDAP	MS Global Catalog	Close
3283	netassistant	Apple Remote Desktop Net Assistant reporting feature	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
3323-3325	unknown	unknown	Close
3333	dec-notes	DEC Notes	Close
3367, 3369-3371, 3476, 3493, 3517, 3527, 3546, 3551, 3659	unknown	unknown	Close
3689	rendezvous	Rendezvous Zeroconf (used by Apple/iTunes)	Close
3690	svn	Subversion	Close
3703, 3737, 3766, 3784, 3827, 3828, 3851, 3878, 3880	unknown	unknown	Close
3905	mupdate	Mailbox Update (MUPDATE) protocol	Close
3914, 3918, 3920, 3945, 3971	unknown	unknown	Close
3986	mapper-ws-ethd	MAPPER workstation server	Close
3995	unknown	unknown	Close
4002	mlchat-proxy	mlnet - MLChat P2P chat proxy	Close
4003, 4005, 4006	unknown	unknown	Close
4545	lockd	NFS lock daemon/manager	Close
4125	rww	Remote Web Workplace for MS Windows Small Business Server	Close
4129	unknown	unknown	Close
4224	xtell	Xtell messenging server	Close
4343	unicall	UNICALL	Close
4443	pharos	Pharos	Close
4445, 4446, 4449	unknown	unknown	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
4662	edonkey	eDonkey file sharing (Donkey)	Close
4848	unknown	unknown	Close
4998	maybe-veritas	maybe-veritas	Close
5003	filemaker	FileMaker, Inc. - Proprietary transport	Close
5009	airport-admin	Apple AirPort WAP Administration	Close
5030	unknown	unknown	Close
5051	ida-agent	ITA agent, Symantec intruder alert	Close
5054	unknown	unknown	Close
5060	SIP	SIP (Session Initiation Protocol)	Close
5061	sip-tls	SIP-TLS	Close
5080	unknown	unknown	Close
5100	admd	(ChiliSoft ASP manager for Cobalt RaQ) or Yahoo pager	Close
5120, 5200, 5221, 5222, 5225, 5269	unknown	unknown	Close
5280, 5298, 5357	unknown	unknown	Close
5405	pcduo	RemCon PC-Duo - new port	Close
5414	unknown	unknown	Close
5432	postgresql	PostgreSQL database server	Close
5440	unknown	unknown	Close
5500	hotline	Hotline file sharing client/server	Close
5550	sdadmind	ACE server services	Close
5555	freeciv	Freeciv gameplay	Close
5631	pcanywheredata	pcANYWHEREdata, Symantec pcAnywhere (version 7.52 and later)	Close if not required
5633, 5718	unknown	unknown	Close
5800	vnc-http	VNC (Virtual Network Computing) HTTP access	Close
5810	unknown	unknown	Close
5811, 5815, 5825, 5850, 5859, 5862	unknown	unknown	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
5901	vnc-1	VNC display 1	Close
5902	vnc-2	VNC display 2	Close
5903	vnc-3	VNC display 3	Close
5904, 5907, 5910, 5915, 5950, 5952, 5960, 5962, 5963, 5987, 5988, 5989	unknown	unknown	Close
5999	ncd-conf	NCD Configuration Telnet	Close
6003	X11:3	X Window Server	Close
6005	X11:5	X Window Server	Close
6007	X11:7	X Window Server	Close
6025	unknown	unknown	Close
6059	X11:59	X Window Server	Close
6100	unknown	unknown	Close
6112	dtspc	CDE subprocess control	Close
6129	damewaremr	DameWare mini remote control	Open
6156	unknown	unknown	Close
6346	gnutella	gnutella-svc (Gnutella P2P file-sharing system)	Close
6502	netop-rc	NetOp remote control (by Danware Data A/S)	Open
6510	unknown	unknown	Close
6543	mythtv	Mythtv; If these services are not installed beware could be Trojan	Close
6547	powerchuteplus	Powerchuteplus	Close
6565-6567, 6646	unknown	unknown	Close
6666, 6668, 6669	irc	IRC (Internet Relay Chat), many Trojans/backdoors also use this port	Close
6689, 6692	unknown	unknown	Close
6699	napster	Napster File (MP3) sharing software	Close
6779	unknown	unknown	Close
6789	ibm-db2-admin	IBM DB2	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
6792, 6839, 6901	unknown	unknown	Close
6969	tcpwrapped	NMAP tcpwrapped	Close
7000	afs3-fileserver	file server itself, msdos; ; If these services are not installed beware could be Trojan	Close
7001	afs3-callback	callbacks to cache managers	Close
7002	afs3-prserver	users & groups database	Close
7007	afs3-bos	basic overseer process	Close
7100	font-service	X Font Service	Close
7103, 7106	unknown	unknown	Close
7200	fodms	FODMS FLIP	Close
7201	dlip	DLIP	Close
7443, 7625, 7676, 7741, 7777	unknown	unknown	Close
7800, 7911, 7920, 7921	unknown	unknown	Close
7937	nsrexecd	Legato NetWorker	Close
7938	lgtomapper	Legato portmapper	Close
7999	unknown	unknown	Close
8000	http-alt	HTTP Alternate (official) for Apache	Close if not required
8001	unknown	If these services are not installed beware could be Trojan	Close
8002	teradataordbms	Teradata ORDBMS	Close
8007	ajp12	Apache JServ Protocol 1.x	Close
8008	HTTP	HTTP Alternate (official)	Close if not required
8009	ajp13	Default configuration Tomcat	Close
8011, 8022, 8031, 8042, 8045	unknown	unknown	Close
8081	blackice-icecap	ICECap user console	Close
8082	blackice-alerts	Blackice Alerts sent to this port	Close
8087-8090, 8093,	unknown	unknown	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
8100, 8180, 8181	unknown	unknown	Close
8193-8194	sophos	Sophos Remote Management System	Close
8200, 8222, 8290, 8291, 8500, 8600, 8649, 8654, 8800, 8873, 8994	unknown	unknown	Close
9000	cslistener	CSlistener; If these services are not installed beware could be Trojan	Close
9009, 9011	unknown	unknown	Close
9050	tor-socks	Tor SocksPort	Close
9071, 9080, 9081, 9091	unknown	unknown	Close
9101-9102	jetdirect	HP JetDirect card	Close
9110	unknown	unknown	Close
9111	DragonIDSConsole	Dragon IDS Console	Close
9207, 9290, 9418, 9485, 9500, 9575, 9593	unknown	unknown	Close
9594	msgsys	Message System	Close
9595	pds	Ping Discovery System	Close
9666	unknown	unknown	Close
9876	sd	Session Director, True Image Remote Agent, Wireshark, NMAP use this port. Trojans that also use this port: Cyber Attacker, Rux, Backdoor.Lolok	Close
9898, 9943, 9968	unknown	unknown	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
9900	iua	IUA	Close
9999	abyss	Abyss web server remote web management interface; ; If these services are not installed beware could be Trojan	Close
10000	snet-sensor-mgmt	SecureNet Pro Sensor https management server or apple airport admin	Close
10002-10004, 10010, 10012, 10025, 10215, 10243, 10617, 10621, 10628, 10778, 11110, 11111, 11967, 12265, 13456	unknown	unknown	Close
13782-13783	netbackup	VERITAS NetBackup, bpcd client	Close
14442	unknown	unknown	Close
15000	hydap	Hypack Data Aquisition	Close
15003, 15004, 15660, 16001, 16012, 16016, 16018, 16992, 16993, 17877, 17988, 18040, 18988, 19101, 19283, 19315, 19842, 20000	unknown	unknown	Close
20005	btx	xcept4 (Interacts with German Telekom's CEPT videotext service)	Close
20828, 21571, 22939, 23502, 24800, 25734	unknown	unknown	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
26214, 27352, 27353, 27355, 27356, 27551, 28201, 30000, 30718, 30951	unknown	unknown	Close
31337	Elite	inetd.conf; If these services are not installed beware could be Trojan	Close
32768, 32769	unknown	unknown	Close
32770	sometimes-rpc3	Sometimes an RPC port on Solaris box	Close
32772	sometimes-rpc7	Sometimes an RPC port on Solaris box (status)	Close
32773	sometimes-rpc9	Sometimes an RPC port on Solaris box (rquotad)	Close
32774	sometimes-rpc11	Sometimes an RPC port on Solaris box (rusersd)	Close
32775	sometimes-rpc13	Sometimes an RPC port on Solaris box (status)	Close
32777	sometimes-rpc17	Sometimes an RPC port on Solaris box (walld)	Close
32778	sometimes-rpc19	Sometimes an RPC port on Solaris box (rstatd)	Close
32779	sometimes-rpc21	Sometimes an RPC port on Solaris box	Close
32780	sometimes-rpc23	Sometimes an RPC port on Solaris box	Close
32781-32785, 33899, 35500	unknown	unknown	Close
38292	landesk-cba	landesk-cba	Close
40193, 41511, 44176	unknown	unknown	Close
44443	coldfusion-auth	ColdFusion Advanced Security/Siteminder Authentication Port	Close
45100, 48080, 49152-49156, 49159, 49160, 49163, 49165, 49175, 49176	unknown	unknown	Close

The overall opened TCP service ports (653) – Epathweb server (A.B.C.179) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
49400	HTTP	Compaq Diagnostics httpd (CompaqHTTPServer 5.7)	Close
49999	unknown	unknown	Close
50002	iiimsf	Internet/Intranet Input Method Server Framework	Close
50006, 50500, 50636, 51493, 52673, 52848, 52869, 54045, 55056, 55555, 56737, 56738, 57294, 60020, 60443, 61532, 61900	unknown	unknown	Close
62078	iphone-sync	Apparently used by iPhone while syncing	Close
63331, 64680, 65129, 65389	unknown	unknown	Close

The overall opened UDP service ports (10) – Epathweb server (A.B.C.179)			
Port no.	**Service**s	**Descriptions, actions or product**s	**Recommendations**
53	UDP	domain	Open
123	NTP	Network Time Protocol	Close
137	NetBIOS-ns	NetBIOS Name Service MS Windows NT NetBIOS-ssn	Close if not required
138	NetBIOS-dgm	NetBIOS Datagram Service	Close if not required
161	SNMP	SNMP	Close
445	ms-ds	MS-DS SMB file sharing	Close if not required
500	isakmp	Internet Security Association and Key Management Protocol	Close if not required
1719	h323gatestat	h323gatestat	Close
4500	nat-t-ike	IPsec NAT-Traversal (RFC 3947)	Close if not required
5060	SIP	Session Initiation Protocol	Close

Appendix C24: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the Epathway server

The overall opened TCP service ports (22) – Epathway server (10.1.15.166)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
21	FTP	File Transfer Protocol; MS FTP service	Close
80	HTTP	MS HTTPAPI httpd 2.0 (SSDP/UPnP)	Open
110	POP3	Post Office Protocol 3	Close
135	MSRPC	MS Remote Procedure Call; MS Windows RPC	Open
139	NetBIOS-ssn	NetBIOS Session Service for MS file and printer sharing	Open
445	ms-ds	MS-DS Active Directory, Windows shares	Open
1025	MSRPC	MS Windows RPC	Open/Close if not required
1079	tcpwrapped	Proxy/socks, If these services are not installed beware could be Trojan	Close if not required
1080	sophos	Sophos message router	Open
1658	MSRPC	MS Windows RPC	Close if not required
3128	tcpwrapped	Proxy/socks, If these services are not installed beware could be Trojan	Close if not required
5800	vnc-http	VNC (Virtual Network Computing) HTTP Access	Close if not required
5900	vnc	Virtual Network Computer display 0	Close if not required
6129	damewaremr	DameWare Mini Remote Control	Open
6502	netop-rc	NetOp Remote Control (by Danware Data A/S)	Open
6969	acmsoda	"Backdoor.Assasin.D Trojan - opens a backdoor on one of the following ports: 5695,6595,6969,27589. Backdoor.Assasin opens port 27589, Backdoor.Assasin.B opens port 6969, Backdoor.Assasin.C opens port 6595, and Backdoor.Assasin.D opens port 5695 to listen for commands from the attacker. Other Trojans that use this port: GateCrasher, IRC 3/IRC Hack, Net Controller, Priority, Danton, 2000Cracks" (Speed Guide, n.d.-j, p. 1)	Close
8080	http_alt	HTTP alternate	Open
8192	sophos	Sophos message router (Interoperable Object Reference Service)	Open
8193	tcpwrapped	Proxy/socks, If these services are not installed beware could be Trojan	Close if not required
8194	sophos	Sophos message router	Open
10000	snet-sensor-mgmt	SecureNet Pro Sensor https management server or apple airport admin	Close if not required
49155	MSRPC	MS Remote Procedure Call; MS Windows RPC	Close if not required

The overall opened UDP service ports (10) – Epathway server (10.1.15.166) (continued)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
123	NTP	Network Time Protocol	Close
137	NetBIOS-ns	NetBIOS Name Service Microsoft Windows NT NetBIOS-ssn (workgroup: COCWORKGROUP)	Open
138	NetBIOS-dgm	NetBIOS Datagram Service	Close if not required
445	ms-ds	MS-DS SMB file sharing	Open/ Close if not required
500	isakmp	Internet Security Association and Key Management Protocol	Close if not required
4500	nat-t-ike	IPsec NAT-Traversal (RFC 3947)	Close if not required

Appendix C25: The overall opened TCP and UDP service ports, and the possible mitigation recommendations of the Pathway server

The overall opened TCP service ports (21) – Pathway server (10.1.15.162)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
21	FTP	File Transfer Protocol; MS FTP service	Close
80	HTTP	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	Open
110	POP3	Post Office Protocol 3	Close
135	MSRPC	Microsoft Remote Procedure Call; MS Windows RPC	Open
139	NetBIOS-ssn	NetBIOS Session Service for MS File and Printer Sharing	Open
445	ms-ds	MS-DS Active Directory, Windows shares	Open
1025	MSRPC	Microsoft Windows RPC	Open/Close if not required
1062	tcpwrapped	Proxy/socks, If these services are not installed beware could be Trojan	Close if not required
1063	sophos	Sophos message router	Open
1433	ms-sql-s	Microsoft SQL Server 2005 9.00. 4035; SP3	Open
3128	tcpwrapped	Proxy/socks, If these services are not installed beware could be Trojan	Close if not required
5800	vnc-http	VNC (Virtual Network Computing) HTTP access	Close if not required
5900	vnc	Virtual Network Computer display 0	Close if not required
6129	damewaremr	DameWare Mini Remote Control	Open
6502	netop-rc	NetOp Remote Control (by Danware Data A/S)	Open
6969	acmsoda	"Backdoor.Assasin.D Trojan - opens a backdoor on one of the following ports: 5695,6595,6969,27589. Backdoor.Assasin opens port 27589, Backdoor.Assasin.B opens port 6969, Backdoor.Assasin.C opens port 6595, and Backdoor.Assasin.D opens port 5695 to listen for commands from the attacker. Other Trojans that use this port: GateCrasher, IRC 3/IRC Hack, Net Controller, Priority, Danton, 2000Cracks." (Speed Guide, n.d.-j, p. 1)	Close
8080	http_alt	HTTP alternate	Open
8192	sophos	Sophos message router (Interoperable Object Reference Service)	Open
8193	tcpwrapped	Proxy/socks, If these services are not installed beware could be Trojan	Close if not required
8194	sophos	Sophos message router	Open
10000	snet-sensor-mgmt	SecureNet Pro Sensor https management server or apple airport admin	Close if not required

The overall opened UDP service ports (7) – Pathway server (10.1.15.162)			
Port no.	**Services**	**Descriptions, actions or products**	**Recommendations**
123	NTP	Network Time Protocol	Close
137	NetBIOS-ns	NetBIOS Name Service Microsoft Windows NT NetBIOS-ssn (workgroup: COCWORKGROUP)	Open
138	NetBIOS-dgm	NetBIOS Datagram Service	Close if not required
445	ms-ds	Microsoft-DS SMB file sharing	Open/close if not required
500	IPSec isakmp	Internet Security Association and Key Management Protocol	Close if not required
1434	ms-sql-m	Microsoft SQL Server 2005 9.00. 4035.00; SP3	Open
4500	nat-t-ike	IPsec NAT-Traversal (RFC 3947)	Close if not required

Appendix C26: A summary of Council C's CoC-DMZ-Web server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of Council C's CoC-DMZ-Web server	
High security vulnerabilities (7)	
Section: Types	**Recommendations**
Backdoors: Open ports commonly used by Trojans (3): Duddie (2002), Duddie (2004) and Duddie (2005)	Disable TCP ports 2002, 2004 and 2005
Miscellaneous: AutoRun is enabled	Disable AutoRun both for CD/DVD drives and also other removable drives.
Services: POP3 server might be vulnerable to a remote buffer overflow exploit	Disable POP3 service port
Software: APSB07-18: Adobe Acrobat mailto: vulnerability	It is recommended that affected users update to Adobe Reader 8.1.1 or Acrobat 8.1.1.
Software: SANS07C1: Multiple vulnerabilities in Adobe Reader earlier than 8.0.0	It is recommended that affected users update to Adobe Reader 8.1.1 or Acrobat 8.1.1 or newer.
Medium security vulnerability (0)	
Section: Type	**Recommendation**
None	None
Low security vulnerabilities (10)	
Section: Types	**Recommendations**
Mail: SMTP server allows relaying	Should be disabled if not required
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Registry: Last logged-on username visible	Should be disabled
Registry: Windows AutoUpdate is enabled but require user intervention for both patch download and installation	No further action is required
Services: HTTP	No further action is required
Services: SSH	If this computer is not administered via secure shell, the SSH service is most likely unnecessary
Services: SMTP	Disable SMTP service port
Services: FTP	Disable FTP service port
Services: HTTPS	No further action is required
Services: POP3	Disable POP3 service port

The vulnerabilities and the possible mitigation recommendations of Council C's CoC-DMZ-Web server (continued)	
Potential vulnerabilities (5)	
Section: Types	**Recommendations**
Information: Administrator account exists	It is recommended to rename this account
Information: User kris-h never logged on	It is recommended to remove this account if not used
Information: MS SQL server	Uninstall MS SQL server if not used
Information: Some POP3 server banners providing information to attacker	The service: POP3 service should be turned off
Information: USB devices installed over time	This check generates a list of all USB devices that have been connected to the scanned computer

Appendix C27: A summary of Council C's CoC-DMZ-CMS server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of Council C's CoC-DMZ-CMS server	
High security vulnerability (0)	
Section: Type	**Recommendation**
None	None
Medium security vulnerability (0)	
Section: Type	**Recommendation**
None	None
Low security vulnerabilities (3)	
Section: Types	**Recommendations**
Services: HTTP	No further action is required
Services: FTP	Disable FTP service port
Services: POP3	Disable POP3 service port
Potential vulnerabilities (3)	
Section: Types	**Recommendations**
Information: Administrator account exists	It is recommended to rename this account
Information: User serveradministrator never logged on	It is recommended to remove this account if not used
Information: User SophosSAUCMSWEB0 never logged	It is recommended to remove this account if not used

Appendix C28: A summary of Council C's CoC-CMS server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of Council C's CoC-CMS server	
High security vulnerability (0)	
Section: Type	**Recommendation**
None	None
Medium security vulnerability (0)	
Section: Type	**Recommendation**
None	None
Low security vulnerabilities (5)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Services: HTTP	No further action is required
Services: FTP	Disable FTP service port
Services: POP3	Disable POP3 service port
Potential vulnerability (1)	
Section: Type	**Recommendation**
Information: Administrator account exists	It is recommended that the account be renamed

Appendix C29: A summary of Council C's Epathweb server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of Council's Epathweb server	
High security vulnerabilities (8)	
Section: Types	**Recommendations**
Miscellaneous: AutoRun is enabled	Disable AutoRun both for CD/DVD drives and also other removable drives.
Miscellaneous: OVAL:5793: MSXML Memory Corruption Vulnerability	Patch Security Update for Windows Server 2003 (KB955069)
Services: POP3 server might be vulnerable to a remote buffer overflow exploit	Disable POP3 service port
Software: OVAL:6237: Remote Code Execution Vulnerability in Microsoft DirectShow (CVE-2009-1537)	Patch Security Update for Windows Server 2003 x64 Edition (KB951698)
Software: OVAL:5897: Word Record Parsing Vulnerability	Check and Patch Microsoft Security Bulletin MS08-042, Vulnerability in Microsoft Word Could Allow Remote Code Execution (955048)
Software: OVAL:332: Word Count Vulnerability	Patch Security Update for Word 2003 (KB929057)
Web: OVAL:4582: Uninitialized Memory Corruption Vulnerability	Check and Patch from Microsoft Security Bulletin MS07-057, Cumulative Security Update for Internet Explorer
Web: OVAL:2109: ActiveX Object Vulnerability	Check and Patch from Microsoft Security Bulletin MS07-045
Medium security vulnerability (1)	
Section: Type	**Recommendation**
WEB: OVAL:4480: Uninitialized Memory Corruption Vulnerability	Check And Patch from Microsoft Security Bulletin MS07-069, Cumulative Security Update for IE
Low security vulnerabilities (8)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Registry: Last logged-on username visible	Should be disabled
Registry: Windows AutoUpdate is enabled but require user intervention for both patch download and installation	No further action is required
Services: HTTP	No further action is required
Services: FTP	Disable FTP service port
Services: HTTPS	No further action is required
Services: POP3	Disable POP3 service port

The vulnerabilities and the possible mitigation recommendations of Council C's Epathweb server (continued)	
Potential vulnerabilities (4)	
Section: Types	**Recommendations**
Information: User opsuser never logged on	It is recommended to remove this account if not used
Information: User SophosSAUEPATHWEB0 never logged on	It is recommended to remove this account if not used
Information: User ckbuser never logged on	It is recommended to remove this account if not used
Information: Some POP3 server banners providing information to attacker	The service: POP3 service should be turned off

Appendix C30: A summary of Council C's Epathway server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of Council C's Epathway server	
High security vulnerabilities (3)	
Section: Types	**Recommendations**
Miscellaneous: AutoRun is enabled	Disable AutoRun both for CD/DVD drives and also other removable drives.
Services: POP3 server might be vulnerable to a remote buffer overflow exploit	Disable POP3 service port
Software: OVAL:6237: Remote Code Execution Vulnerability in MS DirectShow (CVE-2009-1537)	Patch security update for Windows Server 2003 x64 Edition (KB951698)
Medium security vulnerability (0)	
Section: Type	**Recommendation**
None	None
Low security vulnerabilities (7)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Registry: Last logged-on username visible	Should be disabled
Services: HTTP	No further action is required
Services: FTP	Disable FTP service port
Services: POP3	Disable POP3 service port
Web: IIS: Frontpage check	Should be uninstalled if not required
Potential vulnerabilities (2)	
Section: Types	**Recommendations**
Information: Administrator account exists	It is recommended to rename this account
Information: Some POP3 server banners providing information to attacker	The service: POP3 service should be turned off

Appendix C31: A summary of Council C's Pathway server – the vulnerabilities and the possible mitigation recommendations

The vulnerabilities and the possible mitigation recommendations of Council C's Pathway server	
High security vulnerabilities (3)	
Section: Types	**Recommendations**
Miscellaneous: AutoRun is enabled	Disable AutoRun both for CD/DVD drives and also other removable drives.
Services: POP3 server might be vulnerable to a remote buffer overflow exploit	Disable POP3 service port
Software: OVAL:6237: Remote Code Execution Vulnerability in Microsoft DirectShow (CVE-2009-1537)	Patch Security Update for Windows Server 2003 x64 Edition (KB951698)
Medium security vulnerability (0)	
Section: Type	**Recommendation**
None	None
Low security vulnerabilities (6)	
Section: Types	**Recommendations**
Registry: AutoShareServer	Should be turned off
Registry: AutoShareWKS	Should be turned off
Registry: Last logged-on username visible	Should be disabled
Services: HTTP	No further action is required
Services: FTP	Disable FTP service port
Services: POP3	Disable POP3 service port
Potential vulnerabilities (3)	
Section: Types	**Recommendations**
Information: Administrator account exists	It is recommended to rename this account
Information: MS SQL server	No further action is required
Information: Some POP3 server banners providing information to attacker	The service: POP3 service should be turned off

Appendix C32: OS and network specification configuration

OS and network specification configuration				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
1.1	Physical security	Place the MS SQL server in an area where it will be physically secure.	Satisfactory	H
1.2	Domain environment	If the MS SQL Server is in a domain that is trusted by other domains, document the access granted by the trust.	Satisfactory; only IT administrator groups are allowed to access the server.	H
1.3	MS SQL servers accessed via Internet	If the MS SQL server is being accessed via the Internet, place the MS SQL Server inside a DMZ with the Web Server.	Satisfactory; there is a frontend web (Epathway) server located in the DMZ.	H
1.4	MS SQL servers accessed via Internet	Put a firewall between your server and the Internet. Block TCP port 1433 and UDP port 1434 on your perimeter firewall. If named instances are listening on additional ports, block those too. In a multi-tier environment, use multiple firewalls to create more secure screened subnets	Satisfactory; the MS SQL server is located be hide the Internet firewall, and both TCP port 1433 and 1434 are blocked from external access.	H
1.5	Encryption	Implement SSL. Use the fully-qualified DNS name of the server in the certificate to help prevent masquerading.	Satisfactory; the Epathway frontend server uses SSL and fully qualified DNS name.	H
1.6	Test and development servers	Maintain test and development servers on a separate network segment from the production servers.	**Not satisfactory;** the test and development servers are on the same class A network.	H
1.7	Dedicated server	Install the MS SQL server on a computer that does not provide additional services, e.g., web or mail services.	Satisfactory; the MS SQL server is only for MS SQL database operation.	M
1.8	OS benchmark configuration	Configure Windows Server 2003 level I benchmark settings with the following modifications:		
1.8.1	Windows accounts	Make sure the Windows guest account is disabled.	Satisfactory	M
1.8.2	Disk subsystem	Use RAID for critical data files.	Satisfactory; raid level 10: database and temp drives RAID level 5: backup drive.	M

OS and network specification configuration (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
1.8.3	Separate partitions	Create separate partitions for OS/SQL program files, SQL data files, and SQL transaction logs.	Satisfactory	M
1.8.4	Volume / partition type	Format all volumes with NTFS	Satisfactory	H
1.9	Services	Disable the following services on a SQL server machine		
1.9.1		Alerter	Satisfactory	P
1.9.2		Clipbook server	Satisfactory	P
1.9.3		Computer browser	**Not satisfactory;** currently set to Started Automatic.	L
1.9.4		DHCP client	**Not satisfactory;** currently set to Started Automatic.	L
1.9.5		Distributed file system	**Not satisfactory;** currently set to Started Manual.	L
1.9.6		Distributed transaction coordinator	**Not satisfactory;** currently set to Started Automatic.	L
1.9.7		Fax service	Satisfactory; (disabled).	P
1.9.8		Internet connection sharing	Satisfactory; (disabled).	L
1.9.9		IPSec policy agent	**Not satisfactory;** currently set to Started Automatic.	L
1.9.10		License logging	Satisfactory; (disabled).	L
1.9.11		Logical disk manager administrative service	**Not satisfactory;** currently set to Started Automatic (this service is needed by the system administrator).	L
1.9.12		Messenger	Satisfactory; (disabled).	P
1.9.13		NetMeeting remote desktop sharing	Satisfactory; (disabled).	P
1.9.14		Network DDE	Satisfactory; (disabled).	L
1.9.15		Network DDE DSDM	Satisfactory; (disabled).	L
1.9.16		Print spooler	**Not satisfactory;** currently set to Started Manual.	L
1.9.17		Remote access connection manager	**Not satisfactory;** currently set to Started Manual	L
1.9.18		Remote registry	**Not satisfactory;** currently set to Started Automatic (this service is needed by the system administrator)	L
1.9.19		Removable storage	**Not satisfactory;** currently set to Started Manual	P

OS and network specification configuration (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
1.9.20		RunAs service	Satisfactory; (disabled)	M
1.9.21		Smart card	**Not satisfactory;** currently set to Started Manual	P
1.9.22		Smart card helper	Satisfactory; (disabled)	P
1.9.23		Task scheduler	**Not satisfactory;** currently set to Started Automatic (this service is needed by the system administrator)	P
1.9.24		Telephony	**Not satisfactory;** currently set to Started Automatic	P
1.9.25		Telnet	Satisfactory; (disabled)	L
1.9.26		Windows installer	**Not satisfactory;** currently set to Started Manual	L
1.10	MS SQL server service account	Use a low-privileged local or Domain account for the MS SQL server service.	**Not satisfactory;** currently uses local administrator (high-privileged).	M
1.11	SQL server agent service account	Use a low-privileged domain account for the MS SQL server agent if replication, DTS, or other inter-server connection is required.	**Not satisfactory;** currently uses local administrator (high-privileged).	M
1.12	Local users group membership	Assign the local service account as a member of only the users group.	**Not satisfactory;** there is no assigned user in the “users” group.	M
1.13	Domain service account group membership	Make a domain service account a member of only non-privileged groups.	N/A; the current configuration does not use the domain service account group.	M
1.14	MS SQL server service account rights	Grant the MS SQL server service account(s) the following rights:	N/A; there is no MS SQL service account assigned.	
		Log on as a service		M
		Act as part of the OS.		L
		Act as part of the OS.		L
		Log on as a batch job		L
		Replace a process-level token		L
		Bypass traverse checking		M
		Adjust memory quotas for a process		L
		Permission to start the MS SQL server active directory helper		M
		Permission to start the MS SQL writer		M

OS and network specification configuration (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
1.15	MS SQL server agent service account rights	Grant the MS SQL server agent service account(s) the following rights:	N/A; there is no MS SQL service account assigned.	
		Log on as a service		M
		Act as part of the OS		L
		Log on as a batch job		L
		Replace a process-level token		L
		Bypass traverse checking		L
		Adjust memory quotas for a process		M
1.16	Integration service account rights	Grant the integration service account(s) the following rights:	N/A; there is no MS SQL service account assigned.	
		Log on as a service		M
		Permission to write to the application event log		L
		Bypass traverse checking		L
		Create global objects		M
		Impersonate a client after authentication		L
1.17	SQL server services account rights	Deny the service account the “Log on locally” right.	Satisfactory	M
1.18	SQL server services account rights	If a service account is a domain account, configure the account to have the Windows permission “Log on To” the database server only.	**Not satisfactory;** currently the domain/sqladmin account can log on to all computers.	M
1.19.1	SQL server proxy accounts	Create dedicated user accounts specifically for proxies, and only use these proxy user accounts for running job steps.	N/A; there is no proxy account assigned.	M
1.19.2	SQL server proxy accounts	Only grant the necessary permissions to proxy user accounts. Grant only those permissions actually required to run the job steps that are assigned to a given proxy account.	N/A; there is no proxy account assigned.	M
1.19.3	SQL server proxy accounts	Do not run the SQL server agent service under a MS Windows account that is a member of the Windows administrators group.	N/A; there is no proxy account assigned.	M

Appendix C33: MS SQL server installation and patches audit details

MS SQL server installation and patches audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
2.1	MS SQL server install platform	Avoid installing MS SQL server on a domain controller.	Satisfactory	M
2.2	Patches and hotfixes	Ensure the current MS SQL server service pack and hotfixes are installed.	Satisfactory; currently updating both service pack and critical hotfixes every three months	H
2.3	MS SQL server ports	Change MS SQL server default ports from 1433 and 1434.	**Not satisfactory;** the council uses both default TCP ports (1433 and 1434).	H
2.4	Naming conventions	In naming MS SQL Server instances, limit the instance name to less than 16 characters with no reference to a version number or other sensitive information.	Satisfactory; currently the name is less than 16 characters (11).	L
2.5	MS SQL server instances	Keep an inventory of all versions, editions and languages of MS SQL Server.	**Not satisfactory;** there is no inventory process.	P
2.6	Authentication mode	Select Windows authentication mode.	Satisfactory	M
2.7	Rename sa account	The “sa” account should be renamed to something that is not easily identifiable as the “sa” account. ALTER LOGIN sa WITH NAME = <new name>	**Not satisfactory;** the council uses the default account (sa).	M
2.8	Strong password	Use a strong password for the “sa” login account.	**Not satisfactory;** according to the system administrator the password is classified as a medium level password.	M
2.9	Sample databases	Do not install the sample databases. Delete all sample databases if they already exist.	Satisfactory; there is no sample database installed.	L
2.10	Initialisation parameter	C2 Audit Mode– set to 1 if no custom defined audit trace is enabled	**Not satisfactory;** the current setup is 0.	P
2.11	Initialisation parameter	Remote Access– set to 0 unless replication is being used or the requirement is justified	**Not satisfactory;** the current setup is 1.	M
2.12	Initialisation parameter	Scan for Startup Procedures– set to 0 unless justified	Satisfactory; the current setup is 0.	L

Appendix C34: MS SQL server setting audit details

MS SQL server setting audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
3.1	MS SQL server configuration manager	Disable the “Named Pipes” network protocol.	**Not satisfactory**	L
3.2	MS SQL server properties	The following settings are recommended:		
3.2.1	Auto restart MS SQL server	Set the MS SQL server service start mode to “Automatic”	Satisfactory	L
3.2.2	Auto restart MS SQL server agent	If the MS SQL server agent is required, set the “MS SQL server agent” start mode to “Automatic”.	Satisfactory	L
3.2.3	Distributed transaction coordinator	Set the “distributed transaction coordinator” service start mode to “Disabled” if this service is not required.	N/A	L
3.2.4	Cross database-ownership chaining	Disable the cross_db_ownership_chaining option.	Satisfactory	M
3.2.5	Advanced server settings	Do not enable direct modifications to the system catalogs.	N/A	M
3.2.6	Backup/restore from tape timeout	Set the backup/restore from tape timeout period to “Try for 5 minutes”	Satisfactory	L
3.2.7	Media retention	Set the default backup media retention to the minimum number of days needed to retain a full backup of the database. Ideally, this should be as high as your resources permit.	**Not satisfactory;** currently the setting has not been configured.	L
3.3	Data directory	The default data directory should be a dedicated data partition	Satisfactory; (e:\mssql\data)	M
3.4	Data directory	The default log directory should be a dedicated partition separate from all programs and data	Satisfactory; (e:\mssql\logs)	M
3.5	Replication	Do not enable replication.	N/A	L
3.6	Other SQL server configuration options	Set the number of logs retained based on the maximum number of restarts and log cyclings which may occur within your desired log retention window. The default value of 6 may be too low for many installations.	Satisfactory; the default is 6.	P

MS SQL server setting audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
3.7	Database mail	Disable database mail where messaging is not required.	Satisfactory	L
3.8	Trace messages	Error log/include execution trace messages = off	Satisfactory	P
3.9	User-defined stored procedures	Ensure that all user-defined stored procedures are stored in encrypted format.	**Not satisfactory;** stored in unencrypted format.	H
3.10	User-defined extended stored procedures	Avoid using user-defined extended stored procedures. If extended functionality is required, use Common Language Runtime (CLR) assemblies instead.	Not installed	L
3.11	Extended stored procedures	Disable access to the following extended stored procedures:		
3.11.1		xp_available media	Satisfactory	L
3.11.2		xp_cmdshell	Satisfactory	L
3.11.3		xp_dirtree	**Not satisfactory;** (enabled).	P
3.11.4		xp_dsninfo	Satisfactory	P
3.11.5		xp_enumdsn	Satisfactory	P
3.11.6		xp_enumerrorlogs	Satisfactory	P
3.11.7		xp_enumgroups	Satisfactory	P
3.11.8		xp_eventlog	Satisfactory	P
3.11.9		xp_fixeddrives	**Not satisfactory;** (enabled).	P
3.11.10		xp_getfiledetails	Satisfactory	P
3.11.11		xp_getnetname	Satisfactory	P
3.11.12		xp_logevent	Satisfactory	P
3.11.13		xp_loginconfig	Satisfactory	P
3.11.14		xp_msver	Satisfactory	P
3.11.15		xp_readerrorlog	Satisfactory	P
3.11.16		xp_servicecontrol	Satisfactory	P
3.11.17		xp_sprintf	**Not satisfactory;** (enabled).	P
3.11.18		xp_sscanf	**Not satisfactory;** (enabled).	P
3.11.19		xp_subdirs	Satisfactory	P
3.12	SQL Mail extended stored procedures	Disable access to the following SQL Mail extended stored procedures:		
3.12.1		xp_deletemail	Satisfactory	P

MS SQL server setting audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
3.12.2		xp_findnextmsg	Satisfactory	P
3.12.3		xp_get_mapi_default_profile	Satisfactory	P
3.12.4		xp_get_mapi_profiles	Satisfactory	P
3.12.5		xp_readmail	Satisfactory	P
3.12.6		xp_sendmail	Satisfactory	P
3.12.7		xp_startmail	Satisfactory	P
3.12.8		xp_stopmail	Satisfactory	P
3.13	WebTask extended stored procedures	Disable access to the following WebTask extended stored procedures. Delete the xpweb70.dll file that implements the following WebTask extended stored procedures:		
3.13.1		xp_cleanupwebtask	Satisfactory	P
3.13.2		xp_convertwebtask	Satisfactory	P
3.13.3		xp_dropwebtask	Satisfactory	P
3.13.4		xp_enumcodepages	Satisfactory	P
3.13.5		xp_makewebtask	Satisfactory	P
3.13.6		xp_readwebtask	Satisfactory	P
3.13.7		xp_runwebtask	Satisfactory	P
3.14	OLE automation stored procedures	Disable access to the following OLE automation stored procedures:		
3.14.1		sp_OACreate	Satisfactory	L
3.14.2		sp_OADestroy	Satisfactory	L
3.14.3		sp_OAGetErrorInfo	Satisfactory	L
3.14.4		sp_OAGetProperty	Satisfactory	L
3.14.5		sp_OAMethod	Satisfactory	L
3.14.6		sp_OASetProperty	Satisfactory	L
3.14.7		sp_OAStop	Satisfactory	L
3.15	Registry access extended stored procedures	Disable access to the following registry access extended stored procedures:		
3.15.1		xp_regaddmultistring	**Not satisfactory;** (enabled).	P
3.15.2		xp_regdeletekey	**Not satisfactory;** (enabled).	P
3.15.3		xp_regdeletevalue	**Not satisfactory;** (enabled).	P
3.15.4		xp_regenumvalues	**Not satisfactory;** (enabled).	P

MS SQL server setting audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
3.15.5		xp_regremovemultistring	**Not satisfactory;** (enabled).	P
3.15.6		xp_regwrite	**Not satisfactory;** (enabled).	P
3.16	Advanced setting	MS SQL server event forwarding/forward events to a different server = off	Satisfactory; (off).	L
3.17	MS SQL server browser service	Disable MS SQL server browser service	**Not satisfactory;** (enabled).	L

Appendix C35: MS SQL server access controls audit details

MS SQL server access controls audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
4.1	Permissions on OS tools	Restrict access to the executables in the System32 directory e.g. Explorer.exe and cmd.exe.	Satisfactory; remove the Users group's permission to run executables.	H
4.2	MS SQL server install directory permissions	Modify the permissions to the [Drive]:\Program Files\Microsoft SQL server directory.	Satisfactory; remove the Users group's permission to run executables.	H
4.3	MS SQL server database instance directory permissions	Delete or secure old setup files. Protect files in the <system drive>:\Program Files\Microsoft SQL Server\MSSQL.X\MSSQL\Install, e.g., sqlstp.log, sqlsp.log and setup.iss. "X" represents the installations of various SQL server installs due to the fact that multiple instances of SQL server or SQL express can be installed.	Satisfactory; access to the current install folder is allowed for the system administrator groups only.	M
4.4	Assigning system administrators role	When assigning database administrators to the System Administrators role, map their Windows accounts to SQL logins, and then assign them to the role.	Satisfactory	M
4.5	MS SQL logins	Remove the default BUILTIN\administrators SQL login.	**Not satisfactory;** the BUILTIN\administrators SQL login is still exits.	M
4.6	MS SQL logins	Ensure that all SQL logins have strong passwords.	**Not satisfactory;** enforce strong password policy.	M
4.7	OS guests access	Deny database login for the guests OS group.	**Not satisfactory;** the guest user is disabled, but the guests OS group is enabled.	H
4.8	Fixed server roles	Only use the fixed server roles sysadmin, server admin, setup admin etc, to support a database administrator activity.	Satisfactory	L
4.9	MS SQL server database users and roles	Remove the guest user from all databases except master and tempdb.	Satisfactory; disabled the guest user for all databases.	M
4.10	Statement permissions	Grant data definition language or data description language statement permissions to only the database and schema owner, not individual users.	**Not satisfactory**	M

MS SQL server access controls audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
4.11	Database owners permissions	Ensure database owner owns all user-created database schemas	**Not satisfactory**	L
4.12	Low-privileged users	Do not grant object permissions to PUBLIC or GUEST.	N/A	M
4.13	Stored procedure permissions	Grant executes permissions on stored procedures to database roles (not users).	Satisfactory	M
4.14	Using the GRANT option	Do not assign the GRANT option of object permission to a user or role.	N/A	M
4.15	MS SQL server agent subsystem privileges	Restrict proxy access to required/approved subsystems.	N/A; no proxy access.	M
4.16	User-defined database roles	Create user-defined database roles to assign permissions to objects in the database when a pre-defined database role does not supply the appropriate permissions to a group of users.	N/A; no user defined database roles.	M
4.17	Database roles	Avoid nesting database roles.	Satisfactory	M
4.18	Users and roles	Ensure that the members of the roles (users/groups/other roles) in the target database actually exist.	Satisfactory	L
4.19	Application roles	Use application roles to limit access to data to users of specific applications. Use encryption to protect the role name and password in the connection string. Use “EXECUTE AS WITH NO REVERT” or “WITH COOKIE” to allow individuals to access the application without knowing the password.	N/A	M
4.20	Use of predefined roles	Avoid assigning predefined roles to PUBLIC or GUEST.	N/A; no predefined roles created.	L
4.21	Linked or remote servers	Use linked servers rather than remote servers where required. Remove any unused linked servers or disable this feature.	N/A	L
4.22	Linked or remote servers	Configure linked or remote servers to use Windows authentication where required. Disable linked servers otherwise.	**Not satisfactory;** currently the sa account is used instead of windows authentication domain user.	M
4.23	Linked server logins	Allow linked server access only to those logins that need it. Disable linked servers otherwise.	Satisfactory	M

MS SQL server access controls audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
4.24	Ad Hoc data access	Disable ad hoc data access on all providers for all users except members of the sysadmin fixed role.	N/A	L

Appendix C36: MS SQL server auditing and logging audit details

MS SQL server auditing and logging audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
5.1	Auditing – general	Prepare a schedule for reviewing audit information regularly.	Not satisfactory; currently there is no auditing schedule.	P
5.2	MS SQL server properties – security tab	Through the MS SQL server management studio, enable auditing for SQL server.	Satisfactory	P
5.3	MS SQL server logs	MS SQL server audit data must be protected from loss. The MS SQL server and MS SQL server agent logs must be backed up before they are overwritten.	Satisfactory; the default setup is 6.	P
5.4	MS SQL profiler	Use MS SQL profiler to generate and manage audit trails.	Satisfactory	P
5.5	Profiler events	Capture the following events using MS SQL profiler	Currently there is no template created yet.	
		Event		
5.5.1		Audit add database user event	**Not satisfactory**	P
5.5.2		Audit add login to server role	**Not satisfactory**	P
5.5.3		Audit add member to DB role	**Not satisfactory**	P
5.5.4		Audit add role event	**Not satisfactory**	P
5.5.5		Audit add login event	**Not satisfactory**	P
5.5.6		Audit app role change password	**Not satisfactory**	P
5.5.7		Audit backup/restore	**Not satisfactory**	P
5.5.8		Audit broker conversation	**Not satisfactory**	P
5.5.9		Audit broker login	**Not satisfactory**	P
5.5.10		Audit change audit	**Not satisfactory**	P
5.5.11		Audit change DB owner	**Not satisfactory**	P
5.5.12		Audit database consistency check	**Not satisfactory**	P
5.5.13		Audit database management	**Not satisfactory**	P
5.5.14		Audit database object access	**Not satisfactory**	P
5.5.15		Audit database object GDR	**Not satisfactory**	P
5.5.16		Audit database object management	**Not satisfactory**	P
5.5.17		Audit database object take ownership	**Not satisfactory**	P
5.5.18		Audit database operation	**Not satisfactory**	P

MS SQL server auditing and logging audit details (continued)				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk Levels**
5.5.19		Audit database principal impersonation	**Not satisfactory**	P
5.5.20		Audit database principal management	**Not satisfactory**	P
5.5.21		Audit database scope GDR	**Not satisfactory**	P
5.5.22		Audit login change password	**Not satisfactory**	P
5.5.23		Audit login change property	**Not satisfactory**	P
5.5.24		Audit login	**Not satisfactory**	P
5.5.25		Audit login failed	**Not satisfactory**	P
5.5.26		Audit login GDR event	**Not satisfactory**	P
5.5.27		Audit logout	**Not satisfactory**	P
5.5.28		Audit object derived permission event	**Not satisfactory**	P
5.5.29		Audit schema object access	**Not satisfactory**	P
5.5.30		Audit schema object GDR	**Not satisfactory**	P
5.5.31		Audit schema object management	**Not satisfactory**	P
5.5.32		Audit schema object take ownership	**Not satisfactory**	P
5.5.33		Audit server alter trace	**Not satisfactory**	P
5.5.34		Audit server object GDR	**Not satisfactory**	P
5.5.35		Audit server object management	**Not satisfactory**	P
5.5.36		Audit server object take ownership	**Not satisfactory**	P
5.5.37		Audit server operation	**Not satisfactory**	P
5.5.38		Audit server principal impersonation	**Not satisfactory**	P
5.5.39		Audit server principal management	**Not satisfactory**	P
5.5.40		Audit server scope GDR	**Not satisfactory**	P
5.5.41		Audit server starts and stops	**Not satisfactory**	P
5.5.42		Audit statement permission event	**Not satisfactory**	P

Appendix C37: MS SQL server backup and disaster recovery procedures audit details

MS SQL server backup and disaster recovery procedures audit details				
Item no.	**Configuration items**	**Action / recommended parameters**	**Council C**	**Risk levels**
6.1	Backups – general	Use full database backups combined with differential or transaction log backups to restore the database to a specific point in time.	Satisfactory; currently the council's backup is done nightly.	M
6.2	System databases	It is important to include the system databases in your backup plan i.e. the master, msdb and model databases.	Satisfactory	M
6.3	Backing up master database	Backup the master database when any of the following events occur: ▪ A database is created or deleted ▪ Login accounts are created, deleted or modified Server-wide or database settings are modified	Satisfactory	M
6.4	Backing up MSDB database	Backup the msdb database when any of the following events occur: Alerts, jobs, schedules or operators are created, deleted or modified	Satisfactory	M
6.5	Backup media	Password protects the backup media.	**Not satisfactory;** there is no password protect.	H
6.6	Access to backup files	Restrict access to the backup files to system administrators.	**Not satisfactory;** currently all domain users can access the backup files. Access should be granted only to the system administrator group.	H
6.7	Access to backup files	Restrict restore permissions to database administrators	Satisfactory; currently, only the system administrator group can restore the backup files.	H
6.8	Recommended periodic administrative procedures	Run the MS baseline security analyser weekly and follow the security recommendations as closely as possible to secure the OS.	**Not satisfactory;** the MS baseline security analyser not in use.	L
6.9	Recommended periodic administrative procedures	Run the MS SQL best practices analyser regularly and note any changes to the environment.	**Not satisfactory;** the MS SQL best practices analyser not in use.	L

MS SQL server backup and disaster recovery procedures audit details (continued)				
Item no.	**Configuration items**	**Action / recommended Parameters**	**Council C**	**Risk levels**
6.10	Enable password policy enforcement	When a password change mechanism is introduced into clients and applications; enable password expiration. Always specify MUST_CHANGE when specifying a password on behalf of another principal.	**Not satisfactory;** no enforce password policy	M
6.11	Periodic scan of role members	Periodically scan fixed server and database roles to ensure that only trusted individuals are members.	**Not satisfactory;** currently, there are only a few users. Periodic scan may is recommended when number of users increases.	L
6.12	Periodic scan of stored procedures	Verify stored procedures that have been set to AutoStart are secure.	**Not satisfactory;** no AutoStart enabled.	P

Appendix C38: Surface area configuration tool audit details

Surface area configuration tool audit details				
Item no.	**Configuration items**	**Action/recommended parameters**	**Council C**	**Risk levels**
9.1	Ad Hoc Remote Queries	Disable Ad Hoc Remote Queries where not required.	**Not satisfactory;** (enabled).	L
9.2	CLR integration	Disable CLR integration where not required..	Satisfactory	L
9.3	DAC	Disable the remote dedicated administrator connection where not required.	Satisfactory	L
9.4	Database mail	Disable database mail where messaging is not required.	**Not satisfactory;** (enabled).	L
9.5	Native XML web services	Do not configure XML web services endpoints where not required.	Satisfactory	L
9.6	OLE automation	Disable OLE automation where not required.	Satisfactory	L
9.7	Service broker	Do not configure service broker endpoints where not required.	Satisfactory	L
9.8	SQL Mail	Do not enable SQL Mail where not required or where database mail could be used instead.	Satisfactory	L
9.9	Web assistant	Disable web assistant where not required.	Satisfactory	P
9.10	xp_cmdshell	Disable the xp_cmdshell stored procedure where not required.	Satisfactory	L
9.11	Ad Hoc data mining	Disable ad hoc data mining queries where not required.	N/A; no analysis services installed.	L
9.12	Anonymous connections	Disable anonymous connections to the analysis services where not required.	N/A; no analysis services installed.	M
9.13	Linked objects	“Enable links to other instances” should be disabled where not required.	N/A; no analysis services installed.	L
9.14	Linked objects	“Enable links from other instances” should be disabled where not required.	N/A; no analysis services installed.	L
9.15	User-defined functions	Disable loading of user-defined COM functions where not required.	N/A; no analysis services installed.	L
9.16	Scheduled events and report delivery	Disable scheduled events and report delivery where not required.	N/A; no analysis services installed.	P
9.17	Web service and HTTP access	Disable web service and HTTP access where not required.	N/A; no analysis services installed.	L
9.18	Windows integrated security	Enable Windows integrated security for report data source connections.	N/A; no analysis services installed.	M

Appendix C39: Council C's information security policy

Acceptable Use of Computing and Communications Facilities

Council C: COMPUTING SERVICES

POLICY: POL-M-019

1 Purpose

1.1 The purpose of this policy is to establish a Council C position concerning the proper use of the City's computing and communication resources.

1.2 The policy is intended to cover City staff use of the following facilities:

- All computer hardware, network and communications equipment;
- All computer software and applications, including all Internet applications; and
- Telephones and fax machines.

2 Policy

2.1 Council C encourages its staff to enhance customer service, productivity and increase knowledge through the use of available computing and electronic communications resources (including the use of the Internet) within the bounds of their employment and relevant legal and ethical requirements. These resources belong to the City and its suppliers and can only be used in the manner authorised. City staff should treat the resources with respect, always be courteous and professional in their use and represent the City in the best possible way.

2.2 Use of City computing or communication resources by a staff member should be restricted to employment related purposes and associated behaviour must be in keeping with the City's Code of Conduct for employees and legislation applying within the State of Western Australia.

2.3 Limited personal use of facilities is also permitted provided:

- It does not unduly affect or interfere with the proper performance of the duties and responsibilities of the staff member with the City;

- It does not unduly affect or interfere with the ability of other City staff members to perform their duties and responsibilities; or
- It does not involve illegal or unethical behaviour.

2.4 Common sense should dictate what is and is not employment related, and also what constitutes illegal and unethical behaviour in this regard. Notwithstanding this general comment, however, the following are specifically prohibited:

- Private commercial activities for the purpose of personal gain;
- Accessing, distributing or disclosing material prohibited by policy or law;
- Breaching confidentiality;
- Unauthorised copy or transmission of copyrighted material;
- Transmitting threatening, abusive, defamatory or offensive material;
- Distributing chain letters;
- False representation;
- Unauthorised access to, use or release of Council C information; and
- Unauthorised access to or use of computers and software programmes.

2.5 When using the City's computing and communications resources and facilities, staff members are expected to be aware of their responsibilities to:

- Comply with all policy, legislative and administrative arrangements;
- Ensure any action taken serves to enhance the services provided by the City;
- Not bring the City into disrepute;
- Be informed of all security arrangements related to the use of computer facilities;
- In particular the security risks involved of using the Internet and ensure that this is not compromised by their actions; and

- Seek advice if they are unsure about the status of their actions.

2.6 While it is the individual City staff member's responsibility to use the resources appropriately, the City's Managers also have a responsibility to deal with deliberate and inadvertent breaches of this policy.

Systems are routinely monitored to ensure satisfactory levels of service. Monitoring may also be carried out upon the direction of the Chief Executive Officer or as a result of inquiries, investigations or Freedom of Information requests. In these circumstances, information may be scrutinised or made public.

2.7 City staff who breach this policy may be dealt with under relevant industrial award or general industrial law provisions or any relevant legislation.

I have read the Council C policy on Acceptable Use of Computing and Communications Facilities and hereby agree to the terms and conditions.

Applicant's Name: _____

Applicant's Signature: _____

Date: _____