DOCTOR OF PHILOSOPHY

Novel framework to support information security audit in virtual environment

Nagarle Shivashankarappa, Arun

Award date:
2013

Awarding institution:
Coventry University

Novel Framework to Support Information Security Audit in Virtual Environment

Arun Nagarle Shivashankarappa

Submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy in the Faculty of Engineering and Computing at Coventry University, UK

April 2013

Faculty of Engineering and Computing

Abstract

Over the years, the focus of information security has evolved from technical issue to business issue. Heightened competition from globalization compounded by emerging technologies such as cloud computing has given rise to new threats and vulnerabilities which are not only complex but unpredictable. However, there are enormous opportunities which can bring value to business and enhance stakeholders' wealth.

Enterprises in Oman are compelled to embark e-Oman strategy which invariably increases the complexity due to integration of heterogeneous systems and outsourcing with external business partners. This implies that there is a need for a comprehensive model that integrates people, processes and technology and provides enterprise information security focusing on organizational transparency and enhancing business value.

It was evident through interviews with security practitioners that existing security models and frameworks are inadequate to meet the dynamic nature of threats and challenges inherent in virtualization technology which is a catalyst to cloud computing. Hence the intent of this research is to evaluate enterprise information security in Oman and explore the potential of building a balanced model that aligns governance, risk management and compliance with emphasis to auditing in virtual environment.

An integrated enterprise governance, risk and compliance model was developed where enterprise risk management acts as a platform, both mitigating risk on one hand and as a framework for defining cost controls and

quantifying revenue opportunities on the other. Further, security standards and frameworks were evaluated and some limitations were identified. A framework for implementing IT governance focusing on critical success factors was developed after analysing and mapping the four domains of COBIT with various best practices.

Server virtualization using bare metal architecture was practically tested which provides fault-tolerance and automated load balancing with enhanced security. Taxonomy of risks inherent in virtual environments was identified and an audit process flow was devised that provides insight to auditors to assess the adequacy of controls in a virtual environment. A novel framework for a successful audit in virtual environment is the contribution of this research that has changed some of the security assumptions and audit controls in virtual environment.

Dedication

This thesis is dedicated to my beloved parents' **Sri & Srimathi Shivashankarappa**, for their blessings and for instilling in me the value of patience, which was tried and tested in every phase of this doctoral thesis.

I would also like to dedicate this work to my beloved sister **Ms. Anitha Niranjan**, who is a source of inspiration throughout by life.

Acknowledgements

I owe a lot of gratitude and thankfulness to people without whose direct or indirect support this thesis would not have seen the light of the day.

Let me begin with my supervisor and mentor **Dr. Leonid Smalov** for being the ever supportive guide and friend. I would like to thank him from the bottom of my heart for all the encouragement, great ideas, and constructive feedback. He provided me with valuable advice and brilliant insights which made me achieve my goals. His unwavering confidence in my capabilities sustained me through the entire period of the dissertation.

I would like to extend my sincere thanks to **Dr. Abdullah Saif Ahmed Al Sabahy,** Chairman of Middle East College for his continual encouragement and moral support. My heartfelt gratitude goes to **Mr. Lefeer Muhamed Marakkarackayil,** Managing Director of Middle East College who was instrumental in giving me the opportunity and tremendous motivation needed at the right time.

I am extremely grateful to my friend **Mr. Ramalingam** for his entire support in the research and co-authoring various research publications. I am obliged to my friends and colleagues who gave me invaluable assistance during compilation, formatting and proofreading the thesis.

I would like to express my appreciation and gratitude to my wife **Ms. Usha Arun** and my son **Karan** who were the silent force and pillars of support and understanding in every step of my thesis writing and ensuring that I progressed on towards fulfilling my life's aspirations.

Table of Contents

List of Figures

List of Tables

Abbreviations

AI	Acquire and Implement
ALE	Annual Loss Expectancy
BPEL	Business Process Execution Language
BSC	Balanced Scorecard
BIA	Business Impact Analysis
BCP	Business Continuity Plan
CIA	Confidentiality, Integrity and Availability
COPPA	Children's Online Privacy Protection Act
COSO	Committee of Sponsoring Organization
COBIT	Control Objectives for Information and related Technology
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CAS	Client Access Server
DS	Delivery and Support
DRP	Disaster Recovery Plan
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
EAC	Estimated Annual Cost
G to G	Government to Government

G to B	Government to Business
G to C	Government to Citizens
GRC	Governance, Risk and Compliance
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as service
ISMS	Information Security Management Systems
ITA	Information Technology Authority
ITIL	Information Technology Infrastructure Library
ISACA	Information Systems Audit and Control Association
ISA	Internet Security and Acceleration
MoE	Ministry of Education
MoMP	Ministry of Manpower
ME	Monitor and Evaluate
MTPoD	Maximum Tolerable Period of Disruption
NDA	Non-Disclosure Agreement
NLB	Network Load Balancing
NIST	National Institute of Standards and Technology
PaaS	Platform as a service
PASI	Public Authority for Social Insurance
PO	Plan and Organize
RPO	Recovery Point Objective
ROI	Return of Investment

RPO	Recovery Time Objective
SaaS	Software as a service
SLA	Service Level Agreements
SOA	Service-Oriented Architecture
SOX	Sarbanes-Oxley Act of 2002
SCS	Simple Command Structure
SCP	Short Communications Path
SOC	Span of Control
SSL	Secure Socket Layer
SAN	Storage Area Network
UTM	Unified Threat Management
VM	Virtual Machines

CHAPTER 1

INTRODUCTION

1.1. Introduction to Information Security Management

Due to globalization and stiff competition in the contemporary business, there is a phenomenal change in the way business is being conducted. The advancements in network computing have enabled information systems to act as a scaffold to conduct business efficiently. This has drastically shifted the application of computers as a business tool to automate processes, to IT systems supporting information based assets. Recently, the usage of cloud computing has increased, which can provide platform as a service (PaaS), software as a service (SaaS) and infrastructure as service (IaaS) with enormous features for scalability, availability at reduced cost (Farrell 2010).

Cellary and Strykowski (2009) argue that e-government solutions should be based on cloud computing and service-oriented architecture with strong national leadership and changes in regulations. Virtualization technology is the core component of cloud computing which is helping in reaping immense benefits through different cloud computing models and architectures. Virtualization comprises of running multiple operating systems and applications on the same physical server at the same time supporting service-oriented architectures and provisioning flexible deployment. However, virtualization has both advantages and challenges since different forms of virtualization pose different research questions. As enterprises are extending

their operation across borders and becoming more elastic, computer security has evolved into information security (Whitman & Mattord 2007). As there are many definitions of information security, the more comprehensive one is defined in the U.S. National Information Systems Security Glossary edited by Kissel (2011) as “The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats”. In other words, the primary objective of Information security is to ensure confidentiality, integrity and availability (CIA) of information to authenticated and authorized entities. However information security in today’s virtual infrastructure requires a strong process based approach and a sound understanding of the business objectives. By defining security objectives in the context of virtual environment, an enterprise can create and operate a systematic and comprehensive approach to security.

However virtualization has complicated the lives of both security auditors and IT specialists since no mechanism for comparing server audit performance and results across the many nascent vendor standards. Auditing for compliance must be designed to evaluate the strength of critical controls that protect the confidentiality, integrity, and availability of virtual environments.

1.2. Background

Information security is given priority by the government, public and private enterprises and it’s becoming a key agenda in top management initiatives.

Research studies indicate that the enterprises concern about the possibility of a security breach and loss of confidential information combined with threats from natural hazards is ever growing and reached alarming levels (Freeman 2010). The real challenge for the management is the implementation of an information security program that is aligned with the business objectives and takes into consideration other organizational factors. To address this, the British Standard BS 7799 was published in 1995, whose focus is to maintain confidentiality, integrity and availability of information based assets (Barnard & Solms 1988). Later, it evolved as ISO 27001 in year 2005 which encompasses 11 domains consisting of 135 controls to provide a standard for implementing information security management systems (ISMS) for any enterprise (Calder 2009).

Most enterprises still believe that security is a technical problem, and it's the sole responsibility of the information technology (IT) department (Baker & Wallace 2007). Hence, ISMS's scope is reduced to manage IT security. This diminishing scope is mainly due to the lack of understanding of larger business issues which range from the protection of data to the protection of human resources. If the scope is the entire enterprise, which includes external entities such as business partners, suppliers, customers and other departments, then it becomes enterprise information security. It encompasses relevant people from all business units such as top management, IT head, legal experts, HR manager, and physical security staff. Although, ISMS defines processes for creating, operating and governing, it is not a control standard. Rather, it is perceived as a process management and assessment standard.

The enterprise security program essentially consists of ten steps including: Scope of security program, Business Process Mapping, Identify Information Assets, Asset Valuation, Vulnerability Assessment, Risk Assessment & Evaluation, Risk Treatment & Management Approval, Identify Control Objectives and Controls, Create Statement of Applicability and finally Training and Awareness. The implementation is based on the Deming cycle (plan-do-check-act) which provides meaningful guidance on how to manage elements of security (Te-King et al. 2007). In order to successfully implement security policies to ensure compliance one must develop effective dynamic change management strategies which is hard since people are resistant to change. (Beer & Nohria 2000) (Kenneth et al. 2006) (Oakland & Tanner 2007) (Mohan et al. 2008) (Sirkin, Keenan & Jackson 2006). Hence the successful implementation of a security program is directly proportional to organizational culture and the integration of processes. (Huang, Lee & Kao 2006).

However, the management of an enterprise information security program must be aligned to business objectives and at the same time should consider all functional units of the extended enterprise in an integrated manner with specific emphasis to cultural issues.

In the Sultanate of Oman (Oman), which is petroleum rich country in the Arabian Gulf, the government has envisioned diversifying towards industrial developments (MONE 1996). This position has resulted in multinational enterprises to setup their business units or partner with enterprises in Oman to broaden their business opportunity and exchange technical expertise (ITA-OMAN 2008).

Many enterprises rely on outsourcing and the trust between the different people concerning information security within an organization is excessively increasing. Hence the program must be flexible enough to address market pressures and other external organizational factors linked to outsourcing (Bellone, Rodriguez & Juan 2008). The enterprise information security program must be continuously monitored and evaluated through internal auditing for compliance (Raggad & Emilio 2006).

Recently, the Oman's e-government strategy became priority and aims at interlinking government sectors and services through a unified system thus empowering its population through e-Oman initiatives. An interoperability framework was thus built by the Information Technology Authority (ITA) to enable government entities to seamlessly integrate and exchange business related data between e-government systems in order to provide efficient services to its subjects (ITA-OMAN 2008). The e-Oman strategies emphasize in increasing efficiency in government by reengineering the business processes and provide e-services through service oriented architecture (SOA). SOA delivers enterprise agility through service composition, model-driven development, and service virtualization with supporting infrastructure. In order to achieve this it needs to implement core e-government infrastructure & secure the applications in line with international standards. The government of Oman has come up with a strategic plan as shown in the figure-1 to clearly develop a corporate governance structure with well-defined roles and responsibilities. A plan is said to be strategic if it provides direction to management with the required information to make informed decision about security investments and meet one or more business objectives.

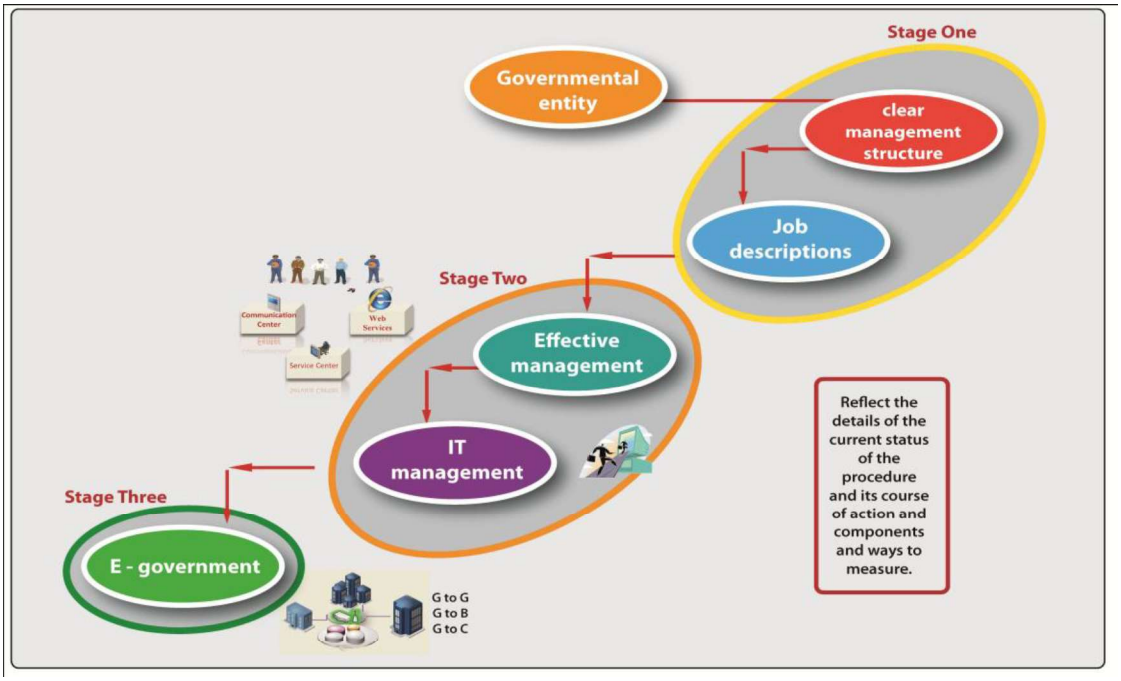


Figure 1 Strategic Objectives of Oman's E-government Initiatives

This structure should have a well-defined IT governance framework and reporting mechanism so that the persons responsible and accountable are properly expressed. The primary objective is to bring all the government web portals hosted out of Oman to within the country. The second objective is to provide a unified system that should integrate all forms of communication on to a single interface (unified communications). The third objective is to provide e-services between government enterprises (G to G), businesses (G to B) and citizens (G to C) flawlessly since integration of disparate systems is complex. However, there are many factors to be considered in such enterprise wide integration of services especially from the risk management perspective.

Research study states that there are several issues to be addressed before such complex heterogeneous information systems are integrated irrespective

of the geographical locations of the collaborating partners (Pulkkinen, Naumenko & Luostarinen 2007). Also, public and private enterprises have realized the need for effective risk management strategy after the cyclone "GONU", which hit the shores of Oman in the year 2007, causing a total of four billion US Dollar losses to many enterprises. Some of them lost data which are unrecoverable and led to the loss of reputation. This incident taught enterprises across the country that the unthinkable can happen and they must be proactive in managing risks and necessary processes need to be implemented and reviewed periodically to minimize the impact of consequences (Al-Badi et al. 2009).

As a result of this, enterprises in Oman have envisioned providing quality services to its citizens and thereby aligning itself to the e-government strategy to increase delivery, integration and quality of electronic government services and drive its adoption by citizens, residents and businesses (ITA-OMAN 2008). Hence all government agencies need to integrate seamlessly to provide electronic services to its stakeholders thus increasing their interaction. For example, the system integration of Ministry of Education with Ministry of Manpower and Public Authority for Social Insurance is necessary for e-government system to verify employment history and social security status in order to provide retirement benefits seamlessly.

The Ministries in Oman had planned for rapid and structured expansion of IT infrastructure to support this initiative with increased vendor association that required greater internal and external compliance. There is a need to meet regulatory requirements with increased focus on security and controlled

change management providing value proposition. Concerns relating to supplier risk assessment with clear accountability had earlier led to multiple points of contacts and inadequate service level agreements (SLA). Also there are wide range of new regulations and growing number of standards, guidelines, checklists, against which the ministry had to comply proactively. Hence a complete documented governance framework with continuous process improvements giving opportunities to value creation is required.

1.3. Aims & Research Objectives

The intent of this research is to evaluate enterprise Information security in Oman and explore the potential of building a balanced Governance, Risk and Compliance (GRC) Model that aligns Enterprise Risk Management (ERM) and compliance so that compliance activities dynamically seek to achieve society's regulatory ends by reducing losses which might create externalities. The proposed GRC model will provide a process-oriented approach which is the priority of this research. The following are the research objectives that guide the development of this study:

1. To critically investigate strategies adopted by enterprises to manage information security in Oman and to determine how information security management could be optimized as a repeatable management process.

2. To evaluate the role of GRC in the management of enterprise information security and to synthesize a novel balanced GRC model for optimizing enterprise information security.

3. To examine the cultural aspects of the environment in Oman and its impact on the professional and ethical issues in managing information security for ensuring shared trust.
4. To identify and mitigate risk across an organization in view of Enterprise Risk Management (ERM), which may involve everything from avoiding litigation to assessing risk.
5. To design a novel framework that supports information security audit in virtual environment to ensure that sensitive information is treated in accordance with law, regulation, and organizational policy.
6. To optimally ensure that operationally critical information is available, accurate, and up- to-date.

1.4. Significance of this Research

This research is relevant within the context of Oman since many enterprises have suffered huge losses after the tropical cyclone “GONU” hit Oman on June 5 2007 which was the worst cyclonic storm ever recorded in North Indian ocean and the Arabian sea. Cyclone GONU showed that both public and private enterprises across the country must be well prepared for such eventualities to ensure business continuity and thus gain public confidence (Al-Badi et al. 2009).

Enterprises must be careful to understand the true nature of risk. If managers go to extremes in their efforts to reduce risk exposure, costs will soar and the financial implications will be significant, potentially causing a loss of competitive advantage and high cost is just as much a risk as the possibility of a security breach. On the other hand, if management accepts risk without

considering the consequences, losses may pile up and eventually drive the enterprise out of business. This research examines strategies that can optimize enterprise information security. Hence governance, risk management and compliance model must be properly understood and applied so that it can help management deal with risk effectively. Enterprises in Oman started to adopt comprehensive ISMS initiatives due to the need to be in compliance with government requirements. There was a compelling reason to implement elements of any information security management system that can turn enterprise security policies into security requirements which can be codified, enforced, and measured to achieve, Confidentiality, Integrity, Availability and Accountability (Tracy 2007).

1.5. Definitions

In this section I have provided definitions to keywords that are used in this report.

Enterprise means an entire business organization, including all of its subsidiaries, business partners, suppliers, vendors, customers and spread across different geographic location. It implies a large corporation or government agency, ministry but it may also refer to a company of any size with many systems and more than 500 users to manage.

Security is a state of well-being of information and infrastructure in which the possibility of successful yet undetected theft, tampering, and disruption of Information and services is kept low or tolerable.

Threat is an action or event that might compromise security. A threat is a potential violation of security.

Vulnerability is the existence of a weakness in the system. This weakness may be due to flaw in the design or an implementation error that can lead to an unexpected and undesirable event compromising the security of the system.

Exploit is a defined way to breach the security of an IT system through its vulnerability.

Attack is an assault on the system security that is derived from an intelligent threat. An attack is any action that violates security.

Confidentiality ensures that only authorized individuals' have access to information. It refers to mechanisms that prevent unauthorized information disclosure (Thompson & Thompson 2007).

Integrity ensures that the information is authentic and has not been modified by additions, deletions, modifications, or rearrangement.

Availability is the percentage of time that a system is working correctly during a time period. It refers to mechanisms that ensure the system or data is available.

Strategic planning is defined by "as a disciplined effort to produce fundamental decisions and actions that shape and guide what an enterprise is, what it does, and why it does it, with a focus on the future" (Whitman & Mattord 2007).

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Kissel 2011).

Risk management is defined by NIST in its Risk Management Guide for Information Technology Systems Document as “a coordinated set of activities and methods that is used to direct an enterprise and to control the many risks that can affect its ability to achieve objectives” (Stoneburner, Goguen & Feringa 2002)

Enterprise Risk Management (ERM) : A widely accepted definition of ERM is given by Committee of Sponsoring Organizations of the Tread way Commission (COSO) as a “Process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives” (Rasmussen & Koetzle 2007).

1.6. Summary

This chapter gives a brief introduction to Information Security Management and its significance within the context of Oman. It also discusses the need to align to the e-government strategy of Oman to enable government entities to seamlessly integrate and exchange data to provide efficient e-services. The research objectives are outlined and supported by relevance of research within the context of Oman since many enterprises suffered huge losses after a tropical cyclone Gonu hit in June 2007. Finally some key definitions are provided along with the progress of the research project from year 2008 to 2013.

CHAPTER 2

RESEARCH PROBLEM

2.1. Statement of Problem

Oman is increasingly dependent on information and communication technology since the nation's e-government strategy became a priority which aims to build confidence in the use of government e-services over internet. Also, private enterprises have realized the need for an effective information security management system after the cyclone GONU hit the shores of Oman. As discussed in the background, many enterprises in Oman still perceive that Information Security is just a technical problem and thus rely on technological innovations such as firewalls, antivirus, intrusion detection, encryption techniques and Unified threat management (UTM) solutions. Literature review reveals that technical approaches alone cannot solve security problems for the simple reason that information security isn't merely a technical problem. Information security is more of an enterprise problem and a business issue not a product that can be purchased out of the shelf. Many enterprises do not have operational controls such as physical access controls, backup capabilities and protection from environment hazards; and management controls such as a security policy, employees training, business continuity planning. Enterprise information security requirements such as Confidentiality, Integrity, Availability, Privacy, Authentication, and Non-Repudiation should respect those aspects of information assets; people, process and technology that addresses the protection of those assets.

Enterprises should refer to information security standards and establish information security strategies in order to form IT security control systems; and through the implementation of these control systems, information audit should be done regularly in order to assess control performance (Hong et al. 2003). Hence, information security must be embedded in the organizational culture and a holistic approach must be followed to efficiently manage information security. Hong et al (2003) combined five related theories such as security policy theory, risk management theory, control and auditing theory, management system theory and contingency theory to arrive at an integrated theory of information security management as shown in the figure-2.

Figure 2 Integrated system theory (adapted from Hong et al. 2003)

However, the limitations of these theories are difficult to translate into operational procedures due to the dynamic nature of contemporary business environments. Also, auditing is done using a standard checklist for all related enterprises but lacks evaluation of Security Posture (Hong et al. 2003). According to Solms (2006) Information security evolution is classified into

four stages where stage one is characterized as a technical issue which is solely managed by the technical experts and in stage two, management dimension was provided in which polices were developed. The third stage was driven by standardization of information security with the international standards by auditing and certifications for compliance requirements. The fourth stage emphasizes the development of information security governance. In order to achieve the fourth stage a comprehensive enterprise governance model is essential and an optimal strategic approach needs to be developed that integrates people, processes and technology to achieve corporate governance which focuses on organizational transparency and business value. Governance is the set of processes through which the organization's leaders ensure that the business implements their policies and directives. Good governance enables management to execute enterprise strategy and mitigate risks. It does not, explicitly specify which decision should be made, by whom, when and for what reasons. Security governance is an enterprise strategy for reducing the risk of unauthorized access to information systems and data. Two examples justify the point

Enron's inability to detect a management fraud was a classic case of governance failure which shocked not only Enron employees and shareholders but also citizens who experienced power outages and increased energy prices (Diesner, Frantz & Carley 2005). Sathyam computers loss of $ 2 billion is not from a single failure but from two failures (Ahmad et al. 2009). The first was a risk management failure where Ramalingam Raju was able to turn off the monitoring controls which should have alerted the enterprise to a magnitude of risk which put the enterprise in danger. The second was a

governance failure; when the Indian computing giant's management apparently failed to take effective action to fix the problem. Failing to clearly identify both failures and who in the enterprise is responsible for addressing each failure would be disastrous for any other enterprise in a similar position.

2.2. Research Questions

The following are the research questions formulated by the author in relation to the problem statement mentioned above.

1. Are the current Information security strategies appropriate in enabling the enterprise to meet its business objectives in Oman?

2. What are the underpinning theoretical philosophies that influence the transition of information security from a technical perspective to information security governance?

3. How can enterprise risk management framework help in optimizing enterprise information security process in virtual environment?

4. What are different types of risks related to compliance in virtual environment?

5. How enterprises can succeed in meeting measurable business objectives through auditing in virtual environment?

2.3. Summary

After a series of interviews and discussions with ministry of education, ITA and security practitioners in Oman, the problem statement was formulated. It was evident that a comprehensive enterprise governance model is essential and information security must be embedded in the organizational culture that focuses on organizational transparency and business value. Finally the research questions are presented to further explore the security strategies used in enterprises across Oman.

CHAPTER 3

RESEARCH METHODOLOGY

3.1. Research Methodology

The basis of this methodology is a combination of qualitative research and quantitative research completed through the case study method in addition to the use of some statistical analysis on auditing and compliance data as it relates to the audit results which have turned into significant revenue opportunities.

The rationale for using qualitative research is that this approach asks open ended questions rather than yes or no question in order to enable people to explain their thoughts, feeling or beliefs in detail (Trauth 2001). The opinions conducted in the above said manner can be used to formulate a theory or arrive at a conclusion. The rationale for using quantitative research is that "this type of research uses closed-ended questions, enabling the researcher to determine the exact percentage of people who answered yes or no to a question or who selected a, b, c or d on a questionnaire. One of the most common quantitative research techniques is the survey in which researchers sample the opinions of a large group of people" (Baskerville 1999).

The research objectives, methodology and approach capitalize on the synthesis of secondary research in the areas of GRC-based strategic development in addition to the fields of enterprise risk management, COBIT-based governance, and audit management accomplished through enterprise compliance management. The focus of this research is in the synchronization

of the aspects of Governance, Risk and Compliance in the context of setting a practical foundation to guide many interconnections and integrations within the enterprise for these systems to work. The research has been organized in the following manner.

1. Review literature to appraise the existing practice and frameworks in information security management and GRC within an enterprise.
2. Take a case study and use audit and compliance data and analyze the case in detail to identify the scope of the problem.
3. Conduct in-depth interviews with security management decision-makers in different enterprises in different industrial domains within Oman.
4. Develop a conceptual model of the solution to the research problem and develop an optimized (balanced solution) framework/solution for an identified enterprise.
5. Present / publish research outcomes of proposed solution at international conferences.
6. Demonstrate the conceptual model by outlining how the conceptual solution could be implemented in an enterprise.
7. Evaluation of Implementation of the conceptual solution.

3.2. Secondary Data Collection

Two of the most outstanding research approaches are inductive and deductive processes. The induction process is when the researchers observe facts and reach a generalization based on those facts. That is, to find patterns in research that is applicable to a theory and may then proceed with further

testing for confirmation of the research. Deduction on the other hand, is the process where the researchers reach a conclusion by having generalized a prior known fact. In other words, deduction starts with theory and proceeds with producing predictions. A deductive approach is characteristic by making conclusions from theory. The author has chosen to use a combination of inductive and deductive research approach since this work needs to consider theoretical aspects and practical implementation issues in the environment of Oman.

3.3. Survey & Interview

In this research, initially qualitative approach was used to design semi structured interviews to get context sensitive relevant information. This is appropriate when there is limited pre-existing knowledge since it offers greater insight as people explain their thoughts, processes and feeling. Open-ended questions were used to a focus group of information security practitioners in Oman. IT administrators and consultants associated with Ministry of Education were interviewed during the later months of year 2008. Discussions were about implementing information security program in order to align to the e-government strategy of Oman (Vision 2020) that mandates every Ministry to integrate with each other seamlessly. So, Ministry of Education was keen to implement a security program to achieve information security assurance. A Non-disclosure agreement (NDA) was signed with Ministry of Education in Oman, and a copy can be found in appendix-J. Since the researcher was involved in the meetings with security consultants and had access to sensitive information the researcher is not disclosing the exact name. It will not be

possible for anyone other than the researcher to identify and/or match respondents to their respective organization. Further discussions with IT security auditors reveled that there are significant gaps in areas such as ERM, IT Governance, Policies and compliance due to various factors.

In the later part of research, quantitative method is used by designing a questionnaire with closed questions in order to explore the application of security controls and practices in enterprises. This questionnaire was distributed as an online survey using Google docs' form and the questions asked were given as Appendix -B. The primary motive of this survey was to explore information security awareness and adoption of ERM in large enterprises in Oman. The questionnaires were distributed to a focused group of practitioners in Information Security, Risk Management and Compliance domains. Out of 110 distributions 66 people responded making an average of 54.5% response rate. The questions were primarily designed to find out whether enterprises in Oman are following any governance framework with appropriate security policies that are approved and communicated by top management to achieve organizational transparency. Further, questions were asked to identify ERM strategies and the implementation challenges of COSO. Finally, questions were also asked to find out the level of information security awareness through training, before and after GONU the tropical cyclone. The findings were critically analyzed and the results along with the recommendations were published in an international conference. The research article published in the proceedings is given as Appendix -E.

3.4. Statistical Concepts and Techniques Adopted in the Study

The following statistical measures were used while testing the main hypotheses and analyzing the raw collected data:

1. Correlation
2. Variance
3. Multivariate Analysis

Correlation analysis is used to find the relationship between two items or variables. Correlation analysis typically gives a result in number that ranges from +1 and -1. The positive sign denotes direct correlation and the number moves towards 1 tells the correlation is strong whereas the negative sign denotes inverse correlation. If the number is zero then it signifies no correlation between the variables. Usually for the correlation to be considered significant, the correlation must be 0.5 or above in either direction.

The variance, in statistical analysis, gives a measure of how the data distributes itself about the mean. Unlike range that only look at the extremes, the variance looks at all the data points and then determines their distribution. In this research, Correlation analysis is used in finding the role of security measures before and after GONU.

Multivariate statistics is a form of statistics that covers the simultaneous observation and analysis of more than one variable. It is used in the analysis of risk prioritization based on its taxonomy and quantification to find effective

value of each type of risk while auditing in virtual environment. The research findings are displayed using radar charts and table-3.

3.5. Summary

This chapter summarizes the research methodology adopted which is a combination of qualitative research and quantitative research. Initially qualitative approach was used to design semi structured interviews to get context sensitive relevant information. In the later part of the research quantitative methods is used in designing a questionnaire with closed questions in order to explore the application of security controls and practices in the enterprise. Appropriate statistical concepts and techniques used are defined.

CHAPTER 4

LITERATURE REVIEW AND FOCAL THEORY

4.1. Importance of Enterprise Information Security Management

In looking for research of the implications of GRC frameworks, there is a dearth of published research on the topic. However, significant amount of research, theories, and quantification of the performance of many forms of electronic communication, shared risk models in the form of ERM, electronic authentication and trust-based initiatives, and the definition of frameworks, standards for defining compliance initiatives and plans are available.

Supporting the integration of GRC strategic components together into an integrated model is the extensive empirical research illustrating the pay-off of firms seeking to stay in compliance, using process-oriented efficiencies as a means to accomplish this strategic initiative (Garbani 2005). The uses of ERM frameworks and models have been successful in taking advantage of the need enterprises have to align their information security strategies with business objectives. This will eventually help to achieve process efficiency and the process workflows for auditing their performance to internal standards (Fox 2009). Given the process-centric approach that ERM implementations undertake to enable the accomplishment of strategic objectives, ERM is considered to be a foundational element of GRC (Garbani 2005). ERM also has an added benefit of having Business Process Execution Language

(BPEL) included in many implementations of this enterprise-wide risk management strategy (Nagaratnam et al. 2005).

For any ERM to be effective in mitigating risk it must also be fully integrated into the market analysis, benchmark environmental factors and benchmark global strategies to form the foundation of a stable benchmarking series of processes (Meybodi 2006). Figure-3 shows how benchmarking can specifically be used in the context of managing audit data from the tactical to the strategic level.

Figure 3 Integrated strategic benchmarking framework (source: (Meybodi 2006))

The fundamental elements of Confidentiality, Integrity and Availability form the foundation of the enterprise Information security plans and implementation

strategies. Figure -4 provides a graphic that illustrates the interrelationship of CIA within the concept of an enterprise Information security implementation. These three aspects of an enterprise Information security implementation have also been included by Siemens in their development of a Service-Oriented Architecture (SOA) that unifies their strategic plans for security management with the ability to respond more efficiently and profitably to customers with very valuable internal data (Doughty 2003). This is made possible through the use of the enterprise governance to safeguard critical customer data with the help of clearly defined enterprise information security architectures. What is happening increasingly with the development of GRC frameworks, the SOA architecture has been seen as Information Technology platform enabling greater inter-process and inter-system integration? As a result CIA are design objectives of SOA architectures and platforms that extend enterprise-wide, making the contribution of security implementations much more pervasive than they had been in the past.

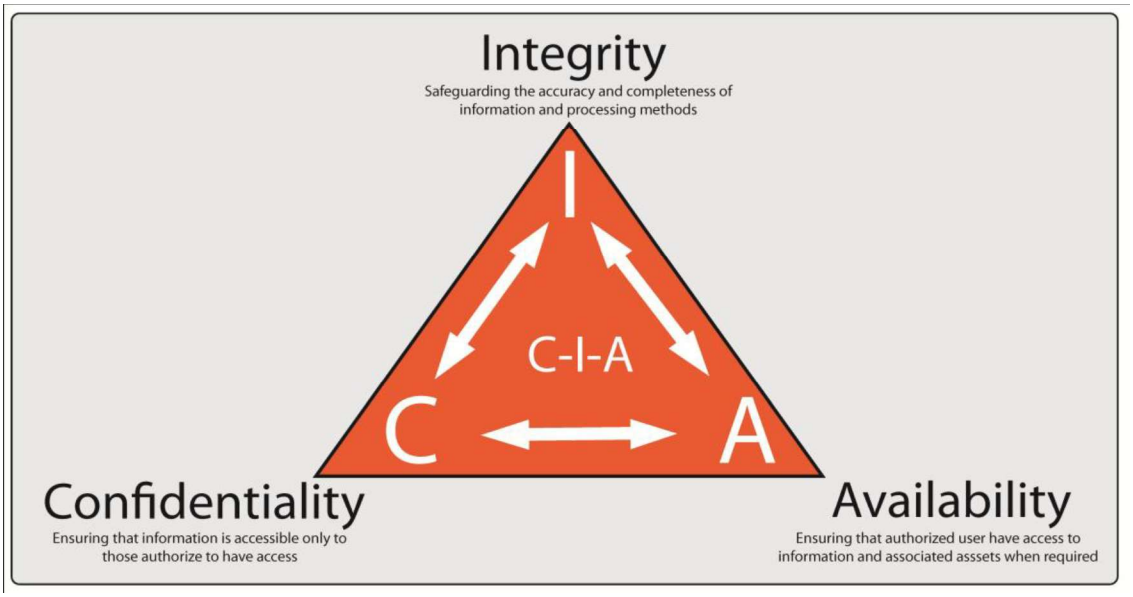


Figure 4 The Building Blocks of a Successful ISMS Implementation

The implementation of enterprise information security requires intensive integration from an economical, consumer, internal process and growth perspective if it is to be successful (Huang, Lee & Kao 2006). This is further highlighted by the eleven different domains that comprise the ISO/IEC 27001 standard (Bodin, Gordon, Loeb, 2008). These eleven domains include defining a security policy, organizing information security, defining Asset Management strategic plans and programs, integrating to Human Resource security and system components, and also planning for enterprise-wide Communications and Operations Management, defining more precise approaches to data and facility Access Control and the development of more strategic and integrated approaches to Information Systems acquisition and underlying supporting processes and Information Security Incident Management. The three remaining domains of the ISO/IEC 27001 standard include defining business continuity management strategic plans, defining governance frameworks that can ensure continued compliance to federal and global requirements, and the continual development of physical & environmental security at the strategic level (Calder 2009).

Integration of all the eleven domains of ISO 27001 is critical in order to successfully implement security convergence across the enterprise due to the rapid expansion of the enterprise. One of the factors that is the most critical for all eleven factors to be successful is defining a stable and sustainable change management strategy that is consistent with the organizations' culture (Chang & Lin 2007). Organizational culture also plays a vital role in social engineering attacks. Social engineering is not a technical skill but a people skill where the intruder would convinces the victim to do something which they

would have not done otherwise. Human beings are the weakest link in the security chain and hence social engineering attacks becomes extremely easy to commit and very difficult to defend against (Applegate & Scott 2009). There are a variety of social engineering attacks like phishing, Trojan email, Impersonation, persuasion, bribery, shoulder surfing and dumpster diving to name a few which relies on trust to gain access to sensitive Information (Applegate & Scott 2009).

Hackers use psychological factors such as fear, uncertainty, doubt, trust and authority combined with emotional interaction to obtain unauthorized confidential information from a trusting individual through non-technical means (Workman 2007). The consequences can include financial damages, loss of public confidence, and legal ramifications. A strategically well designed training and awareness program with appropriate security policy and security plan is essential to defend against social engineering attacks. Peterson (cited in (Okenyi & Owens 2007)), indicates that more than 70% of the attacks are from the insiders and only 30% of the attacks are from outsiders. Hence excessive trust on insiders must be avoided and a framework could be developed across social and cultural contexts. It is a well-known characteristic trait that Omani people invariably trust one another and are very friendly by nature which can be exploited by social engineers to bypass technical controls by attacking the human element in an enterprise. According to Mohan et al (2008) many estimates from security professionals there is at least a 1:10 ratio of dollars spent on actual security risk assessment applications and software to that spent on training, knowledge transfer and assisting those who need to perform their jobs more effectively. The long-term success of any

enterprise information security implementation however isn't necessarily in the systems- or process-level integrations completed, it is in getting people to change how they do their jobs on a daily basis, and this is often referred to as change management (Mohan et al. 2008). Consider the typical Enterprise Resource Planning (ERP) implementation in an enterprise requires a minimum of ten times the amount invested in software to be spent on educating users about the new system (Sirkin, Keenan & Jackson 2006). For every dollar invested in ERP software an additional ten dollars are invested in assisting users of the system learn how to use it, apply it to their specific tasks on their jobs, and design the graphical interfaces so they are easily usable and fit with how the systems' users do their jobs. In short, change management is the most critical task that a security implementation must address, over and above the integration processes and systems throughout an enterprise (Mohan et al. 2008).

According to Booz Allen Hamilton (2005) "As new technologies emerge and threats become increasingly complex and unpredictable, senior security executives recognize the need to merge security functions throughout the enterprise". Further it describes this emerging phenomenon as convergence and defines it as "the identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies" (Booz Allen Hamilton 2005).

Enterprises in Oman are becoming more complex in a global economy where external partners are increasing, with outsourcing and value is shifting from physical to information based assets. Emerging technology is not only

creating an overlaps between physical and logical security functions but also paves ways for new regulations in Oman to counter new threats. Rungta et al. (2004) argued in favor of a new approach to managing information security in the enterprise. As IT security evolved over the years, enterprise information security strategies tended to focus on the perimeter of controls and risk reduction within the enterprise network system.

However, with the increased interaction between multiple computers within the enterprise, across enterprise, and across several geographical boundaries, the study concluded that it was necessary to develop security management strategies to reflect the new technology infrastructure, and that existing policies and management framework for enterprise information security management are inadequate (Rungta et al. 2004). As these events unfolded, it seemed that most of the efforts to manage information security were focused on the technical and operational levels. Even at these levels, there seemed to be an absence of a formal framework or methodology for managing information security. Some researchers have attempted to provide some reasons for the absence of a methodology. It was suggested by Hong et al. (2003) that one of the reasons might be a lack of a theoretical framework for the management of information security in the enterprise. Specifically, they observed that, because of the lack of an information security management theory, there are few empirical studies conducted to examine the effectiveness of management strategies and tools (Hong et al. 2003).

4.2. Managing Enterprise Risk

ERM is undergoing major change within leading enterprises worldwide, and are moving away from the traditional approach to managing risk to governing more comprehensively and coherently. As business leaders seek new ways to build stakeholder value, they have begun to think in new ways about how risk management is tied to value creation. Across industries and organization, many are recognizing that risks are no longer merely hazards to be avoided but, in many cases, opportunities to be embraced. For example the US congress passed the Children's Online Privacy Protection Act (COPPA), which mandates website operators to get parental consent before collecting personal information from children under the age of 13 and also to protect personal information collected from children. Many companies modified their online registration process to prevent children under the age of 13 even though they are selling products and services specifically targeted at children. However Burger King (www.bk.com) which sells food products to children did not ban children from its website. Instead, the company decided to adopt a compliance program which reduced its probability of losses and simultaneously allowed it to accept a risk which added value to the company.

Risk in itself is not bad, what is bad is risk that is mismanaged, misunderstood, mispriced, or unintended. Indeed, many are realizing that risk creates opportunity, that opportunity creates value, and that value ultimately creates shareholder wealth. Identifying and mitigating risks across an enterprise is the purview of enterprise risk management (ERM), which may entail everything from avoiding litigation to assessing credit risk. It encompasses the more traditional security risks, such as asset protection, as

well as broader security issues, such as safety, IT security, and brand integrity. As a rising management discipline, current development of ERM varies across industries although advanced ERM developments are seen in the insurance industry, financial institutions, petroleum industry and the energy industry. The enforcement of ERM in these industries was originally stimulated by regulatory requirements. Recently, more enterprises in other industries, and even the public sector, are becoming aware of the potential value of ERM and risk managers are increasingly bringing it to top executives' agendas.

ERM has emerged as an important new business trend. ERM is a structured and disciplined approach aligning strategy, people, processes, technology, and knowledge with the purpose of evaluating and managing the uncertainties the enterprise faces as it creates value.

Enterprise-wide means the removal of traditional, functional, divisional, departmental, or cultural barriers. A truly holistic, integrated, future-focused, and process-oriented approach helps an enterprise manage all key business risks and opportunities with the intent of maximizing shareholder value for the enterprise as a whole. "ERM is the process of planning, organizing, leading and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings" (Purpura 2007). Enterprise risk management also expands the process to embrace not just risks associated with accidental losses but also financial, strategic, operational and other risks. Enterprise Risk management encompasses all the structures, methods and processes used by organization to identify, measure and

manage risks, or to seize opportunities, related to the achievement of business and strategic objectives as shown in figure-5.

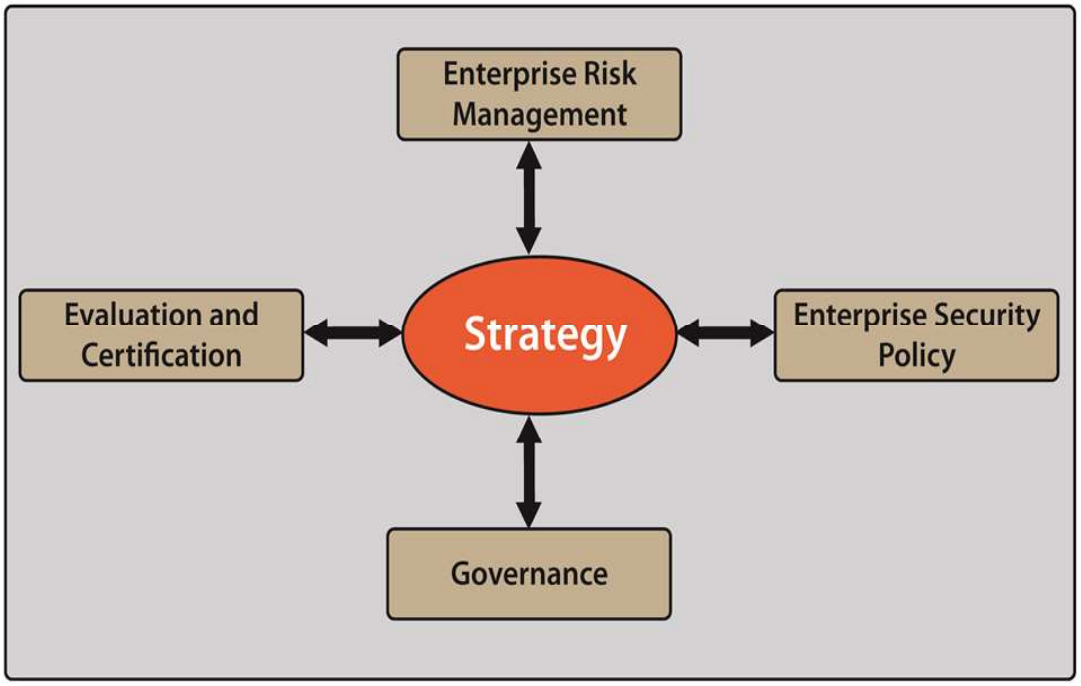


Figure 5 Role of ERM in an Enterprise Information Security Strategy

Traditionally, ERM techniques were used by financial services firms such as bank, insurance companies, who needed to match their liability with their underlying assets. ERM has developed further to include managing all areas of risk, both on- and off-balance sheet, and is now used by firms in all industries. ERM goes beyond normal accounting rules for writing down the assets and liabilities of a firm, working further to place a value both on the true market value of an asset as well as on the risk associated with that asset. The old business adage, "You cannot manage what you do not measure" could be considered a central belief of ERM. By providing more worthwhile information about risk, manager can make more informed decisions. Leaders face a variety of new challenges in their drive to maximize value. Due to

globalization, e-business, new organization partnerships, and the increasing speed of business activity enterprise are rapidly changing and expanding the risk profile. One significant result is that risk management must now extend well beyond traditional financial and insurable hazards to encompasses a wide variety of strategic, operational, reputation, regulatory, and information risks. As a mean of identifying, prioritizing, and managing such risk across an enterprise and linking them to value creation. ERM has the potential to provide enterprise with a new competitive advantage. Most organizations, however, are uncertain about how, exactly, to translate the concept of ERM into concrete action steps that will help them enhance shareholder value. "Leaders agree that as important as ERM might be in theory, it will never be valuable in practice unless it enables organizations to use risk information to drive business value in a way they could not do otherwise" (Purpura 2007).

Of course, no enterprises can operate without some risk. "If there was no risk, there would be no revenue" (Mbuya 2009).The whole idea of doing business is based on the idea of taking risk. Managing risks does not mean eliminating them. Rather, risks must be brought down to a level that will not be fatal to the enterprise. The goal is to "make calculated decision daily to help manage risk to people, reputation, information, and property in that order" (Mbuya 2009). This is essential due to the gradual increase in regulatory requirements, changing internal controls and pressure from audit community mandating all entities to be involved with the enterprise risk management process.

4.3. Assessing Risk

Before an enterprise can manage its risk, it must identify potential risks and assess how risk will affect the company. A variety of formal and informal methods can be used to accomplish these tasks. A key factor is to be selective. If you just start thinking of all the possible risks that might harm your company, you'll end up with a very long list that includes everything. The company business objectives must serve as a starting point. Seeking out the owner of the identified risk is another helpful tactic. The risk owner can be a vice president or other staff member, depending on the risk. That person is responsible for assessing the needed controls, planning the actions, and then implementing, re-assessing, and reporting on the actions in concert with the company's risk management process and policy.

Some organization use visuals to help clarify the risk picture. They use a wheel that expresses the circle of the risk life cycle which starts with the identification of a specific risk, then moves through the ways to eliminate, transfer, mitigate, insure, and evaluate that risk over time. Other uses heat maps, a graphical representation of data that measures gaps and shows through color variations where risks are controlled. Sometimes its clear what the major concerns are. Any enterprise risk management plan must recognize that risks evolve and companies must be prepared to adjust since things are changing faster than ever expected.

4.4. Enterprise Information Security Standards

4.4.1. COSO

COSO is a high-level control framework that requires management to look at risk-related issues and implement risk management processes across the enterprise. But unfortunately it is complex with overlapping organizational objectives dimension and business levels dimension that confuses high level executives. The positive effect of COSO is that it forces more information to come from lower levels in the enterprise and be rolled up into higher-level decisions. Even though the situation is changing in Oman, many current executives unfortunately moved through corporate ranks before IT became important to enterprise operations and survival. As a result, their understanding of the risks related to technology has not kept pace with their understanding of the technology's advantages at improving business efficiency. This mismatch leads to a risk management gap that has resulted in serious negative consequences. COSO applies to the entire enterprise; however it doesn't address security domains, specifically. As a result, its coverage is somewhat out of scope for the security team. It is almost entirely targeted at board and senior management personnel and lacks the level of direction from an implementation perspective. It is less flexible and just focuses on risk management with lack of specificity regarding information technology (IT)/security controls. Although by virtue of SOX, COSO is the de facto enterprise risk management standard.

4.4.2. ISO 27001

ISO 27001 now has a rational path that includes both an enterprise information security control framework and an assessment capability. For those enterprises that don't have a process model, ISO 27001's Deming cycle (plan-do-check-act) provides meaningful guidance for how to manage elements of security. However, more likely, enterprises will have implemented or be implementing other processes such as ITIL and will either need to merge process frameworks or elect to limit ISO 27001 to a certification capability. Given a business environment such as in Oman which increasingly depends on heavy outsourcing, the need for third-party controls assessment is more pressing than ever. ISO 27001 is generally acknowledged to be an excellent standard for coverage of security domain information and most widely employed security-related standard. The standard defines processes for creation, operation, and governance of an Information Security Management System (ISMS). The standard is intentionally aligned to other key ISO standards, such as 9001:2000 for quality management within the enterprise. ISO 27001 is not a control standard per se. Rather; it is a process management and assessment standard. It does not contain actual control stipulations for ISMS; instead, it relies upon other frameworks for such content.

4.4.3. COBIT

COBIT is positioned by ITGI as a governance standard and is broadly focused on implementation rather than management and policy domains. In order to overlay governance, other ITGI documents, mappings, and methodologies are

involved. The standard does implicitly rely on COSO to provide top-level risk management guidance, so one argument is that COBIT should always be paired with such an approach. However, security policy is still lacking, and supplements from core security standards (like ISO 27001) are recommended. COBIT has proven to be a highly successful tool for the audit community. The standard has been promoted as complementary to COSO and therefore a key element of SOX compliance. While this isn't strictly the case, COSO does not mandate a specific framework and many enterprises found COBIT to be immensely helpful in providing additional prescription over internal controls where COSO provided none. At the same time, many large audit firms adapted examination frameworks and audit checklists to correspond with the standard. In short, COBIT experienced a perfect storm: heavy regulatory pressure combined with enterprise need for greater specificity combined with compatible audit community processes. In conversations with security practitioners in Oman, it was apparent that COBIT was frequently employed. Although it rarely serves as the top-level guiding framework for information protection, it is an important part of controls establishment and assessment for IT.

4.4.4. ITIL

It's important to differentiate between ITIL as used for broader IT service management and delivery and ITIL as a security control standard. The former has many positive attributes and is experiencing steady adoption; the latter does not. The ITIL “Security Management” guide should not be used as a standard in any form by any enterprise. Although it is reasonably useful as a startup guide for the new security trainee, it is too long-winded for executives

to read, too naïve for advanced security practitioners to make real use of, and only a shell of ISO 27001, on which it is ultimately based. As newly published ITIL version 3 (which removes an explicit security guide) becomes available and more commonly understood and employed its role in security matters may change. But most likely, enterprise information security management will be guided by ISO 27001 and use ITIL processes as required.

Various standards position their applicability along similar lines, but none is as aggressive as COBIT, which tries to be all things to all people through its various extended documents and mappings. COBIT has been immensely successful in Oman providing real value around governance, controls, audit, and other elements of enterprise information security. This is evident through interviews and discussions with security practitioners and consultants in Oman. Also a survey was administered using a questionnaire where sixty respondents out of one hundred and ten distributions making an average of 54.5 % response rate. Key findings from the survey illustrates that the practitioners are aware of COSO framework but most of them were unable to understand it, since it is too complex from an implementation perspective. Another vital finding is that most enterprises are not giving attention to regulatory risk especially cross border regulatory requirements since it lacks clarity. The detailed findings and suitable recommendations were later published in an international conference.

4.5. Challenges

The scarcity of money and time is a perennial impediment to a more effective risk management process. Difficult economic times increase the problem,

because cost cutting often results in less than optimum combinations of internal controls, increasing risk. Moreover, security officers are asked to do more with less. But risk managers cannot let these barriers affect their efforts.

It's still security manager's responsibility to do the best to manage global risk regardless of what resources are available at a given time. To achieve those objectives, security managers must deliver the right information to the appropriate level of management so that executives can prioritize and make appropriate choices. However money is not the only issue. Another barrier to implementing ERM can be perceptions about what it means to disclose risk on the part of front-line personnel and middle managers. People have to get past the point where disclosing risks makes them feel that they are not doing their jobs. Kounus and Minoli (2010) reiterate that "Establishing a zero fault scenario would be best, so that employees won't hide details the company needs to know and culture can also be a road block".

4.6. Success Factors

To overcome any perceived or real issues to an effective security risk management process, one must rely on their management skills rather than their security knowledge. Quality such as flexibility, diplomacy, and persistence as well as the ability to conceptualize, delegate, build relationships, and deal with ambiguity are essential to an enterprise security risk management leader. Security professionals need to credit courses on leadership, training on enterprise risk management, and advanced degrees in business when polishing executives skills. Developing a thorough

understanding of the enterprises business objectives and participating in its strategic plans are all essential.

Communication of the risk strategy and structure is essential. Such communication should be designed (using appropriate technology and common language and concepts) to ensure that all employees and stakeholders understand the board's vision and objectives. Leaders must clearly demonstrate the relevance of the ERM strategy, providing success stories to maximize the value of the communication process. Communicating effectively is high on everyone's list of essential business skills. Making conversations relevant to the audience and speaking confidently in nontechnical terms are other components of effective communication. Staff will be a lot more supportive if they understand how your plan is going to benefit them directly and that support is the key to accomplishing the ERM mission. The growing recognition of ERM as a holistic view of risk throughout an organization is important; this holistic view helps ensure that the threats that might typically not be recognized in an enterprise risk management program focusing primarily on financial risks (such overlooked risks, for example, might include: risks to brand and reputation; physical supply-chain risks; or loss of consumer confidence if your data is stolen or networks attacked) are now more and more fully identified, prioritized, and mitigated.

It is well known that most security executives would identify that theft, data loss, and terrorism are at the top of the list. But you might not expect to hear that the economic competition and regulatory pressures also rank high. Security professionals are recognizing that whatever risks their organization face, they need to reach across all business units to ensure that every

department collaborates with the goals of enhancing security, increasing the bottom line, and assessing the organization in meeting its objectives. It is a vital element of ERM, which examines the universe of risks such as financial, strategic, operational, legal, accidental, and so on that an organization faces.

4.7. Managing Change to Achieve/Sustain Enterprise Information Security

The most critical aspect of any successful enterprise information security implementation is in diligently planning how process and system change can be tailored to the specific requirements of the organizations' culture (Kenneth et al. 2006). Culture is believed to be particularly vital in change management, however it is not seriously considered in Oman. Change management is a significant tool when implementing strategic objectives within an enterprise since it is an ongoing task in enterprise information security management. The change management process must consider the social side and address all the issues arising from technical changes in the enterprise. It must encourage people to help themselves; and thus enabling the enterprises to successfully meet future challenges as a learning enterprise. Corporate culture determines the enterprise's success or failure since employee behavior has a measurable effect on the enterprise's security effectiveness. Also change management always creates conflicts which arise due to lack of proper communication. Hence a proper communication strategy and a communication plan with two-way communication and feedback is critical to increase acceptance and motivation. As a result of how critical change management and cultural alignment of enterprise information security implementations are, project

managers will evaluate a range of possible change management strategies and theories to decide which one best fits with the enterprise (Mohan et al. 2008). Duration, Integrity of Performance, Commitment and Effort (DICE) model provides an comprehensive reason and direction for planning and implementing change management which is highlighted in the following section.

In defining their DICE model Sirkin, Keenan & Jackson (2006) discusses that the soft factors of change management in general and enterprise information security implementations focusing purely on employee's motivations are excessively relied on. Whereas the duration, integrity, commitment and effort which are the hard factors of change management are given little emphasis but these factors should be measured appropriately as an essential aspect of planning. This approach of measuring change management concentrated on applying quantitative measures to each element of the DICE model, then chart the correlations of completed products to each projects' respective DICE score (Sirkin, Keenan & Jackson 2006).

In calculating DICE scores Sirkin, Keenan &Jackson (2006) suggest quantifying the duration of the project including milestones, integrity of performance in the context of time spent in completing tasks, senior management commitment, local-level or employee commitment, and effort. Enterprises can find out how change projects are progressing by calculating scores either before or after they have made changes to a project's structure to give a clear picture of the project's strengths and weaknesses. DICE Model enables an organization to track the progress of projects over time or before and after changes have been made to the project structure.

Duration is the length of time between project reviews and Integrity is the extent to which an organization can rely on the project team. Commitment can be defined as having senior management assurance in place. Finally, effort is the estimated amount of time spent for those making the change.

DICE Score = D + (2Xi) + (2XC1) + C2 + E

Where Duration [D]

Integrity of Performance [I]

Senior Management Commitment [C1]

Local-Level Commitment [C2] Effort [E]

While Sirkin, Keenan& Jackson (2006) admit that the process of quantifying the performance of these factors can be subjective in nature, but their argument for greater accuracy and precision tends to lean towards security implementation and project management over the statistical precision their equations project. Sirkin, Keenan & Jackson (2006) end their discussion with a return to the common best practices in change management many other experts in the field adopt, which includes C-level commitment and verbalizing of change being needed and personal ownership being critical. In terms of its success in enterprise information security planning the DICE Model has been useful when included as part of a Balanced Scorecard (BSC) method to managing project performance (Huang, Lee & Kao 2006) (Mohan et al. 2008). The use of the DICE Model as the only approach to managing change is not sufficient in enterprise information security implementations. Instead it is

useful as a model for planning and initiating change management programs (Sirkin, Keenan & Jackson 2006).

Modern business increasingly depends on reliable information which is seen an asset that plays a vital role in the success of an enterprise. Over the last decade enterprises rely heavily on Information technology infrastructure to conduct business efficiently and provide value added services cost effectively. Information security has become an indispensable part of all enterprise to meet and exceed the expectations of all the stakeholders. With the heightened competition from globalization, new technologies emerge and thus introducing new threats and vulnerabilities which are not only complex but unpredictable in nature. Network computing has gained momentum and networks are now pervasive and ubiquitous. Enterprises are witnessing a phenomenal thrust in information security and communication Technology with a vision to build a knowledge society. The modern data communication, information processing and storage technologies have created many security issues and demands for robust policies (Bronk 2008). Most standards such as the ISO 27001 give a general guideline which lacks specific details and most times does not take organizational factors. The ISO standard offers a general guideline that risk must be assessed but does not explicitly mention how to assess the risks.

Having systematically assessed and categorized their risks perhaps having tried to understand their impact many enterprise's try to determine which risks should be managed at the corporate level and which risks should be pushed down into the structure of the enterprise.

4.8. Summary

This chapter presents about information security management system and challenges faced to achieve CIA. It also critically investigates the strategies adopted by enterprises to manage information security in Oman and to determine how information security management could be optimized as a repeatable management process. ERM must be integrated into market analysis and consider environment factors so that systematic approach to managing risks can be used thus minimizing issues related to critical change management. The Integration of all the eleven domains of ISO 27001 is critical in order to successfully implement security convergence across the enterprise and ensuring cultural alignment of ISMS implementation is outlined.

CHAPTER 5

DESIGN OF PROPOSED GRC MODEL

5.1. Strategically Balanced Governance, Risk and Compliance Model

There is a need for a model that can balance the interrelationships between the four strategic elements such as enterprise risk management, enterprise information security policy, governance and the processes of certification & evaluation. Kadam (2007) argues that an enterprise information security program's effectiveness depends on a well-designed and implemented security policy. To run any business successfully we need both financial and human resource policy. Similarly in modern business where information systems play a significant role an information security policy is highly critical.

The conceptual model should also create a real-time level of integration through Business Process Execution Language (BPEL) based technologies. BPEL will be useful to define collaborative business processes that span several enterprises having disparate platforms and architectures. Thereby BPEL can also assist the assessment of compliance activities with local information security policies and executed in a distributed infrastructure (Fischer et al. 2007). Taken together the areas of risk management, enterprise information security policy, governance that relies on the COBIT (Control Objectives for Information and related Technology) framework, and the processes of evaluation, certification and audit need to be contained into a strategically balanced GRC framework. In order to achieve this, a strategically

balanced model is required that considers the changing business environment and the influence of cross border regulatory laws which needs to be supported by latest technological infrastructure. Auditing needs to done tactically since extended enterprises produce information supply chains which create interdependencies among business partners which are mostly ignored by the managers. COBIT and ITIL can be used for this purpose since they provide directions from a technology management perspective and service management perspective respectively (Abu-Musa 2009) (Tan, Steel & Toleman 2009).

Auditing is inherently tactically in nature as it seeks to find gaps in performance and reports generated and reviewed from the standpoint of what needs to be improved over time. It is a critical component of the proposed model to ensure a high level of agility and information flexibility within the model. The reliance on BPEL as a unifying technology for ensuring processes that span multiple departments and divisions can also create greater interprocess efficiencies is key to any framework to succeed (Nagaratnam et al. 2005). The reliance on process-based approaches to re-engineering an enterprise however fall short over time as they also must be anchored in metrics of performance as well (Garbani 2005).

This reliance on auditing as a tactical input to a strategic process can be seen in manufacturing industries (Meybodi 2006). Performing gap analysis and variance analysis is a core activity in auditing, and that analysis is the basis for creating dashboards and benchmarks that in turn provide direction, context, prioritization and focus for more strategic and all-encompassing GRC frameworks (Mitchell 2007).

Why it is so significant to review auditing from a manufacturing standpoint is that it integrates the concepts of scorecards for suppliers, strategies for reducing the cost of quality and compliance and managing risks. These are the essentials for the development of a balanced model that encapsulates the concepts of ERM, Enterprise Information Security Policy, IT Governance and audit for evaluation and certification. Using auditing as an information source, all of these components are combined to create a model that seeks to balance risk and IT investment with potential revenue gains and cost reductions over time. Figure-6 shows the proposed conceptual governance, risk and compliance model that puts into context the four strategic areas of coverage within this proposed research effort.

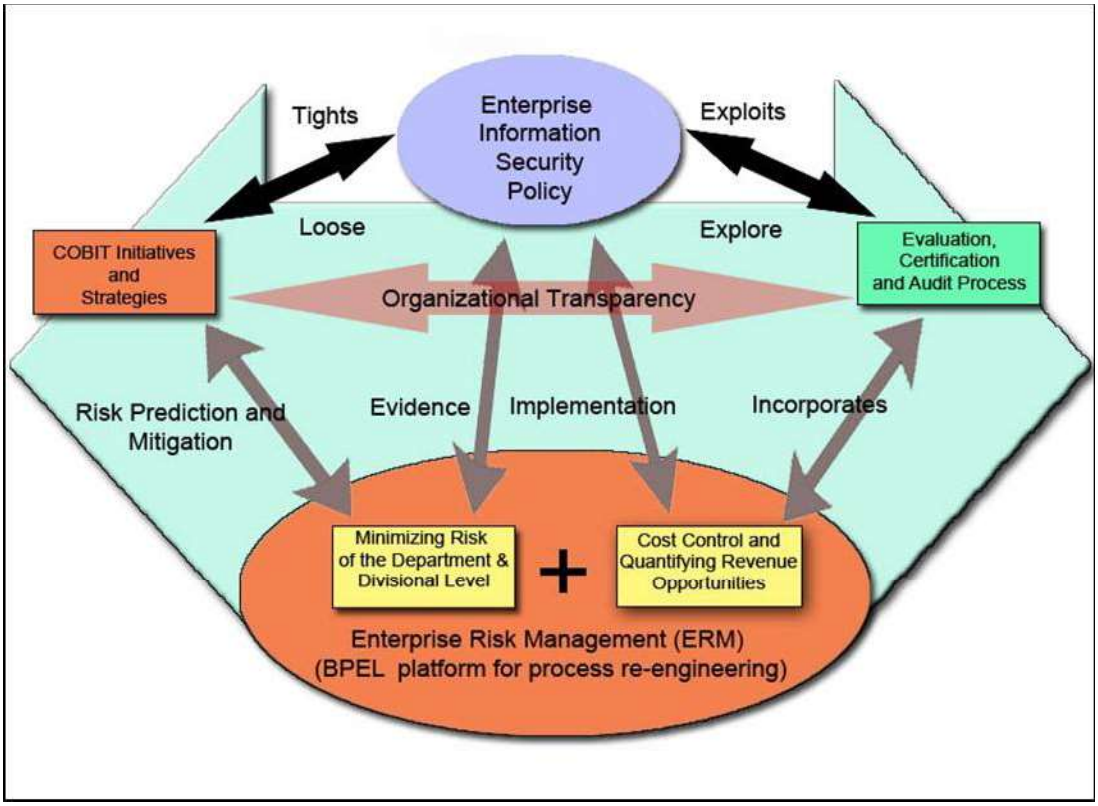


Figure 6 Proposed balanced Governance, Risk and Compliance Model

In this GRC model, enterprise risk management is performed to minimize the risk at departmental and divisional level and ensuring that the security policies are implemented with clear evidence of its actions. ERM platform includes BPEL-based workflow support for recreating process-based integration across all areas of the model. Relying on ERM as a platform both mitigating risk on the one hand and as a framework for defining cost controls and quantifying revenue opportunities through auditing creates a foundation for ensuring transparency and information velocity.

Defining COBIT Initiatives and strategies in conjunction with the information workflows from audits provides the necessary intelligence for creating Enterprise Information Security Policy. Also COBIT initiatives and strategies must create organizational transparency and allows senior management to understand whether the risks the enterprise is taking are prudent and to know how effectively its value-creation and loss-limitation activities are functioning so that these activities can be adjusted (tightening and loosened) if they are not doing the job. Applying enterprise information security policies using appropriate Service Level Agreement (SLA) within the model improves governance, risk and compliance in cloud computing environments.

Taken together this model allows for greater agility in responding to significant change in external environments and more effective levels of risk mitigation as well. In the context of a Service-Oriented Architecture (SOA) the proposed model also creates significant opportunities for creating Web Services that interlink its four key components, as evidenced by previous SOA implementations used as governance, risk and compliance frameworks

(Nagaratnam et al. 2005). Also inherent in the design of the proposed model is the development of strategies to overcome resistance to change as well. With an integration point between cost controls and audit processes, benchmarks can be created that align with their reporting as defined by (Meybodi 2006). Anchoring compliance initiatives within financial results is possible over time using the proposed conceptual model as it has multivariate analysis inherently built into the structure. Instead of having to rely on specific components for their process-based integration, the proposed governance, risk and compliance model concentrates on creating a more efficient approach to having ERM serve as the coordinating layer of the model. This frees up audit, COBIT and evaluation cycles within the model to create more responsiveness and agility to market conditions over time. Lack of trust and accountability which is the major barrier for cloud computing will be addressed by auditing for compliance in cloud environments. During the process of auditing and evaluation new threats and exploits are discovered as a result of which new security policies are formulated and the governance strategies based on COBIT can be periodically adjusted.

Essential to any research effort in this area is the need to seek out process-based and goal-driven integration points across ERM, Enterprise Information Security Policy, and controls based security and a framework for auditing in virtual environment. The following chapters will provide in-depth evaluation from scientific perspective and implementation approaches that is logically structured to support the proposed GRC model.

5.2. Summary

An integrated enterprise governance, risk and compliance model was developed where ERM acts as a platform both mitigating risk on one hand and as a framework for defining cost controls and quantifying revenue opportunities. The controls can be tightened or loosened based on the evaluation and audit process by applying various security policies. The model will help enterprises to maintain optimized risk management strategy, governance and enterprise information security policies in synchronization with each other and at the same time attain a high level of transparency and consistency with auditing and compliance requirement.

CHAPTER 6

IMPLEMENTING ENTERPRISE RISK MANAGEMENT

6.1. Enterprise Risk Management Framework

ERM initiatives are clearly not simple or fast to rollout since it requires strong support from top managers and a commitment from senior management. Corporate-wide councils needs to be chosen with care to ensure that all risks are included and fairly prioritized and each step of the process brings the potential for conflict with other business units. The rewards are well worth it. “For the business, it means ensuring that a much wider range of risks (including many that ERM efforts don’t fully consider, such as reputation, brand, and physical risks) are considered with an expert eye” (Hampton 2009). Security executives, who understand how ERM works and how it can help not only mitigate risks to save money, but also take advantage of opportunities and make money, should be given a place at the board level. Whether ERM can drive chance in an organization ultimately depends on whether management implements ERM in an integrated way. “When risk is used as an organizing principle, in the context of a risk strategy, management can take action in a coordinated and synergistic manner” (Hampton 2009). Using ERM to optimize its risks can help the organization perceived potential structural and/or strategic adjustments that can help enhance organizational effectiveness in building shareholder value. Ultimately, ERM requires the support of the CEO and the board, who drive it through the organization. For

any leader, however, undertaking all of the ERM process at one time can be daunting. The key is to start some where.

ERM is a modern risk management technique where a portfolio of risks is managed in a holistic manner (Beasley, Clune & Hermanson 2005). ERM has inspired interests from various parties including corporate executives, regulators, and rating agencies. Under the ERM framework, enterprises take on necessary risks to pursue their strategic objectives within their respective risk appetite. The core of the ERM process is efficient risk integration. Inter-relations among risks and risk prioritization are highlighted in the risk integration process under ERM. Certain risk measures and aggregation methods are usually involved in its implementation. Effective risk reporting and communication in a well-designed organizational structure are also essential for the success of ERM. Being a evolving process, the ultimate goal of ERM is to move beyond the initial incentive of fulfilling compliance needs to achieving real economic value.

The ERM provides leadership in the development, delivery and maintenance of an information security and risk management program that safeguards the organization's information assets and the supporting infrastructure against unauthorized use, disclosure, modification, damage or loss. The ERM supports a comprehensively program that encompasses information security implementation, monitoring, threat and vulnerability management, cyber incident management, and enterprises business continuity management. "The ERM works with executive branch to help them comply with legal and regulatory requirements, the statewide technical architecture, policies, industry best practices, and other requirements" (Mohan et al. 2008). Working

with government agencies and local authorities, citizens and private sector business, ERM helps to manage risk to support secure and sustainable information technology services to meet the needs of the citizens.

Enterprise risk management can become a strategic competitive advantage if it is used to identify specific action steps that enhance performance and optimize risk. "It can also influence business strategy by identifying potential adjustments related to previously unidentified opportunities and risks." (Mohan et al. 2008). Used appropriately, ERM thus becomes a means of helping the organization shift its focus from crisis response and compliance to evaluating risks in business strategies proactively, to enhancing investment decision-making and to improving shareholder value. Enterprises that develop an ERM framework for linking critical risks with business strategies can become highly formidable competitors in the quest to add value for shareholders.

6.2. Enterprise IT Risk Management Strategies

The researcher conducted a survey to ISACA members in Oman since they form a focused group of security practitioners in information security and risk management domains. The survey was administered during the first two weeks of May 2011 using the questionnaire that is presented in Appendix-B. There were sixty respondents out of one hundred and ten distributions making an average of 54.5 % response rate. Key findings from the survey illustrates that the practitioners are aware of enterprise information security and Risk Management frameworks. But most of them were unable to understand COSO, since it is too complex from an implementation perspective. Others said that they outsourced to third party consultants who unfortunately put checklists in the hands of relatively inexperienced individuals rather than

performing the in-depth analysis of business issues. Before “GONU”, security was viewed as a liability and most Chief Executive Officers’ (CEO) believed that security is a just technical problem and the responsibility lies with the IT managers. Hence, there was minimal or no comprehensive risk assessment and risk response as a result of which few ad-hoc controls were applied without periodic monitoring. Interestingly, “GONU” became an eye opener and the graph illustrates that there is a steady improvement in all the factors of information security and risk management.

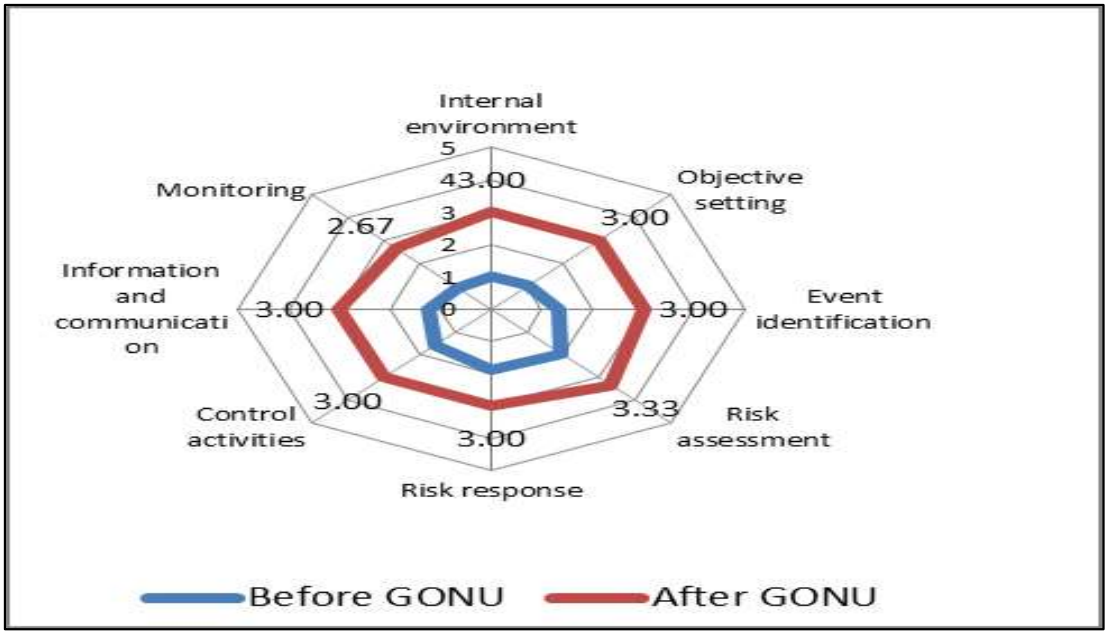


Figure 7 Chart showing the ERM perception before and after GONU

The radar chart in figure-7 illustrates the perception of ERM in Oman, before and after GONU. There was minimal or no comprehensive risk assessment and risk response before GONU as a result of which few controls were applied. It is evident that information security management initiatives gained momentum significantly after the cyclone which triggered active monitoring

and periodic reviews. This shows that enterprises realized the significance of enterprise risk management processes and information security governance.

The detailed findings and recommendations are summarized in table -1.

Table 1 Survey Findings and Recommendations

Security Theme	**Information Security Policy**
Finding	Executives have a fair knowledge about security policies but it is not implemented across the enterprise since it is not ratified and communicated across the enterprise.
Recommendation	Policies and standards must be created with well-defined roles and responsibilities. A formalized compliance program must be developed and closely monitored.
Security Theme	**Enterprise information security Architecture**
Finding	A few Project design artifacts and network diagrams do exist which are developed by IT managers and it solely depends on their expertise. No Security Architect role exists.
Recommendation	Enterprise information security architecture must be developed that is aligned to risk strategy and policies. A security architect role must exist who in turn seeks advice from security experts to architect secure solutions.
Security Theme	**Governance Structure**
Finding	Roles and responsibilities for IT security are not clearly defined and no formal governance structure exists. Security is handled in an ad hoc basis or addressed reactively.
Recommendation	Security Governance framework needs to created and aligned to risk strategy. Roles, Responsibilities must be spelled out clearly with Audit Processes and appropriate Controls implemented.
Security Theme	**Information Asset Profiling**
Finding	Asset classification is not done
Recommendation	Asset profiling process must be defined and operationalized which is aligned to risk strategy and governance process. Controls based on COBIT framework needs to be ratified and implemented.

Security Theme	Security Risk Management
Finding	Enterprise information security Risk Management strategy is somewhat missing.
Recommendation	Define and document enterprise information security strategy and information security policy with senior management commitment.
Security Theme	**Archiving**
Finding	Backup is taken regularly and stored locally
Recommendation	Archiving policy must be defined and information must be encrypted and stored at a remote location in safe and secure environment.
Security Theme	**Security in Business Continuity Planning**
Finding	Disaster recovery and business continuity plan is not in place and there is no formal enterprise risk management process.
Recommendation	Conduct a business impact analysis and develop, test DR/BC plan with established effective security strategies and policies.
Security Theme	**Awareness and Training**
Finding	There is no scheduled awareness training program. However management shows keen awareness only when an incident is reported but it loses focus over a period of time.
Recommendation	Training and awareness program must be scheduled periodically for all employees to ensure that all of them have basic knowledge of security issues.

Besides this, it was evident through interviews that, management tends to neglect security mechanisms that are in place. Hence, measuring and monitoring the effectiveness of security controls needs to be done periodically to provide clarity about the controls that are protecting the organizational assets. Next aspect that is found is that extended enterprises produce information supply chains which create interdependencies among business partners which are mostly ignored by the managers. In these situations,

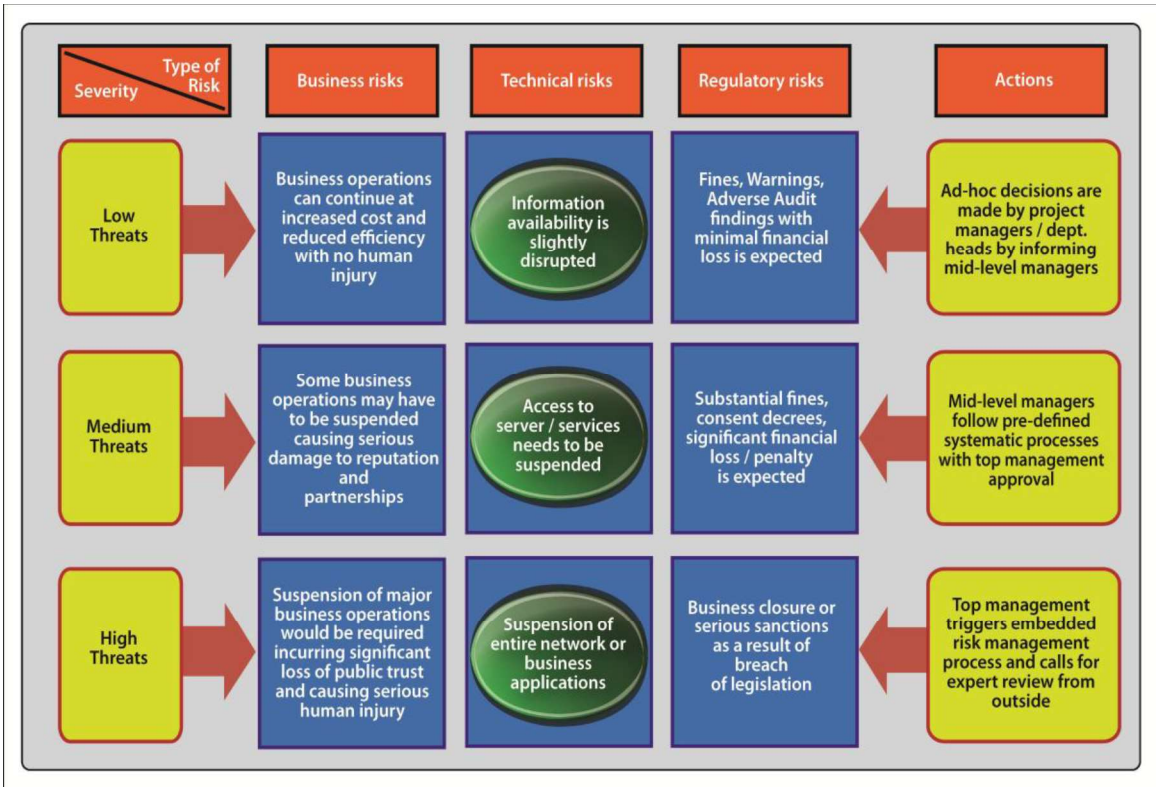
interdependency analysis using scenarios will be helpful. Also, it's evident that most managers underestimate insider threats and rarely attend to the business risks. Due to the cultural setup in Oman, social engineering attacks are relatively easy which is attributed to excessive trust in relationships. Therefore, attention should be given to create awareness among employees and manage business risks to avoid negative publicity which can lead to loss of reputation and brand value. Finally, the threat due to IT is mostly taken care; however it lacks proper documentation which is essential for risk management.

6.3. Classification of Risk Based on Severity and Consequence

A paper titled "An Exploratory Study of ERM Perception in Oman and Proposing a Maturity Model for Risk Optimization" was presented in the 9th Australian Information Security Management Conference (SECAU). It was stated that to achieve the recommendations presented in Table-1 an ERM program should be selected based on the severity of threats and consequences the enterprise actually faces. Hence, threats and consequences must be expressed in business related terms which should be easily understood by non-technical executives. The following table (Please refer Table-2) provides direction for classifying severity vs. consequence of risks. In this Table, the author has broadly classified risk into three types namely business risks, technical risks and regulatory risks. Based on the severity, there are three criteria set such as low, medium and high consequences. Further, for each criterion, the nature of decisions and the typical decision makers are defined. An ERM procedure normally consists of

a set of practices developed by a group with domain expertise who defines prudent controls and perspectives for protecting enterprise information. Security requirements depend on the domain such as healthcare which looks at HIPPAA standards and financial institutions look at SOX and so on.

Table 2 Classification of risks based on its severity



The above classifications will help the CEOs', CFO's and CIOs' to better understand the business risk and establish a standard of due care and derives from practical experience and knowledge in the business. The IT managers and enterprise information security architects will understand technical risks and develop enterprise information security architecture which is aligned to risk strategy and apply control standards to drive the security objectives of confidentiality integrity and availability. Legal advisors need to understand thoroughly the specific regulatory mandates for guidance and legal risks associated with contractors, vendors, employees, and national and

transnational jurisdictions. All risks are understood to a point where they can be accepted by authorized and accountable parties. If risks are not always formally accepted and change management is not consistently applied, it becomes difficult to manage risk within the risk appetite. Hence rrisk appetite needs to be linked to performance monitoring and reporting to fulfill an organizational need to assert progress internally and externally and to identify some framework to lean on. Although, COSO is a high-level control framework that requires management to look at risk-related issues and implement risk management processes, it is somewhat confusing that this requirement should be considered necessary for high-level executives in large enterprises. COSO is really the only viable candidate for top-level risk management which is also supported for regulatory compliance by SOX regulators, making it a de- facto standard for that purpose (Rasmussen & Koetzle 2007). While being complex and generic COSO ERM fails to give enough practical advice from an implementation viewpoint and the approach to ERM is confusing. Rasmussen & Koetzle (2007) in their research report argues that COSO ERM focuses excessively on threats/hazards but it fails to give practical guidance on how you should measure the effectiveness and efficiency of controls.

6.4. Proposed Enterprise Risk Management Approach

The vital parameters in deciding an appropriate enterprise risk management approach encompasses business risks, caused due to external entities, technical risks evolving due to extended networks and regulatory risks caused

due to cross-border relations as a result of outsourcing in Oman. The spectrum generally runs from ad-hoc approach used with due diligence by relatively low level employees to an integrated enterprise risk management achieved through system analysis approach. In the informal stage, enterprises use manual controls with no best practices whereas in reactive stage, it's more project oriented and compliance based. In proactive stage, automated risk assessment and monitoring is done with appropriate process control in place whereas in the optimized stage of maturity, automated risk mitigation/predictive risk analysis is done with an integrated ERM process. The following figure-8 illustrates such an approach.

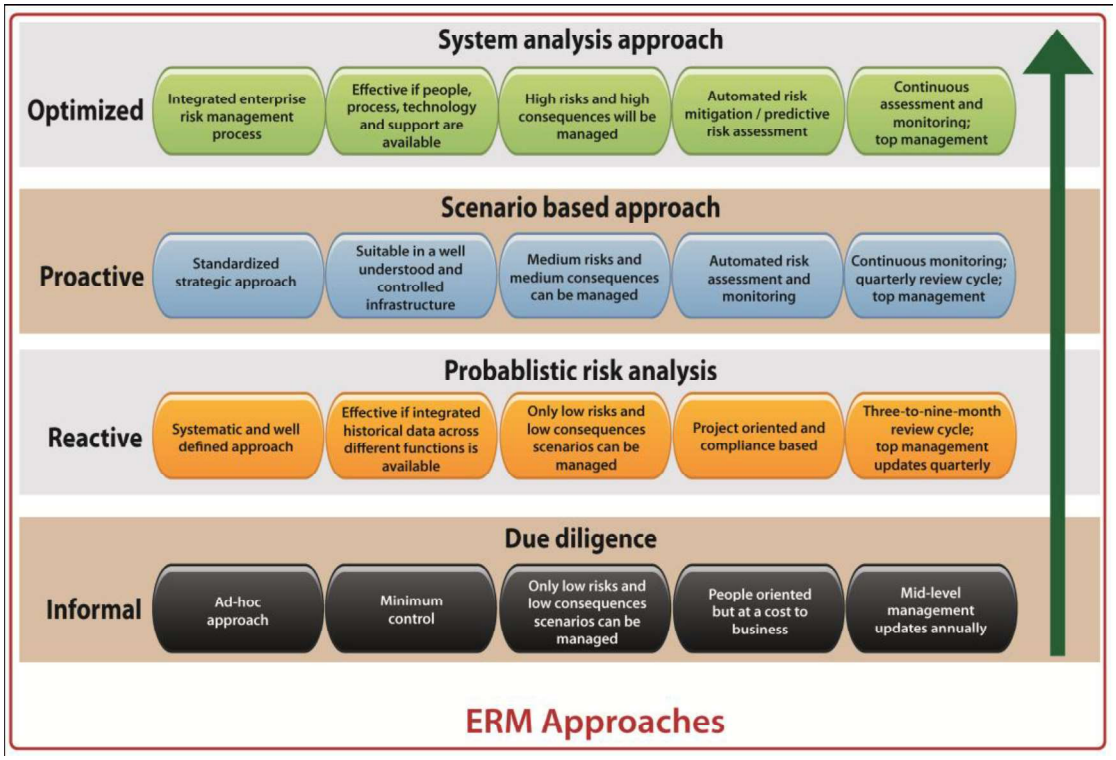


Figure 8 ERM Approaches

Due diligence: By this approach, operational managers make ad-hoc decisions with mid-managers approval. This approach is mostly people

oriented rather than process oriented, where the decisions made are biased towards the individual's opinion and capabilities rather than giving significance to the organizational objectives. Operational managers assume that things are perfect, since nothing untoward has happened which eventually increases the trust in existing systems and protection mechanisms. This approach should be applied at bare minimum although it is not sufficient but can address low risks with low consequences. Hence, mid-managers should review based on detected incidents to ensure the consequences remain low in all such systems.

Probabilistic risk assessment: Probabilistic risk assessment can help in quantifying security risks for both externally initiated and internally initiated events by understanding the likelihood of occurrence and the consequences (Satoh & Kumamoto 2009). This approach is effective when there is access to integrated historical data across different functions and the frequency of change is slow. However debated, managers should take care when interpreting historical InfoSec data especially with new technologies and new threat environments. To gain high assurance in low to medium consequence systems, enterprises need redundant protective measures. When there is inadequate historical data available to perform gap analysis expert consultative guidance can be obtained in order to avoid misinterpretation or misunderstanding of threats and consequences.

Scenario based risk assessment: Scenario based risk assessment is useful in a controlled environment where "what-if" scenarios can be explored and group consensus can be considered. Scenarios are generated to try to cover important events and outcomes. These scenarios can be "gamed" to explore

various options and generate group agreement for dealing with the medium-risks. Reports can be generated with risk management options to facilitate management decisions.

System analysis: This is suitable for high risk situations which are tedious and costly since a sequence of events and interactions between disparate systems needs to be evaluated. It is applicable for analysis of petrochemical plants and defense organizations where the consequences are high. Normally managers ignore interdependencies among business partners, logistics outsourcing and ignore indirect losses. In high-consequence systems, managers should conduct interdependent system analyses with increasing detail at higher levels of threats and consequences. As discussed in this chapter an enterprise should mature from informal state to optimized state by having an integrated risk profile based on the severity of threats and consequences.

6.5. Summary

This chapter addresses the significance of ERM in today's business context which involves external partners, suppliers, vendors and customers interacting from across different nations. Questionaries' were deployed among a cluster of companies in Oman to find the perception of ERM and the findings were analyzed. Based on the findings, COSO implementation issues were identified, risk grouping have been done and a maturity model was proposed to attain optimal risk management. Suitable recommendations were provided which enables enterprises to mature from an informal adhoc approach to an optimized integrated enterprise risk management process through continuous assessment and monitoring. This chapter outlines the

ERM approaches such as due diligence, probabilistic risk analysis, scenario-based analysis and system analysis which offer a wide range of decision making tools to the top management.

CHAPTER 7

IMPLEMENTING IT GOVERNANCE

7.1. Enterprise Vulnerability Analysis

Many enterprises have engaged in the design and development and delivery of content, in addition to providing timely electronic services to citizens of Oman have grown significantly in the last five years. Assessing and measuring, analysing and providing corrective strategies to strengthen weak areas of the enterprise' Information Systems is the purpose of vulnerability assessment.

In the area of application delivery platforms, enterprises are quite vulnerable to security lapses on the one hand and the continual advances in technologies on the other. These two dominant trends in the industry are pulling the enterprises in two directions from an information security strategy standpoint. Here the concentration is on how to secure the entire platform to ensure a high level of data redundancy and the ability to attain high levels of performance as defined by Service Level Agreements (SLAs) (Saleh, Refai & Mashhour 2011). The security levels for the IT infrastructure are also defined in written contracts to vendors, often specifically defined in clauses within contracts and SLA acceleration clauses that reward the vendors for providing the necessary services . By actively providing seamless access to get more of their applications and content, the vulnerabilities with regard to their security systems and practices are placed under increasing stress, thus exposed to more threats. This vulnerability assessment explains the most pressing

threats and provides insights into how best to alleviate them.

The vulnerability assessment of the Enterprise provided insights into three major security issues the company faces today as it attempts to grow its application hosting service. The first and most significant is protecting the proprietary nature of citizen's data. During the vulnerability assessment and audit, the ability of technicians to get access to several different private accounts' data when stored on the same physical server was the most severe. The second-most significant security issue facing the enterprise' Application Hosting Services Division is the lack of consistency to audit data history and analysis. There are security audits back through 2007, none for 2004 to 2006, and a very preliminary one when the company first launched this aspect of their service. There are literally no records or audit data for 2004. This lack of audit data is very significant and puts it at significant risk in terms of managing its SLAs and with greater accuracy than others. The third most significant finding is how integration between the many legacy and 3rd party systems that it relies on are not functioning with real-time data feeds and a high level of secured communication. These legacy systems lack encryption; support for single sign-on authentication and advanced proxy server support across all on application platforms.

7.2. Scope of Assessment

The scope of this vulnerability assessment concentrates on the three most severe areas that the security audit discovered. These are first the proprietary nature of citizen's data; second, the lack of consistency in audit data history and analysis; and third, the lack of secured integration between

the many legacy and 3rd party systems. There are also system-wide vulnerabilities with regard to gaining access and using the Internet, with a lack of best practices in the area of proxy server support for legacy systems. In one instance, database was accessible directly from the Internet, without a proxy server acting as the security authentication point. This is just one of many examples from the vulnerability assessment which showed how critical it is for systems to have more processes to strengthen this weakest area. In completing the vulnerability assessment the following activities are within the scope of the project and have been completed under condition of anonymity of respondents:

- Interviews with members of the IT department including the director of IT, Head of business development and the managers in charge of IT policy, IT system administration, in addition to network facilities management.
- Analysis of Service Level Agreement (SLA) and its audited reports of information security management over time.
- Completion of a randomized series of network scans from outside the company to evaluate each area of potential failure, and also track the success rate of bots designed to penetrate legacy systems. These legacy systems are not protected via proxy servers as of today.
- Evaluation or testing of disaster recovery plans; business continuity plans and the scope of emergency response plans from the standpoint of uptime were tested despite their integral role in SLAs and customer warranties.

7.3. Threat and Vulnerabilities Assessment

Threats to Enterprise

- The Enterprise is also lacking a consistent flow or feed of oversight data for post-incident investigations and audits. There are no enterprise dashboards that provide IT management with the ability to validate that their security programs and initiatives are working either. There is however more broad-based metrics that show overall performance the company relies on to evaluate its security strategies.
- Subcontractors with access to citizen's key account data and systems could easily steal the most critical details out of customer records and either resell them or unethically profit for its use. The Enterprise presently has over 25 different subcontractors working on its content development and application hosting services. The following figures-9 to 11 illustrates the summary of vulnerabilities.

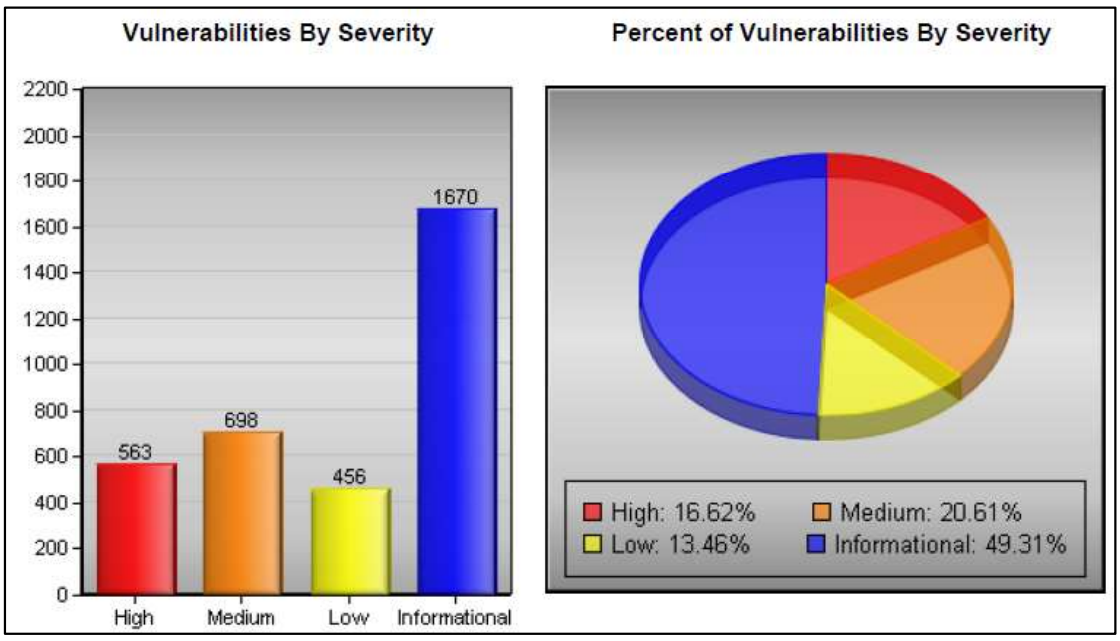
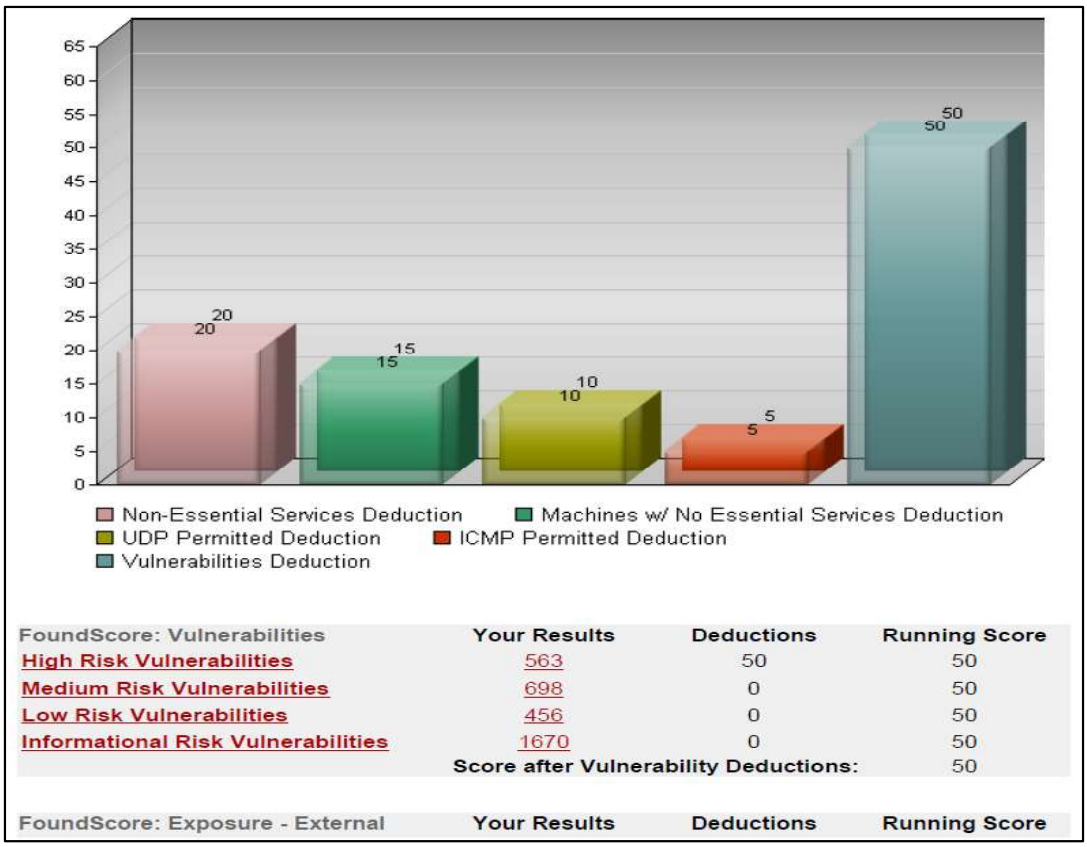


Figure 9 Summary of vulnerabilities based on risk factor



FoundScore: Vulnerabilities	Your Results	Deductions	Running Score
High Risk Vulnerabilities	563	50	50
Medium Risk Vulnerabilities	698	0	50
Low Risk Vulnerabilities	456	0	50
Informational Risk Vulnerabilities	1670	0	50
	Score after Vulnerability Deductions:		50

FoundScore: Exposure - External	Your Results	Deductions	Running Score

Figure 10 Summary of vulnerabilities based on services

Vulnerabilities By Risk

Risk Level	Vulnerability Name	Hosts Discovered	Affected System(s)
High	Oracle Java SE Critical Patch Update June 2011	1	10.146.41.220, vm1001-mobse, VM1001-MOBSE
High	HP Data Protector Client EXEC_CMD Omni_chk_ds.sh Remote Code Execution	10	10.146.4.15, hqxorph01.moj.local, HQXORPH01 10.146.4.30, fingerprint.moj.local, FINGERPRINT 10.146.4.6, hqxeoffice02.moj.local, HQXEOFFICE02 10.146.4.7, hqxeoffice03.moj.local, HQXEOFFICE03 10.146.5.5, hqxivr01.moj.local, HQXIVR01 10.146.7.6, hqxfdc01.moj.local, HQXFDC01 10.146.7.7, hqxfdc02.moj.local, HQXFDC02 10.146.8.18, hqxsccm.moj.local, HQXSCCM 10.146.8.3, hqxbck01.moj.local, HQXBCK01 10.146.8.6, hqxapp.moj.local, HQXAPP
High	HP Data Protector Client EXEC_CMD Perl Remote Code Execution	10	10.146.4.15, hqxorph01.moj.local, HQXORPH01 10.146.4.30, fingerprint.moj.local, FINGERPRINT 10.146.4.6, hqxeoffice02.moj.local, HQXEOFFICE02 10.146.4.7, hqxeoffice03.moj.local, HQXEOFFICE03 10.146.5.5, hqxivr01.moj.local, HQXIVR01 10.146.7.6, hqxfdc01.moj.local, HQXFDC01 10.146.7.7, hqxfdc02.moj.local, HQXFDC02 10.146.8.18, hqxsccm.moj.local, HQXSCCM 10.146.8.3, hqxbck01.moj.local, HQXBCK01 10.146.8.6, hqxapp.moj.local, HQXAPP

Figure 11 Summary of High Risk Systems

7.4. IT Governance Framework

The above said problems call for a robust IT governance framework like COBIT that delivers measurable value to the business while improving the productivity. COBIT 4.1 is identified has a widely adopted framework for IT governance. However, research articulates that, the breadth and depth of COBIT is exhaustive which makes it almost impossible for medium and large enterprises to implement and reap the benefits. In order to achieve governance through COBIT with limited resources and time, IT Governance Institute recommends using the "COBIT Quick Start" as the baseline which can further be broadened depending on the size and type of the enterprise (IT Governance Institute 2007). So, it becomes evident that focusing on the critical success factors will address the most important processes which directly influence the enterprise's performance. The critical success factors were identified by exploring the processes and control objectives that are listed in quick start guide. The various dimensions of the enterprise such as Simple Command Structure (SCS), Short Communications Path (SCP), Span of Control (SOC), IT Sophistication (ITS), IT's Strategic Importance (ITI), IT Expenditure (ITE) and Segregation (SEG) was tested using the suitability assessment tool [19]. The analysis of the results which is shown in figure-12 illustrates that Quick start is suitable for the identified enterprise.

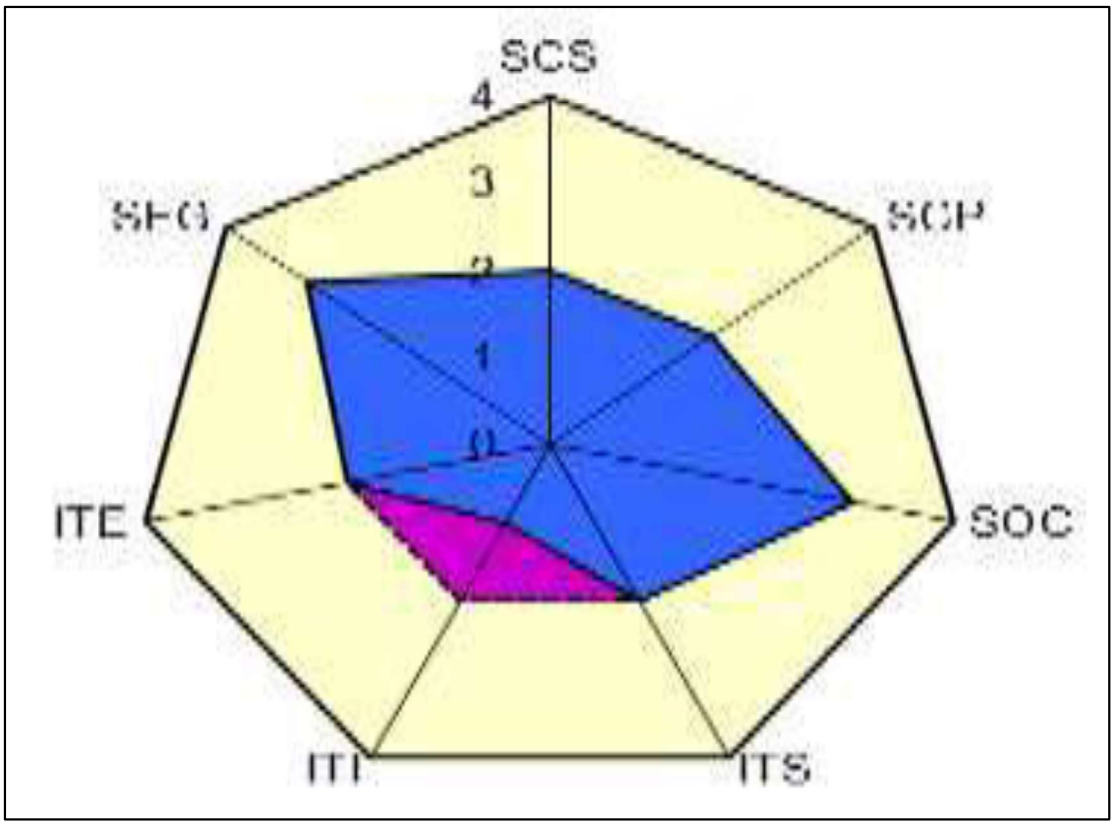


Figure 12 Suitability Assessment

If the results from the assessment are contained mainly in the blue zone then the enterprise can launch a governance initiative using COBIT.

Simple Command Structure (SCS) is indicates primarily informal and verbal control which are tactically medium-term-oriented.

Short Communications Path (SCP) shows that head of entity knows most people's IT-related responsibilities and as a result Span of Control (SOC) implies that he directs and monitors only key personnel's IT-related responsibilities.

IT Sophistication (ITS) indicates that the enterprise is adopting standard technology components like their peers.

IT Strategic Importance (ITI) specifies that reliable IT support is critical to the enterprise's current business operation.

IT Expenditure (ITE) shows that IT expenditure is different from peers and only marginally increasing every year.

Segregation (SEG) implies that monitoring is totally segregated, but design and implementation can be executed by the same person.

After evaluating the 210 control objectives, 24 were carefully selected that are constructively aligned to the enterprise's goals. Although COBIT provides direction to IT governance, it rarely defines the implementation details.

Analysing and providing corrective IT governance strategies by mapping the four domains of COBIT with various best practices and to secure the entire infrastructure to ensure a high level of data availability and the ability to attain high levels of performance through accountability is the main purpose of this effort. Literature provides mapping of COBIT with various best practices such as PRINCE2, ISO 27001and ITIL but the overall mapping of COBIT with any one of the above said best practice is still not suitable from an implementation perspective.

To reap the benefits of best practices based on their proven strength, each domain of COBIT is mapped with a specific best practice which is shown in the figure-13. For example Plan and Organize (PO) domain should make use of PRINCE2 since it provides structured methodology to manage and organize resources strategically.

Similarly, ISO 27001 is an internationally acclaimed standard for Information security management in order to protect the confidentiality, integrity and availability of information. Hence this standard is mapped with Acquire and Implement (AI) and Monitor and Evaluate (ME) to achieve compliance through auditing and operationalizing security policies. Likewise, Delivery and Support

(DS) domain perfectly maps with the ITIL which is the most popular IT service management framework.

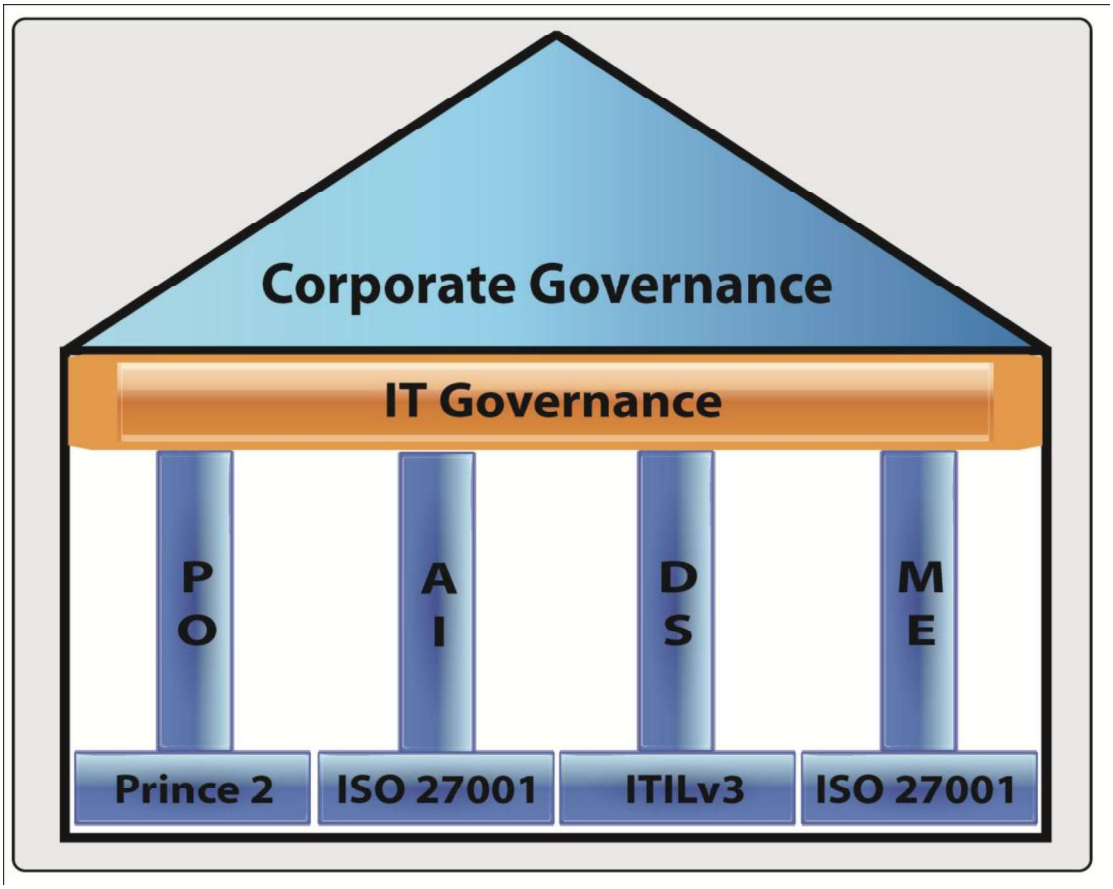


Figure 13 Domain mapping with best practices

7.5. Summary

In this chapter vulnerability assessment of the enterprise has provided insights into three major security issues the company faces today as it attempts to grow its application hosting service. In-depth interviews and analysis of Service Level Agreement (SLA) and randomized series of network scans revealed various threats and vulnerabilities. A framework for implementing IT governance using COBIT, focusing on critical success factors was developed.

CHAPTER 8

STRATEGIES FOR BUSINESS CONTINUITY

8.1. Business Continuity and Disaster Management

Disaster recovery and business continuity planning are processes that help enterprises to get ready for disruptive events, whether an event might be a tornado or simple power outage caused by an accident. Senior Management's commitment and participation in this process can vary from managing the plan, to providing input and support, to placing the plan into operation during an emergency (CXO Media Inc 2006).

Cyclone Gonu showed that enterprises across Oman and United Arab Emirates had to pay a huge price for not having proper disaster recovery/business continuity (Saidani, Shibani & Alawadi 2013). Hence due to increased dependence on IT systems and services it is now normally acknowledged that business continuity planning and disaster recovery are crucial activities (Al-Badi et al. 2009). Yet, the formation of and maintenance of a comprehensive business continuity and disaster recovery plan, is a multifaceted undertaking, involving a series of processes. Prior to creation of the plan itself, it is necessary to consider the possible impacts of disaster and to comprehend the underlying risks. Business Impact Analysis (BIA) must be performed by identifying critical processes and corresponding information systems, considering both internal and external environments that impact financial position as well as the goodwill of the enterprises (Sikdar 2011). This is the basis upon which a comprehensive business continuity plan or disaster

recovery plan should be constructed (CXO Media Inc 2006). The various processes involved in the development of comprehensive business continuity and disaster recovery implementation plan is shown in figure-14.

Figure 14 Processes involved in BCP and DR implementation (Adopted from Business Continuity Management by EC-council.org)

8.2. Business Impact and Risk Analysis

The first step in a rational business continuity process is to think about the probable impacts of each kind of disaster or event by gathering information and date analysis. Having arrived at the impacts, it is now just as important to consider the extent of the risks which could result in these impacts. Again, this is a critical activity as it will establish which scenarios are most likely to take place and which should draw most attention throughout the planning process (CXO Media Inc 2006).

The goal of BIA is to define objectives for the recovery of host computing systems that run the applications that support the business processes and also factoring external dependencies such as suppliers and outsourced service providers (Sikdar 2011). These objectives are declared as the Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO is the time in which systems, activities, applications or functions must be recovered after an outage to resume critical functions. The RTO has to be less than the maximum tolerable period of disruption (MTPoD). RPO describes the maximum amount of data loss the business unit can sustain during an event. For instance, if the RPO is 10 hours, systems should be restored in the state they were in no longer than 10 hours ago. The technical disaster recovery strategy depends upon meeting RTO and RPO stipulations for the critical processes. The RTO and RPO requirements establish which option of disaster recovery plan to put into practice (Bahan 2003). Higher the data availability, the lower the RTO and RPO which makes recovery time and how current data is, the key parameters in determining the level of service a

business process necessitates in the event of a major disturbance. In order to properly put into practice a disaster recovery plan, one must know the RTO and RPO that the enterprise is willing to recognize in case of a disaster. The business continuity management policy and technical disaster recovery strategy of dissimilar options of recovery is based upon an amalgamation of these requirements (Bahan 2003).

BIA is not risk management, which focuses on identifying threats, vulnerabilities, and attacks to determine controls and cost of the protective measure against the value of the asset (Sikdar 2011). Security risk breakdown, otherwise known as risk assessment, is primary to the security of any enterprise which is necessary in ensuring that controls and expenditure are completely appropriate with the risks to which the enterprise is exposed. However, a lot of conventional methods for performing security risk investigation are becoming more and more unsustainable in terms of usability, flexibility, and critically. Security in any system should be proportionate with its risks. However, the process to establish which security controls are suitable and cost effective is quite frequently a multifaceted and sometimes a subjective matter. One of the prime functions of security risk analysis is to put this procedure onto a more objective basis. There are quantities of distinct advances to risk analysis that can be essentially put into two categories: quantitative and qualitative to acquire risk intelligence (CXO Media Inc 2006).

8.3. Quantitative Risk Analysis

This approach uses two fundamental elements; the likelihood of an event occurring and the likely loss should it happen based on independent objective metrics and can be expressed in a management-specific language (e.g.,

monetary value, percentages, probabilities) (Fariborz et al. 2003). “Quantitative risk analysis makes use of a single figure produced from these elements which is called the Annual Loss Expectancy (ALE) or the Estimated Annual Cost (EAC)” that involves complex calculations (riskworld.net 2003).

This approach can help in quantifying security risks for both externally initiated and internally initiated events by understanding the likelihood of occurrence and the consequences (Satoh & Kumamoto 2009). This approach is effective when there is access to integrated historical data across different functions and the frequency of change is slow. It is consequently hypothetically possible to rank events in order of risk (ALE) and to make decisions founded upon this. The problems with this kind of risk analysis are typically connected with the unreliability and inaccuracy of the data since it is not easy to assess risks and put value on damages. Probability can hardly ever be precise and can, in some cases, encourage complacency since metrics in the security space are generally lacking across the board, and there are reasons to believe that for at least some risks, good metrics are impossible because the risks are not quantifiable in principle. In addition, controls and countermeasures frequently tackle a number of possible events and the events themselves are regularly interrelated. In spite of the disadvantages, a number of companies have effectively implemented quantitative risk analysis with various tools (CXO Media Inc 2006).

8.4. Qualitative Risk Analysis

This approach is useful in a controlled environment where what-if scenarios can be explored and group consensus can be considered. Scenarios are generated to try to cover important events and outcomes. These scenarios

can be “gamed” to explore various options and generate group agreement for dealing with the medium-risks. This is suitable for high risk situations which are tedious and costly since a sequence of events and interactions between disparate systems needs to be evaluated. It is applicable for analysis of petrochemical plants and defense organizations where the consequences are high. Normally managers ignore interdependencies among business partners, logistics outsourcing and ignore indirect losses. In high-consequence systems, managers should conduct interdependent system analysis with increasing detail at higher levels of threats and consequences. Enterprise information security policies define high-level controls to mitigate risks by promoting the security objectives.

To achieve the objectives, enterprises develop a security posture or protection portfolio that balances deterrent, preventive, detective, and reactive process or technology mechanisms. Feedback in the form of audits, performance measurement, and other monitoring helps the enterprise adapt security technologies and other components within the context of business risk management. Business needs are not perfectly fulfilled by technology, and technology must therefore be closely controlled in order to have meaningful business effect. Technologies must be interwoven with risk management and other business processes involving people. The architecture is driven by enterprise information security objectives, determined by the chosen security postures, and influenced by the business context

8.5. Leadership and Training

Leadership behavior in communicating and inculcating confidence among team members taking into account peoples’ emotions and attitudes is vital.

Leadership is crucial part of business continuity and recovery since it involves psychological aspect of crisis management. The crisis management and response teams must be educated about their roles and responsibilities periodically. This helps them to be effective in their duties as the testing complexity is increased eventually. The leader possesses the overall knowledge of the scenario and supervises the testing exercise. Based on the result of the exercise the Business Continuity Plan (BCP) will be modified reflecting the critical lessons learned during testing. All staff must be aware of all continuity processes, procedures and infrastructure solutions along their individual role during and after a disaster. The roles and responsibility matrix is developed and communicated to all staff and contractors to raise consciousness and increase the company's readiness. This will ensure at a bare minimum what people should know what to do and what not to do if a crisis were to take place. A focused training program should be developed with mock drills testing and validation for all staff directly responsible for performing recovery and crisis management (CXO Media Inc 2006). Senior management commitment is essential for driving training and awareness activities for business continuity/disaster recovery programs. Motivation from senior management will help raise awareness and increase active participation in the training program (Kirvan 2012). "If it's feasible they should require all individuals other than business continuity/disaster recovery team members, to take part in at least one training session every year, that should support their acceptance and strengthen the importance of business continuity/disaster recovery efforts" (Kirvan 2012).

Another significant strategy is to leverage the Internet since most contemporary enterprises have internet infrastructure. “If an organization has its own intranet with web pages, they should introduce a business continuity/disaster recover web page that describes what the overall business continuity/disaster recovery program does, and include sections on training, frequently asked questions (FAQs), and click-on links to forums and services, schedules and other useful materials” (Kirvan 2012). A well-designed training component should be included in all business continuity/disaster recovery programs in order to exploit the initiatives and ensure that employees are ready to respond when the unthinkable like GONU took place (Kirvan 2012).

8.6. Business Continuity Plan

The business continuity plan deals with how, where, when, and who will be accountable and what they will do when a major disaster takes place. This very well may be a situation where one is starting from scratch, up to and including the loss of the use and access to the primary location, either momentarily or long term, but it also includes a lot of other degrees of disaster. The disaster could be the consequence of incidents such as floods, fires, explosion, contamination, storms, terrorist activities, political unrest, war and many others whose impact may not be plainly evident. Any one or a mixture of these can result in one needing to rebuild their critical infrastructure solutions, possibly in a new location, in the shortest period of time possible. This is where the business resumption plan, completely dependent upon the disaster recovery plan for its achievement, comes in. If one has taken the time to think things through, successfully planned, implemented, and tested

their disaster recovery plan they are on their way to getting back to business (Freeman 2002).

8.7. Disaster Recovery Plan

A sound disaster recovery plan is necessary to guard the well-being of an enterprise from business process disaster, classified asset loss, regulatory liability, customer service failure or damage to brand value. A disaster recovery plan is a comprehensive document that summarizes the procedures for bringing the business back online after a disaster or other emergency in the primary site. It should recognize the key staff, vendors, suppliers, supporting IT infrastructure and critical assets that can recovered on priority. It's vital to identify key workers in the recovery plan. "For a larger business, there might be one representative from each department on the business recovery team" (Hostway 2007). Enterprises should make a list of their key suppliers and most key customers. Look at their locations and the disaster risks they face. These are problems as well. If one finds themselves heavily reliant on one or two key suppliers, their best bet is to find alternate suppliers, in a different geographic location, and begin building relationships with them before they find themselves in a desperate situation. Diversifying ones customer base will help them survive as well. One should make sure it has all of the communications and power resources that will be needed and create a plan for bringing them to the primary site when needed (Hostway 2007).

Communication is very important during an emergency. One should start the communication plan by making a list of key staff those who needs to be contacted in an emergency. This list should start with the managers, and ask each of them to keep a contact list for their staff. Contact information for

important suppliers and customers who you may want to keep in the loop should be included. Some examples include things like payroll data, financial records, strategic plans and insurance records. This is an enduring process and must be done before a disaster strikes. The business recovery plan will include instructions for retrieving this information (Hostway 2007).

8.8. Contingency Plan

Contingency plans are substitute plans that can be put into effect if certain key events do not take place as expected. If contingency plans are not available before a disaster then enterprises will have to source alternate supplier, vendors and resources at a higher price. Contingency planning helps an enterprises to get into a better position to cope effectively with the unpredictable since the actions and resources actually needed depend on the precise nature of the disaster that occur (Gary & Rob 2011). It guarantees enterprises to stay away from the shock of a complete surprise minimizing the fear, doubt when something unthinkable happens. Operations can halt or at least be messed up during emergencies. Thinking ahead and preparing for events that may follow a tragedy allows a company to stay in forward motion. An enterprise with a contingency plan is more likely to react sensibly to an unintentional situation than a firm without a one. Those who have played through possible crises and their reactions to those events avoid panic and damage to the firm and its operations when the real time comes. Contingency planning forces managers to think in terms of possible outcomes. The contingency planning process allows managers to brainstorm and come up with many possible outcomes, preparing for the worst (Mitome & Speer 2001).

Maintenance of the business continuity/disaster recovery plan is critical to the accomplishment of an actual recovery. The plans must reveal changes to the environments that are supported by the plans and be up to date. It is vital that existing change management processes are amended to consider recovery plan maintenance. In areas where change management does not exist, change management procedures should be recommended and implemented.

.

8.9. Summary

The business continuity plan resumes business processes and the disaster recovery plan resumes the IT systems. The purpose of a disaster recovery plan is to restore the operability of systems that support critical business processes to normal operation as promptly as possible. Business continuity planning brings together the business resumption plan, emergency response plan, crisis management plan, continuity of operations plan, and disaster recovery plan. DR/BC plans can be easily implemented as a private cloud service based on the analysis of the cost, RPO and RTO in a cloud service.

Site-to-site replication of VMs and data can be done rapidly which makes disaster recovery and business continuity much more financially attainable with the utilization of cloud technologies. Thus virtualization enables real time replication and high availability, with minimum resource that justifies the return on investment (ROI) and also facilitates in DR testing.

CHAPTER 9

IMPLEMENTING SERVER VIRTUALIZATION

9.1. Significance of Virtualization

Information Technology has witnessed the continuing development of the Internet from its original communication purpose (electronic mail) and Information dissemination (websites) to a platform for Web applications deployment, where increased computing and storage capabilities are constantly being made available to end users systems.

To accommodate this enterprises are deploying robust data centres which are growing in size and complexity in order to achieve high availability and provide scalability. As a result of this more physical servers are added which requires more floor space and power. In spite of this single point of failure and demands for powerful machines coupled with performance issues continue to haunt the enterprise due to unexpected peak time.

As the sizes of IT infrastructure continue to grow, cloud computing is a natural extension of virtualization technologies that enable scalable management of virtual machines over a plethora of physically (Li et al. 2012).

When you think of providing a secure cloud computing solution, it is important to decide on the type of cloud to be implemented. Currently there are three major types of cloud deployment models which can be deployed namely public, private and hybrid cloud. A public cloud is a model which allows users'

access to the cloud via interfaces using mainstream web browsers. A private cloud is set up within an enterprise's internal enterprise data centre which is easier to align with security, compliance, and regulatory requirements, and provides more enterprise control over deployment and use. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the enterprise itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network (Global Netoptex Inc 2009). It provides virtual IT solutions through a mix of both public and private clouds.

Speitkamp & Bichler (2010) argues that many physical servers are underutilized and hence combining multiple underutilized servers into a single larger system can result in significant cost savings and minimize administrative cost. Consolidating all the mail servers into one private cloud will minimize the threats and vulnerabilities as the most recent version of the mail server can be used, patched with security updates and also the license cost can be reduced drastically.

9.2. Analysis of Mail Server Implementation

Based on the research survey conducted in the Sultanate, it was identified that majority of the enterprises have implemented a Microsoft network

infrastructure with Domain Controller, Additional Domain Controller, Microsoft Exchange Server and Microsoft Internet Security and Acceleration (ISA) server. Over a period, these enterprises have grown exponentially with relatively large number of users having large volumes of data being exchanged across different geographical locations. This has led to the implementation of large data centres with more dedicated servers to run business applications, which in turn demand more floor space, energy, and additional administration overhead. Forrest et. al. (2008) in their research article states that the Enterprise-Scale data centres account for approximately half of corporate energy use and resulting carbon footprint (Forrest 2008). The research report by Forester Inc. confirms this argument by delineating that "the power consumption of data centres exceeding a combined $10 billion in the EU and U.S. in 2007 and expected to double again by 2011" (Bartels 2009). There is a global awareness to promote green computing and it is apparent that green computing initiatives are prioritized (Hamm 2008).

A questionnaire was also later deployed among a cluster of ministries in Oman to identify how many different versions of exchange servers are being used in various ministries. Many ministries used older versions of exchange which are vulnerable to attack since some of them are not patched properly and some are not currently supported by the vendor (please refer figure-15 & 16).

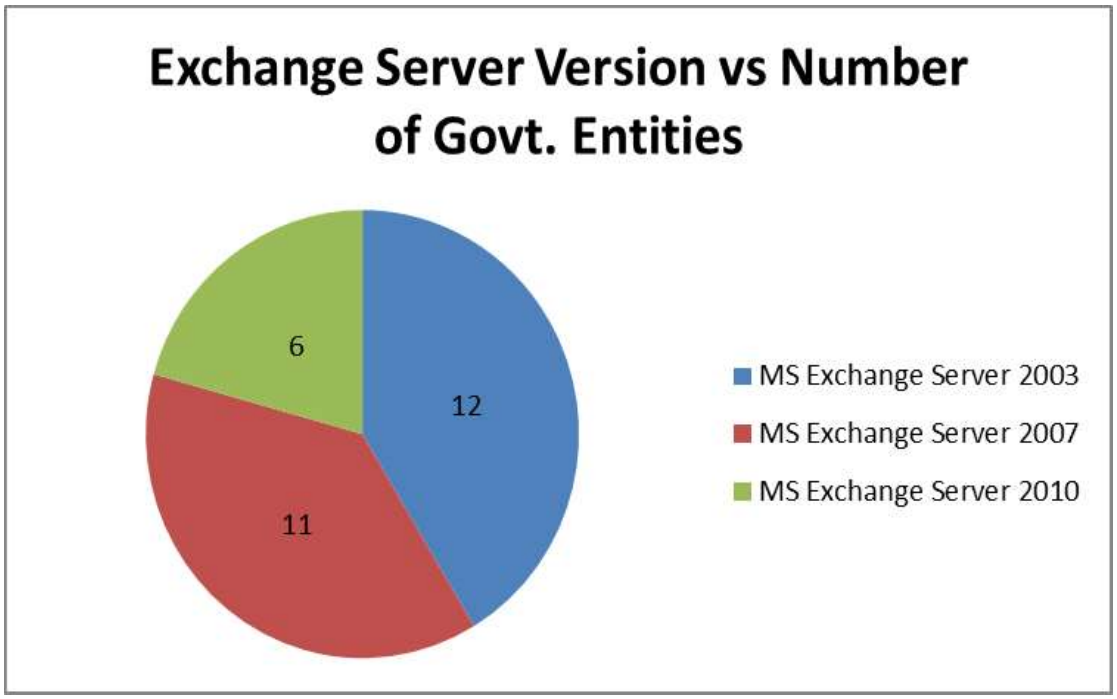


Figure 15 Summary of various Exchange Server Deployments

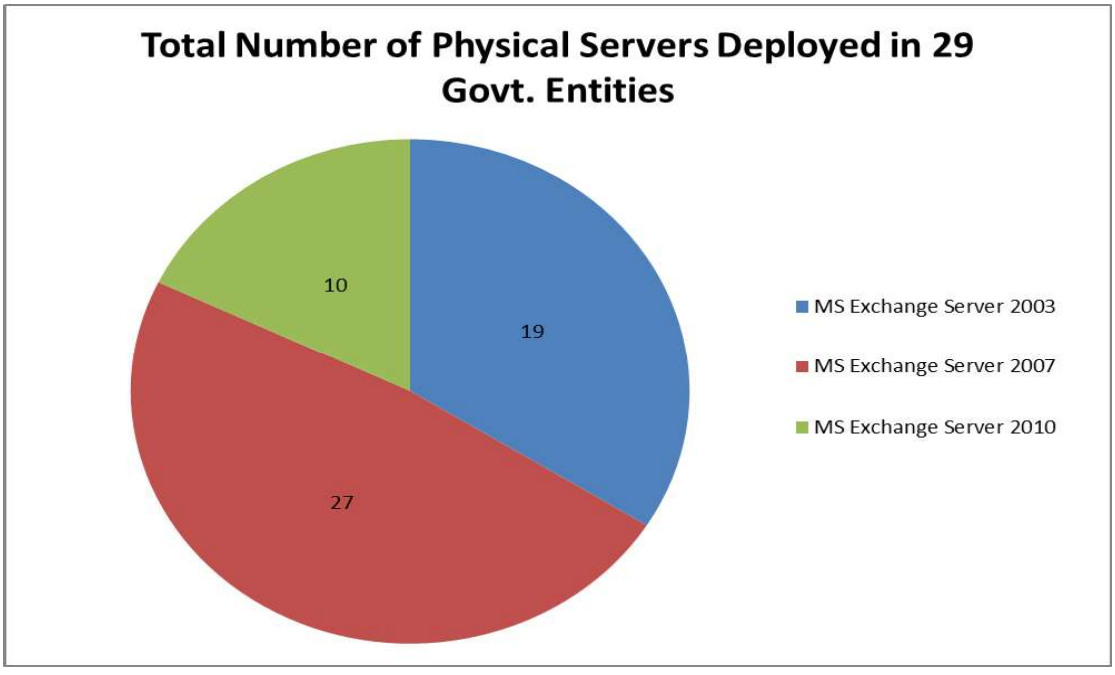


Figure 16 Total number of Physical Email Servers in Utilization

It was suggested to consolidate all the mail servers into one private cloud and provide email services to all the ministries thus improving the server utilization, data centre efficiency and enhanced security.

There are two types of virtualization Type-II and Type-I. The type-II virtualization is known as hosted virtualization where the hypervisor runs on top of the host operating system (Karen et al. 2008). According to Ray and Schultz, all virtual machines and its applications are vulnerable if the underlying host operating system is exploited (Ray & Schultz 2009). Recent developments in virtualization have eliminated the need for host operating system thus introducing the novel technique called as, bare metal virtualization, which is also called as native virtualization or Type-I virtualization as shown in figure-17.

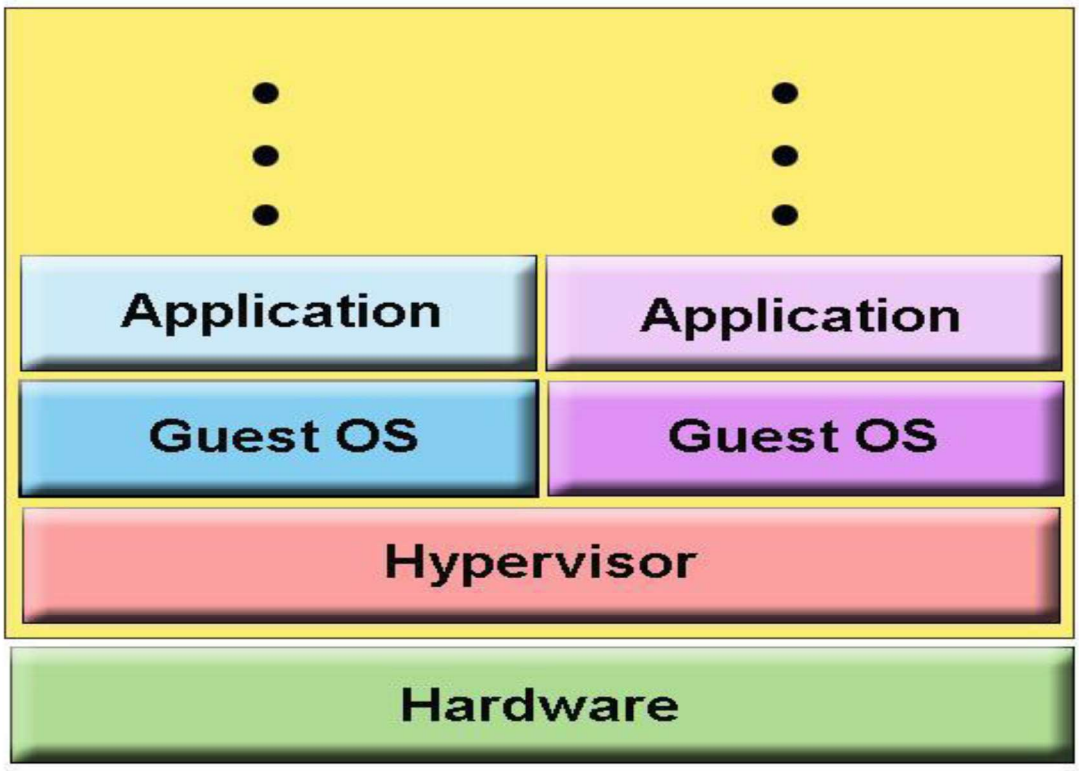


Figure 17 Bare metal Hypervisor Architecture

In this type, the hypervisor runs directly on the underlying hardware, without a host operating system. The hypervisor can also be built into the computer's firmware. This bare metal virtualization improves security, since the possible vulnerabilities of the host operating systems are eliminated. To achieve this, a

well-secured hypervisor and a proper hardening process must be in place (Karen et al. 2008). Hypervisors have specialized management functions that allow multiple virtual machines to co-exist peacefully while sharing physical machine resources. Virtual machines can also provide opportunities for software consolidation and reduced licensing costs (Daniels 2009). Another features of virtualization called as Server consolidation; a process of combining the workloads of several different servers on a set of target server. According to VMware, the traditional approach of one server for one application is over provisioning and leads to the underutilization of the servers. In addition, it states, “most servers operate at only about 5-15% of their total load capacity” (VMware, Inc 2010). The utilization of servers can be significantly improved by server consolidation. As revealed by VMware, “virtualized servers increase the utilization of server hardware from 10-15% to as much as 80%” (VMware, Inc 2010). For many enterprises, server consolidation becomes a key factor in implementing virtual machine technology (Speitkamp & Bichler 2010). Consolidation efforts represent an attempt by IT management to capture cost savings by retiring or decommissioning legacy devices and standardizing support processes. Consolidation projects present the opportunity to minimize the number of physical devices as well as software licenses, various application packages, and management tools. Continuing advances in the hardware components such as multi-core processors and high-speed memory modules up-hold the performance of virtual servers. Gartner Inc. is forecasting that the virtualization technology is set to play a major role in renovating the IT management strategy. The core of this transformation will be based on server

virtualization which will efficiently make use of the current underutilized server architectures (Christy 2008).

Further, Karen et al (2008) recommend that physical partitioning of resources' can enhance security and provide better performance although it may reduce the resource utilization due to the rigid limits established (Karen et al. 2008). In the above design, hard limits are set only to the network interface card so that each guest operating system is associated with a dedicated network interface card, which is further shielded by a properly configured firewall. This approach enhances security by avoiding malware injection or other form of encroachment between guest OS and provides better wire-speed. The kernel of the bare metal hypervisor is highly secure by architecture since it has no public application programming interfaces, possible ways of hacking or cracking this kernel is almost impossible (Ray & Schultz 2009). The possibility of escape attack in the type II virtualization is eliminated in the proposed approach where the type I bare metal architecture is applied. Our model includes a firewall in each guest OS to prevent further attacks and offer monitoring capabilities through introspection. The service console placement is also crucial in an enterprises network. It is recommended to keep the service console out of a demilitarized zone so that it will not easily fall prey to externally initiated attacks. Placing it at a point within a network where a firewall shields it from such attacks is far better from a security perspective (Ray & Schultz 2009). Finally, it is important to ensure that sufficient compliance mechanism coupled with systematic inspection of audit log output has been devised to enhance security.

9.3. Proposed Architecture for Mail Server Virtualization

An anonymous enterprise at Muscat region of the Oman was selected as pilot implementation. The enterprise currently has more than three thousand users being served by thirty-six servers with the business operations spread across Oman.

Based on the on-site analysis, it is found that the existing network infrastructure had lot of performance related issues and relentless downtime. Existing mail server had several drawbacks since there was only one front-end server, which was used to forward internal and external users' request to mailbox server at the back-end. To protect the frontend server, a firewall server was placed to filter internet traffic and to provide security to the mail server by creating SSL connection. The front-end server and the firewall server were not able to handle the surge in traffic due to the increase in the number of users, and thus it stood as a single point of failure. This calls for a highly scalable and robust infrastructure for handling the email system. It was decided to virtualize the data centre of this enterprise using Microsoft Hyper-V technology since the enterprise had licenses for Microsoft products. As a first step in virtualization, authors did a comprehensive capacity planning to arrive at an optimal design and solution. The capacity planning was done to analyse three distinct parameters of the system such as workload characteristics, performance predictions and cost factors. Based on the findings of the capacity planning, a design was made to virtualize the email system in phase-1 as shown in figure-18.

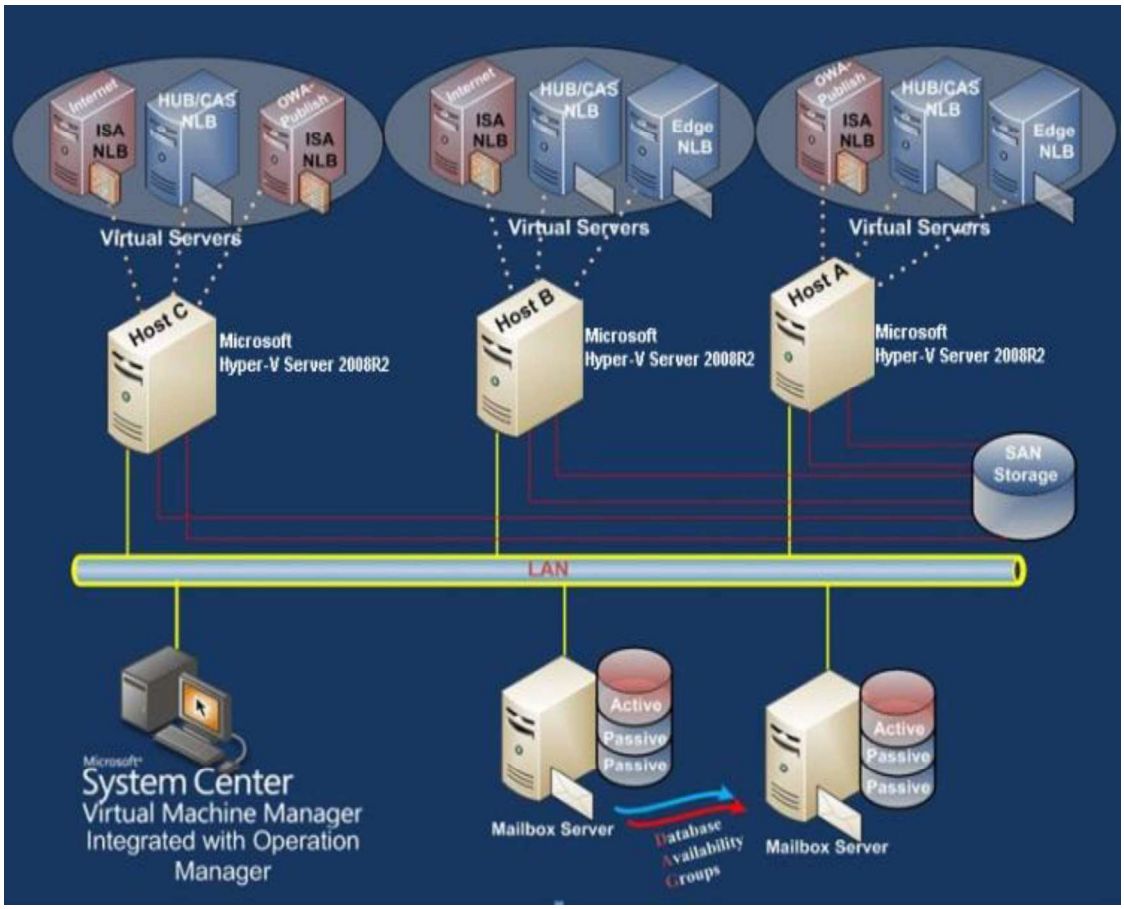


Figure 18 Logical Diagram of Mail Server Virtualization

The devised design has five physical servers dedicated for the email system. Among these five servers, two physical servers are used as mailbox servers (back-end servers) and the remaining three servers as client access servers (front-end servers). Each client access server (CAS) has three guest servers thus making nine virtual servers providing mail access over internet. The back-end and the CAS are connected with high-speed fibre optic channel to the storage area network (SAN) system in order to provide high-speed data access. Besides this, the SAN system helps to provide fault tolerance by quickly switching the virtual machine from one host to other host. The system centre virtual machine manager centrally manages all the servers with minimum administrative cost and time. The Windows network load balancing

(NLB) has been deployed to dynamically distribute the client requests. This enables the clients to experience acceptable performance level and reduced the downtime. Load balancing is given further emphasis by integrating edge load balancing, HUB/CAS load balancing, and firewall load balancing in all the guest servers to achieve optimal performance. Along with the above said features, the following benefits are also achieved by virtualization of the email system.

9.4. Benefits Achieved by Virtualization

9.4.1. High Availability

Business continuity and disaster recovery feature has been integrated in the proposed system. As SAN storage holds all the virtual machine images, these images can be deployed in any virtual machine or physical machine without much configuration overheads thus minimizing the downtown. The provisioning of SAN storage in a different physical location ensures the business continuity in the event of a disaster.

9.4.2. Financial Benefits

Server virtualization typically requires larger and more expensive servers; however, as discussed in the background, most physical servers are underutilized. Hence combining multiple underutilized servers into a single larger system can result in significant cost savings.

9.4.3. Energy and Floor Space Conservation

Virtualization reduces the number of physical servers where by the physical space requirement of the data centre is also saved drastically. Besides this,

reducing the number of physical servers in the datacentre reduces the energy requirement thus reducing the utilization of electricity. This feature is an important aspect in the present world, which is from a green computing perspective.

9.4.4. Enhanced Security

There is no difference in the security of physical server and virtual machine. Edward Ray and Eugene Schultz are confirming this in their research article that from security perspective a virtual machine and a physical server do not differ [8]. Security has been enhanced by the use of bare metal hypervisor. As the hypervisor can access the virtual machine disk files, securing the service console is even more important.

Virtualized server that is running within a bare metal hypervisor provides a sandbox thus limiting the impact of a compromise, since the attack platform is significantly reduced.

9.5. Drawbacks and Methods to Overcome

Like any other technology, server virtualization also has some drawbacks but these drawbacks can be eliminated by a strategic approach. An attempt is made to overcome those drawbacks as far as possible in the following section.

9.5.1. Single Point of Failure

Failure of the physical server hosting multiple virtual machines may affect multiple services. Even though this situation appears to be catastrophic, the chances of such failure can be managed by providing redundant virtual

servers. As the SAN system is used to store all the virtual machines, the failover of the standby server can be commissioned very fast without administrative overheads.

9.5.2. Demands Powerful Machines

As multiple virtual machines are deployed in one physical server, it is obvious that the physical machine needs to have sufficient processing power. This requires the physical machine to have state-of the art configuration and large memory. As the cost of hardware components are relatively cheaper, this issue can be easily overcome.

9.5.3. Performance of Virtual Machines

Even though powerful servers are deployed, performance issues may arise due to various reasons. These issues can be addressed by having a proper capacity planning which is the most critical aspect in server virtualization since it is directly related to server performance. In addition, it is advised not to virtualize some servers, which are running applications that demand more resources such as database applications and applications whose resource requirements are varying frequently or unpredictable such as web servers.

9.6. Summary

Virtualization continues to revolutionize the economics of enterprise software, changing the nature of how enterprises use contemporary applications, platforms and infrastructure for the long-term. Corresponding to this interest in server virtualization, mail servers were practically virtualized using bare metal architecture and demonstrated dynamic allocation of resources.

Through a questionnaire I was able to identify how many ministries used older versions of exchange servers, calculate the number of licences used and the amount of money spent on administration. Later I was able consolidate the nine VMs on three physical servers to provide client access (front end servers) and also provide fault-tolerance and automated load balancing with the help of SAN storage. Virtualization is implemented using bare metal architecture where the hypervisor is installed directly on the hardware without the host operating system thus eliminating the operating system vulnerabilities. I was able to demonstrate how various services such as mail service, web service, file service and application services can be dynamically provisioned to government organisations, cost effectively and align to e-Government strategies.

CHAPTER 10

INFORMATION SECURITY AUDIT AND ATTESTATION

10.1. Role of Information Security Audit

Audits are critical for ensuring the confidentiality, integrity and availability of the entire enterprise systems architecture (Belsis, Kokolakis & Kiountouzis 2005). Of specific interest in the analysis of server audits in Oman is the role they have in ensuring the scalability, security and stability of virtual machines that comprise the foundation of cloud computing, in addition to their contributions to security of virtualized platforms (Ko, Lee & Pearson 2011). Server audit combines the most critical factors such as security, scalability, and performance, especially in enterprise-wide computing environments that rely heavily on virtualization of servers for efficient and economical performance. From the benefits of lowered operating expenses made through the use of virtualization technologies to the streamlining of e-governance strategies, virtualization continues to mature rapidly. At the epicentre of virtualizations' maturation is the role of servers being used in the context of optimizing line-of-business scenarios and workflows.

The nature of cloud computing and the increasing dependency enterprises have on it as their platform of choice makes server performance, security and the reliability of virtualization structures a strategic priority. The first stage should include design and architectural details of VMs, storage, topology and bandwidth management. It should be based on the management functions of the virtualized server architectures enterprises rely on today. The second

stage should include version and configuration management, security and access analysis and validation, and application controls management. This third stage of auditing should look to establish a baseline for monitoring across the network and storage systems of servers used in a virtualized environment. These three areas that unify server virtualization includes baseline for performance, governance and monitoring for compliance further underline the complexities of competing server audits in virtualized environments.

The hypervisor acts as the orchestration agent across physical servers, and also acts as an orchestrating Web Service coordinating VM memory allocation while tracking performance and balancing across VMs and server components (Yunis, Hughes & Roge 2008). Concentrating on the vulnerability of VMs, as they can be relatively easily copied within different partitions on the same physical server, in addition to being copied across a network as well is essential. Based on the finding from this step of monitoring and evaluation, security policies can be improved and new administrative controls can be introduced to minimize the identified threats and vulnerabilities. For example if a network security vulnerabilities is identified then the configuration of firewalls and the level of hypervisor integration and traceability throughout a given servers operating system, security software and application configuration is changed (Yunis, Hughes & Roge 2008).

The intent of the chapter presented in this analysis is to show how a server audit can be designed and implemented to ensure security, scalability and stability of enterprise systems for the long-term.

10.2. Concerns in Auditing Virtualized Environments

The continual evolution of server virtualization technologies by Microsoft, VMware, Citrix and many other vendors underscore the need for a consistently definable, scalable model that can span across the many competing vendor approaches to these technologies. Today, there is no standard framework or methodology for evaluating server audit performance and results among many emerging vendor defined standards. What is evident in this initial period of server audits in virtualized environments is that the many competing and conflicting standards are making it very difficult for the enterprises globally who are early adopters of these technologies to get the full value from them. The need for a server audit in virtualized environments can readily be seen from the studies of how security is lagging in the overall structure of virtualization-based authentication and enterprise-wide security strategies (Collier, Plassman & Pegah 2007). There is an urgent need on the part of enterprises in Oman to be able to attain higher levels of security for their cloud-based initiatives by creating more effective server audits that include key factors of business strategies.

The early adopters of virtualization have been driven primarily by the economic benefits of this technology. The mainstream adopters of virtualization are more focused on how these associated technologies can be used for knowledge management systems development (Belsis, Kokolakis & Kiountouzis 2005) and efficient attainment of business goals and objectives (Yunis, Hughes & Roge 2008). Server audits in virtualized environments are

critically important for ensuring enterprise systems support and bring agility to business strategies. The stability and security of servers being used in virtual environments depends on the enterprise IT architecture which ensures compliance and alignment to business strategies. The reliance on server virtualization as a platform for ensuring greater business strategy execution and performance is the catalyst that continues to push this area forward (Ko, Lee & Pearson 2011). Server audits in virtualized environments are increasingly becoming part of the Return on Investment (ROI) of companies as cloud computing becomes more aligned with business strategies. The indispensable nature of virtualization in the broader strategic initiatives and programs of enterprises is now apparent with the rapid ascent of Software-as-a-Service (SaaS) application growth as well.

These economic factors of better return of investment (ROI) based on cloud computing performance, greater agility and customization of these applications to the need of companies, and the strategic role of cloud computing today all underscore how critical server audits in virtualized environments are.

However many auditors take a conservative stand when auditing physical environments by claiming that physical machines must have only one application layer service such as web server, domain name system (DNS) server, FTP server and so on. Conversely in virtual machines since many applications are hosted on a single machine the assessor is not sure of technical intricacies due to limited expertise in virtualization. Traditionally, auditors inspect data centre racks and check the existence of a firewall that is plugged into a chassis and examine the firewall policies to ascertain

protection capability. But in virtual environments, firewalls that are protecting communication between guest machines are configured in software which is intermingled with the hypervisor management. This causes difficulty in understanding how and where zones are deployed.

The network management tools to monitor and log virtual networks, virtual firewalls, virtual compliance systems, etc. are not as mature as their physical counterparts. Also some guest systems may be inactive or offline which pose a serious challenge since they are inactive when the new patches are applied. In response, the vulnerability management controls must be able to remediate such VMs and provide evidence that both active and passive VMs have equivalent protection applied. The possible risk of information leakage due to segregation of networks and systems must also be evaluated in virtual environment. Information leakage due to improper protection of virtual media is also a cause of concern as shared hosting is an important feature in virtual infrastructure. The intent of the framework presented in this analysis is to show how a server audit can be designed and implemented to ensure security, scalability and stability of enterprise systems for the long-term that use bare metal architecture.

10.3. Framework for Auditing in Virtualized Environments

The first step of the auditing process includes defining a knowledge capture and management strategy to capture the virtualization management architecture. For an effective server audit to be completed, every aspect of the virtualization architecture must be documented, understood with specific

attention to security workflows and authentication levels. In this first step of the proposed framework, server audits in virtualized environments include defining the role-based authentications and workflows that every member of an enterprise would use daily. Using advanced techniques like business process management (BPM) and business process re-engineering (BPR), auditors can quickly determine how effective existing performance, scalability and security levels are within a given virtualization architecture.

Further, server audits in virtualized environments concentrate on defining and validating the software versions of the virtualization systems. It focuses on evaluating the policies and specific security steps that a given enterprise has put into place before creating a VM instance, in addition to the current status of all software licenses and if maintenance has been contracted from server's vendor service enterprise (Yunis, Hughes & Roge 2008). In completing this step of the server audit, virtualization software release levels are evaluated in the context of compatibility and interconnection to other system components. This involves the development of an interconnection matrix that can provide auditors with insight into how each component relates to the broader system performance levels of the entire system architecture of an enterprise (Yunis, Hughes & Roge 2008).

Validation and creation of policies and procedures for each server audit administration including security patches is essential. Server audits need to evaluate the performance of updates relative to schedules while also evaluating and ranking vendor performance levels as well. One of the best approaches to this is to assign a timeliness rating to the server updates, and post this as a metric of system performance and compliance to optimal

system levels. Server audits are based on establishing traceability and transaction records for each of the user accounts and role-based definitions. This specific step concentrates on the specific administrative controls and procedures to add modify, and delete administrator and user accounts for each sever and across the entire virtualized environment. Administrative controls are necessary to ensure the workflow permissions and rights for each server at the operating system and application level (Collier, Plassman & Pegah 2007).

The second step of the proposed server audit is to complete a thorough review at the kernel level of the servers of interest in the audit to see which Application/Web Services are running and what their role is in the enterprise business strategies. This is critical from an audit standpoint as Web Services can and are often modified with cross-scripting code to enable sophisticated attacks of servers (Collier, Plassman & Pegah 2007). The server audit must also evaluate the overall configuration of the Application/Web Services including the definition of configuration options to data services outside the enterprises. The systematic evaluation and auditing of Web Services is essential if the entire virtual infrastructure of an enterprise is going to be protected over the long-term (Collier, Plassman & Pegah 2007). Auditors must also have the insight and system security approvals at the role based level to change integration and security options if needed to ensure hardened security levels and higher performance.

This step of the proposed audit framework concentrates on the development of templates that can be used for configuring and launching multiple VMs on the same physical server. Templates are needed to ensure standardization of

security configurations across all VMs running on a specific physical server, in addition to providing the hypervisor data that is valuable in orchestrating overall infrastructure performance. This template-based approach to defining configuration of servers, VMs and their effects on the hypervisor can significantly improve server performance while reducing the risk of intrusions and security breaches (Yunis, Hughes & Roge 2008). The use of templates can also make the process of completing server audits more automated, which will lead to a more periodic schedule delivering more valuable data over time.

The third step of the proposed framework for completing server audits in virtualized environments is centred on the monitoring/evaluation of virtual machine (VM) activity, access and performance. One of the most traceable activities of any VM is their provisioning and de-provisioning at the individual server and throughout a virtualized server environment (Yunis, Hughes & Roge 2008). Included in this phase is an evaluation of the disaster recovery plan for the server itself, including back-up and recovery tasks. Through internal and external testing hardware capacity of a server can be optimized given the business objectives of the enterprise. Considering the nature of their business model, value chain, scope and structure of their supply chains, and integration to the VM level in advanced settings is tested. (Yunis, Hughes & Roge 2008). This step specifically creates a VM monitoring application or utility service that captures the specific hardware performance by enterprise software application. Metrics captured in this step include the performance of physical virtualization media, communication protocols, and processor and memory performance, and the benchmarked performance of the server

versus its Service Level Agreements (SLA). Here focus is given to evaluating the variation in server performance on the dimensions of individual and aggregate VM performance, and across the key performance indicators of server security as defined in the initial audit objectives (Collier, Plassman & Pegah 2007). The proposed server audit is based on a thorough review of the data redundancy, data storage and data backup plans relative to actual performance and having appropriate controls to prevent data leakage.

The process flow diagram (Figure-19) given below provides an insight to auditors to assess the adequacy of controls in a virtual environment. The audit process flow diagram starts with the previous audit findings and identifies the requirements and the controls along with deficiencies discovered in the previous audit. The audit must also include the technological advancements inherent to change over a period of time and the associated threats that must be captured in the scope of applicability.

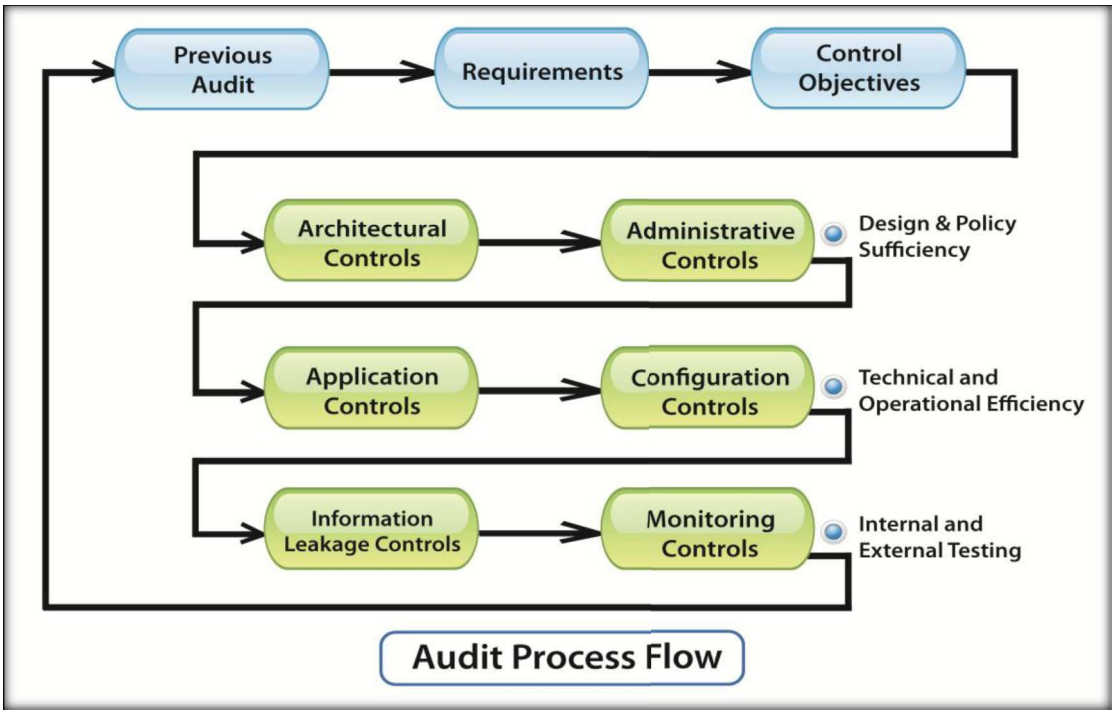


Figure 19 Audit Process Flow Diagram

Risks in virtual environment are classified into six major categories as follows:

1. Architectural risks
2. Administrative risks
3. Application risks
4. Configuration risk
5. Information leakage risks and
6. Monitoring risks.

Architectural risks consist of risks created by the abstraction layer between the physical hardware and the virtualized systems. It focuses on the design of VMs, storage, network topology, bandwidth, management systems, etc.

The audit must capture on, whether defence in depth is implemented with enforcement of least privilege. One important challenge in deploying virtualization is to group appropriate VMs of different trust and security levels associated within the particular virtual machine. Hence, audit must ensure that VMs of different trust levels are not mixed and dormant virtual machines are not inadvertently left out of security procedures.

Administrative risks are the risks associated with the organizational structure that defines the roles and responsibilities to enforce separation of duties and the use of third party tools to provide administrative controls. The audit must emphasis on documentation that identifies who is responsible for each VM and thereby restricting access to administrative interfaces. Relevant policies and procedures need to be examined for sufficiency and completeness.

Application risks are the risks associated in hosting many applications in single VM. The hidden vulnerability in the application is a potential threat for

the VM on which it's hosted and also the vulnerabilities in the hypervisor can be a risk factor for the VM. The audit in virtual environment should validate and create taxonomy of reference policies and procedures for each application.

Configuration risks are ever increasing with the dynamic nature of threats and vulnerabilities. Secure configuration baselines must be maintained in order to keep all the software's up-to-date with security patches applied. Hence audit should look at how hypervisor hardening is implemented based on best practices and ensure that the virtual machines and virtual appliances are hardened.

Information leakage risks deals with sensitive data exiting outside the authorized territory circumventing the security controls. The information leakage can also occur between virtual appliances when resources are being shared by multiple virtual machines. So, the audit must review the kernel level of the hypervisor to safeguard the physical resources such as CPU cores and network interface cards such that appropriate levels of isolation is evident. Further, the audit process should evaluate the network segmentation details.

Monitoring risks are the risks due to lack of proactive management, operational and follow-up procedures. The audit should assess the VM monitoring utility that captures the specific hardware performance for enterprise software applications. The audit must make certain that traceability and transaction records for accountability exist for each of the user accounts from a policy standpoint.

The audit questions were arrived for each classification of risks after discussion with information security auditors. These questions are provided in appendix-I.

The following table-3 illustrates the calculation of effective value of each type of risk and the corresponding figure-20 displays the desired and maximum points.

Table 3 Calculation of effective value of each type of risk

Taxonomy of Risks	Maximum Points	Average value of Desired points	Priority	Effective Value of Desired Points (Average value * Priority /5)
Architectural risks	4	3.304	5	3.304
Configuration Risks	4	3.48	4	2.784
Information Leakage Risks	4	3.5	1	0.7
Application Risks	4	3.37	3	2.022
Monitoring Risks	4	3.33	3	1.998
Administrative Risks	4	3.34	4	2.672

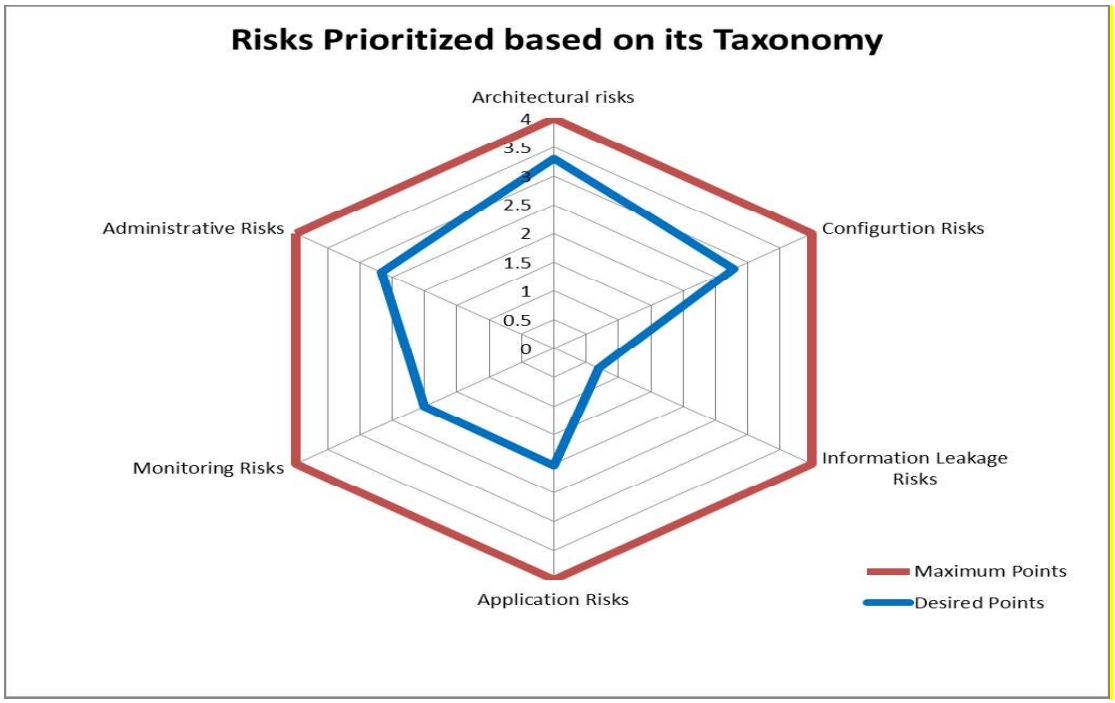


Figure 20 Risks prioritized based on its taxonomy

The audit questions were distributed to the security auditors and their inputs which range from zero (not applicable) to 4 (strongly agree) were collected. The average value of their points for each taxonomy of risk is listed in column-3 of the table-3. The effective values of desired points are arrived by the product of average value and priority which is then divided by maximum range of values (i.e 0 to 4). The highest priority is given to the architectural risks since architectural flaws form the foundation for other risks in virtual environment. However administrative and configuration risks can be dynamically managed based on the output of monitoring reports.

10.4. Summary

Auditing in a virtual environment looks similar to the audit in physical environment however it brings in additional complexities and confusion to the compliance efforts. Due to the lack of comprehensive standards and frameworks to audit a virtual environment, the audit process becomes cumbersome. This chapter provides light on this issue and provides taxonomy of risks inherent in virtual environments and relevant control objectives.

CHAPTER 11

CONCLUSION

11.1. Research Conclusion

Enterprises are continually challenged to increase the breadth and depth of their information security governance especially in virtual environment and security controls, often having to align to their business objectives. This forces the continual management and maintenance of security technologies, frequently requiring enterprises to master specific methods of software design and virtual infrastructure configuration.

Through interview and discussion, it was possible to arrive at a consensus that a strategically balanced approach is required to achieve corporate governance that integrates people, process and technology.

A conceptual model of GRC for optimizing enterprise information security was developed and proposed as a balanced solution, underpinning the theoretical philosophies that influence the transition of information security from a technical perspective to information security governance focusing on virtual environments. Thus governance can be achieved by fostering a security culture that leads to an optimized enterprise information security system in modern complex business environments. Culture in Oman's context is crucial since they excessively trust each other and lack security awareness. An innovative enterprise-wide security governance model providing a flexible decentralized decision making perspective with accountability and focusing on security objectives and strategies is devised.

This conceptual model included ERM as an unifying platform to integrate governance strategy, security polices and certification & evaluation for compliance to achieve organizational transparency. This model provides opportunities to explore and exploit emerging threats and vulnerabilities pertaining to virtual environments and dynamically change security strategies in response to external environments. The findings from the questionnaire show that majority of information security practitioners in Oman are aware of COSO framework but unfortunately COSO is presumed as complex due to excessive grouping of risks and also fails to provide direction from an implementation perspective. To address this problem, risk was classified into three categories such as business risks, technical risks and regulatory risks. Based on these categories, a conceptual maturity model was developed which defines four different approaches such as due-diligence, probabilistic risk analysis, scenario-based approach and system analysis approach for managing enterprise risk.

In order to optimize information security in an enterprise in Oman, the IT infrastructure which acts as an enabler to business, needs to be optimized. To accomplish this, server virtualization strategy using bare-metal architecture was practically implemented to dynamically manage resource allocation. This implementation was successfully tested to help enterprises to overcome the typical concerns of modern data centers and provide many benefits such as high availability, scalability, cost reduction, minimizing floor space and enhanced security.

Vulnerability assessment for a cluster of public sector enterprises was conducted and analyzed the results to find out the areas of potential failure and success rate of threats. Additionally, audit reports, service level agreements (SLA) and other relevant IT infrastructure artifacts were investigated. Assessment of disaster recovery plans; business continuity plans and the scope of emergency response plans from the standpoint of uptime and service availability were also explored.

Research findings in these public sector enterprises which were used as a case study showed that there is lack of analytics and reporting system on the use of information assets and its security implications across the enterprise. This revealed that a robust IT governance framework was missing to deliver measurable value to the business while improving the productivity. Although COBIT provides direction to IT governance, it rarely defines the implementation details applicable to virtual infrastructure. Hence a framework was developed after evaluating the four domains of COBIT and selecting the most critical control objectives and implemented IT governance within a short span of time and with limited resources. The implementation was done by mapping the selected control objectives with various best practices such as Prince2, ITIL and ISO 27002 for effective ITG implementation.

The findings of the interviews show that most of the information security assessors are not experts in virtualization since they do not understand the technical intricacies to ascertain if a specific design and configuration is secure. Also many of them confessed that they struggled with virtualization as no formal frameworks for auditing in virtual environments are prescribed. The

notion of effective auditing in virtual environment was discussed and taxonomy of risks inherent in virtual environments and relevant control objectives was provided. The finding of this research shows that a formal framework for successful auditing in virtual environment is necessary and was devised.

Balancing between the need for continual mastery of system and application configuration on the one hand and the need to stay ahead of the numerous requirements of internal and external stakeholders on the other forms the foundation of the series of recommendations provided in this research.

11.2. Novelty and research contribution

This research made contribution in various research stages, namely research planning, literature review, conceptualization of the solution and research experimentation. These contributions are summarized below.

In the research planning stage, a preliminary review of literature coupled with industry visits to gain insight into enterprise security management practices, enabled the development of the research problem, i.e. lack of comprehensive Governance, Risk and Compliance framework for enterprise information security in virtual environments.

After interviewing information security practitioners about the security implementations in various enterprises, clear research objectives and research questions were formulated. The significance of research within the context of Oman was developed after discussing with decision makers in ITA

so that a private cloud based solution could enhance the services provided by enterprises and align to e-government strategy.

In the literature review stage, extensive review of literature was helpful in understanding the enterprise security practices and the associated gap in literature with regards to inadequate standards and frameworks for information security governance especially in virtual environments. Literature also revealed that virtualization continues to grow in enterprise data centers due to its immense popularity owing to economic benefits and other characteristics such as scalability, availability and high performance. However, virtual machines add complexity and some confusion to compliance efforts which, without proper guidance from appropriate frameworks, would cause problems during audit. The resulting contribution specific to this research was the selection of control objectives based on COBIT and mapping with best practices that aligns to IT governance strategies.

In the conceptualization of solution stage, a Strategically Balanced Governance, Risk and Compliance Model was developed based on the analysis from previous research activities and interview questions. This novel model will help any enterprise in implementing GRC without the need of any software packages. The proposed model is flexible by providing opportunity to adjust and align security strategies according to the objectives of the enterprise.

Later a questionnaire was designed and distributed to security practitioners in Oman on Enterprise Risk Management to check if they are adhering to international ERM framework such as COSO. The findings were analyzed and

a conceptual maturity model was proposed to attain optimal risk management by integrating predictive risk analysis into enterprise management process.

In the research experimentation a project on server virtualization was implemented using bare metal hypervisor architecture for one of the ministries in Oman to ensure that operationally critical information is available, accurate, and up-to-date. Later, through interviews and practical experiments complexities of auditing in virtual environment were explored and an audit process flow was devised that provides insight to auditors to assess the adequacy of controls in a virtual environment. Although PCI DSS is the first compliance standard to encounter virtualization issues; most auditors don't interpret this consistently due to their lack of understanding of the implications of virtualization. Many also confessed that they struggled with virtualization as no formal frameworks for auditing in virtual environments are prescribed.

The proposed audit process flow diagram starts with the previous audit findings and identifies the requirements and the controls along with deficiencies discovered in the previous audit. The audit also includes the technological advancements inherent to change over a period of time and the associated threats that must be captured in the scope of applicability. Hence risks in virtual environment were classified into six major categories as follows:

Architectural risks, Administrative risks, Application risks, Configuration risks, Information leakage risks and Monitoring risks.

A total of 32 questions were devised based on the taxonomy of risks that is appropriate for auditing and attestation in virtual environment. The findings

were analyzed and the resulting framework for a successful audit in virtual environments is contribution that has changed some of the security assumptions and audit controls in virtual environments.

11.3. Evaluation

E-government fosters collaboration between government entities thus improving the public services by providing access to citizens, residents and external partners. E-government initiatives need to build governance mechanisms to respond to the twin challenges of alignment to external entities and internal integration of systems.

Many government organizations are embracing cloud computing to address the pressures and challenges across the wider economy. They are beginning to explore the use of cloud computing services in many areas such as manpower, education, health and housing, which will ultimately serve to transform government services using cloud technology on a large scale.

Cloud computing is evolving as a web based service that delivers on- demand services cost effectively across a large pool of users with amazing scalability and availability. It was predicted by McGee in a Gartner report, that cloud computing could be a US$149 billion market by 2014 and by 2016 could have 100% penetration in Forbes list of the Global 2000 companies (McGee, 2011).

However cloud computing poses several challenges due to complexity of sharing data across multiple tenants, coupled with storage of data and application integration on behalf of clients. Information security governance plays a vital role since access to several different accounts should be

provided while data is stored on the same physical server using multitenancy-based configurations.

It is evident from analysis of MOE network infrastructure and its audited reports that the current security strategies are inadequate to meet the business objectives since they do not support the complexities associated with virtual network infrastructure as required by cloud computing.

Through discussions with public sector enterprises showed the importance of aligning to e-government strategies. This calls for an implementable framework, which was developed after evaluating the four domains of COBIT and selecting critical processes and control objectives which are then mapped with Prince2, ITIL and ISO 270002 for effective ITG implementation.

Due to the lack of comprehensive standards and frameworks to audit a virtual environment, first taxonomy of risks inherent in virtual environments was devised and relevant audit questions developed that will provide new dimension in auditing a virtual environment. Finally as a highlight, a novel framework for auditing in virtual environment was developed which provides a comprehensive view into the types of risks in virtual infrastructure and provides a concrete checklist with relevant questions for auditing. The risk grouping and prioritization has been arrived by applying multivariate analysis which helps the auditors in quantifying the risk factor.

11.4. Recommendations

Following are the recommendations provided:

1. A strategically balanced GRC model should be adopted to maintain optimized risk management, governance and enterprise information security policies in synchronization with each other and at the same time attaining a high level of transparency.
2. Enterprise information security policy should be used to ensure that its taxonomies created and outputs can be used for compliance and effective governance.
3. Information security should not be treated as just a technical issue rather as a business issue which can stimulate high degree of transparency and information velocity throughout an enterprise.
4. Risk management function should be integrated across the enterprise with insights into just how mitigation of risks, cost controls and process integration are all contributing to overall financial performance.
5. IT governance should be implemented using COBIT framework by identifying critical success factors in an enterprise and make use various best practices available. Further, the data collected from analytics has been used to track performance and revisit the control objectives thus making the adoption of COBIT controls more consistent.
6. Access controls need to segregate the responsibility for administration and approval of network access and non-administrative access. There also needs to be clear differences between approvers and account

creators to ensure no conflict of interest in creating and updating records.

7. A configuration management system must adhere to enterprise designated baseline security-hardening standards and all assets must be entered and tracked in the configuration management database system (CMDB) to ensure a system of record is created and continually updated.
8. Business units need to control the overall definition of wireless and mobile access, in addition to defining public key infrastructure strategies that align with their specific business models and needs. This will also serve to unify system configuration and stakeholder requirements as well.
9. Emerging technologies such as virtualization and cloud computing should be utilized to enhance revenue opportunities with optimal security.
10. Management should develop a culture of compliance through auditing such that security functions and accountability within the enterprise fit the governance structure.
11. Auditing framework should be used to audit virtual infrastructure for compliance that leads towards achieving certification through evaluation and a structured and reporting mechanism to the senior management for effective governance.
12. A structured reporting mechanism with defined roles and responsibilities and segregation of duties is essential for the prevention of conflict of interest and detection of control failures.

13. Finally to attain the highest level of best practices with audit and accountability, all audit reports need to be captured on non-changeable media and all reports must be aggregated and used through a common tracking system to see which roles and administrators are accessing the data.

11.5. Limitations

Use date from private sector organizations and consulting companies such as Ernst & Young, PricewaterhouseCoopers etc. to evaluate the efficiency of the model. Considering the sensitivity of the research topic and the data collected actual names of the enterprises could not revealed

11.6. Future Work

Outsourcing aspect of cloud computing raises serious concerns about the security and privacy of the data assets that are outsourced to providers of cloud services especially in public cloud is worth researching.

A mathematical model or algorithm should be explored to optimize information security in an enterprise which should capture technical and non-technical aspects along with information security culture.

References

Abu-Musa, A 2009, 'Exploring the importance and implementation of COBIT processes in Saudi organizations An empirical study', *Information Management & Computer Security*, vol 17, no. 2, pp. 73-95.

Ahmad, T, Malawat, T, Kochar, Y & Roy, A 2009, 'Satyam Scam in the Contemporary Corporate World: A Case Study in Indian Perspective', *IUP Journal*, viewed 10 February 2010, < HYPERLINK "Available at SSRN: http://ssrn.com/abstract=1460022" Available at SSRN: http://ssrn.com/abstract=1460022 >.

Ajay, K, David C. M., W, Helen C,.S & Anil K., J 2003, 'Personal verification using palmprint and hand geometry biometric', *4th international conference on Audio- and video-based biometric person authentication*, Springer-Verlag, Berlin, Heidelberg.

Akyuz, GA & Erkan, TE 2009, 'Supply chain performance measurement: a literature review', *International Journal of Production Research*, vol 48, no. 17, pp. 5137-5155.

Al-Badi, AH, Ashrafi, R, Al-Majeeni, AO & Mayhew, PJ 2009, 'IT disaster recovery: Oman and Cyclone Gonu lessons learned', *Information Management & Computer Security*, vol 17, no. 2, pp. 114-126.

Applegate & Scott, D 2009, 'Social Engineering: Hacking the Wetware!', *Information Security Journal: A Global Perspective*, vol 18, no. 1, pp. 40-46.

Arun 2011, *A Survey on Information Security and Enterprise Risk Management (ERM) awareness in Sultanate of Oman*, < HYPERLINK "https://docs.google.com/spreadsheet/viewform?pli=1&formkey=dGNGcjVRNm1GM2N6SmlVbEdGWkVHRGc6MQ" \l "gid=0" https://docs.google.com/spreadsheet/viewform?pli=1&formkey=dGNGcjVRNm1GM2N6SmlVbEdGWkVHRGc6MQ#gid=0 >.

Asosheh, A, Nalchigar, S & Jamporazmey, M, 'Information technology project evaluation: An integrated data envelopment analysis and balanced scorecard approach', *Expert Systems with Applications* , vol 37, no. 8, pp. 5931-5938.

Bahan, C 2003, 'The Disaster Recovery Plan', GSEC Practical Assignment version 1.4b, SANS Institute.

Baker, WH & Wallace, L 2007, 'Is Information Security Under Control?: Investigating Quality in Information Security Management', *IEEE Security & Privacy*, vol 5, no. 1, pp. 36-44.

Barnard, L & Solms, RV 1988, 'The evaluation and certification of information security against BS 7799', *Information Management & Computer Security*, vol 6, no. 2, pp. 72-77.

Bartels, A,DEAAM, 2009, 'US And Global IT Market Outlook: 2009', Forrester Research.

Baskerville, RL 1999, 'Investigating information systems with action research', *Journal of Communications of Association for Information Systems* , vol 2, no. 3, p. 4.

Beasley, MS, Clune, R & Hermanson, DR 2005, 'Enterprise risk management: An empirical analysis of factors associated with the extent of implementation', *Journal of Accounting and Public Policy*, vol 24, no. 6, pp. 521-531, http://www.sciencedirect.com/science/article/B6VBG-4HMNG8Y-2/2/9d314776cac564f3a20d0f98b1521add.

Beer, M & Nohria, N 2000, 'Cracking the Code of Change', *HARVARD BUSINESS REVIEW*, 1 May-June 2000, pp. 133-142.

Bellone, J, Rodriguez, DS & Juan, B 2008, 'Reaching escape velocity: A practiced approach to information security management system implementation', *Information Management & Computer Security*, vol 16, no. 1, pp. 49 - 57.

Belsis, P, Kokolakis, S & Kiountouzis, E 2005, 'Information Systems Security from a knowledge management perspective', *Information management & Computer Security*, vol 13, no. 3, pp. 189-202.

Blakely, Bob 2008, *Another buzzword to muddy the water*, viewed 29 February 2012, < HYPERLINK "http://www.computing.co.uk/ctg/opinion/1822494/another-buzzword-muddy-water" http://www.computing.co.uk/ctg/opinion/1822494/another-buzzword-muddy-water >.

Boehmer, W 2008, 'Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001', *SECURWARE '08. Second International Conference on Emerging Security Information, Systems and Technologies*, IEEE Explorer, Cap Esterel.

Booz Allen Hamilton 2005, 'Convergence of Enterprise Security Organizations', Reserch report, The Alliance for Enterprise Security Risk Management.

Brenner, J 2007, 'ISO 27001: Risk Management and Compliance', *Risk Management Magazine*, 1 January 2007, http://www.rmmagazine.com/MGTemplate.cfm?Section=MagArchive&NavMenuID=304&template=/Magazine/DisplayMagazines.cfm&Archive=1&IssueID=286&AID=3255&Volume=54&ShowArticle=1.

Brisebois, R, Boyd, G & Shadid, Z 2007, 'What is IT Governance ? and why is it important for the IS auditor', *intoIT*, pp. 30-35, viewed 12 January 2012, < HYPERLINK "http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf" http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf >.

Bronk, C 2008, 'Hacking the Nation-State: Security, Information Technology and Policies of Assurance', *Information Security Journal: A Global Perspective*, vol 17, no. 3, pp. 132-142.

Burkhardt, ME 1985, 'Applying a System Development Cycle to Information Security', *Security Management*, 1 July 1985, pp. 32-37.

Calder, A 2009, *Information Security Based on ISO 27001/ISO 17799: A Management Guide*, 2nd edn, Van Haren Publishing.

Cellary, W, Strykowski,S, 2009, 'E-Government Based on Cloud Computing and Service-Oriented Architecture.' *Procedings of the 3rd International conference on Theory and practice of electronic governance*. Bogota, Colombia: ACM, pp. 5-10.

Chang, SE & Lin, CS 2007, 'Exploring organizational culture for information security management', *Industrial Management & Data Systems*, vol 107, no. 3, pp. 438 - 458.

Chiu Yaw Han, LLCP 2011, 'Study on Correlation between Critical Successful Factors of IT Governance and Governance Performance', *Journal of Convergence Information Technology*, vol 6, no. 5, pp. 329-338, < HYPERLINK "http://www.aicit.org/jcit/ppl/%20JCIT_MAY_38.pdf" http://www.aicit.org/jcit/ppl/%20JCIT_MAY_38.pdf >.

Christy, P 2008, 'Virtualization will be the Highest-Impact Trend in Infrastructure and Operations Market Through 2012', News Room, Gartner, Gartner, Stamford , USA.

Clementi, S & Carvalho, T 2006, *Methodology for IT Governance Assessment and Design*, Springer Boston, viewed 28 February 2012, < HYPERLINK "http://dx.doi.org/10.1007/978-0-387-39229-5_16" http://dx.doi.org/10.1007/978-0-387-39229-5_16 >.

Collier, G, Plassman, D & Pegah, M 2007, 'virtualization's next frontier:Security', *Procedings of the 35th annual ACM SIGUCCS fall conference*, ACM, New York, USA.

Creasy, RJ 1981, 'The origin of the VM/370 time-sharing system', *IBM Journal of Research and Development*, vol 25, no. 5, pp. 483-490.

CXO Media Inc 2006, *Business Continuity and Disaster Recovery Planning Definition and Solutions*, viewed 12 August 2012, < HYPERLINK "http://www.cio.com/article/40287/Business_Continuity_and_Disaster_Recovery_Planning_Definition_and_Solutions" http://www.cio.com/article/40287/Business_Continuity_and_Disaster_Recovery_Planning_Definition_and_Solutions >.

Daniels, J 2009, 'Server Virtualization Architecture and Implementation', *Crossroads*, vol 16, no. 1.

Diesner, J, Frantz, TL & Carley, KM 2005, 'Communication Networks from the Enron Email Corpus "It's Always About the People. Enron is no Different"', *Comput. Math. Organ. Theory*, vol 11, no. 3, pp. 201-228.

Dietz, J, Proper, E, Tribolet, J (eds.) 2009, *Enterprise Architecture: Creating Value by Informed Governance*, Springer, Netherlands.

Doughty, K 2003, 'A Framework for Incident and Change Management', *Enterprise Operations Management*, vol 27, no. 6, pp. 1-11.

Eloff, JHP & Eloff, MM 2005, 'Information security architecture', *Computer Fraud & Security*, vol 2005, no. 11, pp. 10-16.

Fariborz, F, Shamkant B, N, Philip H, E & Gunter P, S 2003, 'Managing vulnerabilities of information systems to security incidents', *Proceedings of the 5th international conference on Electronic commerce (ICEC '03), ACM*, pp. 348-354.

Farrell, R 2010, 'Securing the Cloud—Governance, Risk, and Compliance Issues Reign Supreme', *Information Security Journal: A Global Perspective*, vol 19, no. 6, pp. 310 - 319.

Fischer, K, Bleimann, U, W, F & S M, F 2007, 'Analysis of security-relevant semantics of BPEL in cross-domain defined business processes', *Information Management & Computer Security*, vol 15, no. 2, pp. 116-127, < HYPERLINK "www.emeraldinsight.com/0968-5227.htm" www.emeraldinsight.com/0968-5227.htm >.

Forrest, W,JMKANK 2008, 'Data Centers:How to Cut Carbon Emissions and Costs', *The McKinsey Quarterly*, 2008.

Fox, C 2009, 'A Guide to Starting an ERM Program', *Risk Management*, 1 April 2009, pp. 42-47.

Freeman, W 2002, 'Business Resumption Planning: A Progressive Approach', SANS Institute, SANS Institute.

Freeman, E 2010, 'Information and Computer Security Risk Management', in E Turrini (ed.), *Cybercrimes: A Multidisciplinary Analysis*, Springer Berlin Heidelberg.

Garbani, J-P 2005, 'Building Blocks Of Process And Innovation', *Optimize*, 11 November 2005, pp. 93-95.

Gary, H & Rob, S 2011, 'Forty Hard-won Business Continuity Lessons from the 2011 Earthquakes in New Zealand and Japan', *EDPACS*, vol 44, no. 3, pp. 1-18.

Global Netoptex Inc 2009, 'Demystifying the cloud', White Paper, Global Netoptex Inc, Global Netoptex Inc, San Jose, Ca.

Goldberg, RP 1973, 'Architecture of virtual machines', *Proceedings of the Workshop on Virtual Computer Systems*, Cambridge, Massachusetts, United States, , DOI= http://doi.acm.org/10.1145/800122.803950.

Guldentops, E 2004, *Governing Information Technology through COBIT*, IT Governance Institute, USA, viewed 12 January 2012, < HYPERLINK "http://mail.stei.itb.ac.id/~ssarwono/KU1073/.buku/Idea%20Group,.Strategies%20for%20Information%20Technology%20Governance.%5B2003.ISBN1591402840%5D.pdf" \l "page=282" http://mail.stei.itb.ac.id/~ssarwono/KU1073/.buku/Idea%20Group.Strategies%20for%20Information%20Technology%20Governance.%5B2003.ISBN1591402840%5D.pdf#page=282 >.

Hamm, S 2008, 'It's Too Darn Hot', *Businessweek*, March 20, 2008 2008, pp. 1-16, http://www.gndatacenter.com/green-data-center/images/weblinks/bw_too_hot.pdf.

Hampton, JJ 2009, *Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity*, 1st edn, AMACOM, American Management Association, New York.

Hawkins, KW, Alhajjaj, S & Kelley, SS 2003, 'Using CobiT to secure information assets', *The Journal of Government Financial Management*, http://www.highbeam.com/doc/1P3-353250971.html.

Hong, K-S, Chi, Y-P, Chao, LR & Tang, J-H 2003, 'An integrated system theory of information security management', *Information Management & Computer Security*, vol 11, no. 5, pp. 243 - 248.

Hostway 2007, 'How to Prepare a Business Recovery Plan', *Hostway Global Web Solutions*, August 2007.

Huang, S-M, Lee, C-L & Kao, A-C 2006, 'Balancing performance measures for information security management: A balanced scorecard framework', *Industrial Management & Data Systems*, vol 106, no. 2, pp. 242 - 255.

Huang, W, Liu, J, Abali, B & Panda, DK 2006, 'A case for high performance computing with virtual machines', *Proceedings of the 20th Annual international Conference on Supercomputing*, Cairns, Queensland, Australia, DOI= http://doi.acm.org/10.1145/1183401.1183421.

IT Governance Institute 2007, *COBIT Quickstart*, 2nd edn, IT Governance Institute, United States of America.

ITA-OMAN 2008, 'e.oman Strategy', Government Strategy, Information Technology Authority, Sultanate of Oman, Muscat.

Jain, AK, Karthik, N & Abhishek, N 2008, 'Biometric Template Security', *EURASIP Journal on Advances in Signal Processing*, vol 2008.

Jain, AK & Pankant, S 2006, 'A touch of money', *IEEE Spectrum*, 2006, pp. 22-27.

John, W & Lainhart, I 2000, 'COBIT ™ : A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities', *Journal of Information Systems*, vol 14, no. s1, pp. 21-25.

Kadam, AW 2007, 'Information Security Policy Development and Implementation', *Information Security Journal: A Global Perspective*, vol 16, no. 5, pp. 246-256.

Kambil, A 2008, 'Purposeful abstractions: thoughts on creating business network models', *Journal of Business Strategy*, vol 29, no. 1, pp. 52-54.

Kaplan, RS & Norton, DP 1996, *The balanced scorecard: translating strategy into action*, Harvard Business Press, Boston.

Karen Scarfone, MSH 2011, 'Guide to Security for Full Virtualization', NIST Special Publication 800-125, ,National Institute of Standards and Technology, Gaithersburg, MD 20899-8930.

Karen, S, Murugiah, S, Amanda, C & Angela, O 2008, 'Technical Guide to Information Security Testing and Assessment', Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, Special Publication 800-115, Gaithersburg, MD.

Kenneth, JK, Thomas E, M, R Kelly, R & F Nelson, F 2006, 'Information security: management's effect on culture and policy', *Information Management & Computer Security*, vol 14, no. 1, pp. 24-36.

Kirvan, P 2012, *Developing a disaster recovery and business continuity training program*, viewed 23 August 2012, < HYPERLINK "http://searchdisasterrecovery.techtarget.com/tip/Developing-a-disaster-recovery-and-business-continuity-training-program" http://searchdisasterrecovery.techtarget.com/tip/Developing-a-disaster-recovery-and-business-continuity-training-program >.

Kissel, R 2011, *Glossary of Key Information Security Terms*, viewed 11 June 2011, < HYPERLINK "http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf" http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf >.

Ko, RK, Lee, BS & Pearson, S 2011, 'Towards achieving accountability, auditability and trust in cloud computing', *Advances in Computing and Communications*, pp. 432-444.

Kouns, J & Minoli, D 2010, *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*, 1st edn, Wiley-Interscience.

Kreuter, D 2004, 'Where Server Virtualization Was Born', *Virtual Strategy Magazine*, 21 July 2004, http://www.virtual-strategy.com/Migration/Where-Server-Virtualization-Was-Born.html.

Lichstein, HA 1969, 'When should you emulate?', *Datamation*, 1969, pp. 205-201.

Li, J, Li, B, Wo, T, Hu, C, Huai, J, Liu, L & Lam, KP 2012, 'CyberGuarder: A virtualization security assurance architecture for green cloud computing', *Future Generation Computer Systems*, vol 28, no. 2, pp. 379-390.

Maltoni, D, Maio, D, Jain, AK & Prabhaka, S 2003, *Handbook of Fingerprint Recognition,* Springer, Berlin, Germany.

Mbuya, JC 2009, *Risk Management Strategy*, 1st edn, Brixton Book Binders, Wierda Park.

McNaughtona, B, Ray, P & Lewis, L 2010, 'Designing an evaluation framework for IT service management', *Information & Management*, vol 47, no. 4, pp. 219-225, < HYPERLINK "http://www.sciencedirect.com/science/article/pii/S0378720610000236" http://www.sciencedirect.com/science/article/pii/S0378720610000236 >.

Meybodi, M 2006, 'Internal manufacturing strategy audit: the first step in integrated strategic benchmarking', *Benchmarking: An International Journal*, vol 13, no. 5, pp. 580-595.

Mitchell, SL 2007, 'GRC360: A framework to help organisations drive principled performance', *International Journal of Disclosure and Governance*, vol 44, no. 4, pp. 279-296.

Mitome, Y & Speer, KD 2001, 'Embracing disaster with contingency planning', *Risk Management*, vol 48, no. 5, pp. 18-21.

Mohan, K, Xu, P, Cao, L & Ramesh, B 2008, 'Improving change management in software development: Integrating traceability and software configuration management', *Decision Support Systems*, vol 45, no. 4, pp. 922-936.

MONE 1996, 'http://www.moneoman.gov.om/loader.aspx?view=planning-diverse&type=plan', Planning and Development Strategy: Vision 2020, Ministry of National Economy, Sultanate of Oman, Muscat.

Murray, A 2009, *Managing successful projects with PRINCE2*, The Stationary Office, < HYPERLINK "http://hdl.handle.net/1961/8717" http://hdl.handle.net/1961/8717 >.

Nagaratnam, N, Nadalin, A, Hondo, M, McIntosh, M & Austel, P 2005, 'Business-driven application security: From modeling to managing secure applications', *IBM SYSTEMS JOURNAL*, vol 44, no. 4, pp. 847-867.

National biometric security project 2008, 'Biometric Technology Application Manual', The National Biometric Security Project, Bowie, MD.

Neubauer, T, Ekelhart, A & Fenz, S 2008, 'Interactive Selection of ISO 27001 Controls under Multiple Objectives', in S Jajodia, P Samarati, S Cimato (eds.), *Proceedings of The Ifip Tc 11 23rd International Information Security Conference*, Springer , Boston, < HYPERLINK "http://dx.doi.org/10.1007/978-0-387-09699-5_31" http://dx.doi.org/10.1007/978-0-387-09699-5_31 >.

Oakland, JS & Tanner, SJ 2007, 'A new framework for managing change', *The TQM Magazine*, vol 19, no. 6, pp. 572-589.

Okenyi, PO & Owens, TJ 2007, 'On the anatomy of human hacking', *Information Security Journal: A Global Perspective*, vol 16, no. 6, pp. 302-314.

Pulkkinen, M, Naumenko, A & Luostarinen, K 2007, 'Managing information security in a business network of machinery maintenance services business - Enterprise architecture as a coordination tool', *The Journal of Systems and Software*, vol 80, no. 10, pp. 1607-1620, DOI=10.1016/j.jss.2007.01.044 http://dx.doi.org/10.1016/j.jss.2007.01.044.

Purpura, P 2007, *Security and Loss Prevention : An Introduction*, 5th edn, Butterworth-Heinemann, Burlington.

Raggad, BG & Emilio, C 2006, 'The Simple Information Security Audit Process: SISAP', *International Journal of Computer Science and Network Security*, vol 6, no. 6, pp. 189-198.

Ramanathan, S 2007, 'IT Governance—Challenges in Implementation From an Asian Perspective ', *ISACA Journal*, vol 5.

Rasmussen, M & Koetzle, L 2007, 'AS/NZ 4360 — A Practical Choice Over COSO ERM', Best Practices, Forrester.

Ray, E & Schultz, E 2009, 'Virtualization Security', *In Proceedings of the 5th Annual Workshop on Cyber Security and information intelligence Research: Cyber Security and information intelligence Challenges and Strategies (Oak Ridge, Tennessee, April 13 - 15, 2009)*, ACM, New York, Article Number 42.

Ridley, G, Young, J & Carroll, P 200, 'COBIT and its utilization: a framework from the literature', *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*.

riskworld.net 2003, *Introduction to Security Risk Analysis*, viewed 12 December 2012, < HYPERLINK "http://www.security-risk-analysis.com/" http://www.security-risk-analysis.com/ >.

Robinson, N 2005, 'IT excellence starts with governance', *Journal of Investment Compliance*, vol 6, no. 3, pp. 45-49.

Ross, Shah, J & Jain, AK 2007, 'From template to image: reconstructing fingerprints from minutiae points', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol 29, no. 4, p. 544–560.

Rungta, S, Raman, A, Kohlenberg, T, Li, H, Dave, M & Kime, G 2004, 'Bringing Security Proactively into the Enterprise', *Intel Technology Journal*, vol 8, no. 4, pp. 303-312.

Sahibudin, S, Sharifi, M & Ayat, M 2008, 'Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations', *Asia International Conference on Modeling & Simulation*, pp. 749 - 753.

Saidani, M, Shibani, A & Alawadi, K 2013, 'Managing data security in the United Arab Emirates', *Prime Research on Education*, vol 3, no. 3, pp. 458-464, < HYPERLINK "http://www.primejournal.org/PRE/pdf/2013/apr/Messaoud.pdf" http://www.primejournal.org/PRE/pdf/2013/apr/Messaoud.pdf >.

Saint-Germain, R 2005, 'Information Security Management Best Practice Based on ISO/IEC 17799', *T h e I n f o r m a t i o n M a n a g e m e n t J o u r n a l* , pp. 60-66.

Saleh, ZI, Refai, H & Mashhour, A 2011, 'Proposed Framework for Security Risk Assessment', *Journal of Information Security*, vol 2, no. 2, pp. 85-90.

Satoh, N & Kumamoto, H 2009, 'An Application of Probabilistic Risk Assessment to Information Security Audit', *Proceedings of the 9th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC '09)*, Kyoto.

Schniederjans, MJ, Hamaker, JL & Schniederjans, AM 2010, *Information Technology Investment: Decision-Making Methodology*, World Scientific.

Sharifi, M, Ayat, M, Rahman, AA & Sahibudin, S 2008, 'Lessons learned in ITIL implementation failure', *International Symposium on Information Technology*, Kuala Lumpur.

Sikdar, P 2011, 'Alternate Approaches to Business Impact Analysis', *Information Security Journal: A Global Perspective*, vol 20, no. 3, pp. 128-134.

Singh, A,KM,AMD 2008, 'Server-storage virtualization: integration and load balancing in data centers', *Proceedings of the 2008 ACM/IEEE Conference on Supercomputing (Austin, Texas, November 15 - 21, 2008)*, Austin, Texas.

Sirkin, HL, Keenan, P & Jackson, A 2006, 'The Hard Side of Change Management', *Harvard Business Review*, 26 April 2006, pp. 1-13.

Software management systems Inc 2005, 'How companies incraese profitability,valuation and shareholder returns by adopting IT governance for software asset management ', White paper, An IT Governance White Paper, Software Management Systems, Inc.

Solms, BV 2005, 'Information Security governance COBIT or ISO 17799 or both', *Computers & Security*, vol 24, no. 2, pp. 99-104, viewed 12 January 2012, < HYPERLINK "http://66.160.138.180/documents/Cobit_ISO17799.pdf" http://66.160.138.180/documents/Cobit_ISO17799.pdf >.

Solms, BV 2006, 'Information Security – The Fourth Wave', *computers & s e c u rity*, vol 25, no. 3, pp. 165-168.

Speitkamp, B & Bichler, M 2010, 'A Mathematical Programming Approach for Server Consolidation Problems in Virtualized Data Centers', *IEEE Transactions on Services Computing*, vol 3, no. 4, pp. 266-278,.

Stoneburner, G, Goguen, A & Feringa, A 2002, 'Risk Management Guide for Information Technology Systems', NIST Special Publication 800-30 , Computer Security Division , National Institute of Standards and Technology , National Institute of Standards and Technology , Gaithersburg.

Symantec Corporation 2007, , viewed 21 January 2010, < HYPERLINK "http://www.symantec.com/about/news/release/article.jsp?prid=20071030_01" http://www.symantec.com/about/news/release/article.jsp?prid=20071030_01 >.

Tallon, P, Kraemer, KL & Gurbaxani, V 2001, 'Executives' Perceptions of the Business Value of Information Technology: A Process-Oriented Approach', viewed 12 February 2012, < HYPERLINK "http://escholarship.org/uc/item/9193h7v4 " http://escholarship.org/uc/item/9193h7v4 >.

Tanaka, T,TT,ANK 2009, 'Investigating suitability for server virtualization using business application benchmarks', *Proceedings of the 3rd international Workshop on Virtualization Technologies in Distributed Computing*, ACM, Barcelona, Spain, June 15 - 15, 2009, http://doi.acm.org/10.1145/1555336.1555344.

Tan, W-G, Steel, AC & Toleman, M 2009, 'Implementing IT service management: a case study focussing on critical success factors', *Journal of Computer Information Systems*, vol Winter, pp. 1-12.

Te-King, C, Wen-Lin, L, Wei-Chen, H & Mei-Fang, W 2007, 'A Study of ISMS Implementation Road Map', *Proceedings of International Conference on Business and Information*, Academy of Taiwan Information Systems Research, Tokyo.

Thompson, CW & Thompson, DR 2007, 'Identity Management', *IEEE Internet Computing*, May 2007, pp. 82-85.

Tong, CKS, Fung, KH, Huang, HYH & Chan, KK 2003, 'Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard', *Proceedings of the 17th International Congress and Exhibition*, International Congress Series, Volume 1256, CARS 2003. Comp.

Tracy, RP 2007, 'IT Security Management and Business Process Automation: Challenges,Approaches, and Rewards', *Information Security Journal: A Global Perspective*, vol 16, no. 2, pp. 114-122.

Trauth, EM 2001, *Qualitative Research in Is: Issues and Trends*, 1st edn, Idea Group Pub.

Veiga, DA & Eloff, JH 2007, 'An Information Security Governance Framework', *Information Systems Management*, vol 24, no. 4, pp. 361-372.

VMware, Inc 2010, 'Server Consolidation', White Paper, VmWare, www.vmware.com/solutions/consolidation/consolidate.html.

Wayman 1981, 'Biometrics-Now and Then: The Development of Biometrics Over the Last 40 Years', New York Times article:, New York.

Weill, P & Ross, J 2004, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business Review Press.

Wheeler, BC 2003, 'Aligning IT Strategy to open source partering and web services', Reserch Bulletin, Indiana University, Center for Applied Research, Boulder, Colorado.

Whitman, M & Mattord, H 2007, *Management of Information Security*, 2nd edn, Course Technology Press, Boston, MA, United States, ISBN-13: 978-1423901303.

Workman, M 2007, 'Gaining Access with Social Engineering: An Empirical Study of the Threat', *Information Security Journal : A global perspective*, vol 16, no. 6, pp. 315-331.

Yunis, MM, Hughes, J & Roge, J 2008, 'Real Security in virtual systems: a proposed model for a comprehensive approach to securing virtualized environments', *48 th Annual IACIS International Conference*, International Association for Information Systems, Georgia.

APPENDIX–A

Progress of the Research Project

This part of the document summarizes the work done by the author based on the valuable inputs provided by his supervisor.

Year	Achieved
2008	A taught course on research methodology was taken and a proposal was submitted as part of the course work after preliminary literature review. The proposal was later changed completely to information security domain with due approval from the supervisor.
	An initial study of various information security standards and frameworks such as ISO 27001, COBIT, ITIL and COSO was done.
	Research aims and objectives were defined after studying the information security implementations issues in ministry of education and ITA.
2009	A detailed literature review was done to study the information security practices followed globally and Oman in particular.
	Analyzed background theory and the importance of ISMS and previous research finding to arrive at the research problem.
	Conducted in-depth interviews with security management practitioners in various enterprises in different industrial domains
2010	A detailed literature review was done on enterprise information security and a strategically balanced governance risk and

	compliance (GRC) model was developed.
	A paper was presented in the 2010 International conference on security and management (**SAM10**) in Las Vegas USA (Please refer Appendix-C for the article).
2011	A project on server virtualization was implemented using bare metal hypervisor architecture for one of the ministries in Oman to ensure that operationally critical information is available, accurate, and up-to-date.
	A paper was presented in the world congress on Internet security (World CIS 2011) London. It was later published in **IEEE Xplore** (Please refer Appendix-D for the article)
	A questionnaire was designed and distributed to security practitioners in Oman on Enterprise Risk Management to check if they are in following international ERM framework such as COSO.
	The findings were analyzed and recommendations provided which resulted in a paper that was presented in the 9th Australian Information Security Management Conference (**SECAU**) (Please refer Appendix-E for the article).
2012	To ensure that sensitive information is treated in accordance with law, regulation, and organizational policy, critical control objectives based on COBIT were selected and mapped with best practices that aligns to the goals of the enterprise and implemented IT governance.
	The findings were analyzed and recommendations provided

	resulted in a paper which was presented in the World Congress on Internet Security (WorldCIS-2012) in Canada. It was later published in **IEEE Xplore** (Please refer Appendix-F for the article).
	The extended version of the above paper has been refereed and accepted to be published in the International Journal of Internet Technology and Secured Transactions (**IJITST**), ISSN (Online): 1748-5703 - ISSN (Print): 1748-569X. (Please refer Appendix-G for the article).
	Through interviews and practical experiments complexities of auditing in virtual environment were explored and an audit process flow was defined.
	The taxonomy of risks inherent in virtual environments was explored and a novel framework was provided. The findings were analyzed and resulted in a paper which was presented in The 2013 CICEM, conference sponsored by (**ACM**) Amman, Jordan April 29-May 1, 2013. (Please refer Appendix-H for the article).
2013	Document and Assemble Dissertation Chapters, Review for Consistency, Completeness and prepare presentation for defense.

APPENDIX –B

Audit Questions

Sl. No	Risk Taxonomy	Audit Question	Strongly Agree (4)	Agree (3)	Somewhat agree (2)	Disagree (1)	NA (0)
1	Administrative risks	Are all the operational policies and procedures regularly updated?					
2	Administrative risks	Do you have controls for ensuring integrity?					
3	Administrative risks	Do the documents for change control refer to the correct partition on the correct server?					
4	Administrative risks	Evaluate backup/ DR capabilities.					
5	Administrative risks	Is a physically separated administrative					

		infrastructure used for management functions, such as creating new VMs or changing existing images?					
6	Administrative risks	Are there management-approved initiatives to prevent spoofed source address attacks, connection hijacking, route hijacking and man-in-the-middle attacks?					
7	Administrative risks	Is a documented configuration management (CM) process utilized for all VM additions, changes or deletions of users, groups, roles and permissions?					
8	Administrative risks	Logical access controls such as application security and segregation of duties should be applied for all					

		levels of users.					
9	Administrative risks	Training the staff on virtualization technology and security features in a virtual IT system					
10	Application risks	Do you have application redundancy?					
11	Application risks	Is all the applications tested for functionality and performance?					
12	Application risks	Are the software's developed to address application security issues? (issues such as: sql injection, buffer overflow etc.,)					
13	Architectural Risks	Do you have fault tolerant network?					
14	Architectural Risks	Do you have Fault tolerance					

		Data storage?					
15	Architectural Risks	Are the virtual machines separated by sensitivity?					
16	Architectural Risks	Is all network traffic managed on a dedicated virtual local area network (VLAN) or network segment?					
17	Configuration risks	Do you have firewall protection for each VM?					
18	Configuration risks	Are the configurations of virtual machines are secured such that vulnerabilities in one function cannot impact the security of other functions?					
19	Configuration risks	Does the management console of the virtual machine manager have tight access controls, locked					

		down to specific users and specific partitions or machines?					
20	Configuration risks	Are there controls for specific users that limit access and read/write capabilities?					
21	Configuration risks	Does the system have orphaned images?					
22	Configuration risks	Are the host firewalls capable of detecting intrusions/ malware analysis?					
23	Configuration risks	Is the host configured to log changes to the VMs including incidents of copying, moving or deleting from the host?					
24	Configuration risks	Do you have a Configuration management database (CMDB)					

25	Information leakage risks	Is there a provision to prevent file stealing using external media (e.g., floppy, CD/DVDRW, USB/flash drives)?					
26	Information leakage risks	Is there a provision to capture traffic coming into or out of the network interfaces?					
27	Monitoring Risks	Do you have a separate log server with restricted access?					
28	Monitoring Risks	Evaluation of Policies, Procedures and documentation					
29	Monitoring Risks	Evaluation of Controls					
30	Monitoring Risks	Evaluate the business continuity and capacity management strategies for the					

		virtual IT systems.					
31	Monitoring Risks	Evaluate the management, operational and technical controls in practice for the virtual IT systems, and evaluate whether there are any loopholes.					
32	Monitoring risks	Does the system automatically trigger alarms and generate incident reports?					

APPENDIX –C

Governance, Risk and Compliance Equilibrium Model for Optimizing Enterprise Information Security

APPENDIX –D

Effective Server Virtualization with Enhanced Security Strategy for Large Organizations

APPENDIX –E

AN EXPLORATORY STUDY OF ERM PERCEPTION IN OMAN AND PROPOSING A MATURITY MODEL FOR RISK OPTIMIZATION

APPENDIX –F

IMPLEMENTING IT GOVERNANCE USING COBIT: A CASE STUDY FOCUSING ON CRITICAL SUCCESS FACTORS

APPENDIX –G

INFORMATION SECURITY GOVERNANCE USING COBIT: FOCUSING ON CRITICAL SUCCESS FACTORS

APPENDIX –H

Information Security Audit in Virtual Environment

Ramalingam Dharmalingam
Faculty of Information Technology
Majan College,
Muscat, Sultanate of Oman

Arun Nagarle Shivashankarappa
Department of Computer Science
Middle East College,
Muscat, Oman

Leonid Smalov
Faculty of Engineering and Computing,
Coventry University, Coventry, United Kingdom
csx211@coventry.ac.uk

Anbazhagan Neelamegham
Faculty of Science,
Alagappa University, Karaikudi, India
Anbazhagan_n@yahoo.co.in

APPENDIX –I