Title Methods for developing secure software and environments for small and medium enterprises

Name Sean Pollonais

Methods for developing secure software and environments for small and medium enterprises

by

Sean Pollonais

A thesis submitted for the degree of Master of Science by Research at the University of Bedfordshire

2007

Declaration

I declare that this thesis is my own unaided work. It is being submitted for the degree of Master of Science by Research at the University of Bedfordshire.

It has not been submitted before for any degree or examination in any other university.

Name of candidate: Sean Pollonais

Signature:

Date:

Abstract

Information Security covers activity concerned with the protection of data to ensure that information remains available, to those with rightful access, in the condition that it was originally stored or transmitted. The push to interact via electronic data is constantly increasing. Businesses are demanding that software designers find novel ways of facilitating electronic commerce, creating new business models that have only become possible with the development of the Internet.

With the increase of traffic in information across the Internet, the risks associated with data have multiplied, matching the global growth in connectivity. Web application security deals with the measures taken to secure software built to promote e-commerce. Because it is necessary to accept user input across the Internet these applications carry a particular set of vulnerabilities that require a more technical approach to their mitigation. The applications themselves are usually composed of modules that interact across trust boundaries which all require hardening.

Information Security governance controls how a company secures its data and that of its clients. While there are laws and standards that address the security requirement, applying them to all magnitude of businesses is difficult because the policies are biased towards large organisations in their assumptions of resources. This thesis investigates an international standard that can be used by small businesses to achieve legal compliance and a reasonable level of security.

The thesis brings together a method for producing secure web applications and a checklist procedure for improving a company's data protection practices. Both offerings apply to small software production houses where there may be some overlap in role function and the pressure to meet software production deadlines can sometimes lead to a culture where security is seen as an avoidable expense.

List of Contents

List of Tables

List of Figures

1 Introduction

We are in an information age where quality information has become the foundation of success for organisations in any sphere of activity. Advances in computer processing power and storage capabilities have increased the uses of the technology including streaming of video, audio, instant messaging, remote working and buying and selling online (e-commerce). Information is now recognised as an organisation's most valuable asset and that brings the need for Information Security (InfoSec) into prominence.

The Internet increased the exposure of all data because it linked networks to other networks and made it possible to access data from outside of individual networks. The volume of information available has led to the success of search engines such as Google whose name has now become the generic word for researching a topic online. One company in the UK (IssueBits Ltd., 2006) offers a text messaging service that answers questions from the public. We now expect information quickly and around the clock not only in the form of questions answered but also in goods bought, access to information and friends and family contacted. E-cards, for example, have increased the accuracy of delivery to match the date of an occasion. Online banking has nearly replaced the need to visit the local branch and has been encouraged by banks with higher rates of interest on accounts set up online. Retailers give online discounts to increase their volume of online sales and number of customers because of the efficiency of operating via the Internet.

Information collection has been made easier by automated processes and hence the volume of customer data resident in organisations' systems is tremendous. Users are encouraged to register their details in order to enjoy the benefits of remote interaction. One example is the Financial Times (FT.com, 2006) a newspaper website which offers readers two levels of paid membership with the higher grade giving access to special articles and promotions. Both levels require registration of details including email address and a password. There would be the choice of saving that password to the reader's machine for future automatic login. Those details are now stored in two places, the machine and the newspaper's servers. On accessing the site those details are transmitted across the Internet. The competition for web users' attention has led to the majority of websites devising ways of collecting information from visitors to enhance and make easy any subsequent marketing interaction.

The value attached to information has not gone unnoticed by the hackers. Digital crime is a constant concern for everyone operating via the Internet because the threats to InfoSec are rising in proportion with the reliance on computers to collect, process and store information. A high percentage of businesses have installed firewalls on their networks to keep out malicious traffic but this is not the final solution as crime conducted over the Internet (cyber-crime) has shifted its attention to the vulnerabilities within web applications which are allowed through firewalls as authorised traffic. Once entry is gained to private networks the threats to the information include interception of telecommunications (voice or data), theft / breach of

proprietary or confidential information, degradation of network performance, blackmail and denial of service (AIC, 2006). One recent threat is that of criminals gaining access to a system, encrypting the resident information and offering a price to the data owners for the decryption key (Payton, 2005).

The quality of information can be qualified using criteria including Confidentiality, Integrity, Availability, Authorisation, Authentication and Non-repudiation. These would rank differently in importance depending on the nature of the organisation. Confidentiality would be of primary concern to the military that depends on secrecy for its success over an enemy. In an online shopping website, the prices of goods require integrity because if tampered with, the seller can lose money on a sale. When users attempt to access information it should be available as promised because the expectation of constant availability has shaped the scheduling of tasks, which before were only possible within the eight-hour working window. International collaboration on projects is an example of this need for continual access to data. Information must also be protected by proper authentication methods that support the classifications used to grant access to authorised persons. Non-repudiation ensures that when information is sent there is no chance of denying that it has been received as in the case of online contracts where there must be certainty as to who has accepted the information. Networks remain vulnerable to insider attacks or accidental breaches and the proliferation of these has in large part been a result of the dichotomy of having to allow access to insiders

while limiting it to authorised users. The biggest threat to an organisation's InfoSec comes from the staff members but it is not clear how much is accidental or malicious. There is also the threat of social engineering, where authorised persons are coerced to access the information on the criminals' behalf.

Web applications enable e-commerce. They are designed to accept users' information, process purchases, inform users of the status of their order, deliver software and perform other functions that are added to enhance the customers' experience. Vulnerabilities are present across the entire pipeline and increase with the number of entities involved in completing a transaction. Building a secure web application requires software designers to identify the flow of information and the boundaries between processes. The application should be designed to mitigate these threats and during production developers need to test the design at every stage to ensure that the design meets the requirements when put into practice. There also has to be some mechanism whereby the security of an application can be rated with respect to current threats as these continue to mutate as the power of computers and the skills of criminals increase.

Organisations are subject to legislation that governs how information should be dealt with. There are many laws and standards, some of which have global significance while others are designed for specific industries. In a bibliography compiled by the Corporate Information Security Working Group (CISWG, 2004), 81 different standards are listed. These standards

have increased in tandem with the use of the Internet as a vehicle for information exchange.

To fulfil their obligation to protect information, organisations need to make decisions on the policies, strategies and controls they employ. It is prudent that the cost of mitigating the expected damage should not exceed the value of the information. This makes it apparent that not all risks can be cost-effectively defended therefore organisations have to take a decision as to the level of security an asset can be afforded.

In the UK the Data Protection Act (DPA) and the Computer Misuse Act (CMA) are two laws that apply to all organisations dealing with digital information regardless of size. The ISO27001 standard (BSI, 2007) is a widely accepted guide that supports the intent of the above-mentioned laws and provides controls that go further in elevating an organisation's security level. The number of controls listed in ISO27001 and the infrastructure assumed by the standard makes it difficult for small business to achieve full compliance and certification.

This thesis presents two new contributions to InfoSec by delivering a new software development method and a bespoke set of controls derived from ISO27001 both aimed at small businesses. Small businesses are classed as having less than fifty employees. In the UK roughly 99% of enterprises are small with 73% being sole proprietorships (SME Statistics, 2005). The contributions' main focuses are companies where staff resources are limited and the business case for staffing a Security Department does not

make sense. In these enterprises there is much overlap of roles and in order to secure information successfully, Best Practice must be adapted to suit the lack of staff and area-specific knowledge.

The software method is an amalgam of techniques which involves auditing what is already produced and recording the findings in a matrix that allows the necessary improvements to be measured. The development team adopts a "Secure-by-Design" approach to planning the program. They also use a suite of tests to complement a production method called Test Driven Development (TDD) (Beck, 2002) which helps produce secure software at less expense.

The laws and standards developed over the years have shown a bias towards medium and large companies where the manpower is more likely available to be dedicated to fulfilling the legislated recommendations. A small company would welcome external help in raising the level of InfoSec in all its operations. The ISO27001 adaptation strips away all the seemingly heavyweight overheads and presents a list of controls that would provide protection of data to an acceptable level. It is also meant to raise security awareness within a company so that staff can contribute to the constant vigilance needed where InfoSec is concerned.

2 Existing Work

2.1 Introduction

This chapter looks at the research that has been done in the field of information security starting from as early as 1998 until as late as 2006. The researchers offered solutions ranging from technical innovations to improvements in the approach to policy design. Research into InfoSec at SMEs is also referenced as this topic is the focus of this thesis.

2.2 Application Security

Web application security is a relatively new field. In 1998 web applications' security mechanisms were described as a collection of clever ad hoc efforts to retrofit security (Rubin and Geer, 1998). This paper recognised the need for a more serious approach where security is considered as part of the design stage.

Since this time the research into web application security has produced technological and logical systems to enhance the security offerings of developers. One such proposal was for a three-part framework of systems comprised of tools employing:

- an XML-based language for specifying credentials and access control policies;
- secure mechanisms to check the consistency of access control information at the global and local levels;
- authorisation constraints on user assignments to tasks (Thuraisingham

et al, 2001).

Lavery and Boldyreff's project in 2001 looked at the use of web applications in a university environment. This is relevant because universities have the dilemma of having systems that require many access points for administrators across departments but whose systems must also offer access to students within their account privileges. Their proposal for a technological solution implementing web-based, user oriented portals built around the identity of the user, allowed the security to be dynamically maintained. This was also an early example of including security at the design stage.

Web application security continued to score below expectation and researchers aimed to assist programmers by providing tools and techniques that allow developers to concentrate on the functionality of an application (Scott and Sharp, 2002). In another paper published that year, the lack of knowledge to create web software of sufficient quality was highlighted and the use of traditional software engineering practices was suggested (Offutt, 2002).

Further research brought out more issues for development teams to consider. The dynamism of the Internet and the variety of components that go into a successful client / server interaction pointed to the need for a holistic view of the security to be designed into the system because the lack of structure, where security critical code is scattered throughout the application, made threat mitigation difficult (Scott and Sharp, 2003).

The approach to security in web applications continued to focus on the awareness of the risks involved and the method of development. Added to this was the recognition that business goals determine risks with causal links that arrived at the repair and enhancement of web application security (Verdon and McGraw, 2004). This study highlighted the inclusion of the business owners in the process of determining the scope and security measures of web applications.

In 2004 Sneed listed some of the difficulties involved in building secure applications and highlighted the mercurial nature of web architecture stating that "the moment an error is corrected in the server, the interface to that server may no longer respond in the same manner." The main suggestion was that applications should be tested to ensure that they are protected from failure in all anticipated situations. The feasibility of this approach can be questioned as it does not cater for unforeseen problems but it is considered as a step in the right direction where some form of product testing is added to the development process.

Today web application developers no longer look for a one-stop technological or methodological solution that can be plugged into a project to solve all security issues. It is accepted that the technology of the Internet is constantly changing with updates to present platforms and rival technologies arising continuously, creating new security threats that will require additional security upgrades to existing applications.

Despite the advances made in web application security, in 2001 Birnieks

claimed that some of the same vulnerabilities still exist. He pointed out that most projects set to go live on the Internet are rushed with security viewed as a hidden benefit with lower priority against 'interface' development, developers still lacked security awareness and projects were not always coded to specification. Recognition was also given to the fact that today's web environments are more complex than before.

2.3 Novel Offering

With this knowledge, the approach in this thesis to improving the security offering of web applications focuses on making development teams aware of the necessity of adopting a constantly vigilant attitude to the systems they build. The first transformation would be to adopt a "Secure by Design" approach which takes a holistic view of a web transaction and highlights the various security issues associated with that transaction as shown, for example, in Figure 1, shown below.

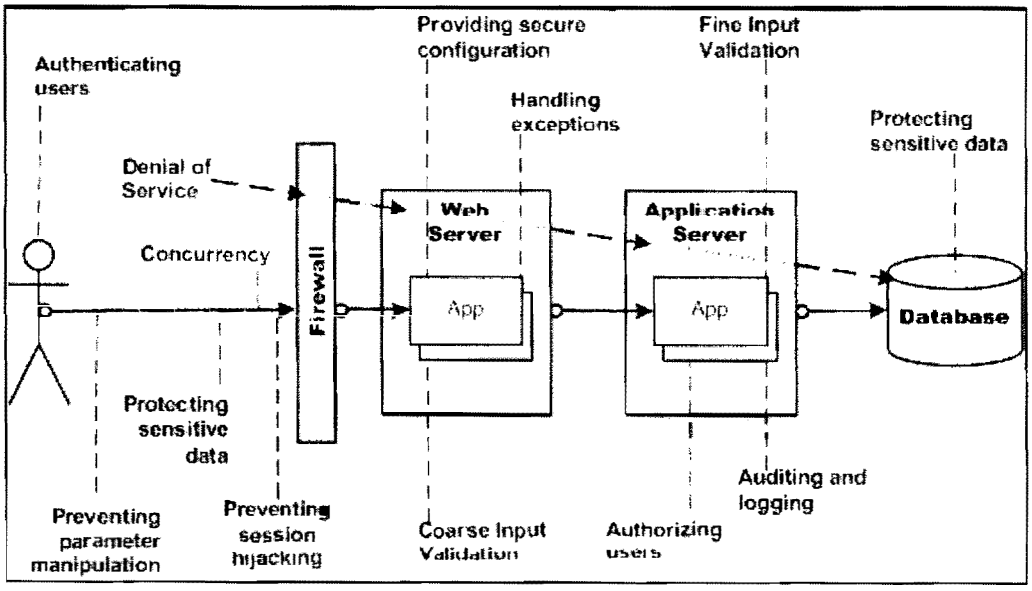

Figure 1. Common web application security concerns (Graf, 2005)

The diagram shows the transaction pipeline of a typical web application and some of the security concerns that are present when data is transferred across the Internet and between different applications and machines.

The second change put in place is the use of a TDD method. The two techniques were chosen in combination to bring to developers a new culture of production that should prove more efficient and produce applications that are reliable and secure. The two methodologies are described in later chapters.

2.4 Laws and Standards

Academic studies into the various InfoSec laws and standards have mostly offered explanations of the foundations and ways to improve the applicability of these laws and standards to an ever-changing business environment. The studies offer improvements to the scope and utility of the laws and standards that are in use today. They do not specifically focus on small UK businesses but are useful to the theme of this thesis because in them we find common concerns among organisations with respect to InfoSec.

In 2001 Blakley and McDermott said that InfoSec was in the early stages of protecting the information resident on and exchanged among the systems of organisations. They speculated that there were similarities between the state of InfoSec then and medicine in the 19th Century where doctors and pharmacologists were at a naïve stage of understanding the

causes and cures of diseases. They said a solution similar to that taken within the medical profession of certifying doctors and establishing a code of practice among them was needed to improve the state of InfoSec. InfoSec professionals should subscribe to a code of practice and regularly update their subscriptions. Information from research should also be shared more vigorously in order for InfoSec professionals to remain up to date with the latest developments.

The criminology theories that are at the base of the standards devised for InfoSec have been considered with the intention of improving standards. Theoharidou's study (2005) suggests that to develop better standards a multi-paradigm and multi-disciplinary approach towards InfoSec management and insider threat mitigation is needed. This new approach should look at recent criminology theories that would enhance the General Deterrence Theory (Nagin, 2001) that forms the base of ISO17799.

The level of security attached to information needs to comply with a common standard when information is shared among business partners. The Internet has made this sharing of data easier than before and has also brought new models of collaboration that involve the exchange of valuable private data. Information systems must also be properly guarded from malicious use as gateways into other systems. Business partners now demand an acceptable level of InfoSec from one another and would depend on standards to play a role in this regard. (von Solms, 1999)

Data resident within company systems has to be secure to a level

providing accountability for whatever transactions are conducted on that data. Controlling access to documents with passwords is not considered secure enough and biometrics is recommended as the technology best suited to providing the correct level of security and accountability. Foote and Neudenberger (2005) declare that biometrics is the only way to uniquely identify the user and provide proper accountability.

A top-down approach that allows the business needs to dictate the level of security of a piece of information is needed in order to update InfoSec (Gerber et al, 2001). A business impact analysis mapped against a business related set of questions is used to provide a lookup matrix which determines the level of protection needed for a piece of information. The focus in this case is on expanding the remit of security from protecting the infrastructure only to include adding security profiles to the information itself.

Dhillon and Backhouse (2000) stated that the accepted triad of InfoSec - Confidentiality, Integrity and Availability - were no longer adequate for the new ways organisations conduct business and proposed that the quartet of. Responsibility, Integrity, Trust and Ethicality (RITE) were more in tandem with the changes that were taking place in the business world due to the high use of Information Technology. Technical controls were vital and provided security and accountability but as the form of organisations changed with the pace of technology, new ways of addressing the role of information in the organisation were needed. For the purposes of this

thesis, RITE would not be used as it adds complexity while not improving its security offering proportionately.

InfoSec changes with the way information is used among businesses. Information Technology is growing rapidly and therefore security has moved from being a technical issue to being standardised across organisations interacting with a number of human / social factors. The next step is for InfoSec to become an integral part of Corporate Governance and this is evidenced up by the growing influence InfoSec professionals are having on the boards of major companies because technical solutions no longer work alone. This development is seen as the so-called Fourth Wave of InfoSec (von Solms, 2006) that is defined as the process of the explicit inclusion of InfoSec as an integral part of good Corporate Governance, and the maturing of the concept of InfoSec Governance.

These studies all offer improvements on the present standards through various means. Small and medium enterprises (less than 250 employees) are unlikely to have the resources and sophistication available to larger organizations. Consequently, a more modest subset of metrics advocating the "Fundamental Five" (CISWG, 2004) as minimum essential practices appropriate for SMEs is listed as:

- Malware protection, including worms and viruses
- Change management, including patch management
- Identity and access management, including privilege assignment and

authentication

- Firewalls including workstation, host, sub-network, and perimeter as required

- Configuration management

Additionally, security awareness training prior to being granted access to the organization's networks and periodically as condition of continued access is recommended. One survey in the UK showed that only 23% of business employees received ongoing training in the security policies of companies (DTI, 2004).

Security should be engineered to provide a level of protection that is considered "good enough" for the purpose (Sandhu, 2003) because the cost of mitigating vulnerabilities must not exceed the value of the asset being protected. As it stands at the moment, end users are oblivious to the risks their actions have on systems (Finch, 2003) and the number of instances of lax practices remain a concern (Furnell, 2004). Sandhu's recommendation is that security be designed to operate without the knowledge of the end user.

Security is not a one-stop fix but a continual process evidenced by statements such as "efforts should be made to ensure that it is not annoying for employees, and users should be rewarded for their good behaviour" (Langue, 2005).

Small businesses make up the majority of registered businesses and yet

their security concerns have not been as extensively researched as big businesses. The assumption that big businesses provide all the answers needed for security research is erroneous because small companies operate with fewer resources and due to an overall lack of technological resources would often decide to omit security controls where the understanding of the techniques would require a high cost in time and labour. Small businesses perform worse than large organisations not only in compliance issues but also in areas such as the deployment of firewalls and antivirus software. For a clearer picture more research needs to be aimed at small businesses (Dimopoulos, 2004).

2.5 Summary

This thesis looks at the difficulty faced by small businesses in attempting to address compliance with the security levels proscribed and presents two contributions aimed at small businesses that are designed to provide security solutions that require a level of knowledge that is more likely available in the small businesses sector.

3 Ensuring Quality Software Development

3.1 Introduction

In the early stages of software development, applications were built by programmers who followed a simple approach that worked for small projects. As the size of applications became bigger and their complexity grew it became important to structure the method used for the increasingly large teams of developers.

3.2 Software Development Methods

3.2.1 Waterfall

The oldest and best-known method is the Waterfall Life Cycle (OIT, 2005) that is made up of a succession of stages where the output of one stage is the input of the following. Figure 2 shows the stages and how they are linked.

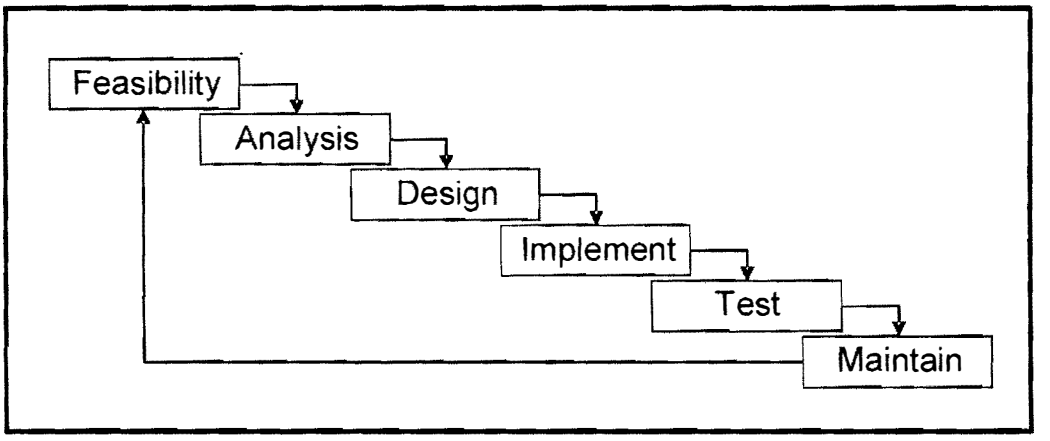

Figure 2. Waterfall Software Development Life Cycle

A description of the phases follows:

- Feasibility study: A high-level view of the proposed project where goals are determined.

- Analysis: Project goals are translated into defined functions and how the application will process data. End-user needs are defined.

- Design: Describes application operations in detail, including layouts, process diagrams, business rules, pseudo code and all necessary documentation.

- Implement: Code is written.

- Test: Create a testing environment to check for errors, bugs and vulnerabilities.

- Maintain: Adjusting the application as it is released in the real world and has to cope with different operating environments and unanticipated usage.

The limitations of the Waterfall model include its ability to cater for changing user requirements as the project progresses. Original specifications are usually altered when the user is made to be part of the development process. The Waterfall method is no longer considered useful although many others have been developed based on this model. In a 1991 Information Center Quarterly article, Larry Runge stated that the Waterfall "works very well when we are automating the activities of clerks and accountants. It doesn't work nearly as well, if at all, when building systems for knowledge workers -- people at help desks, experts trying to solve problems, or executives trying to lead their company into the Fortune 100."

A software development life cycle (SDLC) should be flexible to include new ideas for the performance of the application and should accommodate methods that reduce the time taken to deliver a working product. Other SDLCs adopted by software developers include the following; the Fountain Model, the Build and Fix Model, the Spiral Model and the Rapid Application Development (RAD) model (OIT, 2005). The last two are briefly described below;

3.2.2 Spiral

The Spiral Model (OIT, 2005) was developed by Barry Boehm in 1998 to provide developers with a clearer explanation of the incremental development of a system. The Waterfall model is used to define each step to help manage risks. Details of the highest priority features are first defined and implemented. Evolutionary progress is made with feedback from customers and the system is built up as more details of the entire specification are added to the product.

The model offers advantages such as more realistic budgeting due to the early identification of elements, more adaptability to change and an earlier start to programming as shown in Figure 3 on the following page.

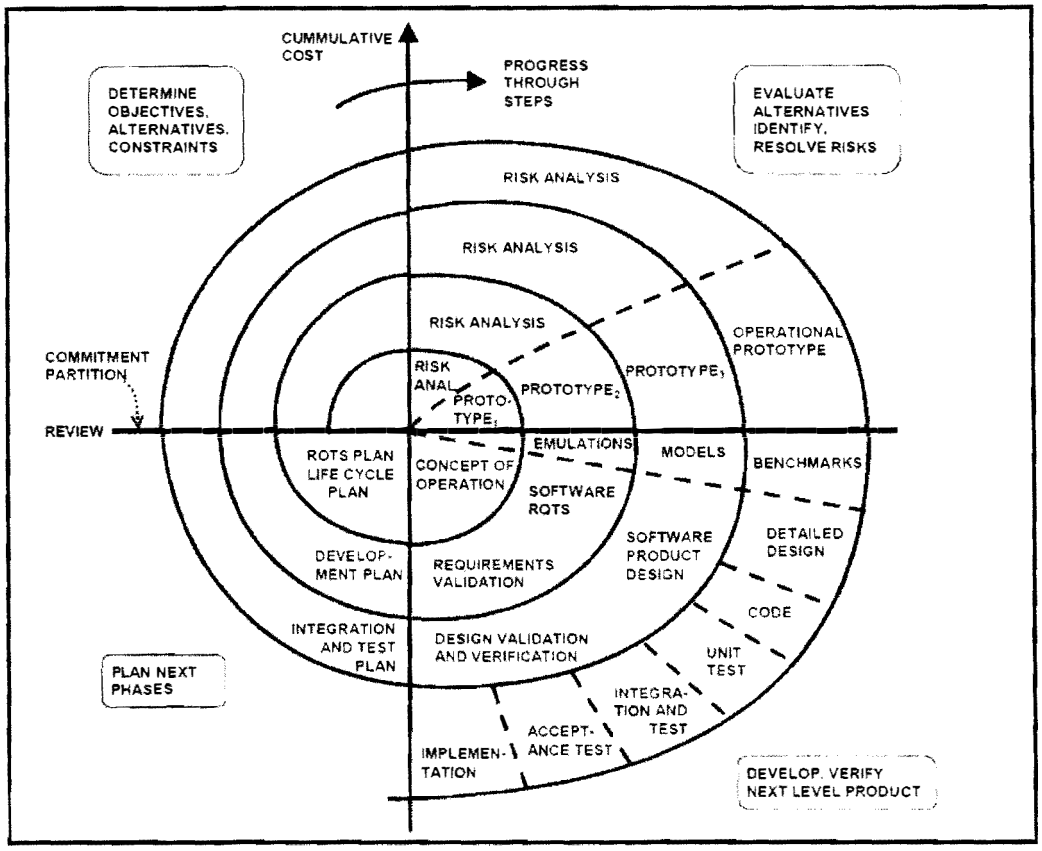

Figure 3. The Spiral Model (Boehm, 2000)

3.2.3 Rapid Application Development

James Martin developed RAD in the 1980s. It does away with the linear progression of the Waterfall and allows customers and developers to work closely to build thoroughly engineered portions of a system at a very early stage of the project. With each version both parties are able to judge the effectiveness of the previous specifications, correct mistakes and tune the performance of the system. This process is repeated until the final product is delivered.

RAD offers software production that is faster and of higher quality by defining requirements using focus groups, reiterative user testing of designs, re-use of software components and production schedule that

waives design improvements until the next product version, shown in Figure 4 below.

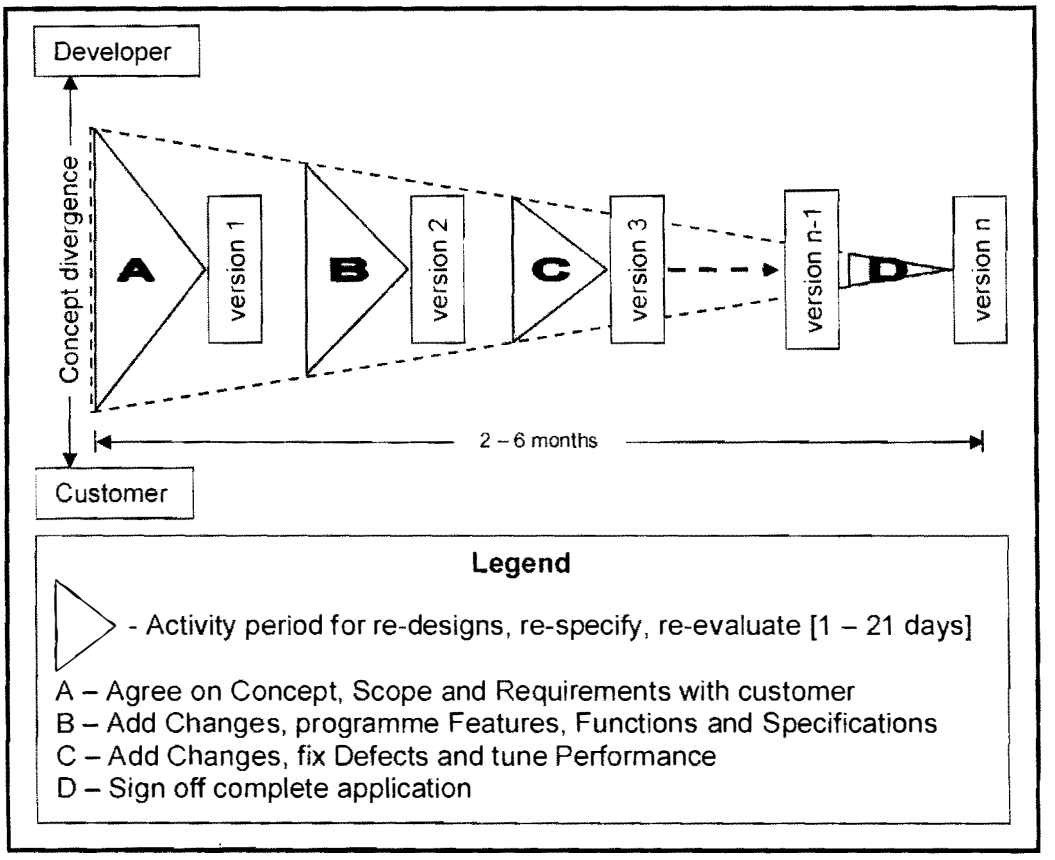

Figure 4. Rapid Application Development

3.3 Hybrid Method

This thesis accepts the idea that a SDLC could be chosen and adapted to best suit the operational demands of the software company. Two established methodologies, Secure by Design and TDD, were amalgamated to give developers a schema for the production of secure applications within a cost-effective time frame.

3.3.1 Secure by Design

Secure by Design is a software production approach that takes a high

level view of the transactions involved across the network when a user interacts with a web application. The development team draws up the list of assets marking where along the data pipeline they reside creating trust boundaries between entities that interact with each other. By adopting this high level view of the entire process, security features can be built into the application to counter threats at their locations. It is this type of threat awareness that translates into developers producing applications secured with an in depth knowledge of the software capabilities to mitigate localised threats.

Securing an application from the design stage is meant to make it more protected and fault tolerant. This includes such safeguards as the program not breaking when it receives an incorrect type of input to operate a certain function. For example, in some cases a null input can cause a poorly built application to throw an exception.

During the design stage, programmers will look at the application's documentation and imagine how a user would interact with the program. For example, the web site might need a user to log in with a username and a password. Developers will look at the many ways a user can enter information and what types of information can be entered. The best way to ensure that the application gets the information it needs is to design limits on the input boxes that accept only what is needed. This avoids having to screen for every type of input that might damage the program but rather screen for correct input only by verifying that input data is in the specified

format. In the username input box the application would check that the input is within a certain length, usually a maximum of 20 characters and is of a certain type, again, usually alphanumeric with no special characters.

Across the transaction pipeline between user, application and database there are points of interaction. The user logs into the application, the application logs into the database, the application might also get information from another web service and the application returns data to the user. The guiding principle of Secure by Design is to never trust inputs.

At each interaction point some form of input is accepted by another object within the application or by a web service. It is important that the information being passed is in the correct format and it is what the receiving object or web service is expecting. By taking a high level view of these transactions it is possible for programmers to work out the trust boundaries and what type of security is needed across each. This knowledge informs the design of the application and what security features need to be built into the program.

Another practice that enhances this method is the principle of Least Privilege where programmers are encouraged to write code while operating as a user (Saltzer and Schroeder, 1974). By doing this, the developer gets to experience the program in much the same way as the user and avoids building a program that runs smoothly on administrative rights but crashes when the level of privilege is lowered to that of the user. Across the transaction pipeline the least privilege principle should be

adhered to with all users and objects being given the level of privilege that is needed to do their function and no more.

The advantages of the Secure by Design method are that the application is built with:

- necessary security measures at each trust boundary it comes across in its operation;
- least privileges being given to users and objects;
- the programmer operating in a least privilege mode to ensure that the users' experience is closely mimicked throughout.

3.3.2 Test Driven Development

TDD is a code production technique that is the central aspect of the Extreme Programming method. Programmers break programs down into all the necessary functions and build their programs one function at a time.

TDD cuts the gap between decision-making and feedback to a minimum. As the code develops in snippets it is possible to eliminate mistakes at a very early stage and avoid the cost of having code errors remain in the system long enough to affect other parts as they are added.

Programmers' skill in testing is improved with TDD because programmers acquire the habit of reviewing the effectiveness of the tests they write as the construction of the application goes along. The tests are all recorded and this accumulation makes it easier to test the entire application

automatically at any stage of its development (Appendix D). When new features are added to an application the effect that the update has on the entire application can be easily checked as shown in Figure 5, next page.

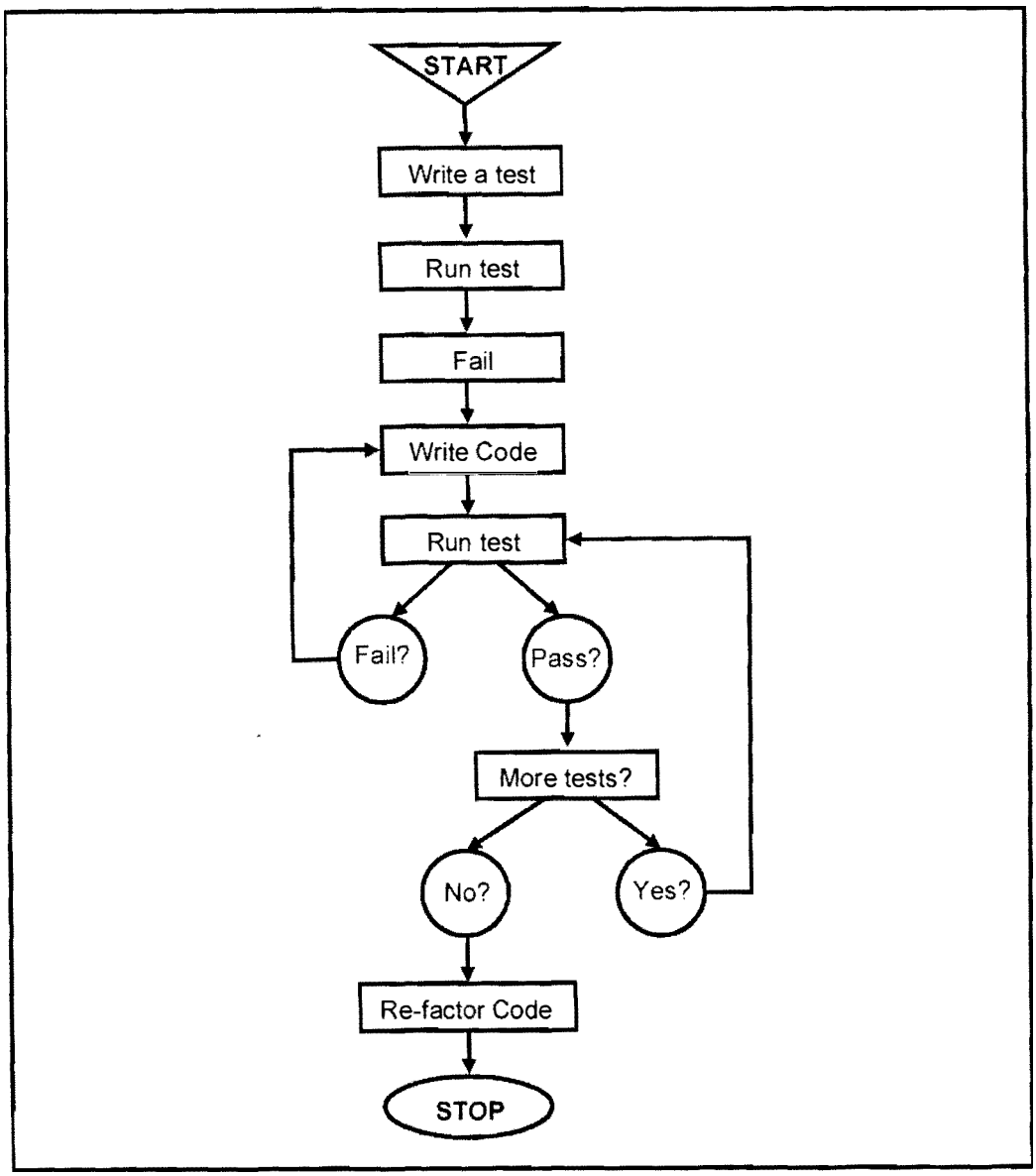

Figure 5. Test Driven Development

A study of the TDD method (George and Williams, 2003) highlighted some of the advantages that have brought this method to the attention of

developers. The main findings of that research are listed below:

- TDD approach appears to yield code with superior external code quality when compared with code developed with a more traditional waterfall-like model practice.

- TDD developers took 16% more time than control group developers. ...the control group did not primarily write any worthwhile automated test cases.

- On an average, 78% of the professional developers believed that the approach improves programmers' productivity.

- TDD approach facilitates simpler design.

In a study of the return on investment of TDD (Muller and Padberg, 2002) it was shown that the conventional development cycle is shorter but quality assurance is added after the code is written. With TDD quality assurance is integral to the development stage and the entire length of that stage results in a shorter project time.

3.3.3 Advantages

The amalgamation of Secure by Design and TDD produces a code production method that results in applications that protect the information they process and are reliably available for online business. Security by its nature is always a moving target making the process of guarding information a never-ending activity even after the deployment of applications. With a solid design foundation and the ability to test the

effects of additional safeguards, this hybrid method provides software companies with an advantage in offering a high level of InfoSec.

The tests used in TDD are informed by clear security goals and should be written to ensure that new code maintains these goals and safeguards the application against anticipated threats. As new threats are encountered, new tests are written to ensure the respective countermeasures are in place. Researchers at Microsoft have categorised the security threats to software, representing them with the acronym STRIDE (Hernan, 2006). Below are brief explanations of these threats.

- Spoofing: Impersonating a trusted entity so to induce an incorrect action.
- Tampering: Altering data without the appropriate rights.
- Repudiation: Denying participation in a transaction.
- Information Disclosure: Exposing data illegally.
- Denial of Service: Suspending the normal use of a system.
- Elevation of Privilege: Gaining higher unauthorised rights to data.

We use the general framework to demonstrate vulnerabilities and countermeasures. The vulnerabilities and countermeasures are given in Table 1 and are a superset of recommendations from Microsoft, research at a commercial software enterprise and the researcher's own experiences.

3.3.4 Vulnerabilities

There is a link between these threats and the vulnerabilities that are found within software systems. Some vulnerabilities expose a system to more threats than others. Table 1 helps developers design more accurate tests because it makes it easier to identify what vulnerabilities to test for and what threats to mitigate.

Vulnerability	STRIDE Threat	Countermeasures
Auditing and Logging	Repudiation	Secure Log File Management policies used on the administrative side.
Authentication	Spoofing Tampering Elevation of privilege	Special account set up to access the administrative privileges. Student group leaders have more rights than group members. SQL authentication between the web server and the database.
Authorization	Spoofing Tampering Repudiation Information disclosure Elevation of privilege	Access the database using stored procedures. Code access security through the roles and the privileges granted.
Configuration Management	Information disclosure Elevation of privilege	Distinct administrative and student privileges. Access is restricted from the student side. The configuration store is kept off the Web.
Cryptography	Tampering Information disclosure	Strong industry standard cryptography. Secure hashing algorithm (SHA1). Keys recycled regularly.
Exception Management	Information disclosure	Structured Exception Handling. Error messages give limited information to the customer.
Input validation	Denial of service	All input is managed within only one page. Web page input validated& Arguments and the query strings are encrypted.

Parameter Manipulation	Tampering Information disclosure Denial of service	Sensitive data not passed in parameters. Sensitive data not passed in query strings or form fields.
Session Management	Spoofing Information disclosure	Session lifetime is restricted. Session identifiers passed over encrypted channels with SSL.
Sensitive Data	Information disclosure	Storage of secrets handled with platform-provided Data Protection-API (DPAPI).

Table 1. Vulnerabilities, STRIDE and Countermeasures

Table 2 lists vulnerabilities and the technical countermeasures that can be used by the team. Note that the technology in this case is designed by Microsoft and the majority of solutions come from this software provider while others are the result of the researcher's own expertise.

Vulnerability	Proposed Technical Countermeasures
Input& Data Validation	• Buffer Overflows: Traditional C++, C, Memory Overruns, handled by .NET Framework, so not an issue. • Buffer Overflows: Form Level Validation (Required Field, Minimum Length, Maximum Length, Custom Rules). • Buffer Overflows & SQL Injection: Database Level& Validation (DB Required, DB Min Length, DB Max Length, SQL Injection, Double Encoding). • Buffer Overflows: Business Logic Validation, held in Business Logic Layer, not Web Layer. • Cross-Site Scripting: .NET Framework 1.1 has built in Cross Site Scripting Protection Code. • SQL Injection: SQL Injection Validation performed at Data Access Level • Canonicalization: Microsoft Canonicalization Fix Applied.
Authentication	• Login Retry Logic • Separate anonymous from authenticated pages (Use Built in Web.Config Deny Settings) • Encrypt communication channels to secure authentication tokens. • Use HTTPS only with forms authentication cookies • Use authentication mechanisms that do not require

	clear text credentials to be passed over the network • Do not store credentials. • Forms Authentication Still to be implemented. • Forms Authentication Routines (Cookie Encryption, Protection = All)
Authorization	• Use least privilege accounts. • SSPI Database Connections.
Configuration Management	• Unauthorized access to administration interfaces: No administrative interfaces initially provided. • Unauthorized access to configuration stores: Configuration Files are stored on the machine, and are encrypted (See Cryptography). • Unauthorized access to configuration stores: Avoid storing sensitive information in the Web space (XML Form Files, Configuration Files). • Retrieval of clear text configuration secrets: Credentials are not stored in clear text, No use of Local Security Authority (LSA). • Over-privileged process and service accounts: Use least privileged service accounts (ASP.NET account for website, SQL Server SSPI account for application). • Sensitive files not shown in webspace. • Configure to run under medium trust still needs to be implemented. • Over-privileged process and service accounts: Application should be able to run under Medium Trust. • Lack of individual accountability.
Sensitive Data	• No Hard Coded Sensitive Data in the Software. • Encrypt sensitive data over the network. • Secure the channel.
Session Management	• Session Hijacking: Session Timeout Expiration Code in place. • Session Hijacking: Configure Session Timeouts to a minimum. • Session Hijacking: Ability to configure a maximum number of website hits within a session. • Session Hijacking: Cookie Based, not Query String based Session Identifier. • Session Hijacking & Man in the Middle Attacks: SSL. • Session Hijacking & Session Replay: Ability to configure an absolute Session Expiry on top of the sliding expiration. • Session Replay: Critical Functions (such as Online Contract signing), require a revalidation of Credentials.

	• Avoid storing sensitive data in session stores. • Secure the channel to the session store. • Authenticate and authorize access to the session store. • Enhance Framework's support for Session Management, if using Windows Authentication rather than the current forms authentication. This is because we utilise the Encryption, Verification & MAC, built into the .NET Framework for forms authentication. • Forms Authentication still to be implemented. • Session Hijacking & Man in the Middle Attacks: Forms Authentication Cookies set to Protection=All (Encrypted, Verified, MAC).
Cryptography	• Use Microsoft Enterprise Library Encryption Routines where possible. • Encryption of Configuration Files. • Encryption of Sensitive Data in the Database (where appropriate). • URL Encryption. • Cookie Encryption. • Encrypted Communication Channels. • Encrypted Viewstate. • .NET Web Application Configuration Files are encrypted using the Microsoft Enterprise Library Configuration / Encryption routines. • Avoid key management. Use the Windows Data Protection API (DPAPI) where appropriate.
Parameter Manipulation	• Query string manipulation: URL Encryption. • Form field manipulation: See Input Validation Section. • Form Field Manipulation: Viewstate Encryption. • Cookie manipulation: Only Authentication Cookies are used, which are secured. • All Manipulation: Use of SSL. • All Manipulation: Avoidance of storing sensitive data. • All Manipulation: Non Reliance of passed data.
Exception Management	• Revealing sensitive system or application details: Use of Default Error Page, so where an un-handled exception filters through, a custom error page is displayed. • Revealing sensitive system or application details: Passwords and sensitive data will not be published to the Error Publishing Log. • Use structured exception handling (by using try / catch blocks).

	• Catch and wrap exceptions only if the operation adds value / information.
Auditing & Logging	• Failed Logins etc automatically logged • Form Level Logging available to Form Builders. • Error Publishing still to be implemented. • All Security Exceptions / Un-handled Exceptions are published to the Error Publishing Web Service (and if it's not available to the Event log).

Table 2. Vulnerabilities and Technical Countermeasures

3.3.5 Visualising Changes in Threats and Countermeasures

A development team securing an application would be best aided by a system of recording and measuring the steps taken to fortify the application. When a countermeasure is added, the team should be made aware of the effect this has on the overall security of the application. The first contribution of this thesis is a visual metric for the measurement of the strength of countermeasures built into an application, Figure 6.

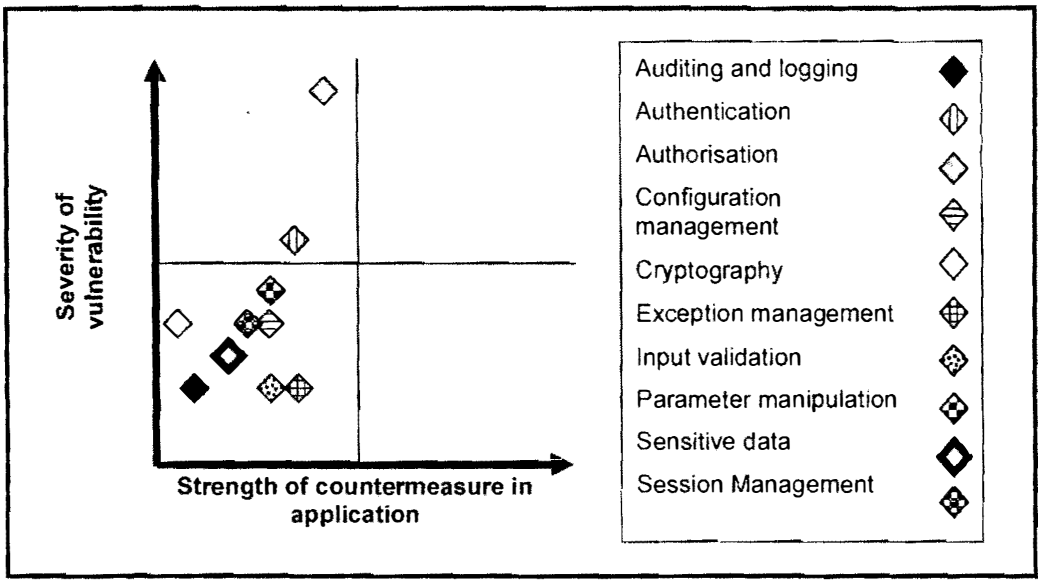

Figure 6. Strength of a countermeasure against the severity of vulnerabilities

The Y-axis plots the severity of the threats, calculated by the number of STRIDE components that apply to the vulnerability. Authorisation, the

process whereby a user is granted rights to data, is affected by five elements of the STRIDE acronym and thus ranks as the most vulnerable. Sensitive data does not score reflectively of this calculation as the value of the secrets kept in the Data Protection Application Program Interface (DPAPI) was considered of high value and this raised the severity of the threat posed by an attack on the sensitive data held by the system. The initial Y-axis values given are not likely to be changed throughout the development process.

The X-axis records the effects of the countermeasures designed into the application and these values are updated with each additional countermeasure. In Figure 6 the system has little or no cryptographic protection of its data. As cryptography is added to the system, the symbol would move to the right to indicate a strengthening of the countermeasure. The graph represents a relative summary of the strength of a countermeasure. If the strongest known encryption is applied to the system the symbol would be at the far right of the graph but if that algorithm is compromised, the symbol moves back to the left to indicate there is a margin for improvement.

The aim of the exercise is to reach the levels of countermeasure strength, across all the vulnerabilities, which are considered appropriate by the developers. That level must be a decision taken by the company as security always involves a cost–benefit analysis. Auditing and Logging is an example of a security feature that depends on the deployment

environment. It requires the client to host large files and run additional options of the software that can always be decision-based on a return on security investment calculation. A software engineer would assess the deployment environment of an application; determine the severity of a threat and the effect of strengthening a particular vulnerability in relation to the other countermeasures. The volatility of security requires that these measurements must be regularly reviewed in order to stay abreast with the latest threats.

A team can illustrate its agreed minimal by a line across the graph indicating that symbols to the right of that line would represent vulnerabilities that have been sufficiently fortified. Figure 7 on the following page shows the results of adding countermeasures to the application and how the team rates its security activity. This method for including security into the fabric of applications must be made available to developers to make the production of secure applications a co-ordinated operation that produces code that is pre-emptive by default.

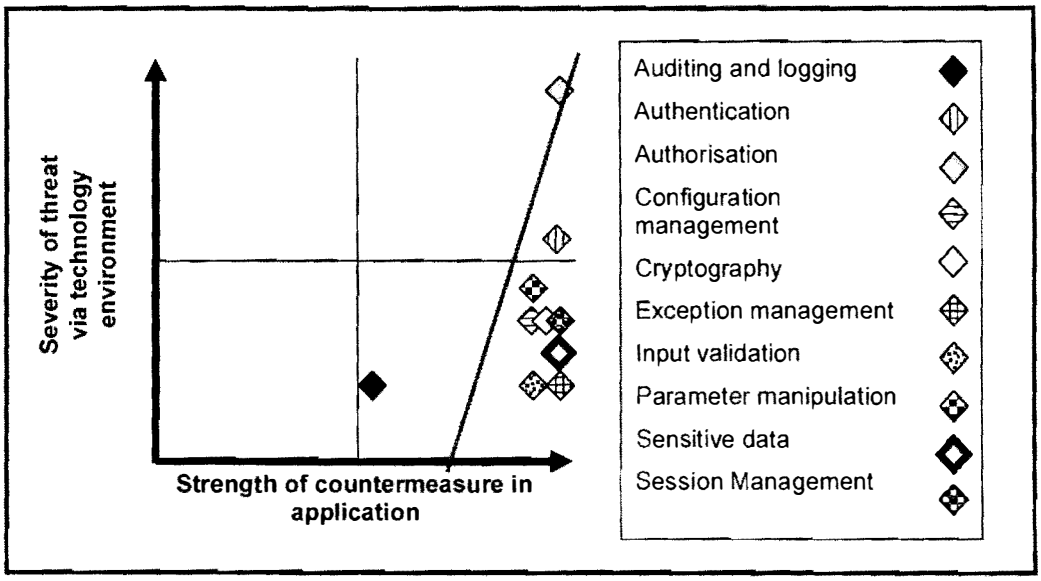

Figure 7. Strengths of Countermeasures

The development team decides on the limits of the countermeasures built into the application by the use of risk analysis to rate the severity of a threat. To do a proper analysis developers need to have knowledge of hacking techniques to know what are the threats and how likely they are to occur. Risk is proportionately associated with the value of the asset to be protected.

For example Authorisation might score as the most severely threatened vulnerability but the development team might possibly decide that the value of the data processed does not carry a great risk therefore the number of countermeasures can be fewer than what is needed to provide optimum strength.

The graph presents a visual, easy to read progress report for the team to share while building a secure application. It would serve as an ideal tool when the security level of a legacy application is being audited in order to

update the InfoSec to an appropriate present-day level. The graph is useful regardless of method because it records what the team considers to be the main vulnerabilities and helps measure where the team is in the process of building the necessary countermeasures.

3.4 Summary

This chapter presented the first contribution of this thesis which is a new approach to software development supplemented by a measurement tool for developers to gauge the strength of the countermeasures added to applications. The development method offered is a hybrid of Secure by Design and Test Driven Development which is meant o offer companies an efficient method of producing secure applications. The following chapter highlights the other contribution of this thesis which offers SMEs a tool to improve their InfoSec management.

4 Information Security Governance

4.1 Introduction

Information systems make use of the Internet and e-commerce by its nature involves possible international transactions and interactions, adding complexity in knowing which InfoSec standard applies to which type of business. The standards themselves have not achieved international conformance and this presents a challenge to business owners who wish to address the issue of compliance with the relevant laws and standards within their organisation.

Adhering to these standards ensures businesses that they are able to protect their information, which is often their most valuable asset. This overhead poses a problem for small businesses (less than fifty staff members) where there is often a multiplicity of roles at times resulting in the inability to research and enforce such measures as separation of duties or job rotation. Research into the recognised standards gives the impression that they are aimed at businesses that have developed a structure of accountability that can be absent in small businesses.

4.2 SME Challenge

Small companies are likely to be primarily concerned with maintaining the growth needed to ensure they achieve their long-term goals. While the focus is on maximizing the company's resources to meet short and medium term objectives, capital also has to be devoted to InfoSec. For example, in the software development industry, programs are produced to

process private information gathered by the users of the software. The software companies are responsible for the security of the application and also have to be mindful of the security levels of their entire operation.

4.2.1 Laws

There are laws that are incumbent on businesses to control the handling of data and along with the guidance of standards provide a proper starting point for the upgrading of a company's InfoSec status. The language and volume of the laws and standards, some of which are listed in Table 3, can prompt many small business owners to abandon the idea of developing security policies and providing the supporting procedures.

LAWS	STANDARDS
Data Protection Act 1998 (DPA)	ISO27001
Computer Misuse Act 1990 (CMA)	COBIT
Disability Discrimination Act 1995 (DDA)	GASSP
The Regulation of Investigative Powers Act 2000	ITIL
The Copyright, Designs and Patents Act 1988, including moral rights	GMITS
The Human Rights Act 1998	HIPPA
Freedom of Information Act (FOIA)	GAISP
The Electronic Communications Act 2000	OECD Guidelines
The Copyright and Rights in Databases Regulations 1997	IFAC
The Defamation Act 1996	CICA
Sarbanes Oxley Act 2002 (SOx)	BASEL II

Table 3. A Sample of Laws and Standards affecting Information

The standards and laws are sometimes complementary to each other and sometimes contradictory (Baer and Dietrich, 2006). Deciding exactly which laws and standards to follow is a challenge for businesses made more formidable by the absence of a tool to rate the level of compliance a company should achieve with respect to its circumstances.

The majority of business information systems are based on Information Technology systems and use the internet to make information available to staff and clients and to also enhance functionality of systems that have traditionally operated in closed networks. There are many laws that govern the handling of information on IT systems and they can range from the DPA, which helps secure the correct handling of data gathered by companies to the DDA, which is enacted to secure usability of websites for people with physical disabilities.

4.2.2 Standards

The number of standards that affect operations involving digital information is also high with the most recognised ones being referenced by the International Standards Organisation (ISO). This thesis uses the latest Information Security Management Systems (ISMS) standard, ISO27001, as the basis of a set of controls for UK small businesses to assess what InfoSec activities support legal compliance and a sound level of protection.

BS7799 was developed by the Department of Trade & Industry in 1995 as a code of practice to guide UK businesses in implementing an ISMS. The

standard was basically recommendatory but with its popularity came the call for a certification process to be added. The standard was split into two parts, BS7799-1 being the Code of Practice and BS7799-2 the specification for controls needed to attain certification.

BS7799-2 was updated in 2002 and further in 2005 to become ISO27001 giving UK companies a list of controls needed to achieve certification. Until the last update companies were free to make omissions of controls that do not apply to their situation and needed only to record those omissions. Now ISO27001 requires organisations to list and explain why omissions were made. ISO17799-2005 is the Code of Practice that forms the base of ISO27001 and is used in this thesis as an additional source of recommendations that support the controls within the specifications.

4.3 SME Compliance

In the UK the majority of businesses are small and the number of sole proprietorships has increased from 69% to 73% within the last four years with an estimated turnover in 2005 of £190 billion (SBS, 2006). This trend indicates the importance of providing focus on the security needs of companies that do not often have the ability to maintain InfoSec activity at the required level.

These companies are involved in industries that handle private information in new ways that are made possible through the use of the Internet. A novel example of this being a farm that sells its produce online. This involves handling personal financial data over the Internet and having to

take steps to secure that data.

Companies wishing to operate legally and provide reasonable protection for their data need to know which laws and standards pertain to the nature of their business. Small businesses could be tempted to view legal and standards compliance as something necessary only for large companies that are publicly listed. This is not the case: laws such as the DPA and CMA apply to all businesses that use Information Technology to gather and store information. Adopting all or part of ISO27001 would best serve any company seeking to improve the security of their data.

ISO27001 lists close to 370 items to assist with policy creation and each item needs to be considered and documented in order to achieve full compliance. This can seem an arduous task and examining the entire list is time-consuming. For a small business it can mean putting aside valuable resources, time and personnel, to sift through the items and devise ways of aligning the company's policies and operation to achieve an improvement in security standards. The items are described in a clear simple language but still require a certain level of InfoSec knowledge to help establish a hierarchy among the list that would allow a business owner to concentrate on the essential steps.

The threats to the data owned by a business can come from either offline or online sources affecting confidentiality, integrity and availability (Pfleeger, 2002). The confidentiality affects the level of disclosure of information such as trade secrets and customers' private data stored on

the business' computers. Integrity of the data is important because it affects all aspects of commercial activity from ordering from suppliers to receiving payments from customers. All businesses face the threat of not having their data available to conduct business. Each business has a Maximum Tolerable Downtime (Harris, 2005) during which it must get its operation going again before it becomes impossible to restart the business after an interruption of service.

The need to comply with information security laws and standards can at times be viewed as an additional overhead which hopefully can be avoided due to the rationale that a security breach has never been experienced by the company. This view is erroneous and can lead to a false sense of security. It can also leave the company legally liable in the event of a security breach that exposes its clients' private information.

Legal and regulatory pressures also increase as companies expand creating a need for clear, concise, internal governance. This adjustment can bring real benefits in terms of efficiency as well as a means of reducing information risk (DTI, 2005). A clear information security policy can:

- reduce ambiguity
- provide clear management direction and commitment
- establish agreed roles and responsibilities

A well thought out security policy can provide a means of dealing with the

unavoidable difficulties of managing information such as balancing the need to share information with the need to restrict access to it.

Security is a cost-benefit decision. Owners of assets would gauge the cost of the item and the level of security needed, aiming to minimize security costs but maximize security benefits (Butler, 2002). A risk analysis assists a company in the decision of where to spend its security budget. From the calculations performed on different eventualities, a company can see where it stands to lose most, which are its greatest threats and what cost effective measures it can take to mitigate such threats.

Risk analysis is a technique used to calculate the likelihood of a damage-causing event. Damage is considered any harm to a prized asset and in the scope of this thesis that asset is business information. As an exercise it is important to focus on accurate calculations more than the aim to achieve precise measurements of such quantitative items as the cost of being attacked. It must be remembered the numbers arrived at would be subjective and apply to the particular company as no two companies would assign the same value to a certain asset.

The cost of damage is usually quantified with more certainty than the chance of the event occurring and these two assigned values are used in an equation that covers the time span of a calendar year. The basic calculation is:

cost of incident x *annual probability* = *Annual Loss Expectancy (ALE)*

For example, an attack on the business' network that takes it off the Internet can cost a company £50 000 and the chances of it happening within a calendar year can be 40 percent. The ALE associated with that risk would be £50 000 x 0.4 = £20 000.

The measures to mitigate that loss can be used in another calculation called the Modified Annual Loss Expectancy (modALE). The measures reduce the probability and this affects the final outcome. A further example would be if a staff security awareness program reduces the risk of the attack by 10 percent then the new probability is;

annual probability x (1- mitigation)& 0.4 x 0.9 = 0.&6.

The modALE is then £50 000 x 0.36 = £18 000. The savings made in the case of staff education would be&

ALE – modALE, £20 000 - £18 000 = £2 000.

The cost of the education program can then be justified as a positive return on investment if it is anything less than the £2 000 (Berinato, 2002).

4.4 Adapting ISO27001

For small businesses without the technical and legal knowledge, compliance can be expensive because of the time it takes to do a risk analysis, research the applicable laws and source useful guidance. ISO27001 offers advice towards a certifiable level of security that in many cases would be considered overkill for the size of the company. A smart approach would be to use the parts of the standard that would improve the

security of the organisation in a cost effective manner.

The ratings of the controls of ISO27001 in this thesis are originally based on five criteria. The first two are the laws that apply to UK firms; the third and forth being items considered necessary but with decreasing degrees of applicability in a small business environment. The last group being the controls where the cost of investigation may prove too high for the security returns. There is a certain amount of subjectivity based on the researchers' knowledge of information security and experience of the operations of small businesses but this is supported by the use of a risk-benefit analysis that considers the likelihood of an event against the cost of mitigating that threat.

The ratings are used to assist in the prioritisation of actions needed to achieve legal compliance and a level of acceptable security for their systems. The controls ranked DPA and CMA as the first priorities as they are both legally binding. Acting on these would also provide a business with the primary steps for providing a safe legal environment for the company's system and data. A brief introduction to the two laws follows:

The Computer Misuse Act of 1990 (CMA, 1990) defines offences that cover a broad range of activities that are carried out by those having mischievous intent.

The Act identifies three specific offences:

- Unauthorised access to computer material.

- Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.

- Unauthorised modification of computer material.

The Data Protection Act of 1998 (DPA, 1998) sets out rules for processing personal information on paper as well as on computer. The Act imposes obligations on those who record and use personal information to be clear about how information is used and gives certain rights to individuals. The Act follows eight data protection principles:

Data must be&

- processed fairly and lawfully

- obtained for specified and lawful purposes

- adequate, relevant and not excessive

- accurate and, where necessary, kept up-to-date

- not kept for longer than necessary

- processed in accordance with the subject's rights

- kept secure

- not transferred abroad without adequate protection

Abiding by laws is never enough to curb criminal intent. That then points to a need for social and technical constraints that anticipate malicious

conduct. The 'High' and 'Medium' priority controls provide cost effective security against the threats present both within and outside of a company. There may be some overlap with the legally required items but the main criteria for the high rating was the level of risk reduction achieved when the controls were put in place. This is important because other than the CMA and DPA items, the remaining controls from the ISO27001 standard would be over 300.

The CMA and DPA rankings cover the legislative obligations of a company across all areas of InfoSec. The 'High' ranked controls are those considered critical and universal to any business operating a network whether private or via the Internet. The implementation of these controls is expected to have a positive security investment return.

The 'Medium' controls are those considered less applicable to small businesses but useful in situations where they apply with a probably lower return on security investment.

The 'Low' ranked controls are the ones least likely to be applied to a small business and when implemented the return on security investment is not expected to register an automatic benefit. An example of the rating of the controls in Controlling Access to Information and Systems section is given in Table 4, on the following page.

Rank	Specifications
CMA	Securing Against Unauthorized Physical Access, Managing User Access, Securing Unattended Workstations, Types of Access Granted to Third Parties
DPA	Granting Access to Customers
High	Controlling Access to Operating System Software, Managing Network Access Controls, Managing Passwords, Managing Access Control Standards
Med	Controlling Remote User Access, Giving Access to Files and Documents, Managing Higher Risk System Access, Acceptable Usage of Information Assets, Access Control Framework, Monitoring System Access and Use, Node authentication, Monitoring Third Party Services, Controlled pathway, Management Duties, Third Party Service Changes
Low	Access Policy, Diagnostic and Configuration Port Controls, Third Party Service Management, Why access is granted to third parties

Table 4. Rating controls in Controlling Access to Information and Systems

The controls are presented to business as a questionnaire about an organisation's level of compliance with each specification. ISO27001 is kept in its original structure with the 'Low' ranked controls deleted in order to provide a sharper focus with positive security investment returns for small businesses seeking to improve the security of the company's information.

4.5 InfoSec Questionnaire

The remaining controls' rank labels are removed and the result is a list of controls that would ensure a business is legally compliant and can achieve a high cost-effective level of InfoSec. To create a questionnaire, the majority of the controls are developed into questions that require a Yes /

No answer. This was not always possible as in the case of querying staff awareness of a Security Policy in which case a choice of 'SOME', 'ALL' or 'NONE' was given.

The questionnaire is designed to make it possible in the future to add scoring features based on the number of positive answers submitted. At the time of Thesis submission the questionnaire is useful as an InfoSec audit tool that uses the ISO27001 standard as a base for its investigation and supplies businesses with the rationalisation and implementation logic for each control.

4.6 Summary

The laws and standards that apply to UK companies were listed along with the history of ISO27001 which lists 367 controls for businesses to account for if they wish to gain compliance with this standard. The standard is adapted for SMEs by rating the controls from those that are compulsory to LOW which are considered to produce a negative return on investment. A questionnaire is produced from the compulsory, High and Med rated controls and is presented in the following chapter.

5 Information Security Check List

1. INFORMATION SECURITY ORGANIZATION

Information Security Policy

Question:	**Is there an information security policy?**					
Options:	YES		NO		LIMITED	

Information Security must be management led before filtering down through the organisation to involve everyone. This ensures that the security plans are closely tied to the strategic decisions of the company and that the resources needed to provide an adequate level of security are made available. Managerial involvement also guides policy towards providing a better business case for proposed controls.

Without managerial involvement and support a security policy risks becoming a useless document that does not mirror the business' processes and lacks the financial support needed to implement the necessary controls. In large companies personnel in charge of security have been promoted to board level in order to provide support to an activity that has become vital because of the risks associated with digitisation of data.

A security policy is an established set of rules for safeguarding information from accidental or malicious damage. It establishes responsibility and accountability for Information Security (InfoSec) and raises security awareness throughout the organisation. It provides a framework for best practice throughout the organisation and ensures that a company remains legally compliant.

The objective of an InfoSec policy is to communicate the risks posed to information and the preventive measures taken. The security policy should be brief and in a language easily understood by employees with statutes that are easy to follow. An InfoSec policy can be developed along the following suggested outline.

Subject: Highlights the InfoSec risks addressed by the policy. The policy should reflect the operation of the business in order to convince readers of its justification.

Scope: Specifies the areas of concern that the policy will address. Records the departments, individuals and technical systems referred to in the policy.

Description: Gives the background, describe the risks that have been identified, state the security expectations that the policy will fulfil.

Procedures and Guidelines: Mandatory practices: This is the minimum standard which has to be implemented. Procedure for implementation: A step-by-step procedure that will be followed for implementation of the policy. References will be made to forms, templates, standards, guidelines etc. that could be found in the attachments.

Roles and Responsibilities: Duties of different staff roles as related to InfoSec.

Definitions: The meaning of terms used throughout the policy.

Enforcement: How the compliance will be monitored. How non-compliance will be reported and what actions would be taken. Disciplinary actions, agreed to by HR / Management, to be taken if the policy is not adhered to including names of the persons appointed to enforce these policies.

Point of Contact: Person or office a staff member can contact with policy queries.

Attachments: Forms, Templates Standards, Technical guidelines

Authority: List the essential policies, legislation and company directives under various and applicable controls. Authors of the policy should be listed.

Location: Where all staff can access the policy.

Effective Date: Start date of policy.

Revision History: Changes made to policy on last revision.

Review Schedule: Timetable for policy review.

The nature of the threats to information changes along with the growth of the business and the advancement of technology. A security policy should be reviewed at least annually.

The review would address questions of change to the business' operation and the technology used to support it. Have new products been added since the last policy review? Are the new processes covered by the InfoSec policy? Have new staff roles been introduced to the business? Has new technology been introduced to the business? Are the new threats covered by the policy?

The time needed to conduct a review of the InfoSec policy would depend on the size of the company, its operations and the complexity of the technology used in the business. Regular recording of the changes to operation, staff and technology throughout the year would help provide ready documentation of the factors that affect its relevance.

Attached in Appendix C is an example of an InfoSec Policy

Information Security Organization

Question:	**Are staff aware of this policy?**					
Options:	SOME		ALL		NONE	

Staff should sign up to the security policy offered by the company. The policy may include or be separate from such items as a don-disclosure agreement and an accepted usage policy. This can be a condition of employment stating that reading and accepting the conditions of the security policy is a necessary part of the contract.

The company sets the respect the staff would have for the value of its information by insisting that staff members be aware of its security policy. If this is followed up with regular security awareness training and effective updating of the policy, a company is better positioned to protect its data through the cooperation of its staff.

The InfoSec policy should be readily available to staff either as a printed document or on the local intranet. Staff should have the ability to access guidance on issues as they arise without always having to confer with management.

If this policy is made readily available staff can easily refer to it in times of doubt and when their judgement is challenged in situations such as working remotely, travelling with company information, disposing of data, social engineering attacks and adhering to a clear desk policy.

Social engineering attacks are a good example of such situations because the attacker is attempting to coerce a staff member into giving vital information either through the use of confidence tricks that can take many forms. The term was popularised by Kevin Mitnick, a reformed computer hacker and security consultant who points out that it is easier to get information from humans than spend the effort hacking networks.

There should be deterrents for violating the security policy and staff should be aware of possible consequences. Indication of these penalties should be written in the security policy of the company. The penalties should also give staff the impression that the company takes security seriously and would not tolerate activities that put the business at risk.

Question:	**Is information security a regular item on the agenda of managerial meetings?**					
Options:	YES		NO		LIMITED	

Management should include security of information as a regular item at meetings because Information Security not only protects the information systems but also the Intellectual property of the business and thus is a value protection exercise.

When management actively directs and supports InfoSec, it moves from being a technical to a business pursuit. This makes it easy for the company to quantify the return on security investment. Changes made to the business processes are likely to be quickly covered by security measures because the two processes are no longer separate.

2. CLASSIFYING INFORMATION AND DATA

Setting Classification Standards

Question:	**Is information classified?**					
Options:	YES			NO		

Classifying information helps with decisions as to how much resources

should be put towards securing a piece of information. It breaks down the information into smaller definitions leading to the appropriate budget per classification. The number of classifications should be kept to a minimum.

Question:	**Is there a guideline for classifying information?**					
Options:	YES			NO		

Information can be classed in many ways. For the business owner it is important to know what information is crucial to the life of the company, what is important for its daily operation and what information can be exposed to the public. A higher security level should be accepted as default. A guide is also good for staff who will be dealing with information far removed from management but which will need to be protected to an appropriate level all the same.

With a simplified categorisation of data it is easier to create guidelines for labelling data because all staff would then be able to link the function that a piece of data performs to its role in the business. This guide should be made readily available to all staff perhaps via the company's network, Intranet, a poster or any other form that is regularly visible.

Each classification would require a different approach to its storage and handling. Such a policy acts as a guide for all staff.

Information can be classified as follows;

- What is crucial to the life of the business e.g. strategic plans, all user IDs and passwords used and customers' private data.
- What needs to remain internal to the business e.g. policies and procedures for employees.
- What can be made public e.g. news that the company wishes to make available outside of the company.

A consistent method for labelling information would help the company handle and store data more efficiently. Within Microsoft Word for example there are features within the File& Properties section for securing a document.

Question:	**Is someone appointed as the owner of classified information?**					
Options:	YES		NO			

The owner would decide the level of security and the rights attached to the information. The owner is also accountable for the information's security. All information owners need to be identified and assigned this responsibility.

It is to the owner other users would apply for permissions to the data. This system adds accountability, as the owner knows who has access to what and what rights are assigned. Without an owner it is possible for users to

gain access to privileged data and not have this recorded.

The presence of someone who handles the distribution of data privileges protects staff from making decisions that may not be in line with company policy when they receive access requests from other users. For example, a new staff member might ask for access to an application from someone in the company. If that person decides to "lend" them their ID and password, the new member would have gained all the privileges of an established staff member and this might not be officially recorded.

Question:	**Is confidential information kept separately?**					
Options:	YES		NO			

Top-secret information requires the highest protection as this can mean the difference between success and failure of a business. Business strategic plans, staff private data, staff passwords and financial records are examples of top-secret data.

As personal valuables are sometimes kept in safe boxes in a bank, businesses should consider vaulting their most valuable information safely and remotely. The remote storage is used to as a back up in the event of some disaster at the company's location.

3. CONTROLLING ACCESS TO INFORMATION AND SYSTEMS

Controlling Access to Information and Systems

Question:	**Is there an overall access policy?**					
Options:	YES		NO			

Access policies describe who gets access to what. A policy based on the classification of data and rules of those who own the data would help staff decide how access rights are granted to data objects. A well-designed access policy prevents the corruption of access rights.

In small companies the owners are usually involved with all the business processes and serve also as the person giving access to anyone who joins the company. A joiner can be on a permanent or project basis and the company would have to decide how much of the company's data should be exposed.

An access policy would provide a thought out, disciplined approach to the process of granting access to data. If for example an accountant visits the company's office monthly to update the accounts, it might be prudent to limit access to the financial data and perhaps applications also.

While this approach might seem extravagant, the accidental or malicious damage to company information must not be overlooked. An accountant with access to a company's software development application can wreak damage that can prove to be very expensive.

Question:	**Is access to information controlled?**					
Options:	YES		NO			

Each piece of information should be classified and be appropriately secured. The data owner would assign rights to the information based on an agreed policy. With proper accountability in place, the control of information can be monitored.

Information is a highly valuable asset of a company and some of it must necessarily be kept secret. The keys to cabinets, drawers must be the responsibility of someone in the business and not placed in areas of public access. Passwords to company information should be treated as top secret and changed if ever a breach is suspected.

Encryption protects data by making it unreadable to anyone without the correct keys. Many operating systems come with an encryption facility and are quite simple to use. The level of encryption can be chosen and the distribution of keys is done automatically.

Question:	**Is the business' main application password protected?**					
Options:	YES		NO			

Many businesses conduct their main business processes through an application. It is important to secure access to that application to those in the company that are responsible.

For example, Customer Relationship Management (CRM) packages where vital customer data is processed should only be accessed by staff that are trusted to handle this information. An application such as this would contain all the company's vital customer information including contacts and histories. Exposure of this information into the wrong hands can lead to serious competitive disadvantage to the company. If the information is lost, damaged or made inaccessible the company can suffer a tremendous setback.

Question:	**Is access to files and documents controlled?**					
Options:	YES		NO			

Each file should be classified and data owners should assign access rights to that file. Secure areas should be established on the network to correspond to data classification.

Files and documents can be password protected. Documents can be produced in the Adobe PDF format to protect them from being altered. Microsoft Word has the facility to lock documents also. Folders can be password protected to safeguard a selection of files.

Question:	**Are users formally registered before access is permitted?**					
Options:	YES		NO			

Registration facilitates a decision process regarding the granting of access.

This extends to persons outside of the company. A registration process would record such information as the role of the person or their level of membership.

When the company begins a relationship with an individual& system in whatever capacity be it staff, consultant, supplier or client there should be some record of this and a decision as to what level of the company's information would be granted.

A register would also be useful when the access levels of an individual& system has to be altered or deleted. Systems can be any other application or computer that interacts with the company's information.

Assess rights can easily be overlooked at a time of change and it is possible for there to be 'access creep' without a pruning of privileges which are no longer needed.

Question:	**Is there documentation of access requests and authorisations?**					
Options:	YES		NO			

There should be a record of who has access to what within the company. When new rights are to be assigned a record of the request should be kept. With such records it is easier to review a person's access right when roles change or employment terminates.

A spreadsheet can be used to record a name against the access rights held by that person or system and when those privileges were assigned.

Question:	**Is there is periodic review of access rights?**					
Options:	YES		NO			

It is very important to review and update the access rights as the business changes and roles in the company change and staff members assume different responsibilities.

A proper record of the assignment of access rights would make this a simpler exercise because all the information would be in one location. A periodic review should be scheduled which is in tandem with the growth of the business. It can be expected that the reviews be conducted quarterly.

Corruption of staff is also a possibility that should be guarded against with regular questioning of the appropriateness of the rights given to an individual.

Question:	**Is there a formal process for allocating passwords?**					
Options:	YES		NO			

Passwords to company files, documents, applications and equipment should be allocated to only to required staff and this process should be recorded. This would complement tracking of access rights given to an

employee throughout his time with the company.

It is not always possible to create a user list for an application or document where each user can create their password. The default passwords should be kept as safe as possible and if recorded in a document, that document should be given the highest level of protection, which might include encryption.

Passwords should be easy to remember but difficult to guess. A mixture of letters and numbers with upper and lower cases would normally provide a password that is unique. Initialising of personal phrases would provide a memorable password. E.g. "I want to make a secure password" can become "iwtmasp" which can be changed to "1wtmaSP".

Staff should be given these guidelines if they have to form their own passwords. Remember passwords are private and once under the control of staff there is not much the business owner can do to ensure that passwords are of a high quality.

That is not entirely true as 'regex' scripts can be used on applications to ensure the presence of certain characters in a password when it is first constructed. This is not always available so the education of staff of the need to have a strong password and how to devise one is a sound investment towards the protection of company information.

Default passwords tend to be quite standard, e.g. pword, and can easily become widely known throughout a company. They should be changed on initialisation. A reminder should be shown to users about the importance of using strong unique passwords. This is usual handled automatically by applications that are designed to force users to change the default password on the first use. If this is not automated the data owner can make manual checks with the default password to ensure that it has been changed

Question:	**Are there controls on access to the operating system?**					
Options:	YES		NO			

The operating system is the basis of the company's information technology and should be protected from any damage. Passwords on the servers and local machines keep out unauthorised users.

Firewalls also help in preventing malicious traffic coming in from the internet that may deliver viruses that cause harm to the operating system. While firewalls continue to provide protection, hackers have moved their focus to using web applications as the method of delivery and this can be countered by limiting the internet traffic on the company's network, building secure web applications if the company's business is to interact with the public online and regularly updating anti-virus and anti-spyware.

Question:	**Is there a restriction on users sharing IDs?**					
Options:	YES		NO			

Shared IDs carry the danger of granting authorisation to the wrong person. They also are an indication of low security awareness likely leading to shared default passwords that remain unchanged.

Shared IDs can also give a staff member access to parts of the network that he would not usually have. Sometimes someone with an ID might have access added to his role as time goes by due to the number of projects and responsibilities he might take on. To share this person's ID with anyone else would grant that other person all the accumulated rights of the original ID owner.

A safer practice is to design roles within the company and assign a basic level of access for each role so when someone joins the company he can be assigned a 'starter's' role ID which would be expected to be altered in time as that person's responsibilities grow.

Question:	**Is there a policy controlling information usage?**					
Options:	YES		NO			

Information should be used for a specified purpose and should not be misused otherwise. E.g. the Data Protection Act does not allow customers data to be used as test data for newly developed systems. A policy stating what safeguards are needed for each classification of data would help staff properly handle data and avoid such mishaps as placing restricted information in confidential or lower level documents.

An example of the above is the production of manuals for the company's systems that include screen shots containing information that should not be exposed in a document that has a low-level security rating. A manual can get into the hands of someone wishing to use the revealed information maliciously.

Question:	**Is system access and use monitored?**					
Options:	YES		NO			

Monitoring helps measure the effectiveness of security policies and also collects evidence in the event of a breach. With a monitoring system in place a company can also impose rules such as locking out a user after a certain number of failed attempts to log in. Repeated failed attempts can signal a brute force attack on the system and locking out a user stops the approach. A legitimate user can always get in touch with the system owner and reset the password.

Traffic across the network can be monitored to get an idea of usage patterns among staff. Network intruders would tend to leave unusual patterns with can be recorded to help strengthen points of entry within the company's system.

Question:	**Is third party access to information controlled?**					
Options:	YES		NO			

Contractors, business partners and outsourcing companies would need to have access to information. This access should be recorded and tightly controlled. Access should be restricted to information that is needed only. Third party access should be viewed as temporary and revoked at the end of each project / interaction.

4. PROCESSING INFORMATION AND DOCUMENTS

Networks

Question:	**Is someone in charge of network security?**					
Options:	YES		NO			

This is an important security function and should be assigned to a role that provides accountability. In a small company such a role would be most likely handled by the business owner.

The responsibility for the security of the company's information should be recognised as being in the hands of one person. This adds control to process of assigning access to the company's information.

The person in charge of network security should be able to adjust software settings on the PCs and servers in the business in order to create a secure operating environment.

Question:	**Are the skills needed to defend the network present in the company?**					
Options:	YES		NO			

A skilled network manager makes a difference in the level of security of a system. Proper implementation of security guidelines requires someone who is skilled in this field.

The skill to secure a network and the computers within it might not be available within the company. A company can source an expert who would set up a secure network and provide regular support service.

Question:	**Is the network protected from remote attacks?**					
Options:	YES		NO			

Firewalls, Intrusion Detection Systems and Intrusion Prevention System are three technologies to help secure a network. User log-on, logging of traffic and regular updating of security patches would add to the level of a network's security.

There should be strict controls on the access to the network from remote locations. Extra checks should be carried out to verify a users' identity and access to sections of the network should be limited.

Small businesses can use a manual login process whereby someone can phone in a request to log onto the network and that can be done by the

person in the office. This approach is effective but limited in application as it requires someone to be in the office at the time the other person requires remote access. Creating a remote access account and giving the credentials to the user while in the privacy of the office is an effective strategy. The user must memorise the information to avoid having it found by anyone else.

Question:	**Is the network protected from internal attacks?**					
Options:	YES		NO			

Access to computers in the network should be password controlled. The cabling should be protected from physical damage and the server equipment should be kept in a secured room. Logs should be kept of all activity on the network.

If networks are shared across an organisation there should be some form of standardisation that ensures that one part of the network is as secure as the other. When a new system is added to the network the overall security level becomes that of the weakest point.

The security of a system should be gauged before adding it to a network and the resulting strength of a merger should be evaluated before the entire network goes live.

Question:	**Are security patches applied immediately to network components?**					
Options:	YES		NO			

Security patches must be applied as soon as they are sent from vendors. Patches fix vulnerabilities and without them a system is susceptible to new attacks on the weak points within the network.

Patches protect systems from the lower skilled hackers who are not on the cutting edge of software exploiting and are usually the practitioners of second hand knowledge by which time the vendors might have produced a patch to neutralise any attack on the previous vulnerability. The sooner a system is patched the less time a hacker has to exploit a known vulnerability.

System Operations and Administration

Question:	**Are there controls on how data is distributed?**					
Options:	YES		NO			

Data copies should be limited to only what is necessary and should be tracked. Data classification should always be applied to company information to make it easier for staff to understand the necessity of the controls placed on individual pieces of data.

Data can be distributed by a number of means, each with their own hazards. Printed data is usually unencrypted and can be misplaced by its owner. Digital data carries the risk of having malicious alterations go

undetected. It is also easier to copy and distribute to a wide audience.

Laptops carry the infamous reputation of being lost with important company information. Encrypting important information held on laptops would render the information useless to whoever captures the laptop if it becomes lost or stolen.

Question:	**Are there controls over online transactions?**					
Options:	YES		NO			

Data transmitted online faces a high risk of being intercepted. Controls such as encryption and secure transmission channels should be used. Instant messaging is being used as a cheap reliable way for businesses to work together but not all instant messaging applications offer the appropriate level of privacy a company might require. Some do allow some fine tuning of the security settings and this should always be looked at to ensure that channels are encrypted when necessary, conversations are saved in a secure environment or not at all, file transfers are virus checked and the application does not automatically log on start up.

Traffic in and out of the company's network should be monitored. Firewalls can be set to restrict certain types of traffic. Web browsers allow the adjusting of security levels and this can be used to help restrict staff Internet access. Records of instant messaging conversations can be saved along with a record of what files have been transferred.

Question:	**Are there safeguards from data corruption?**					
Options:	YES		NO			

Is data reviewed regularly to check it's retrievable? The pace of IT renders files unreadable within a few years. Floppy disks are no longer used in new machines and would soon be obsolete.

A large sized external drive promises the longest life for digital data at this moment. The interface, a USB plug, should be able to interface with future machines if only via adapters.

Whenever the company changes computing equipment it has to consider the formats of its present information and if they are supported by the new technology. If not, a transferring exercise should be done as a priority before the host machine suffers some form of damage that renders all the resident data useless.

Question:	**Are there guidelines for responding to system faults?**					
Options:	YES		NO			

Staff should recognise when a problem requires expert attention. A 'hands off' policy should be the default best practice if staff are not trained to handle IT security incidents. An untrained person can easily make worse and incident or remove vital evidence in an attempt to fix an apparent

problem.

Turning off a computer is not always the best way to deal with an incident because this may lead to a permanent loss of data which may include forensic evidence of the security breach&

Someone trained in the handling of such incidents would be better prepared to make the correct decisions. For example when an Internet-borne attack is detected it is best to disconnect the machine from the Internet and also quarantine it from other machines in the company. This course of action might not be obvious to someone without training.

Experts should deal with system faults as an untrained person can do more damage to a most vital part of a company's operational assets. An expert also ensures that faults are dealt with speedily.

Small companies are probably better off hiring this sort of support when needed rather than maintaining a specialist or retaining a support package from vendors. The best option would be to train a member of staff in additional skills that would help the company in IT emergencies.

Question:	**Is someone in charge of system operations?**					
Options:	YES		NO			

Someone skilled in the technology of networks with an awareness of security should be responsible for the safe operation of the system. With a small number of staff it might not be possible to have a specialist position but someone should take the responsibility and control of system operations. Anyone working in or with the company would then have one person to go to in matters related to the company's IT operation.

Up to date documentation of the system helps users get the most out of its intended use. Without these documents the company is dependent on experts to handle all manner of incidents. Documents should be available to authorised staff on a shared drive with new versions of the documents saved along with older versions. Older versions should be kept to provide evidence of the recommended procedures staff should have used at a particular time in the past. This sort of evidence might be needed in a court of law.

Question:	**Is there a set log-on procedure?**					
Options:	YES		NO			

The servers and computers should be password protected. The logon window can be coded to give a concise reminder of the need for security awareness when using the company's systems. Systems can be adjusted to require a logged off user to log on if he wishes to turn off the computer. In this way an authorised user cannot turn off someone's computer.

Question:	**Are transactions reports managed?**					
Options:	YES		NO			

All network activity should be logged and these records should be kept safe from any form of tampering. System owners should review these logs periodically looking for activities that may jeopardise the safety of the system. Sites visited, request made to the server, accounts set up are some of the activity areas that may contain risky transactions.

Question:	**Are error logs monitored?**					
Options:	YES		NO			

It is important that the error logs are kept secured from any malicious alterations. They should also be regularly reviewed to check for usage anomalies. Encryption would help keep them unreadable in the event they fall in the wrong hands. The primary goal is to ensure the integrity of the logs.

Operation audit logs record changes made to records and system files. They must be secured from alteration because a system owner needs to know the state of the system and these logs record what has been done.

Logs would record the installation of new applications some of which might be needed for a very short period and if deleted after use would return resources to the system. Without an updated log, old inactive applications can continue to exact a toll on the company's IT system.

E-mail and the Worldwide Web

Question:	**Are there controls for downloading data from the Internet?**					
Options:	YES		NO			

Files should be downloaded to a secure area on the network. Licences for software must be current. Staff should have training in a secure procedure for receiving files and information from the Internet. Firewall settings help in controlling what type of traffic comes to the network from the Internet. Browsers have security options that can restrict the content a company allows onto its network.

Question:	**Is internet traffic filtered for inappropriate material?**					
Options:	YES		NO			

Firewalls can be used to filter certain material from the Internet. Staff should also have guidelines on dealing with the acceptance of material from the Internet. Aside from the morals of viewing pornographic material online there is a serious danger of allowing viruses onto the network as hackers use pornography to ship viruses. The law also forbids the viewing of certain types of images and if evidence of these is found on a machine the owner of the business would be liable to criminal prosecution.

Restricting Internet traffic to a company's network is also a way of preventing the wastage of company time as the volume of information and activity on the Internet can prove quite seductive to undisciplined staff.

Question:	**Are guidelines in place for certifying the origin of documents?**					
Options:	YES		NO			
Documents can easily be falsified and used to mislead staff to making incorrect decisions. This also applies to software from third parties.						

Question:	**Is& was security a design concern when developing the company's website?**					
Options:	YES		NO			
Websites can have many vulnerabilities and act as a gateway to a company's network. The main concern is the security of the input information from website users.						

Question:	**Is there a policy for the handling of email?**					
Options:	YES		NO			
Storage of email can be expensive. A policy as to what gets saved would help staff decide what to retain. Staff should also be trained to exercise caution when receiving emails. Do not preview mail from suspicious sources.						

Question:	**Are digital signatures used?**					
Options:	YES		NO			
Digital signatures help with ensuring the authenticity and validity of emails. It is advisable for company to make use of this technology that is available in the main email applications..						

Telephones & Fax

Question:	**Is extra security taken when using telecommunication?**					
Options:	YES		NO			
The telephone is unfortunately a social engineering tool and staff need to be certain of the identity of whoever is on the other end of a telephone conversation. Policies can help by describing procedures for authenticating caller Ids over the telephone and on video conferences. Conference and video calls can expose more data than is available or needed via other mediums. Keep all private data away from cameras and brief staff about the content of their conversations. There should also be a protocol for staff behaviour during conference calls that would present a professional impression and avoid giving away any company information.						

Data Management

Question:	**Is data that is received on disks checked for viruses?**					
Options:	YES		NO			

New data received on disks should be opened in a secure environment preferably outside of the company's network.

Question:	**Is there a policy for archiving documents?**					
Options:	YES		NO			

Documents should be archived securely and checked annually for their readability. Information technology is rendering storage mediums obsolete in a short space of time and it is important that the correct equipment for retrieving data is maintained.

A policy regarding the retention of data would help determine which information should be kept for how long and the level of security needed.

Question:	**Is there a policy for updating customer information?**					
Options:	YES		NO			

Customer data must be kept current. The DPA lists this as one of its requirements. Outdated data is a business' inconvenience and also a record source of a customer's past actions that can be used to create an identity closely related to that of the customer.

Question:	**Are staff trained about using customer and other third party files?**					
Options:	YES		NO			

Customer and third party data should only be used for the purpose it is intended. Companies are not allowed to test software with individuals' data.

Within the company the staff should be always aware of security when creating files and folders. The facility is available on major office applications to add security settings to documents and to their file structures. Very sensitive documents can be encrypted in storage making it difficult to read if all other defences have been breached.

Question:	**When data is exchanged, are the security measures of other companies checked?**					
Options:	YES		NO			

Third party arrangements should be written to a contract to protect the company. Before sharing information with a third party the company should investigate what actions would be carried out on its data and the location of the data. Companies need to exchange information about their security measures and create secure working environments for the data that is transmitted between them.

Project management systems are regularly used to handle collaborative ventures but theses application can have security vulnerabilities that should be checked before use. A risk analysis would inform both parties if the

application is secure enough for the purposes required.

The services outsourced to third parties should be checked for the level of security they provide for the data that they would likely handle and for what likely effect the processed information would have on the company's system when it is re-introduced to the network.

Question:	**Could system controls be overridden to amend data in a controlled manner?**					
Options:	YES		NO			

Sometimes information needs to be amended in order to correct data that might be confirmed within the system. This right should be given to someone accountable.

Backup, Recovery and Archiving

Question:	**Is data from portable computers backed up?**					
Options:	YES		NO			

To secure the continuity of business, information gathered on laptops, PDAs or other portable devices should be backed up in the event of loss or theft.

Question:	**Is someone in charge of backup and recovery of company data?**					
Options:	YES		NO			

This should be assigned to a staff member who would record the backup procedure and a schedule. This person has to account for the backup of the company's data.

Security awareness among staff is the key to maintaining a protective environment for the company's data. Backing up data on a regular basis helps a company survive a current data loss. Staff should be assigned folders on the network where they can store copies of their work on a regular basis. Regular reviews of staff backups should be conducted.

Document Handling

Question:	**Are staff trained about secure document management?**					
Options:	YES		NO			

Staff should feel responsible for the safety of the information they handle. They should be aware of the hazards associated with certain types of transactions and know how to safeguard data from these threats.

Question:	**Is there a process for approving documents?**					
Options:	YES		NO			

Documents should go through a formal approval procedure before being sent out of the company on its behalf. Digital signatures help with verifying

ownership.

Question:	**Are there procedures for the filing of data?**					
Options:	YES		NO			
Staff must know what data should be filed and the level of security needed to protect that data.						

Securing Data

Question:	**Is the deletion of data created& owned by others prevented?**					
Options:	YES		NO			
Data ownership and proper back up procedures help avoid the damage done by the accidental deletion of data.						

Question:	**Is customer information kept confidential?**					
Options:	YES		NO			
Care must be taken to secure customers' private data. If stored it should be encrypted and password protected. The data should be transported over secured channels and not passed among staff without due diligence.						

Question:	**Is the security level of third parties equal to those of the company?**					
Options:	YES		NO			
The security of a company's outsourcing partners should at least match the levels of the company as data is shared between them. Sharing information with a third party company can present risks to the safety of the data shared. Companies working together should establish baselines for security among themselves.						

Question:	**Are documents password protected?**					
Options:	YES		NO			
Documents can be password protected and this should be done according to the classification level of the document.						

Question:	**Are passwords recorded and securely archived?**					
Options:	YES		NO			
There are products available for storing passwords with the protection of one password. In databases passwords should be encrypted.						

Other Information Handling and Processing

Question:	**Are the proper procedures observed when checking customer credit data?**

Options:	YES		NO			
Customer credit data can be gotten from a credit report company. Each application for credit should be handled individually. It is also helpful to check the customer's own references.						

Question:	**Are staff aware of the security risks associated with speaking to customers?**					
Options:	YES		NO			
The identity and intention of customers must be verified before staff give information that can be used to the detriment of the company.						

Question:	**Are staff trained to exercise diligence while away on business?**					
Options:	YES		NO			
There should be guidelines as to the best safety practises with regard to equipment and information for staff on business trips. Laptops for example should always be secured.						

Question:	**Are duties separated among staff with some activities performed as a team?**					
Options:	YES		NO			
It is best to divide the duties and hence access rights of individuals across the company. Splitting a task among a team makes it impossible for one person to act unilaterally.						

5. PURCHASING AND MAINTAINING COMMERCIAL SOFTWARE

Purchasing and Installing Software

Question:	**Are all software licenses up to date?**					
Options:	YES		NO			
It is illegal to run software without the proper licence. Keep an inventory of software and their licence agreement.						

Software Maintenance & Upgrade

Question:	**Are security issues considered before accepting upgrades?**					
Options:	YES		NO			
Upgrades of older software carry a risk of introducing new vulnerabilities. A review of the security offerings of an upgrade should be taken into account.						

6. SECURING HARDWARE, PERIPHERALS AND OTHER EQUIPMENT

Purchasing and Installing Hardware

Question:	**Are the security requirements of new hardware properly considered?**					
Options:	YES		NO			
New hardware has to maintain or enhance the security levels of the existing system. Security must be a consideration when acquiring new hardware.						

Question:	**Is hardware tested when new to assure proper security functionality?**					
Options:	YES		NO			
Hardware should be tested before being implemented into the company's system.						

UPS, Printers and Modems

Question:	**Is there a UPS for critical equipment?**					
Options:	YES		NO			
UPSs provide power temporarily in the event of a power failure or brownout. This gives staff the time to safely shut down all processes.						

Question:	**Is there a power generator to support the UPS?**					
Options:	YES		NO			
A power generator would allow the company to conduct business in the absence of the regular power supply.						

Using Secure Storage

Question:	**Are storage areas secured?**					
Options:	YES		NO			
Cabinets should be locked according to the level of security needed for its contents. High security items should always be locked away with access controlled by one person. Operational information should be locked outside of working hours. Only public information could remain unprotected. Servers should be in locked cabinets, as should all other critical equipment. Fire can render data useless and a company can take a long time to recover from such a loss. Place important data in fireproof storage. Network cable can be compromised affecting the system. The cables should be secured from tampering. A safe offers a higher level of protection than a locked cabinet and limits access to the holders of the combination only. The company's most valuable items should put in a safe. The safe should be in a secured area						

and not exposed to being taken away by unauthorised persons.

Other Hardware Issues

Question:	**Is data thoroughly removed before equipment is disposed?**					
Options:	YES		NO			
Data should be thoroughly removed from equipment before disposal. Destruction of hard drives is the surest way to delete old data. There are disposal professionals who offer data cleaning services.						

Question:	**Is there insurance on the hardware?**					
Options:	YES		NO			
Insurance cover can help a company replace equipment after a disaster.						

7. COMBATING CYBER CRIME

Combating Cyber Crime

Question:	**Are security safeguards in place to prevent attacks to the system?**					
Options:	YES		NO			

Access to the NETBIOS and MSRPC ports should be denied. Prevent access to TCP ports 135, 139 and 445. Also to the UDP ports 135, 137 and 445. Active X controls should be turned off on browsers. Use a host-based IDS& IPS to protect equipment inside of the network's perimeter.

Identify the primary defence mechanisms throughout the network and verify that they are in use and up to date with their security patches. Good anti-spyware software would help identify software that resident on the network that got past the firewall and pose a threat to security. Anti-virus software must be in place and automatically updated. System scans should be run regularly.

Anti-virus should be deployed on all critical host machines throughout the network. Applications that transport data should also be scanned by anti-virus software.

Configure intrusion detection to identify DOS attacks. Monitor resource usage for near full utilisation. Disable all unnecessary services on host machines. Configure perimeter firewalls to block all traffic that is not needed.

Question:	**Is the anti-virus software up to date?**					
Options:	YES		NO			
The features of the anti-virus software should be verified to be appropriate						

for the nature of the business before purchase.

Updates are the solutions to the latest viruses detected by the security vendors. For a system to be protected against new viruses the updates need to be installed as soon as they are released. Most anti-virus software have automatic update facilities and this is the more secure option. Schedule regular automatic scans of the system

A plan for handling attacks should be documented. Staff should be given an overview of how viruses work and what to do in the event of an attack, e.g. isolate infected machines. Security vendors give a lot of information and their bulletins can be excellent sources.

Question:	**Are loopholes and backdoors into the system investigated for vulnerabilities?**					
Options:	YES		NO			

Systems can be set up in ways other than the norm to permit access to system administrators. These should be kept to a minimum.

8. CONTROLLING E-COMMERCE INFORMATION SECURITY

E-Commerce Issues

Question:	**Is the e-commerce system built on a secure network?**					
Options:	YES		NO			

Networks hosting e-commerce systems require extra security as customers' financial details are being passed over the Internet. A secure site should also be available for business on a continuous basis because this is the expectation of customers and also 24-hour availability means that a user situated anywhere around the globe, at his convenience, can access the site. Continuous access also builds customer trust.

E-commerce activity should be isolated from the rest of the network, perhaps in a DMZ and the ecommerce site should be administered from a single computer that has access controls in force. Access to the website should also be tightened with the use of smart cards for example.

Another option for small companies to consider when conducting online sales is the use of payment providers. Such companies offer to conduct the entire payment process for a small fee and in the end the company gets the money for it goods / service without having the responsibility of securing the customers' financial details.

Question:	**Is the website running on least-privilege rights?**					
Options:	YES		NO			

Websites like other applications are sometimes developed using administrative rights to enable developers to control the code to a higher degree. While this approach helps with the efficiency of the development

process, it is not a secure practice. The level of rights should be changed to least privilege before the website becomes live. All backdoors and trapdoors should be removed. The hard coded access information should also be deleted from the script.

Another reason for developers to practise working in 'least privilege' mode is to allow programmers to experience the application in as much the same way as the users. An application can exhibit different behaviours depending on the rights of the user and designers need to 'see' what end users would encounter in order to ensure that the application delivers its intended function when deployed.

9. DEVELOPING AND MAINTAINING IN-HOUSE SOFTWARE

Software Development

Question:	**Is the code documented?**					
Options:	YES		NO			

Documented code saves a company time when problems occur with the code. The original developer should make clear his approach to a problem though the documentation so that others can follow the logic.

Properly documented code protects a company from being unable to support its product in the event of the absence of the original developer. Documented code makes it easier to repair problems, add functionality and reuse code.

Testing & Training

Question:	**Is mock data available for testing of software?**					
Options:	YES		NO			

The DPA requires that real customers' data should not be used for testing software. When real data is used in testing it can become labelled with a lower level security classification and could fall into the wrong hands. A safer practice is to create a mock database for testing.

For the testing of online purchase applications, some payment providers provide a sandbox environment where a mock purchase would go to completion in the same way a real transaction would be conducted. Mock data can be used In the sandbox. This example coming from larger companies that have to deal with securing customer information should serve as a best practice example to other developers.

The test environment should be password protected to ensure access to authorised and skilled persons.

Question:	**Is regression testing carried out before introducing new software?**					
Options:	YES		NO			

Before installing new software, tests should be run in a secure environment to verify the effects of the new software on the system and the user interfaces. The focus should be on the functional aspect of the code to ensure that recent changes have not introduced new bugs.

A library of regression tests can be built up over the lifetime of an application / system from each update event. It is not necessary to keep all tests in use, as this can be a time waster. The most effective tests should be kept and duplication should be avoided&

10. DEALING WITH PREMISES RELATED CONSIDERATIONS

Premises Security

Question:	**Is there an intruder alarm on the premises?**					
Options:	YES		NO			

Alarms should be placed on the perimeter of the building. Insurance rates are lower for buildings with alarms. They can also be linked to a security company that would check the premises when the alarm sounds.

A panic button such as those installed in banks is a good investment as it involves staff making a decision as to how critical a situation has become. Staff would need training in the use of this.

These provide evidence of intrusions and can also be set up to trigger alarms. The records should be secured in the event that they are needed for an investigation.

Question:	**Is the access to areas housing computers controlled?**					
Options:	YES		NO			

Offices should remain locked after hours. Staff should be trained to interrogate anyone who enters the building during working hours. Computers should be secured by locking stations when users are away, log on procedures to the machines and if feasible cable locks to their desks.

The ceiling, air ducts and windows are weak points in an office's security and should always be evaluated for security. Home based businesses can benefit from the level of security usually attached to a home but the separate value of a business' information must always remain at the fore and information systems must remain protected from anyone outside of the company's staff.

Question:	**Are visitors escorted through the premises?**					
Options:	YES		NO			

Visitors should not be left unattended when on the premises. A procedure for receiving deliveries should be in place for all staff to follow. Strangers should not be allowed to roam freely on a company's premises. If a cleaner

works in the office after hours, a clear desk policy should be practised among staff who should also lock away all documents in a drawer or cabinet at the end of each day.

Question:	**Is the impact of environmental disasters considered when securing the premises?**					
Options:	YES		NO			

The threat of an environmental disaster should be considered when an office is being set up. This consideration would affect the placement of the critical equipment and what safeguards are used.

For example, the threat of flood would lead to the locating of critical equipment on as high a placement as considered safe. Bush fires, excessive dust, high temperatures, high humidity, sea spray and other naturally occurring hazards need to be catered for when a company is setting up premises and wants to make sure that its data is safeguarded in the event of a natural disaster.

Data Stores

Question:	**Is staff access monitored?**					
Options:	YES		NO			

Some sort of monitoring system should be in place. This can be as simple as placing the desk of an authorised person near the data storage area or it can involve CCTV or electronic access controls that record entrance to the area.

11. ADDRESSING PERSONNEL ISSUES RELATING TO SECURITY

Contractual Documentation

Question:	**Are checks made on the claims made by prospective employees of their past?**					
Options:	YES		NO			

A condition of the employment process should be that candidates provide more than one reference from past employers and give the company permission to contact these referees. The company should check these references to verify the work history of the candidate and the opinion of past employers.

When contacting past employers, make a clear introduction of the company, the position of the recruiter and the nature of the role being filled. The same questions should be used for all applicants applying for a certain position and these should be open questions that do not lead the either way.

Question:	**Are staff required to sign individual contracts with non-disclosure clauses?**

Options:	YES		NO			

This is important as it makes each member of staff responsible for their actions. A breach of confidentiality can be damaging for a company. The information a company handles can be of many types and although non-disclosure clauses are guided by the internal classification, other information might have value to outsiders.

Employees should have a clear demarcation between the work they do in the business and what happens outside of the company.

Non-disclosure clauses also protect the company from ex-employees using proprietary information to help a competitor. Trade secrets, code, strategic documents, customer lists and employees' information are examples of information that an ex-employee might be privy too but should not disclose to others upon leaving the company.

In some companies, employees are sent on 'gardening leave' normally three months before their leaving date to deny them the opportunity to gather intelligence that might be useful to another company or perhaps damaging to the firm if exposed.

Confidential Personnel Data

Question:	**Is staff data held in a secure storage area?**					
Options:	YES		NO			

HR records should be kept in a locked cabinet with access limited to authorised department staff only. The DPA categorises data such as ethnic origin, health, religion, sexual orientation and criminal record as sensitive information and should be treated as such.

Staff records should be afforded a protection level suited to its classification that would ensure only the authorised people in a company can view such data. A locked cabinet, password protected files, encryption, password protected machines are some steps that can help secure this type of information.

Question:	**Are staff subject to security clearance checks?**					
Options:	YES		NO			

Security clearance checks should be done throughout an employee's time with a company. It is not enough for this to be done only at hiring time. Periodic reviews of entitlements would reveal the access creep than can happen due to the need to facilitate participation in projects run by the company.

Staff clearance should be logged and regularly presented for review to the staff member. If rights are no longer needed they should be revoked. A practice of given access on a 'need to know' basis would help keep a tight reign on the security clearances allowed.

Companies also work on the assumption that one security clearance check

at hiring based on a background check is not a valid dynamic evaluation of an employee's trust level. Trust levels are not treated as constants and need regular review and updating.

Personnel Information Security Responsibilities

Question:	**Is someone responsible for the security of the company's credit cards?**					
Options:	YES		NO			

Authorised staff members should handle purchases made on the company's credit cards. The details of the cards should be kept secret. Trusted suppliers are also a better approach to the company's purchase plans as it means that the company's credit details are stored in fewer places.

The sharing of card details like PINs and online passwords should not be allowed as these credentials are usually valid for the life of the card which might be longer than staff tenure. If staff access rights are properly monitored, the departure of a staff member can prompt the changing of a card's identity credentials.

The company should have a record of which suppliers have their credit details and regularly perform changes to passwords and probably PINs.

12. DELIVERING TRAINING AND STAFF AWARENESS

Awareness

Question:	**Is there a staff security awareness programme in place?**					
Options:	YES		NO			

For information security policies to be successful within a company, the staff must have a high appreciation of the relevance of such measures. Posters, vendors' bulletins, security workshops, short articles about security, books in the company's library and subscriptions to online forums are some ways to raise the security awareness level of the entire company.

An awareness program would be most effective if designed to address the way that information technology is used in the company. This means that there is no one-size-fits-all solution to training of staff. In a small, one office company it might be sufficient for the owner to regularly include the topic in casual conversations where staff feedback can easily be accepted. This approach might be considered too informal in another setting where the use of policy and scheduled training sessions might be needed to drive home the importance of security awareness.

Training

Question:	**Is information security addressed when training staff on new systems?**					
Options:	YES		NO			

New equipment&software can introduce new vulnerabilities or new ways of securing information. Staff should be trained about the security issues before a new system is put in place. When testing, attention should be given to possible vulnerabilities such as how much access does logging in to the new system allow with respect to the entire network. The security treatment of data from the network might be different in the new system and secure work-arounds should be devised.

13. COMPLYING WITH LEGAL AND POLICY REQUIREMENTS

Complying with Legal Obligations

Question:	**Are there controls on what data is copied and distributed among staff?**					
Options:	YES		NO			

Information distribution should be tightly controlled. The more copies there are of data the harder it becomes to control the security of a piece of information. An outdated copy of a record can re-enter the system and corrupt present data.

Working collaboratively from a common file is more efficient and more secure than working on separate copies and having to update each with the latest changes. Access rights to documents should also be kept under control. If a staff member just needs to read the data then that is all the rights that should be given. If the document is to be distributed it can be password protected from changes and sent out as a read only file.

Question:	**Is the company registered under the DPA?**					
Options:	YES		NO			

The DPA requires that companies that record on computer, the personal data of customers must register with the Office of the Data Protection Commissioner.

Personal data relates to:

(i) racial origin

(ii) political opinions or religious beliefs,

(iii) physical or mental health (other than any such data reasonably kept by them in relation to the physical or mental health of their employees in the ordinary course of personnel administration and not used or disclosed for any other purpose),

(iv) sexual life, or

(v) criminal convictions.

The legislation also requires registration of businesses that wholly or mainly collect debts. The aim of registration is to put into the public domain the type of information that is collected and the reasons for doing so.

Complying with Policies

Question:	**Are there internal audits to check the level of compliance to the security policy?**					
Options:	YES		NO			

Procedures for checking the level of compliance should be prepared and made known to staff. A security audit can be considered the final step in the implementation of InfoSec defences.

After the policy has been decided and the defence measures put in place an audit is used to check the level of effectiveness of the previous actions. The audit checks that the entire security process is effective in protecting the data of the company.

An audit can show up such shortcomings as poorly tuned firewalls or IDSs. A company might buy itself security products and& or security consultation and consider that the work is done and they are now secure from any threats to the data. This cannot be taken from granted and an audit helps prove what the ROI on the security spending is.

A small company that has a security policy in place can do an audit in-house. If for example the policy demands staff create strong passwords and change them every three months, an audit of the log-in over a four month period would show whether staff are adhering to the policy.

Avoiding Litigation

Question:	**Are the proper copyright permissions sought before using internet material?**					
Options:	YES		NO			

Information on the Internet carries the same copyright restrictions as printed material. If the business needs to use any information published by another author for financial gain, it should first seek the author's permission.

There is not one sure way of obtaining permission to use copyrighted material and the correct procedure depends on the type of material being used. The Copyright Legislative Agency is a good place to start making inquiries for businesses based in the UK.

Other Legal Issues

Question:	**Is legal guidance sought in the handling of information security breaches?**					
Options:	YES		NO			

A company should have legal advice on the handling of information security issues. The company should choose lawyers who have expertise in this field.

The first step is to delegate someone in the company to be the first point of contact for staff when they discover a security breach. This person must

have knowledge of the legal requirements of dealing with a security breach and how to keep the evidence intact.

When the situation is contained the company can hand over the evidence to its lawyers in the event that the incident has to be taken further through a court process.

Question:	**Is there a periodic review of the compliance levels of the entire system?**					
Options:	YES		NO			

The company should annually review its security policy. Within that time the changes to the information systems should be recorded and if need be used to amend the security policy.

A review of the entire system's compliance should be done along with the annual policy review to prove the effectiveness of the policies and countermeasures used. When the internal review is done and the amended policy proves effective it should be reviewed by a legal expert before being considered approved for use.

14. DETECTING AND RESPONDING TO IS INCIDENTS

Reporting Information Security Incidents

Question:	**Are staff aware of their duty to report information security breaches?**					
Options:	YES		NO			

This should be included in the information security policy. Increasing legislation is insisting that security breaches be reported because the idea is that businesses would pay more attention to information security if they are required to report any breaches. Companies having to report security incidents that put that customers data at risk stand to lose a lot of money and therefore the case for better security becomes more of a business decision than a technical one.

Including the staff's responsibility to report breaches in the security policy that is signed on recruitment makes it clear that the company expects everyone to play a part in the defence of all information.

The policy should also state that failure to report incidents would be punishable. This helps reinforce the perception that the company is serious about data protection.

Question:	**Is there a formal reporting procedure in place?**					
Options:	YES		NO			

A documented procedure for handling incidents should include the hierarchy of responsibility and whom staff should report to.

A formal process removes doubt as to what to do when an incident is

detected and to whom it should be reported. The process should be designed to encourage reporting while protecting the whistle blower because it must be remembered that there is a higher chance of the company's information being threatened from within. Issues with staff members should be handled confidentially.

Corrective Activity

Question:	**Is there a database of past information security breaches and their solutions?**					
Options:	YES		NO			

Records of past incidents should be kept and used in reviews of how incidents were handled. Properly reported incidents can also serve as examples when training staff about the importance of information security.

Recorded incidents would give a history of the steps taken to improve the system's security and provide reference points if ever there is the need to roll back the security level of the system in the event of a major change to the system.

15. PLANNING FOR BUSINESS CONTINUITY

Business Continuity Management

Question:	**Is there a business continuity plan (BCP)?**					
Options:	YES		NO			

The threats to a business' continued operation could come from many different areas. Threats can be natural or man-made. Businesses must have a plan as to how to continue operating in the event of a disaster. The plan must envisage different likely scenarios and document procedures to ensure that the company continues to operate.

Different staff members can be responsible for implementing different parts of the recovery of operations. A separate backup location should be chosen to use if the normal office was damaged.

The BCP should be available to all staff members. Posting the BCP on the company's intranet is a good idea. The plan should be tested end-to-end at least annually, run under as near authentic conditions as feasible.

6 Summary

The Internet is increasingly used for commerce and this has given businesses international and unlimited access to customers. Websites are no longer exclusively brochure sites for companies and now offer users the ability to interact with others for work, commerce and socializing. All these activities require the processing of personal data ranging from a username and password to banking information to personal histories.

Securing the data processed by the web-applications is very important for the trust a company would like its customers to have in ability to keep their details private and also to prevent itself from attack from cyber-criminals. Web applications are particularly vulnerable because Internet traffic is allowed through most firewalls and an attacker can piggyback an application and gain entry to a company's data. The STRIDE model is used to assess the standard threats posed to a web application. For each threat a set of technical countermeasures have been listed giving developers methods for strengthening the code behind web-applications.

The methods of code production have changed to reflect the complexity of the projects and the demand for more secure applications. The challenge is to provide development teams with a method that allows the code to be produced in as short a time as possible and as secure as can be. The methodology provided in this thesis allows regular auditing, via the use of a matrix, of the code while it is being written.

The matrix maps the progress made in adding countermeasures to

safeguard the application. The steps taken are guided by tests that are run on the application at the production point of each function within the application. The overarching method is called Secure-by-Design and is meant to produce applications that are secure in a shorter space of time than other traditional production cycles.

The securing of web applications and a proposed method of production are presented as one of the offerings of this thesis. Supporting these is a tool to help businesses secure their information systems that goes beyond the application level and involves all the data used by the organisation. The tool is based on the laws and standards that apply to UK companies.

The laws apply to all businesses and individuals who handle personal data of customers. The threats to customers include credit card fraud, unwanted harassment and identity theft. The standards also apply to all who process and store customer data but the assumptions made by the standards suggest that the big businesses are the target audience for these best practice guides.

This section of the thesis brings together the mandatory laws and the best practices outlined in the highest industry standard, ISO27001&and creates a 99 point questionnaire that small businesses can use to form policies and procedures to protect the data they work with.

The questions used in the InfoSec Checklist are the final distillation of the original 367 items in ISO27001 (Appendix E). The criteria came from a combination of two laws that are compulsory for UK businesses and three

categories that ranked each ISO27001 item as being of HIGH, MEDIUM or LOW practicality for a small business. The LOW items were deleted because they were considered a poor return on security investment. The remaining items were screened for duplication with an aim of bringing the questionnaire to less than one hundred items.

This questionnaire can act as a pro forma for an audit of a company's information security status. The items address the legal compliance and the other highly practical steps that can be put in place to secure a company's information. With a predominantly YES / NO choice of answers to the questions it is easy to gauge the company's security on a percentage basis.

7 Discussion

We've discussed the need for Information Security in any business that stores and processes data. The Internet has made interaction between people and systems more ubiquitous than ever before and in order to protect that data, laws and standards have been drawn up that give businesses guidelines in to securing information.

The growth of the Internet is assured for the foreseeable future and businesses and developers are putting new commercial models into play constantly. An example begin search engine technology which was first developed without a commercial model but has since gained such prevalence that income streams eventually evolved and now many sites use pay-per-click and other search-related revenue builders.

Cyber crime would continue to increase because criminals would find the lack of a physical engagement attractive. While digital forensic investigations are still a relatively new and specialized field, criminals would rate favourably their chances of being undetected.

ISO27001 is a highly respected InfoSec standard and therefore any audit based on the items listed in the standard should yield a result that is comparable to what is required for a safe environment for data. The format of this Check List makes it easier for a company to do an audit, get a result and then implement the recommended actions needed for a higher score.

InfoSec is not a static activity where a company can ever say their data is 100% percent secure. If a business achieves full marks on the Check List, it can only be regarded as a short pause for celebration as criminals are investing constantly to find new ways to gain control of business information. The Check List acts as a guide to securing information and would be an excellent starting point for small businesses that wish to operate legally and treat InfoSec seriously.

8 Future Work

The work done in this thesis addresses two important trends in the commercial world. The use of information technology to automate business activity and the increase in the number of small businesses trading in niche markets and sharing an equal presence in the new market fronts of the Internet with older bigger businesses.

The Check List can be further improved by weighting the scoring to reflect the importance of the legislative items. Audit tabulations would yield recommendations in order of legal priority followed by the practicality of an item. This can be used as a software tool that would help businesses keep their information systems secure on a continual basis because answering the questions, getting a rating and suggestions for improvement would be simple.

A website can host the Check List and all supporting information that would explain first the need for a regular audit of the company's data protection and secondly how to go about a security audit. The audit can be done online and a score returned to the user giving a rating and a list of suggestions for ways to move forward towards a more secure environment for the organisation's data.

9 References

AIC (Australian Institute of Criminology), 2005, Australian Crime: Facts and Figures 2005, pp 54, http://www.aic.gov.au/publications/facts/2005/facts_and_figures_2005.pdf

Baer, R. and Dietrich, M., 2006, Validation of IT-Security Measurement Tools, Proceedings of The First International Conference on Availability, Reliability and Security, ARES 2006, The International Dependability Conference - Bridging Theory and Practice, Vienna, Austria, pp. 980-981

Beck, K., 2003, Test Driven Development: By Example, Addison-Wesley Professional, ISBN 0321146530

Berinato, S., 2002, Return on Security Investment: Calculated Risk, http://www.csoonline.com/read/120902/calculate.html

Birznieks G., 2001, Web Application Security: Tying the Past and Present Together, ApacheCon 2001 Santa Clara, California, USA April 4-6, 2001, http://www.extropia.com/presentations/birznieks/pdf/cgi_security_history.pdf

Blakley, B. et al, 2001, Information security is information risk management. In *Proceedings of the 2001 Workshop on New Security Paradigms* (Cloudcroft, New Mexico, September 10 - 13, 2001). NSPW '01. ACM Press, New York, NY, 97-104. DOI= http://dx.doi.org/10.1145/508171.508187

Boehm, B., edited by Hansen, W. J., 2000, Spiral Development: Experience, Principles, and Refinements, Software Engineering Institute, Carnegie Mellon University, Special Report CMU/SEI-00-SR-08, ESC-SR-00-08, (June, 2000) www.sei.cmu.edu/cbs/spiral2000/february2000/BoehmSR.html

Butler, S., 2002, *Security Attribute Evaluation Method: A Cost-Benefit Approach*, Proceedings of International Conference on Software Engineering, Orlando, USA, pp. 232-240

BSI (British Standard Institute), 2007, http://www.bsi-global.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/ISO-IEC-27001/

CISWG (Corporate Information Security Working Group), 2004, Information Security Management References, Putnam A. H., Chairman; Subcommittee, U.S. House of Representatives, http://reform.house.gov/UploadedFiles/Best Practices Bibliography.pdf

CMA (Computer Misuse Act) 1990, 1990, http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Computer Misuse Act 1990, 1990, http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

CSG (Common Sense Guide) to Cyber Security for Small Businesses, 2004, Common Sense Guide) to Cyber Security for Small Businesses, Recommended Actions for Information Security 1st Edition – March 2004, http://www.us-cert.gov/reading_room/CSG-small-business.pdf

Data Protection Act, 1998, 1998, http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm

Dhillon, G. and Backhouse, J., 2000, Technical opinion: Information system security management in the new millennium. *Commun. ACM* 43, 7 (Jul. 2000), 125-128. DOI= http://dx.doi.org/10.1145/341852.341877

Dimopoulos, V. et al, 2004, Approaches to IT Security in Small and Medium Enterprises, In Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia, pp73-82, 2004

DPA (Data Protection Act) 1998, 1998, http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm

DTI, 2004, Achieving Best Practice in Your Business, Information Security: A Business Manager's Guide, http://www.dti.gov.uk/files/file9981spdf

DTI, 2004, DTI Information Security Breaches Survey 2004 Executive Summary, http://www.dti.gov.uk/files/file9987.pdf

DTI, 2005, *Information Security: How to Write an Information Security Policy,* http://www.dti.gov.uk/files/file9959.pdf

Financial Times, 2006, Welcome to FT.com, https://registration.ft.com/registration/subscription-service/signup?segid=01289&segsrc=fthome

Finch, J.W. et al, 2003, Assessing IT Security Culture: System Administrator and End-User Perspectives, to appear in Proceedings of ISOneWorld 2003 conference and convention, Las Vegas, Nevada, USA, April 23-25, 2003

Foote, P. and Neudenberger, T., 2005, Beyond Sarbanes-Oxley compliance, *Computers & Security*, Vol. 24, No. 7, pp. 516-518. DOI= http://dx.doi.org/10.1016/j.cose.2005.07.005

Furnell, S.M., Bolakis, S., 2004, Helping us to help ourselves: assessing administrators' use of security analysis tools, Network Security, February 2004, pp12-15

George, B. and Williams, L., 2003, An Initial Investigation of Test Driven Development in Industry, Proceedings of Association for Computing Machinery (ACM) Symposium on Applied Computing (SAC), Melbourne, FL, pp. 1135-1139.

Gerber, M. et al, 2001, Formalizing information security requirements, *Information Management & Computer Security*, Vol.9, No. 1, pp. 32–37

Harris, S., 2005, *CISSP Certification All-in-one Exam Guide, Third Edition*, McGraw-Hill, Emeryville, CA., USA

Hernan, S. et al, 2006, Uncover Security Design Flaws Using The STRIDE Approach, MSDN, http://msdn.microsoft.com/msdnmag/issues/06/11/ThreatModeling/default.aspx

Huseby, S., 2004, Innocent Code: A security wake-up call for web programmers, John Wiley and Sons, England.

IssueBits Ltd., 2006, http://www.issuebits.com/

Langue, C. et al, 2005, Approaches to Establishing IT Security Culture, in proceedings of Advances in Network & Communication Engineering 2, pp 43-48, 2005

Lavery, J. and Boldyreff, C., 2001, Issues in Securing Web-Accessible Information Systems. In *Proceedings of the 10th IEEE international Workshops on Enabling Technologies: infrastructure For Collaborative Enterprises* (June 20 - 22, 2001). WETICE. IEEE Computer Society, Washington, DC, 189-193

Müller, M. and Padberg, F., 2003, About the Return on Investment of Test-Driven Development, Proceedings of the 9th European software engineering conference held jointly with 11th ACM SIGSOFT international symposium on Foundations of software engineering, Helsinki, Finland, pp. 168-177.

NaCTSO (National Counter Terrorism Security Office), 2005, Secure in the knowledge: Building a secure business, http://www.continuityforum.org/files/pdf/secure.pdf

Nagin, D. and Pogarsky, G., 2001, Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence*, Criminology Vol. 39, No. 4, pp. 865–892. doi:10.1111/j.1745-9125.2001.tb00943.x

Offutt, J., 2002, Quality Attributes of Web Software Applications. *IEEE Software*. 19. 2 (Mar. 2002), 25-32. DOI= http://dx.doi.org/10.1109/52.991329

OIT (Office of Information Technology), 2005, Software Development Methodology Reference, http://www.nh.gov/oit/internet/documents/AppendixE-SoftwarDevelopmentMethodologyReference021805.pdf

Payton, A., 2005, Determining the proper response to online extortion. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development (Kennesaw, Georgia, September 23 - 24, 2005). InfoSecCD '05. ACM Press, New York, NY, pp. 122-126. DOI= http://dx.doi.org/10.1145/1107622.1107651

Pfleeger, C. and Pfleeger, S., 2003, *Security in Computing*, 3rd Int edn, Prentice Hall, Upper Saddle River, N.J., USA

Rubin, A. and Geer, D., 1998, A Survey of Web Security, IEEE Computer, Vol. 31, No.9, pp. 34-41n DOI= http://dx.doi.org/10n1109/2.708448

Saltzer, J. and Schroeder, M., 1975, The Protection of Information in Computer Systems, Proceedings of the IEEE, Vol. 63, No. 9, pp. 1278 - 1308.

Sandhu, R., 2003, "Good-Enough Security: Toward a Pragmatic Business-Driven Discipline," IEEE Internet Computing, vol. 07, no. 1, pp. 66-68, Jan/Feb, 2003, http://dx.doi.org/10.1109/MIC.2003.1167341

SBS, Small Business Service, 2006, SME Statistics, http://www.sbs.gov.uk/sbsgov/action/layer?r.l2=7000000243&r.l1=7000000229&r.s=sm&topicId=700001n1759

Scott, D. and Sharp, R., 2002, Developing Secure Web Applications, IEEE Internet Computing, Vol. 06, No.6, pp. 38-45. DOI= http://dx.doi.org/10.1109/MIC.2002.1067735

Scott, D. and Sharp, R., 2003, Specifying and Enforcing Application-Level Web Security Policies, IEEE Transactions on Knowledge and Data Engineering, Vol.15, No.4, pp. 771-783. DOI= http://dx.doi.org/10.1109/TKDE.2003.1208998

SME Statistical Press Release, 2005, http://www.sbs.gov.uk/SBS_Gov_files/researchandstats/SMEStats2004.pdf

Sneed, H., 2004, Testing a Web Application, Sixth IEEE International Workshop on Web Site Evolution, Chicago, IL, pp. 3-10. DOI= http://dx.doi.org/10.1109/WSE.2004.10011

Theoharidou, M. et al, 2005, The insider threat to information systems and the effectiveness of ISO17799, *Computers & Security*, Vol. 24, No. 6, pp. 472-484. DOI= http://dx.doi.org/10.1016/j.cose.2005.05.002

Thuraisingham, B. et al, 2001, Directions for Web and E-Commerce Applications Security, Proceedings of the 10th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Cambridge, MA, pp. 200-204. DOI= http://dx.doi.org/10.1109/ENABL.2001.953414

Verdon, D. and McGraw, G., 2004, Risk Analysis in Software Design, IEEE Security and Privacy, Vol.2 No.4, pp. 79-84. DOI= http://dx.doi.org/10.1109/MSP.2004.55

Von Solms, H., 2006, Information Security - The Fourth Wave, *Computers & Security*, Vol. 25, No. 3, pp. 165-168. DOI= http://dx.doi.org/10.1016/j.cose.2006.03.004

Von Solms, R, 1999, Information security management: why standards are important, *Information Management & Computer Security*, Vol. 7, No. 1, pp. 5-5(1). DOI= http://dx.doi.org/10.1108/09685229910255223

Witman, P., 2004, Information Security & Shared Leadership, Proceedings of the 7th Annual Conference of the Southern Association for Information Systems, pp. 244-249, Savannah, Georgia, USA, Feb 27/28 2004

10 Appendix

Appendix A

Vulnerability	STRIDE Threat	Countermeasures
Auditing and Logging	• Repudiation	Secure Log File Management policies used on the administrative side.
Authentication	• Spoofing • Tampering • Elevation of privilege	• Special account set up to access the administrative privileges. • Student group leaders have more rights than group members. SQL authentication between the web server and the database.
Authorization	• Spoofing • Tampering • Repudiation • Information disclosure • Elevation of privilege	• Access the database using stored procedures. • Code access security through the roles and the privileges granted.
Configuration Management	• Information disclosure • Elevation of privilege	• Distinct administrative and student privileges. • Access is restricted from the student side. The configuration store is kept off the Web.
Cryptography	• Tampering • Information disclosure	• Strong industry standard cryptography. • Secure hashing algorithm (SHA1). Keys recycled regularly.
Exception Management	• Information disclosure	• Structured Exception Handling. Error messages give limited information to the customer.
Input validation	• Denial of service	• All input is managed within only one page. • Web page input validated. Arguments and the query strings are encrypted.
Parameter Manipulation	• Tampering • Information	• Sensitive data not passed in parameters.

	disclosure • Denial of service	Sensitive data not passed in query strings or form fields.
Session Management	• Spoofing • Information disclosure	• Session lifetime is restricted. Session identifiers passed over encrypted channels with SSL.
Sensitive Data	• Information disclosure	• Storage of secrets handled with platform-provided Data Protection-API (DPAPI).

Appendix A. Vulnerabilities, Threats and Countermeasures

Appendix B

Vulnerability	Proposed Technical Countermeasures
Input& Data Validation	• Buffer Overflows: Traditional C++, C, Memory Overruns, handled by .NET Framework, so not an issue. • Buffer Overflows: Form Level Validation (Required Field, Minimum Length, Maximum Length, Custom Rules). • Buffer Overflows & SQL Injection: Database Level Validation (DB Required, DB Min Length, DB Max Length, SQL Injection, Double Encoding). • Buffer Overflows: Business Logic Validation, held in Business Logic Layer, not Web Layer. • Cross-Site Scripting: .NET Framework 1.1 has built in Cross Site Scripting Protection Code. • SQL Injection: SQL Injection Validation performed at Data Access Level • Canonicalization: Microsoft Canonicalization Fix Applied.
Authentication	• Login Retry Logic • Separate anonymous from authenticated pages (Use Built in Web.Config Deny Settings) • Encrypt communication channels to secure authentication tokens. • Use HTTPS only with forms authentication cookies • Use authentication mechanisms that do not require clear text credentials to be passed over the network • Do not store credentials. • Forms Authentication Still to be implemented. • Forms Authentication Routines (Cookie Encryption, Protection = All)
Authorization	• Use least privilege accounts. • SSPI Database Connections.
Configuration Management	• Unauthorized access to administration interfaces: No administrative interfaces initially provided. • Unauthorized access to configuration stores: Configuration Files are stored on the machine, and are encrypted (See Cryptography). • Unauthorized access to configuration stores: Avoid storing sensitive information in the Web space (XML Form Files, Configuration Files). • Retrieval of clear text configuration secrets: Credentials are not stored in clear text, No use of

	Local Security Authority (LSA). • Over-privileged process and service accounts: Use least privileged service accounts (ASP.NET account for website, SQL Server SSPI account for application). • Sensitive files not shown in webspace. • Configure to run under medium trust still needs to be implemented. • Over-privileged process and service accounts: Application should be able to run under Medium Trust. • Lack of individual accountability.
Sensitive Data	• No Hard Coded Sensitive Data in the Software. • Encrypt sensitive data over the network. • Secure the channel.
Session Management	• Session Hijacking: Session Timeout Expiration Code in place. • Session Hijacking: Configure Session Timeouts to a minimum. • Session Hijacking: Ability to configure a maximum number of website hits within a session. • Session Hijacking: Cookie Based, not Query String based Session Identifier. • Session Hijacking & Man in the Middle Attacks: SSL. • Session Hijacking & Session Replay: Ability to configure an absolute Session Expiry on top of the sliding expiration. • Session Replay: Critical Functions (such as Online Contract signing), require a revalidation of Credentials. • Avoid storing sensitive data in session stores. • Secure the channel to the session store. • Authenticate and authorize access to the session store. • Enhance Framework's support for Session Management, if using Windows Authentication rather than the current forms authentication. This is because we utilise the Encryption, Verification & MAC, built into the .NET Framework for forms authentication. • Forms Authentication still to be implemented. • Session Hijacking & Man in the Middle Attacks: Forms Authentication Cookies set to Protection=All (Encrypted, Verified, MAC).

Cryptography	• Use Microsoft Enterprise Library Encryption Routines where possible. • Encryption of Configuration Files. • Encryption of Sensitive Data in the Database (where appropriate). • URL Encryption. • Cookie Encryption. • Encrypted Communication Channels. • Encrypted Viewstate. • .NET Web Application Configuration Files are encrypted using the Microsoft Enterprise Library Configuration / Encryption routines. • Avoid key management. Use the Windows Data Protection API (DPAPI) where appropriate.
Parameter Manipulation	• Query string manipulation: URL Encryption. • Form field manipulation: See Input Validation Section. • Form Field Manipulation: Viewstate Encryption. • Cookie manipulation: Only Authentication Cookies are used, which are secured. • All Manipulation: Use of SSL. • All Manipulation: Avoidance of storing sensitive data. • All Manipulation: Non Reliance of passed data.
Exception Management	• Revealing sensitive system or application details: Use of Default Error Page, so where an un-handled exception filters through, a custom error page is displayed. • Revealing sensitive system or application details: Passwords and sensitive data will not be published to the Error Publishing Log. • Use structured exception handling (by using try / catch blocks). • Catch and wrap exceptions only if the operation adds value / information.
Auditing & Logging	• Failed Logins etc automatically logged • Form Level Logging available to Form Builders. • Error Publishing still to be Implemented. • All Security Exceptions / Un-handled Exceptions are published to the Error Publishing Web Service (and if it's not available to the Event log).

Appendix C

Information Security Policy Sample

<<Company>> Information Systems Security Program

ASSET MANAGEMENT

1. SUBJECT:
All information assets must be tracked and managed to ensure that they are not lost or misused.

2. SCOPE:
This policy applies to all <<Company>> information assets, including but not limited to workstations, servers, network devices, printers, personal digital assistants (PDAs), phones, software, and licenses.

3. DESCRIPTION:
Each year, thousands of information assets are lost or stolen. Often agencies simply lose track of these items, sometimes resulting in scandals that appear in the news, and at minimum incurring the wrath of auditing organizations. Not only would loss of information assets result in a financial impact on <<Company>>, but it could also result in unauthorized access to data stored on or accessed through these assets, and could have a detrimental effect on the reputation of the agency. Additionally, the tracking and management of information assets is mandated by several national regulations, such as the Data Protection Act.

4. PROCEDURES & GUIDELINES:
(a) <<Company>> must keep a record of all information assets, including those mentioned in the scope above.
(1) Information assets are to be added to the record upon receipt by <<Company>> and assigned a barcode.
(2) For each information asset, <<Company>> will track at least the following information:

- The brand, model, and type of asset
- Serial number and <<Company>> barcode
- The person to whom the asset is assigned
- The location of the asset
- Any maintenance agreements for the asset
- The date of receipt of the item
- Date the record was last updated or inventoried

(3) Upon disposal of an information asset, <<Company>> will track the date of disposal, the method of disposal (e.g., transfer, destruction, donation, etc.), and the name of the new owner (if there is one).
(b) Periodic inventories are to be performed to verify records and account for all information assets.

(1) Each asset is to be inventoried at least annually.

5. ROLES & RESPONSIBILITIES:
(a) Information Owners are responsible for inventorying, tracking, and protecting <<Company>> information resources that they own.
(b) Information Custodians are responsible for assisting information owners with inventorying, tracking, and protecting <<Company>> information resources in their care.
(c) Information Users are responsible for exercising due diligence in protecting information resources entrusted to them, and immediately reporting the loss, theft or damage of any <<Company>> information resource.
(d) Supervisors are responsible for ensuring their employees understand their responsibilities regarding protection of information resources.
(e) The Information Systems Security Officer (ISSO) is responsible for auditing to ensure that information assets are being tracked and managed in accordance with this policy.

6. DEFINITIONS:
(a) Information Asset - An information resource that has tangible value.
(b) Information Resource - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

7. ENFORCEMENT:
Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and / or legal action, including termination of employment or referral for criminal prosecution.

8. POINT OF CONTACT:
Information Systems Security Officer (ISSO)

9. ATTACHMENTS:
None

10. AUTHORITY:
(a) <<Company>> Directive 00-01&Information Systems Security Program.
(b) Data Protection Act.
(c) Computer Misuse Act.
(d) ISO 27001.

11. LOCATION:
A Copy of this policy is available on <<Company>> intranet at https://forexample/issp.pdf

12. EFFECTIVE DATE:
15th January 2007

13. REVISION HISTORY:
14th January 2008

14. REVIEW SCHEDULE:
This policy should be reviewed and updated annually.

Appendix D

Example of a suite of tests

TEST	DESCRIPTION
2005_2006Accepted	Test layout of Accommodation Offer Details page.
2005_2006AcceptOffer	Layout of Contract page.
2005_2006AcceptOfferBlank 01	Accept with all blank checkboxes.
2005_2006AcceptOfferBlank 02	Accept with nine checkboxes.
2005_2006AcceptOfferLong Pwd	Accept with password > 20 characters.
2005_2006AcceptOfferLong User	Accept with username > 20 characters.
2005_2006AcceptOfferShort Pwd	Accept with password < 6 characters.
2005_2006AcceptOfferShort User	Accept with username < 6 characters.
2005_2006Offered	Test layout of Offer page.
2005_2006AcceptOfferSQL Pwd	SQL Injection code in Password input box (' OR 1=1 --).
2005_2006AcceptOfferSQL User	SQL Injection code in User input box.
2005_2006AcceptOfferSQL UserPwd	SQL Injection code in User and Password input box.
2005_2006AcceptOfferStore dProcPwd	Stored Procedure code in Password input box
2005_2006AcceptOfferStore dProcUser	Stored Procedure code in User input box.
AcceptContract	Test layout of Signed contract page.
loginBlank	Login w/o credentials.
loginLockout	Login with invalid credentials five times.
loginLockoutCoded	Login with invalid credentials five times.
loginLongPwd	Login with password > 20 characters.
loginLongUser	Login with username > 20 characters.
loginPage	Test layout of Login page.
loginShortPwd	Login with password < 6 characters.
loginShortUser	Login with username < 6 characters.
loginSQLPwd	SQL Injection code in Password input box (' OR 1=1 --).
loginSQLUser	SQL Injection code in User input box.
loginSQLUserPwd	SQL Injection code in User and Password

	input box.
loginStoredProcPwd	Stored Procedure code in Password input box
loginStoredProcUser	Stored Procedure code in User input box.
loginSuccess	Login with correct credentials. Test for new page.
loginUnsuccess	Login with wrong credentials.
registerBlank	Register w/o data.
registerBlankDoB	Register w/o Date of Birth.
registerBlankPwd	Register w/o Passwords.
registerBlankStudID	Register w/o Student ID
registerBlankSurname	Register w/o Surname.
registerBlankUser	Register w/o Username.
registerDuplicate	Register duplicate details.
registerInvalidDoB	Register with a date of birth in wrong format.
registerLongPwd	Register with password > 20 characters
registerLongUser	Register with username > 20 characters.
registerPage	Test layout of Register page.
registerShortPwd	Register with password < 6 characters.
registerShortUser	Register with username < 6 characters.
registerSQLDoB	SQL Injection code in Date of Birth input box&' OR 1=1 --).
registerSQLPassword	SQL Injection code in Password and Confirm Password input boxes.
registerSQLStudentID	SQL Injection code in Student ID input box.
registerSQLSurname	SQL Injection code in Surname input box.
registerSQLUser	SQL Injection code in User input box.
registerStoredProcDoB	Stored Procedure code in Date of Birth input box.
registerStoredProcPwd	Stored Procedure code in Password and Confirm Password input boxes.
registerStoredProcStudentID	Stored Procedure code in Student ID input box.
registerStoredProcSurname	Stored Procedure code in Surname input box.
registerStoredProcUser	Stored Procedure code in User input box.
resetPwdBlank	Submit w/o Student ID / UCAS Serial Number.
resetPwdLong	Submit with Student ID& UCAS Serial Number& 50 characters.
resetPwdPage	Test layout of Reset Password page.
resetPwdShort	Submit with Student ID / UCAS Serial Number < 6 characters.

resetPwdSQL	SQL Injection code in Student ID / UCAS Serial Number input box (' OR 1=1 --).
resetPwdStoredProc	Stored Procedure code in Student ID / UCAS Serial Number input box.
'Browse To' Test	**Browse to:**
BrowseToBin	http://localhost/kinetic.kx.web.student.website/bin/
BrowseToConfiguration	http://localhost/kinetic.kx.web.student.website/Configuration/
BrowseToCustomLinks	http://localhost/kinetic.kx.web.student.website/CustomLinks/
BrowseToDocuments	http://localhost/kinetic.kx.web.student.website/Documents/
BrowseToEmails	http://localhost/kinetic.kx.web.student.website/Emails/
BrowseToForms	http://localhost/kinetic.kx.web.student.website/Forms/
BrowseToHTMLTemplates	http://localhost/kinetic.kx.web.student.website/HTMLTemplates/
BrowseToImages	http://localhost/kinetic.kx.web.student.website/Images/
BrowseToLogin	http://localhost/kinetic.kx.web.student.website/Login/
BrowseToModules	http://localhost/kinetic.kx.web.student.website/Modules/
BrowseToNavigation	http://localhost/kinetic.kx.web.student.website/Navigation/
BrowseToPayment	http://localhost/kinetic.kx.web.student.website/Payment/
BrowseToTestArea	http://localhost/kinetic.kx.web.student.website/TestArea/

Appendix E

List of ISO 27001 Items

1. INFORMATION SECURITY ORGANIZATION

Information Security Policy

Information Security policy
Senior Management Support
Information Security Policy Review
Inter-departmental collaboration

Information Security Organization

Independent Review of Information Security Policy
Sharing Information with other Organizations

2. CLASSIFYING INFORMATION AND DATA

Setting Classification Standards

Defining Information
Classifying Information
Accepting Ownership for Classified Information
Labelling Classified Information
Storing and Handling Classified Information
Isolating Top Secret Information
Managing Network Security

3. CONTROLLING ACCESS TO INFORMATION AND SYSTEMS

Controlling Access to Information and Systems

Managing Access Control Standards
Managing User Access
Securing Unattended Workstations
Management Duties
Third Party Service Management
Managing Network Access Controls
Controlling Access to Operating System Software
Managing Passwords
Securing Against Unauthorized Physical Access
Access Control Framework
Access Policy
Restricting Access
Monitoring System Access and Use
Giving Access to Files and Documents
Managing Higher Risk System Access

Controlling Remote User Access
Types of Access Granted to Third Parties
Why access is granted to third parties
Controlled pathway
Node authentication
Diagnostic and Configuration Port Controls
Granting Access to Customers
Acceptable Usage of Information Assets
Monitoring Third Party Services
Third Party Service Changes

4. PROCESSING INFORMATION AND DOCUMENTS

Networks

Configuring Networks
Managing the Network
Network Segregation
Controlling Shared Networks
Routing Controls
Network Security
Accessing your Network Remotely
Defending your Network Information from Malicious Attack
Time-out Facility
Exploitation of Covert Channels
Authentication of Network Connecting Equipment

System Operations and Administration

Appointing System Administrators
Administrating Systems
Controlling Data Distribution
System Utilities
System Use Procedures
Internal Processing Controls
Permitting Third Party Access
Managing Electronic Keys
Managing System Operations and System Administration
Managing System Documentation
Synchronizing System Clocks
Monitoring Error Logs
Scheduling Systems Operations
Scheduling Changes to Routine Systems Operations
Monitoring Operational Audit Logs
Responding to System Faults
Managing or Using Transaction / Processing Reports
Commissioning Facilities Management - FM
Third Party Service Delivery
Log-on Procedures

Corruption of Data
Corrupt Data Controls
Controlling On-Line Transactions

E-mail and the Worldwide Web

Downloading Files and Information from the Internet
Electronic Business Communications
Policy on Electronic Business Communications
Using and Receiving Digital Signatures
Sending Electronic Mail (E-mail)
Receiving Electronic Mail (E-mail)
Retaining or Deleting Electronic Mail
Developing a Web Site
Receiving Misdirected Information by E-mail
Forwarding E-mail
Using Internet for Work Purposes
Giving Information when Ordering Goods on Internet
Setting up Intranet Access
Setting up Extranet Access
Setting up Internet Access
'Out of the Box' Web Browser Issues
Using Internet 'Search Engines'
Maintaining your Web Site
Filtering Inappropriate Material from the Internet
Certainty of File Origin
Cryptographic Keys
Key Management Procedures
Controlling Mobile Code

Telephones & Fax

Making Conference Calls
Recording of Telephone Conversations
Receiving Misdirected Information by Fax
Giving Information when Ordering Goods on Telephone
Persons Giving Instructions over the Telephone
Using Video Conferencing Facilities
Persons Requesting Information over the Telephone
Receiving Unsolicited Faxes

Data Management

Transferring and Exchanging Data
Permitting Emergency Data Amendment
Receiving Information on Disks
Setting up a New Folder& Directory
Amending Directory Structures
Sharing Data on Project Management Systems
Archiving Documents

Information Retention Policy
Setting up New Spreadsheets
Setting up New Databases
Linking Information between Documents and Files
Updating Draft Reports
Deleting Draft Reports
Using Version Control Systems
Updating Customer Information
Using Meaningful File Names
Managing Data Storage
Managing Databases
Using Headers and Footers
Using and Deleting 'Temp' Files
Using Customer and Other Third Party Data Files
Saving Data / Information by Individual Users

Backup, Recovery and Archiving

Restarting or Recovering your System
Archiving Information
Backing up Data on Portable Computers
Managing Backup and Recovery Procedures
Archiving Electronic Files
Recovery and Restoring of Data Files

Document Handling

Managing Hard Copy Printouts
The Countersigning of Documents
Checking Document Correctness
Approving Documents
Verifying Signatures
Receiving Unsolicited Mail
Style and Presentation of Reports
Photocopying Confidential Information
Filing of Documents and Information
Transporting Sensitive Documents
Shredding of Unwanted Hardcopy
Using Good Document Management Practice

Securing Data

Using Encryption Techniques
Sending Information to Third Parties
Maintaining Customer Information Confidentiality
Handling of Customer Credit Card Details
Fire Risks to Your Information
Sending Out Reports
Sharing Information
Dealing with Sensitive Financial Information

Deleting Data Created& Owned by Others
Protecting Documents with Passwords
Printing of Classified Documents

Other Information Handling and Processing

Using Dual Input Controls
Loading Personal Screen Savers
Speaking to the Media
Speaking to Customers
Need for Dual Control / Segregation of Duties
Using Clear Desk Policy
Misaddressing Communications to Third Parties
Using External Disposal Firms
Using Photocopier for Personal Use
Verifying Correctness of Information
Travelling on Business
Checking Customer Credit Limits

5. PURCHASING AND MAINTAINING COMMERCIAL SOFTWARE

Purchasing and Installing Software

Specifying User Requirements for Software
Implementing New& Upgraded Software
Selecting Business Software Packages
Selecting Office Software Packages
Using Licensed Software
Technical Vulnerability Management

Software Maintenance & Upgrade

Applying 'Patches' to Software
Responding to Vendor Recommended Upgrades to Software
Interfacing Applications Software& Systems
Supporting Application Software
Operating System Software Upgrades
Upgrading Software
Support for Operating Systems
Recording and Reporting Software Faults

Other Software Issues

Disposing of Software

6. SECURING HARDWARE, PERIPHERALS AND OTHER EQUIPMENT

Purchasing and Installing Hardware

Specifying Information Security Requirements for New Hardware

Specifying Detailed Functional Needs for New Hardware
Installing New Hardware
Testing Systems and Equipment

Cabling, UPS, Printers and Modems

Supplying Continuous Power to Critical Equipment
Using Centralized, Networked or Stand-Alone Printers
Managing and Maintaining Backup Power Generators
Using Fax Machines / Fax Modems
Using Modems / ISDN& DSL connections
Installing and Maintaining Network Cabling

Consumables

Controlling IT Consumables
Using Removable Storage Media including Diskettes and CDs

Working Off Premises or Using Outsourced Processing

Contracting or Using Outsourced Processing
Using Mobile Phones
Using Business Centre Facilities
Issuing Laptop / Portable Computers to Personnel
Using Laptop / Portable Computers
Working from Home or Other Off-Site Location (Tele-working)
Moving Hardware from One Location to Another
Day to Day Use of Laptop / Portable Computers

Using Secure Storage

Using Lockable Storage Cupboards
Using Lockable Filing Cabinets
Using Fire Protected Storage Cabinets
Using a Safe

Documenting Hardware

Managing and Using Hardware Documentation
Maintaining a Hardware Inventory or Register

Other Hardware Issues

Disposing of Obsolete Equipment
Recording and Reporting Hardware Faults
Clear Screen Policy
Logon and Logoff from your Computer
Dealing with Answering Machines / Voice Mail
Taking Equipment off the Premises
Maintaining Hardware (On-site or Off-site Support)
Using Speed Dialling Telephone Options
Cleaning of Keyboards and Screens

Damage to Equipment
Insuring Hardware
Insuring Laptops& Portables for use domestically or abroad

7. COMBATING CYBER CRIME

Combating Cyber Crime

Defending Against Premeditated Cyber Crime Attacks
Minimizing the Impact of Cyber Attacks
Collecting Evidence for Cyber Crime Prosecution
Defending Against Premeditated Internal Attacks
Defending Against Opportunistic Cyber Crime Attacks
Safeguarding Against Malicious Denial of Service Attack
Defending Against Hackers, Stealth-and Techno-Vandalism
Handling Hoax Virus Warnings
Defending Against Virus Attacks
Responding to Virus Incidents
Collecting Evidence for Cyber Crime Prosecution
Installing Virus Scanning Software

8. CONTROLLING E-COMMERCE INFORMATION SECURITY

E-Commerce Issues

Structuring E-Commerce Systems including Web Sites
Securing E-Commerce Networks
Configuring E-Commerce Web Sites
Using External Service Providers for E-Commerce

9. DEVELOPING AND MAINTAINING IN-HOUSE SOFTWARE

Controlling Software Code

Managing Operational Program Libraries
Controlling Software Code during Software Development
Controlling Program Listings
Controlling Program Source Libraries
Controlling Old Versions of Programs
Managing Program Source Libraries

Software Development

Software Development
Establishing ownership for System Enhancements
Justifying New System Development
Managing Change Control Procedures
Making Emergency Amendments to Software
Separating Systems Development and Operations

Testing & Training

Controlling Test Environments
Using Live Data for Testing
Testing Software before Transferring to a Live Environment
Capacity Planning and Testing of New Systems
Parallel Running
Training in New Systems

Documentation

Documenting New and Enhanced Systems

Other Software Development

Acquiring Vendor Developed Software

10. DEALING WITH PREMISES RELATED CONSIDERATIONS

Premises Security

Preparing Premises to Site Computers
Securing Physical Protection of Computer Premises
Challenging Strangers on the Premises
High Security Locations
Delivery and loading areas
Duress Alarm
Ensuring Suitable Environmental Conditions
Physical Access Control to Secure Areas
Environmental and other external threats

Data Stores

Managing On-Site Data Stores
Managing Remote Data Stores

Other Premises Issues

Electronic Eavesdropping
Cabling Security
Disaster Recovery Plan

11. ADDRESSING PERSONNEL ISSUES RELATING TO SECURITY

Contractual Documentation

Preparing Terms and Conditions of Employment
Using Non Disclosure Agreements (Staff and Third Party)
Misuse of Organization Stationery
Lending Keys to Secure Areas to Others
Lending Money to Work Colleagues

Complying with Information Security Policy
Establishing Ownership of Intellectual Property Rights
Employing / Contracting New Staff
Contracting with External Suppliers& other Service Providers
Employees' Responsibility to Protect Confidentiality of Data

Confidential Personnel Data

Respecting Privacy in the Workplace
Handling Confidential Employee Information
Giving References on Staff
Checking Staff Security Clearance
Sharing Employee Information with Other Employees
Sharing Personal Salary Information

Personnel Information Security Responsibilities

Using the Internet in an Acceptable Way
Keeping Passwords& PIN Numbers Confidential
Sharing Organization Information with Other Employees
Signing for the Delivery of Goods
Signing for Work done by Third Parties
Ordering Goods and Services
Verifying Financial Claims and Invoices
Approving and Authorization of Expenditure
Responding to Telephone Enquiries
Sharing Confidential Information with Family Members
Gossiping and Disclosing Information
Spreading Information through the Office 'Grape Vine'
Using E-Mail and Postal Mail Facilities for Personal Reasons
Using Telephone Systems for Personal Reasons
Using the Organization's Mobile Phones for Personal Use
Using Organization Credit Cards
Playing Games on Office Computers
Using Office Computers for Personal Use

HR Management

Dealing with Disaffected Staff
Taking Official Notes of Employee Meetings

Staff Leaving Employment

Handling Staff Resignations
Completing Procedures for Terminating Staff or Contractors
Obligations of Staff Transferring to Competitors

HR Issues Other

Recommending Professional Advisors

12. DELIVERING TRAINING AND STAFF AWARENESS

Awareness

Delivering Awareness Programmes to Permanent Staff
Drafting Top Management Security Communications to Staff
Third Party Contractor: Awareness Programmes
Delivering Awareness Programmes to Temporary Staff
Providing Regular Information Updates to Staff

Training

Information Security Training on New Systems
Information Security Officer: Training
User: Information Security Training
Technical Staff: Information Security Training
Training New Recruits in Information Security

13. COMPLYING WITH LEGAL AND POLICY REQUIREMENTS

Complying with Legal Obligations

Being Aware of Legal Obligations
Complying with Copyright and Software Licensing Legislation
Complying with the Data Protection Act or Equivalent
Complying with General Copyright Legislation
Complying with Database Copyright Legislation
Legal Safeguards against Computer Misuse

Complying with Policies

Managing Media Storage and Record Retention
Complying with Information Security Policy

Avoiding Litigation

Safeguarding against Libel and Slander
Using Copyrighted Information from the Internet
Sending Copyrighted Information Electronically
Using Text directly from Reports, Books or Documents
Infringement of Copyright

Other Legal Issues

Recording Evidence of Incidents (Information Security)
Reviewing System Compliance Levels
Renewing Domain Name Licenses – Web Sites
Insuring Risks
Recording Telephone Conversations
Admissibility of Evidence
Adequacy of Evidence

Collection of Evidence

14. DETECTING AND RESPONDING TO IS INCIDENTS

Reporting Information Security Incidents

Reporting Information Security Incidents
Reporting IS Incidents to Outside Authorities
Reporting Information Security Breaches
Software Errors and Weaknesses
Notifying Information Security Weaknesses
Witnessing an Information Security Breach
Being Alert for Fraudulent Activities
When and How to Notify Authorities

Investigating Information Security Incidents

Investigating the Cause and Impact of IS Incidents
Collecting Evidence of an Information Security Breach
Recording Information Security Breaches
Responding to Information Security Incidents

Corrective Activity

Establishing Remedies to Information Security Breaches

Other Information Security Incident Issues

Ensuring the Integrity of IS Incident Investigations
Analyzing IS Incidents Resulting from System Failures
Monitoring Confidentiality of Information Security Incidents
Breaching Confidentiality
Establishing Dual Control / Segregation of Duties
Using Information Security Incident Check Lists
Detecting Electronic Eavesdropping and Espionage Activities
Risks in System Usage
Reviewing System Usage

15. PLANNING FOR BUSINESS CONTINUITY

Business Continuity Management

Initiating the Business Continuity Project
Assessing the Business Continuity Security Risk
Developing the Business Continuity Plan
Testing the Business Continuity Plan
Training and Staff Awareness on Business Continuity
Maintaining and Updating the Business Continuity Plan
Realistic Testing Environment for Business Continuity Plans
Impact of the Pace of change on the Business Continuity Plan