

Executive Summery

Information security is an important aspect of any business process, ecommerce or governance, hence protection of organization Information Systems (IS) from the threats of Confidentiality, Integrity and Availability must be ensured at all times. The methodology adopted by security managers to safeguard against potential threats largely depends on the organization's risk management protocols. However, in security classes, some organizations try to secure their Information Systems by complying to risk management Standards like ISO27000, British Standard 7799 (BS7799) or American NIST rather than carrying out risk analysis, assessments and reviews. In such cases, system security is guided by control requirements outlined in the risk management Standards. In contrast, some organizations secure their systems through the use of software based security assessment tools like CRAMM, OCTAVE or COBRA and then safeguard their IS based on the countermeasure recommendations output by the tools.

This project investigates and compares two different approaches to risk assessment: the application of security Standard i.e. British Standard BS7799 and the application of security assessment tool CRAMM. It then evaluates a complete and secured conceptual smart infrastructure model based on the application of both security management methodologies; in order to determine the differences in risk exposure, risk measurement and control effectiveness. The research is purely investigatory, hence it is more of type II with project type weighting ratio of (I/II/III):0/100/0. The research involves a good measure of theoretical discussions and review analysis involving risk assessment and management procedures.

In addition to what was stated in the review, due to the amount of time and steep learning curve required to use the CRAMM software, the project has been adapted to use CRAMM logic instead; which is essentially focusing on the manual risk calculation aspect of CRAMM. In the thesis, we present the result of using BS7799 and CRAMM Logic in a business enterprise conceptual model and compare the risk mitigation controls offered by both methodologies in terms of risk exposure and control measurements. Finally, the evaluation and comparison of two different risk assessment methods reported in this thesis, leads to the following insight:

- The BS7799 Standard is too generic and security control technologies are not embedded in Standards. Hence, achieving compliance with security Standard BS7799 is a substantially daunting task and operationally intensive process.
- BS7799 does not account for the scale of security controls and it is difficult to measure the effectiveness of security guidelines in the Standard. While CRAMM provides a calculation-based approach to measure and comparing the scale of one risk relative to others.
- If an organization holds certification to BS7799, it is suggested that proceedings should be commenced on establishing a clearly defined set of security control measurements.

Table of Contents

Executive Summary.....	3
Acknowledgement.....	4
Table of Contents.....	5
List of Tables.....	8
List of Figures.....	9
Chapter 1: Introduction.....	10
1.1 - Introduction to the Project.....	10
1.2 - Motivation behind the project.....	11
1.3 - Project Aim Objective.....	11
1.3.1 - Objective Outlines.....	12
1.4 - Report Layout.....	12
1.5 - Summary.....	12
Chapter 2: Background.....	13
2.1 – Introduction.....	13
2.2 - Terms Definition.....	13
2.3 - Threat Categorization.....	15
2.3.1 - Human.....	15
2.3.2 - Natural.....	15
2.3.3 - Technical.....	15
2.4 - Risk Management Overview.....	16
2.5 - Adopted risk management methodologies.....	18

2.5.1 - The British Standard 7799 (BS7799).....	18
2.5.1.1 - BS7799 Process Approach.....	19
2.5.2 - CCTA Risk Analysis and Management Method (CRAMM)..	22
2.5.2.1 - Asset identification and valuation.....	22
2.5.2.2 - Threat-Vulnerability Assessment & Risk Calculation.....	23
2.5.2.3 - Identify and Prioritize Countermeasures.....	26
2.6 - Other Risk Assessment Methodologies.....	26
2.6.1 - The ISO/IEC 27002.....	27
2.6.2 - Risk Management Guide.....	27
2.6.3 - OCTAVE.....	28
2.6.4 - COBRA.....	28
2.7 - Summary.....	28
Chapter 3: Conceptual Model System Description.....	29
3.1 - Introduction.....	29
3.2 - Scope.....	29
3.3 - Information Asset Classification.....	29
3.4 - Inventory of major Information Asset.....	34
3.5 - Initial Risk Ranking Order.....	36
3.6 - Summery.....	38
Chapter 4: Implementation of Threat Assessment.....	39
4.1 - Introduction.....	39
4.2 - Applying BS7799-2:2002 Methodology.....	39
4.3 - Applying CRAMM Logic Methodology.....	43

Chapter 5: Results and Analysis.....	48
Chapter 6: Conclusion and Discussion.....	51
Chapter 7: Future Work.....	53
References.....	54
Appendix.....	57

List of Tables

Table 1: BS7799 Clause A.7.....	21
Table 2: Risk Likelihood and Severity Description.....	24
Table 3: Risk Rating Table.....	25
Table 4: Risk Assessment Matrix.....	25
Table 5: Inventory of Assets.....	35
Table 6: Catalogue of Threats.....	36
Table 7: Initial Risk Ranking Table.....	37
Table 8: BS7799 Controls.....	42
Table 9: Measure of Risk and Final Threat Ranking.....	44
Table 10: CRAMM Controls.....	47

List of Figures

Figure 1: Risk Management Cycle.....	17
Figure 2: PCDA Model applied to ISMS Process.....	20
Figure 3: CRAMM Graphical Interface.....	23
Figure 4: High Level Conceptual Model Diagram.....	31
Figure 5: Low Level Conceptual Model Diagram.....	33
Figure 6: Gross Risk Map.....	48
Figure 7: Risk Management.....	49
Figure 8: Net Risk Map.....	49
Figure 9: Pre Mitigation Risk Ratio.....	50
Figure 10: Post Mitigation Risk Ratio.....	50

Chapter 1

Introduction

1.1 - Introduction to the Project

In recent years, especially the last two decades, seamless augmentation of Information Technology (IT) applications in homes, offices and other infrastructures have become the norm. Advancement in technology, i.e. computing processing power, communication bandwidth, digital storage and databases have resulted in a true ubiquitous computing environment whereby systems fit around users rather than the other way round. Similarly, smart buildings which incorporate system critical services have witnessed tremendous changes over the same period of time, with respect to the increasingly reliant on interconnected and automated systems that perform specific functions. As such, IT security has become quite an important consideration for modern organizations. Importance of information security cannot be over emphasized, especially in today's areas of key interest which spans network security, disaster recovery planning, and risk analysis and management [1].

This project describes the feasibility of using two clearly different risk management techniques to guide a smart infrastructure security policy and architectural design decisions. However, the 'Hacking the Bridge' component of this project is basically about penetrating any smart infrastructure that depends on intelligent technologies rather than a 'bridge' in specific sense. It is more about any civil bridges like a motorway, airport, business enterprise or any other infrastructure and we are addressing the hacking aspect of it as well as major potential cases where somebody can cause security breach in the systems like that. Information security is undoubtedly the most important challenge faced by IT managers in order to remain on top of their games against adversaries; "The aim of information security is to ensure business continuity by preventing and minimizing the impact of security incidents" [2]. Security risk assessment also known as risk analysis is an essential and fundamental component of security control in any organization. By carrying out risk analysis, it is possible to realize the scale of potential damage that may be caused by breaching the security of such infrastructure, against the backdrop of confidentiality, integrity and availability.

Over the years, IT industry regulatory bodies have proposed various Standards and controls which are benchmark for security management guidelines. Similarly, vendors in the industry have provided various automated software packages for risk analysis of information systems and associated threats. However, applying the appropriate tool usually depends on organizations peculiar security risks and security policies. A lot of the conventional methods in use today for performing security risk analysis are becoming more and more untenable in terms of usability, flexibility, measurability and end user output [3]. Naturally, organizations, government establishments and business enterprises protect their IT infrastructures through by

using two different basic approaches; either by complying with industry regulatory Standards or by using risks assessment tools. This project investigates the adoption of both approaches in order to determine the most effective and measurable risk assessment method.

In the project, we conceptualized a particular case study of a private college in Stratford, London. The idea is to incorporate a large number of IT systems that manage vital services such as servers, databases, energy consumption monitoring, surveillance & access control, fire detection, air-conditioning, lift performance adjustments etc., and then critically evaluate the IT systems against potential risks of disaster and risks of abuse in equal measures.

1.2 - Motivation behind the project

A lot of the modern infrastructures i.e. airports, motorways, rail networks, business enterprises etc. depends on critical IT infrastructure these days and are more increasingly reliant on essential networks like access control, information processing and monitoring systems which are all part of integrated computer networks; such that if the essential networks are taken away, breached or hacked in any way, it then becomes more difficult to manage such infrastructure. Therefore, understanding organizational risk acceptance threshold is vital in order to channel resources to control, prevented or transfer risks in the most appropriate manner. In other words, it is not good management if a lot of resources are dedicated to security solutions in order to prevent risks that are of no significant impact to an organization, similarly, it is equally wrong not to channel the right amount of resources or not acquiring the right security solution to mitigate risks of potentially colossal consequences, while hoping that such risk will never happen.

Information Security Management is an interesting area that is part of motivation for this project. There has been a lot of work documented on the risk assessment of different types of infrastructure i.e. a home office or small business enterprise model but this work is different in the sense that it investigates the differences in two different methodologies adopted to secure a smart infrastructure. It specifically compares and evaluates the use of BS7799 and CRAMM Logic in terms of security control metrics or measurements.

1.3 - Project Aim Objective

The aim of the project is to conduct information risk analysis of a smart infrastructure in order to understand the potential risks and exposures of Information System (IS) in it and propose appropriate countermeasures recommendations to address such risks.

1.3.1 - Objective Outlines

Objectives outline to accomplish the overall aim of his project are as follows:

- Provide comprehensive background information on the two assessment methodologies adopted for this project. The British Standard BS7799 and CRAMM risk assessment software.
- Develop a conceptual model of a smart infrastructure while taking into account different types of IT applications likely to exist within it. Produce a top level and low level graphical representation of the conceptual model.
- Prepare survey questionnaire and obtain dataset from real system users/owners in order to relate similar IT applications to our model.
- Carry out risk analysis on the conceptualised model using both methodologies mentioned above, and present in-depth analysis of the project results.

1.4 - Report Layout

This project report is divided into chapters starting from the introduction, which describes the project overview and provides general information on the direction of this report. Chapter 2 covers the project research background, term definitions and clarifies some gray areas that were highlighted during the interim review feedback. It covered security management Standards and security assessment tools with emphasis on those that are in line with UK requirements. Chapter 3 covers the description of systems in our conceptual model, including asset classification, threat ranking as well as top level and low level model diagram. Chapter 4 describes the process of applying BS7799 and CRAMM Logic methodologies to secure our conceptual model. Chapter 5 presents the project results and analysis of measurements. Chapter 6 showcases the project conclusion and in-depth discussion to sum up the investigation conducted in this project. Finally, Chapter 7 suggests possible areas of future work based on some limitations identified in this project.

1.5 - Summary

This chapter has been able to set the scene for the overall project report, it has touched on the increasing ubiquitous nature of IT systems, the importance of security risk assessment, the project aim and objectives outline, the project report layout and most importantly, the motivation for this project. There have been a slight change in the objectives of this project since the project review period; this is largely due to unavailability of CRAMM software among other reasons. However, we are still able to stick with the overall aim of this project.

Chapter 2

Background

2.1 - Introduction

This chapter introduces the two security risk assessment methodologies we have adopted for this project as well as brief description of other risk assessment methodologies not considered for this project. It also covers general background on risk management and definition of terms used throughout the context of this report. Later on in chapter 4 of this report, some assumptions were considered in the implementation stage; analysis of the two adopted methodologies in this chapter will help the reader to understand the rationale behind those assumptions.

2.2 - Terms Definition

In order to discuss security assessment within the scope of this project, we find it necessary to define a number of terms used in this work as described in [3] and [4].

Availability: Protection of systems and data from intentional and accidental attempt to cause denial of service, unauthorized deletion or unauthorized purposes. It is also about ensuring timely and reliable access to and use of information.

Integrity: Ensuring systems remain operable throughout organization life cycle by guarding against improper destruction and modification of information, including authentication and non-repudiation.

Asset: General support systems and high impact programs including personnel, mission critical systems, equipment, physical plant or logically related group of systems.

Accountability: Security objective that generates requirement for action of an entity to be uniquely traced to that entity at individual level. It supports intrusion detection and prevention, non-repudiation, deterrence and fault isolation.

Confidentiality: Preserving authorized restriction to sensitive information from individuals, entities or processes while it is in storage, being processed or in transit.

Assessment Method: It is one of the three types of action: examine, interview or test taken by assessors during an assessment in order to obtain evidence.

Attack: Any kind of malicious action that attempts to compromise system activities or gain unauthorized access to information resources and system services.

Risk Assessment: Part of risk management framework which identify, prioritize and estimate risks as well as determines the impact of adverse circumstances on an enterprise.

Risk Mitigation: The evaluation, prioritization and implementation of appropriate risk reducing controls based on the recommendation of risk assessment processes.

Threat: Potential circumstances or event of adverse impact on organization, assets, individuals and operations as a result of unauthorized disclosure, destruction, access and modification of information, and denial of service.

Baseline Security: Minimum level of security controls required for safeguarding an IT system against the threat of integrity, confidentiality and availability protection.

Business Continuity Plan (BCP): A document that describes predetermined set of procedure and instructions that details organization plan of action to sustain any significant disruption to its mission/business functions.

Business Impact Analysis (BIA): Analysis of enterprise information system requirements, interdependencies and processes used to characterize contingency requirements and priorities in the case of disruption of significant scale.

Chief Information Officer (CIO): Organization official responsible for: 1) providing advice to head of the executive agency in order to ensure that information resources are managed and consistent with the requirements of legislation or industry Standards. 2) Develop, facilitate and maintain integrated information technology for the organization.

Countermeasures: Techniques, processes, devices, actions and other measures that reduce prevent or eliminate vulnerability of an information system.

Risk: Information system related security risks are the risks that arise from the loss of integrity, confidentiality and availability of information systems. It is a measure of the degree to which Information System is threatened based on the function of 1) the adverse impact of an event occurring and 2) the likelihood of the occurrence.

Impact: The magnitude of harm that can occur as a consequence of unauthorized disclosure, modification, destruction of information or information system, and loss of availability.

Information Security Policy: Aggregate of direction, practices, rules and regulations that describe how an organization distributes, protects and manages information.

2.3 - Threat Categorization

Every security risk assessment process should begin with threat identification procedures and understanding potential threat factors such as sources, methods, motivation and consequences. Similarly, since organization operational environment, information systems, policies and physical resources can influence different types of risk sources, it is essential that potential threats are grouped or defined in a common set of criteria which can be used for comparison and evaluation purposes [5]. Threats classification is an important step towards the implementation of information security management. Though, different types of threat classifications have been proposed by industry Standards, government and security experts but they are generally incompatible and difficult to be compared [6], in the context of this report however, we shall focus on threat categorization as proposed in [7], which posits that there are three intuitive categories of threats:

2.3.1 - Human

These are people oriented threats that usually involve individuals within and outside an organization. Insider oriented threats are some of the most difficult threats to deal with because of insiders familiarity with system resources, capabilities, locations and performances. This is a broad category with range of capabilities and motivations which can be further divided into sub-groups for independent assessment. These include hackers, crackers, terrorists; partners and competitors est. Human threats also include indiscipline and negligence.

2.3.2 - Natural

These threats are of non-human nature and occur in circumstances that are beyond organization control. These include all forms of natural disaster like fire, earthquake, flood, storm, hurricane est. although, no business enterprise, government institutions or organizations is exempted from the exposure to natural threats, it is possible to predict the likelihood of occurrence based on indicators like geographical location among others.

2.3.3 - Technical

These types of threats are capable of causing extensive damage to information systems with little or no human supervision at all. They are characterized with a blend of human/non-human involvement especially during the development stage and once completed, they can take up the 'form of life' and execute human-like commands. This category of threats is usually deployed on networks and examples include viruses, Trojan horse, worms and logic bomb. Technical threats can also include genuine technical mistakes like communication error, malfunctions, software defects and unavailability of systems (down time errors).

2.4 - Risk Management Overview

In general terms, all Information Systems (IS) involve risk of some sort at one stage or the other, as such it can be implied that risk is an intrinsic part of any organization IS and business processes. How to mitigate those risks therefore forms an important component of any management decision making process [8]. According to the definitions proposed in [9] and [10], "Risk is a function of the likelihood of a given threat, exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization". It is the adverse effect as a result of actualized threat. In the context of Information Systems, [11] posits that "the likelihood that a firm's information systems are insufficiently protected against certain kinds of damage or loss is known as system risk". It was further affirmed that system risk has been a back-burner issues for too long, even among the top practitioners and managers of Information Technology (IT).

Information System risk varies depending on organizational risk acceptance level; however, risks are generally described under the broad categorization of disaster or abuse. Top priority of Chief Information Officers (CIO) and managers (to a larger extent) is to ensure constant functionality of IT resources throughout all levels of operations. They ensure that organizational risk exposure that could undermine the confidentiality; integrity and availability of mission-critical systems are adequately managed. Usually, unmitigated risks lead to negative corporal image, bad reputation and sometimes colossal financial losses. This assumption was buttressed in [11], where it was reported that based on studies proposed over the years to quantify the actual and potential value of losses as a result of successful system breaches; the value was put in the region of \$500 million and \$5 billion per year in the United States alone and this trend continues to grow. As such, the importance of risk management cannot be over emphasized.

Risk management (RM) can be described as a systematic and logical approach to identifying, treating, analyzing and monitoring risks in any process. Managers benefit from risk management methodologies because it directly influences how available resources are put to best use [12]. RM practice transcends a wide range of jobs, activities and operations that cover public and private sectors: health care, government establishments, insurance, finance and investments, educational institutions est. in fact, RM has become an essential component of business planning. However, in the context of Information Security (which is basically about the protection of information assets), the need for security risk management is even stronger than physical asset protection with respect to corporate government responsibilities. Information Security Risk Management is defined in [13] as "the protection of information from a wide range of threats in order to ensure business continuity, manage business risk and maximize return on investment". Risk management involves the implementation of appropriate controls to mitigate risks. However, since risks and threats changes all the time, it is essential that the effectiveness and appropriateness of selected controls must be reassessed and reconsidered periodically by the organization. This is an important element of risk management cycle [14]. There are various reasons why an organization may require

some measures of security control against potential threats; these could stem from internal factors i.e. corporate regulations and organizational policies or externally influences i.e. data protection acts [15] or to comply to industry regulatory Standards. Typically, risk management cycle involves 7 distinct steps irrespective of organization business or function, as shown in the risk management cycle diagram in figure 1. The 7 risk management steps are described here according to [13].



Figure 1: Risk Management Cycle

Establish the Context: This covers basic understanding of an organization business process in a broader perspective. It includes overview of the nature of risks inherent in the business model as well as how management prioritizes those risks.

Identify the Risks: this covers the identification of risks and how such risks affect to organization goals and objectives. It takes into account how stakeholders are affected or involved in risks while considering past events and future developments.

Analyze the Risk: this covers analysis of the probability and frequency of risk events happening as well as the political, social and economical impact or financial consequences of such events happening.

Evaluate the Risk: this covers ranking of inherent risk levels based on the likelihood and consequence of risks according to management proprieties.

Treat the Risk: this involves developing and implementing countermeasures to mitigate identified risks while taking into account management priorities, resources and risk acceptance level.

Monitor and Review: this involves continuous monitoring of activities and processes through the use of data evaluation, compliance measurement or audit methods in order to determine the effectiveness of measures adopted to treat risks. Risk management policies and decisions must be reviewed regularly.

Communicate and Consult: given that risks are dynamic, the process of communication and consultation must be regular in order to recognize when there is a shift in organization risk acceptance threshold.

2.5 - Adopted Risk Management Methodologies

There is no regulation that spells out in legal terms the need for specific IT controls to mitigate risks like security logging, back-ups, and password management etc. instead, Security Management Standards focus on the fundamental need for confidentiality, integrity and availability in the realms of operational, physical and technical security [3]. Similarly, software risk assessment tools simplify the process of risk management through automated risk scoring matrix. Software tools automate the processing of security inputs in order to ease the burden of security management [16]. Different organizations adopt different approach to risk management depending on peculiar security requirements. This section introduces the risk assessment methodologies adopted for this project, although, these risk management methodologies does not represent all of the techniques available to CIOs and managers but the methodologies were used based on the amount of support is receives from IS stakeholders. The BS7799 Standard discussed here is arguably the most common Standard for security management and it has been adopted and published in several countries including the UK [17]. Similarly, the CRAMM software assessment tool is one of the most popular security assessment tools among security managers and also approved by the British Government. It is the most widely used methodology in Europe for risk analysis and management [18]. This section will aid the reader to understand the working order and basic differences of these methodologies before they are applied to the risk assessment process in our model.

2.5.1 - The British Standard 7799 (BS7799)

Collaboration between some British companies, international companies as well as the department of trade and industries led to the development of the Code of Practice (CoP) for information security management which later became the British Standard 7799 (BS 7799). The Standard contained in a publication released in 1993 was basically a compilation of the best Information System (IS) practices sampled from international companies. Over 100 controls were included in the code of practice, which collectively form the baseline of good security practice.

A revised version of the Standard known as BS 7799-2: 2002 was later published in 2002 to include ten key control areas that are essential for all organizations. The British Standard 7799 (BS7799) is arguable the most widely used and recognized security Standard in the world and also has comprehensive coverage of security issues. BS7799 is a framework for security best practices and contains guidelines for the improvement of organization security [19], such that business managers and staff can use the model for setting up effective security management systems. It is also used by certification bodies to assess organization abilities to meet regulatory and customer demands as well as organizational ability to meet its own requirements. BS7799 is a comprehensive guideline with significant number of control requirements which can be complex to implement sometimes; hence it is recommended that using the Standard to obtain full certification should be carried out in 'step by step' order. It is a very detailed document organized into 10 major sections (version BS7799-2:2002) for ease of implementation, and each section cover different topic areas.

BS7799 is guided by a process approach called Plan-Do-Check-Act (PCDA) principles [20], which ensures that organizations information security systems and accreditation are in line with industry best practices. As stated earlier in this report, some organizations secure their systems by applying control requirements and demands of the BS7799 Standard; next, this report briefly describes the PCDA model of BS7799 so that the reader can understand the Standard process approach.

2.5.1.1 - BS7799 Process Approach

BS7799 uses a process approach for monitoring, implementing and maintain organization's Information Security Management Systems (ISMS) effectively. Process approach can be referred to as the identification, interaction and management of systems or processes within an organization in order to understand its information security requirements. It covers the implementation of operational security controls, overall business risks and performance review of ISMS. A process model adopted in BS7799 which can be applied to all business models is known as the Plan-Do-Check-Act (PCDA) model. PCDA model is a virtual cycle of activities that ensures organization best practices are documented, reinforced and improved with time. The end of one phase is an input to the next, and it is expected to be a continuous cycle of activities for all ISMS processes.

The model essentially takes information security requirement and expectations as input, through actions and processes that meets those requirements; then produces an output of a managed information; figure 2 illustrates the PCDA model process and each phase of the model is described as follows [21].

The plan phase: This design ensures that scope and context of ISMS is established correctly and takes into account plans to identify security risks as well as appropriate treatment for each risk. Basically, the plan phase covers information security policy, scope of the ISMS, risk identification, assessment and treatment plan.

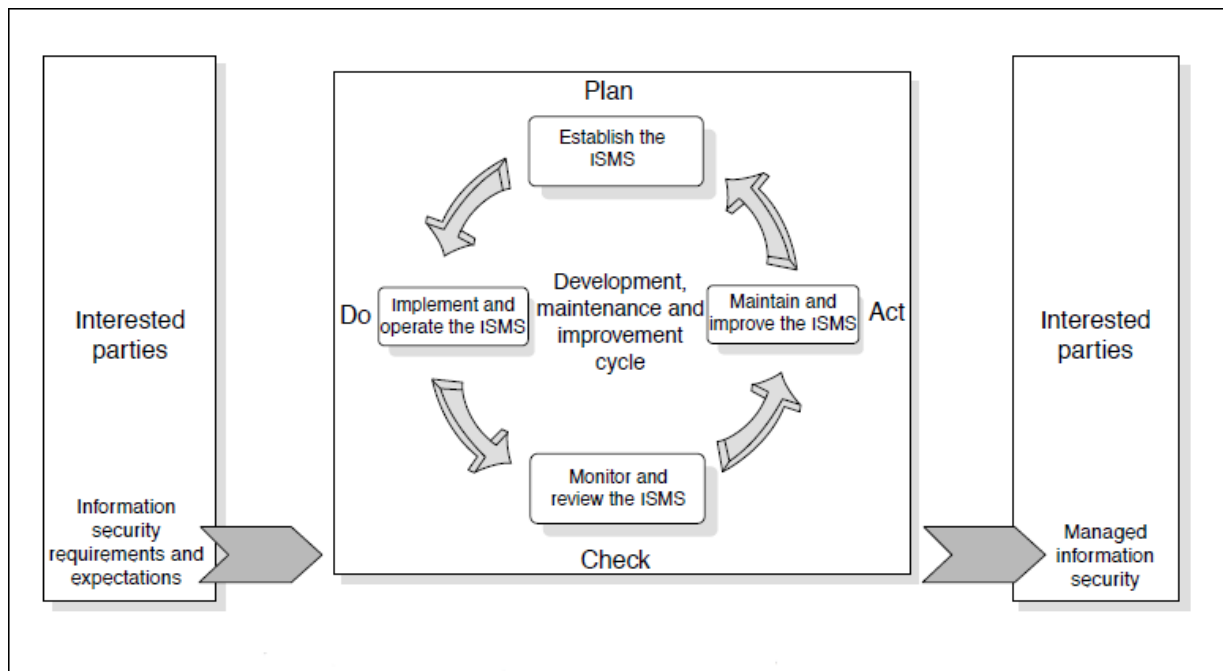


Figure 2: PCDA Model applied to ISMS processes (Adopted from BSI, 2002)

The Do Phase: this cycle implements and promotes selected controls for the management of information security risk, in line with all decisions take in the plan phase. This phase covers resource training and awareness, and risk treatment.

The check phase: this cycle is designed to check the effective of controls as ensure they are working as expected; and if such controls are found to be inadequate either as a result of change to the scope or assumption of security assessment, then necessary corrective actions are determined. The check phase covers routine checking, management review, ISMS audit and trend analysis.

The Act Phase: this phase is concerned with regular improvement of the information collected during the check phase in order to maintain effective ISMS. The purpose of this phase is to take appropriate action based on the result of the check phase activities. In fact, any non-conformity issues i.e. failure or absence to implement any of the requirements of ISMS is acted upon by taking corrective action at the Act Phase.

Using BS7799 to secure Information Systems involve meeting control objective requirements of the Standard by implementing controls listed in the code of practice guidance BS ISO/IEC 17799; covering Clauses A.3 to A.12. The Clauses outlined implementation guidelines for best practices in support of organization security requirements.

A quick scenario of using BS7799: If areas of security concern based on scope of the organization (and as part of the PCDA process) has been identified to be physical and environment security related. Then using BS7799 clause A.7 which addresses Physical and environmental security as shown in Table 1 (BS7799 Clause A.7); our control objective is to prevent unauthorized access, damage and interference to business premises and information (sub clause number A.7.1 Secure Areas) or 7.1 (if we are using BS ISO/IEC 17799:2000 numbering system). We only need to identify required control and implement the requirement/guidelines proposed by the Standard. Using table 1, it can be seen that implementing control A.7.1.2 to secure physical entry requires carrying out corresponding security guideline in the Standard which states that “secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access”. However, the type of security solution deployed to this effect depends on the requirement of individual ISMS. Detailed control objective and controls are documented in [21].

			BS ISO/IEC 17799:2000 numbering
A.7.1 Secure areas			7.1
Control objective: To prevent unauthorized physical access, damage and interference to business premises and information.			
Controls			
A.7.1.1	Physical security perimeter	Organizations shall use security perimeters to protect areas that contain information processing facilities.	7.1.1
A.7.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	7.1.2
A.7.1.3	Securing offices, rooms and facilities	Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.	7.1.3
A.7.1.4	Working in secure areas	Additional controls and guidelines for working in secure areas shall be used to enhance the security of secure areas.	7.1.4
A.7.1.5	Isolated delivery and loading areas	Delivery and loading areas shall be controlled, and where possible, isolated from information processing facilities to avoid unauthorized access.	7.1.5
A.7.2 Equipment security			7.2
Control objective: To prevent loss, damage or compromise of assets and interruption to business activities.			
Controls			
A.7.2.1	Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	7.2.1
A.7.2.2	Power supplies	Equipment shall be protected from power failures and other electrical anomalies.	7.2.2
A.7.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	7.2.3
A.7.2.4	Equipment maintenance	Equipment shall be correctly maintained to enable its continued availability and integrity.	7.2.4
A.7.2.5	Security of equipment off-premises	Any use of equipment for information processing outside an organization's premises shall require authorization by management.	7.2.5
A.7.2.6	Secure disposal or re-use of equipment	Information shall be erased from equipment prior to disposal or re-use.	7.2.6
A.7.3 General controls			7.3
Control objective: To prevent compromise or theft of information and information processing facilities.			
Controls			
A.7.3.1	Clear desk and clear screen policy	Organizations shall have a clear desk and a clear screen policy aimed at reducing the risks of unauthorized access, loss of, and damage to information.	7.3.1
A.7.3.2	Removal of property	Equipment, information or software belonging to the organization shall not be removed without authorization of the management.	7.3.2

Table 1: BS7799 Clause A.7 (Adopted from BSI, 2002)

2.5.2 - CCTA Risk Analysis and Management Method (CRAMM)

CRAMM is an automated risk analysis and management tool based on quantitative risk assessment methodology and extensively used since 1987 [22] and [23]. It does not require much resource and runs on standard windows operating system. Though a flexible tool, it is comprehensive and requires qualified and experienced user to ensure efficient result. It is consistent with the UK Government security policy and Standard BS99: 1995, now ISO/IEC 2007 code of practice for information management [22] and [24]. CRAMM is more suitable for systems that are already operational rather than those still in developments but it can be used for any IT infrastructure security assessment. The CRAMM software tool has a graphical interface that guides the review process as shown in figure 3. Basically, CRAMM follows a fundamental approach to establish a consistent measure of risk matrix [25], these approach focuses on: 1) the possibility, level and frequency with which threats might occur. 2) The level of vulnerability of threat. 3) The impact of threat.

CRAMM is the Risk Analysis (RA) tool adopted for this project because of its extensive use and mandatory choice for UK governmental organizations. Therefore, there is more assessment of its features than other RA tools mentioned in this report. CRAMM review risk in three distinct stages, these stages are itemized below and briefly described as proposed in [22], [24] and [25]:

- Identify and value assets,
- Identify threats, vulnerabilities and calculate risks;
- Identify and prioritize countermeasures;

2.5.2.1 - Asset identification and valuation

This phase deals with identification and valuation of assets where all interrelated assets are defined in asset model. Modeling is an important feature of CRAMM; it ensures that important assets are not missed out due to too fine or too coarse granularity. CRAMM considers both tangible assets e.g. IT equipments and intangible assets e.g. information and draws asset valuation against the backdrop of confidentiality, integrity, availability and non-repudiation of resources. Measures of the severity of these impacts are then compared to the guidelines of CRAMM to generate values within the range of 1 to 10 e.g. the effect of crashed mail server over 1 hour or 10 months. In the case of physical assets or application software, financial cost of replacement or reconstruction is determined by interviewing the personnel privy to such information; feedbacks are then translated to the same scale value described above.

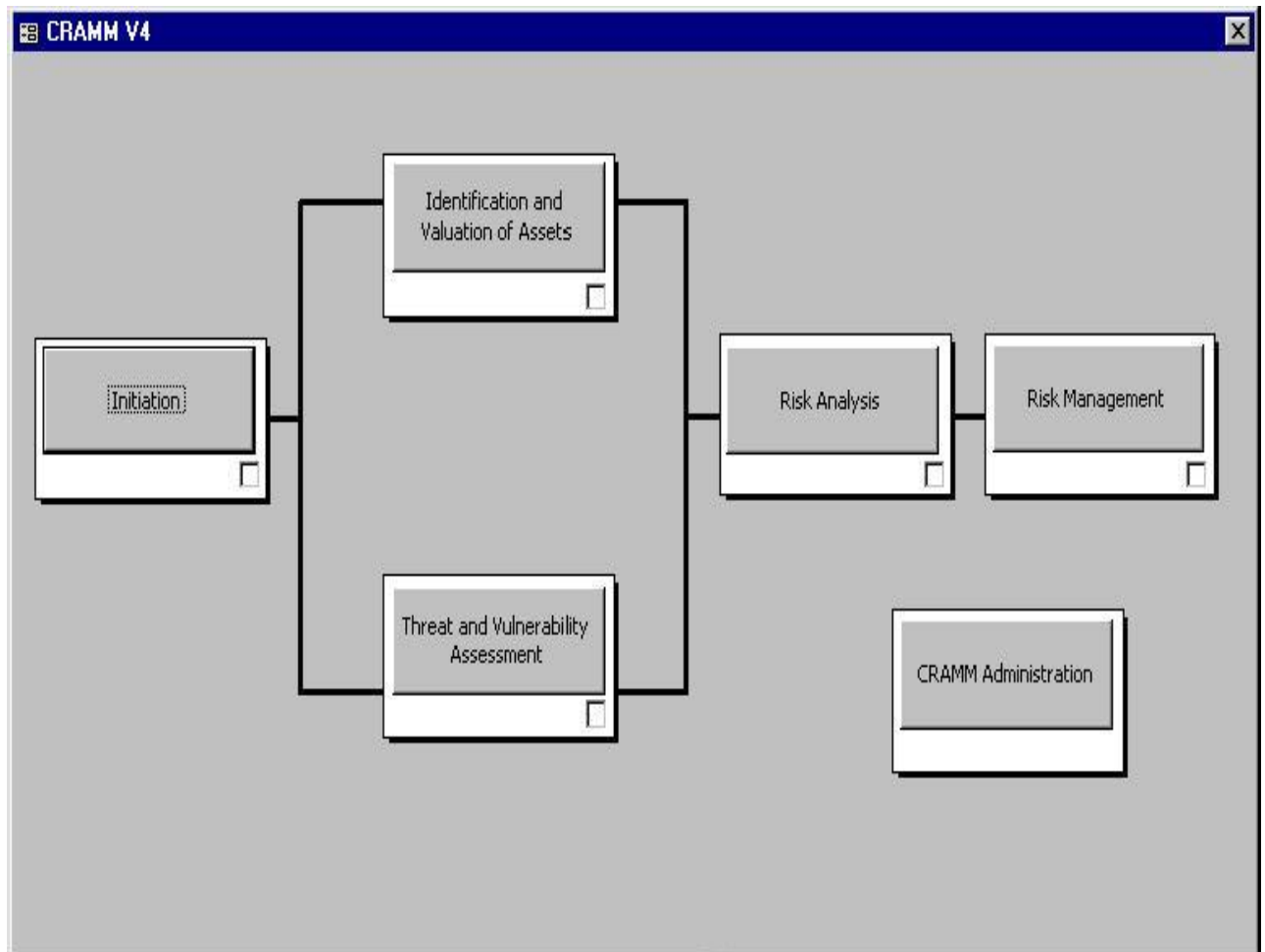


Figure 3: CRAMM Graphical Interface – (Adopted from Yazar, Z. 2002)

2.5.2.2 - Threat-vulnerability assessment and Risk calculation

The next phase involves the assessment of threats identified above and the vulnerability as a result of those threats. Although, CRAMM comes with pre-defined table of threats and impact combinations but not only is the list exhaustive, it is more productive if reviewers chose threats and assets in accordance to customers need. Structured questionnaires are used to obtain feedback from support personnel; the feedback is then used as input to CRAMM. It then generates risk/vulnerability output based on five scale levels of very low, low, medium, high and very high. For the purpose of this work, we are using manual calculations based on CRAMM Logic [25], See table 2 for description of likelihood and severity of risk, especially in terms of financial impact. Likelihood of risk is ranked on the scale of 1 to 5 where 1 is rare or very low and 5 is frequent or very high.

Likelihood	Description	Frequency of Occurrences
1	An incident is expected to occur in exceptional circumstances, e.g. once in 10 years	Rare/Very Low
2	An incident may occur at some point, e.g. once in 3 years	Possible/Low
3	An incident will occasionally recur, e.g. once in a year	Probable/Medium
4	An incident will occur in most circumstances, e.g. once every 4 months	Certain/High
5	An incident is certain to occur in most circumstances, e.g. once every month	Frequent/Very High
Severity	Description	Example of Business Impact
1	None: no disruption of service	Financial loss < £1000
2	Minor	Financial loss < £10, 000
5	Moderate	Financial loss < £100, 000
10	Significant	Financial loss < £1, 000 000
15	High	Financial loss > £1, 000 000

Table 2: Risk likelihood and severity description

Similarly, table 3 shows the risk scoring matrix by taking into account the likelihood and severity value of each risk.

Risk is scored based on the formula:

$$\text{Risk} = \text{Likelihood of Risk (Occurrence)} \times \text{Severity of Risk (Impact)}$$

Risk scoring is carried out by applying a simple multiplication process whereby the likelihood of risk is multiplied by the severity of the risk occurrence.

Risk Rating Table – Likelihood x Severity						
Severity → Likelihood ↓		None	Minor	Moderate	Significant	High
		1	2	5	10	15
Frequent	5	5	10	25	50	75
Certain	4	4	8	20	40	60
Probable	3	3	6	15	30	45
Possible	2	2	4	10	20	30
Rare	1	1	2	5	10	15

Table 3: Risk rating table (Adapted from West Essex PCT 2010)

After scoring each risk, risk rating is then applied by choosing the most appropriate definition under likelihood and the most appropriate definition under severity, and then the numbers are looked up on the risk matrix table and matched to obtain the risk rating. Table 4 shows the risk assessment matrix which describes the relationship between risk rating, colour code, risk description and expected management actions.






Risk Rating	Color Code	Description	Action
1 – 5		Very Low Risk	Effective control measures are in place and severity of risk is very low.
6 – 14		Low Risk	If control measures are not implemented, probability of harm is low but risk mitigating action is required within 6 months.
15 -30		Moderate Risk	If control measures are not implemented, probability of harm is moderate but risk mitigating action is required within 3 months.
40 -60		High Risk	If control measures are not implemented, probability of harm is significant. Risk mitigating action is required immediately.
75		Unacceptable Risk	Risk is unacceptable and all services processes and procedures must be stopped. Immediate risk mitigating action is required.

Table 4: Risk Assessment Matrix

2.5.2.3 - Identify and Prioritize Countermeasures

CRAMM comes with over 3000 predefined library of countermeasures grouped with respect to security requirements in hardware, software, communication, procedural, physical and personal resource [23]. After the risk analysis phase, CRAMM output sets of countermeasures relevant to the management of risks in context. Security countermeasures are also rated on a scale of 1 to 7, with 7 being very high. This is based on 'Annual Loss Expectancy' figures which are translated into CRAMM measure of risk scale. The idea is to compare existing security measures to CRAMM recommended security profile, so that areas of low protection and overprotection can be identified. Each of the countermeasures in the CRAMM library contains the following information:

- a reference number;
- a narrative description;
- the position in the countermeasure hierarchical structure;
- a cross-reference to other related countermeasures (where applicable);
- Minimum and maximum measures of risk/security level for the impacts each threat.

However, due to the steep learning curve required to be comfortable with the CRAMM software as well as time constraints, this project has been modified from using CRAMM software to using CRAMM Logic (risk scoring matrix), which is calculation based approach to determining appropriate countermeasures. The process still follows similar fashion as CRAMM software especially in the areas of asset identification and evaluation, and threat identification and calculation, though calculations are carried out manually. Finally, countermeasures are derived from the over 3000 library of countermeasures (in our case, it was obtained from CRAMM v5.1 manual and mapped appropriately to the results of risk scoring matrix.

CRAMM has many advantages over other security assessment methodologies, notable one is its structured approach to risk analysis and a method that is well established. However, major shortcoming of CRAMM is that full review can take months to generate report and it also requires experienced practitioner.

2.6 - Other Risk Assessment Methodologies

There are other security assessment and management methodologies as well as tools but because they are not selected for this project based on the discussions in section 2.5. There is no point conducting extensive review of the tools. However, for the purpose of completeness, some of the notable RA methodologies are summarized below as described in [9]:

2.6.1 - The ISO/IEC 27002

ISO/IEC 27002 was published by the international Organization for Standardization (ISO) and the International Electro technical Committee (IEC) published in 2002. It is a derivative of the original British Standard BS7799. Though, ISO/IEC 27002 is currently under review, it is a normal occurrence every few years in order to preserve the relevance of the Standard in the face of today's dynamic and sophisticated range of information security threats. The ISO/IEC provides area of comprehensive coverage that meets the risk management requirement of organizations in the area of business involving people, services, process, information technology and physical assets [27]. The ISO/IEC Standard have now become a globally recognized framework for the provision of a sound information security management and organizations continue to seek certification to it. It is robust enough to be adopted by both commercial and government organizations yet flexible to be used by small organizations as well. Control areas covered by the ISO/IEC 27002 Standard are:

- Information security policy
- Organization information security
- Asset management
- Physical environment security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- compliance

2.6.2 - Risk Management Guide

Risk Management Guide for Information Technology Systems is a US government standard methodology developed by the National Institute of Standards & Technology (NIST). It is anchored on the NIST special publication (SP) 800-30. Risk Management Guide is a qualitative and comprehensive risk assessment tool designed for skilled security analysts and technical experts for risk management. It follows nine distinct steps of threat evaluation processes:

- System Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation

2.6.3 - OCTAVE

Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE) methodology is a workshop based process developed by the Software Engineering Institute (SEI) of Carnegie Mellon University. The primary aim of OCTAVE is to assist organizations to improve the management and protection against information risks. Workshop-based approach of OCTAVE implies that organizations will understand risk evaluation more than the tool based approach; as such final decisions like countermeasures will be made by the organizations rather than the tool. The three phases of OCTAVE process include: knowledge gathering about important assets phase, which involve identifying senior management knowledge, operational management knowledge, staff knowledge and creation of threat profiles. Knowledge gathering from operational managers' phase involves identifying key threat components and evaluation of selected components. The knowledge gathering from staff phase includes risk analysis and the development of protection strategy. OCTAVE process output results in the following stages:

- Protection Strategy
- Mitigation Plan
- Action List

2.6.4 - COBRA

The Consultative, Objective and Bi-functional risk analysis (COBRA) methodology is a risk assessment tool that utilizes embedded expert knowledge to generate result for self assessment of risk. It was developed in 1991 by C and A Systems Security Ltd for risk assessment as a business issue rather than technical issues. Primary knowledge base of COBRA includes:

- IT Security (or default)
- Operational Risk
- Quick Risk' or 'high level risk'
- e-Security

2.7 - Summary

This chapter has been able to cover the project background starting with definition of terms that the reader will come across more often as the chapters unfold. A fair description of applying BS7799 control subjects to risk areas has also been covered so that the reader understands how the Standard guidelines work. Although, we did not have access to CRAMM software, there was also a fair description of the CRAMM tool working process and how the automated process differs from the manual risk scoring matrix. The resolve to use CRAMM Logic has been a backup plan (in case we fail to secure access to CRAMM software) and did not hinder the overall aim of the project.

Chapter 3

Conceptual Model Systems Description

3.1 - Introduction

This chapter focuses on the description of our system model including activities, participants and dataset obtained from the enterprise used as case study for our model. Dataset was obtained through interview questions as part of the Business Impact Analysis (BIA). The interview was conducted over a period of three days and the major point of contact was the enterprise system administrator who is largely responsible for the management of the organization IT systems. This section will also allow the reader to understand how our case study scenario is adopted for our conceptual model architecture, especially on asset inventory and risk ranking.

3.2 - Scope

The enterprise used as a case study for this project is a medium size private college in East London called DTK College. The college is under the regulatory directives of OFTED and has over 80 staff and students. It is also a certified Prometrics and Pearson Vue examination centre. The enterprise has one information system department but there is no any security management program currently in place and no dedicated CIO for the college. The college has about 60 computers attached to its intranet network. It operates on relaxed and loosely enforced corporate policy that governs the use of IT resources for personal activities like web browsing, online chatting, games and personal emails. The major focus of the management with respect to risk awareness among other areas is on virus attacks. As a result of series of events that have crippled learning activities, the management recognized the need to secure its network and removable storage resources with up to date semantic antivirus software. The main participant in this case study is the system administrator who is also responsible for the development of the enterprise corporate security requirements and security architectural design. He is familiar with the security technologies and threats presented in the scope as well as having good experience using them. All the resource units and asset classification described below are included in the enterprise policy, and mirrored in our model.

3.3 - Information Asset Classification

Identifying high level information assets that underpin the enterprise business process is a first step required in order to grasp a full understanding of the ISMS scope. After all, in order to maintain level of protection that is appropriate for corporate assets in terms of money, effort and time; we need to understand asset

grouping and asset interdependencies within the boundary of our model ISMS. Asset Classification Benchmark proposed in [13] was adopted to develop high level information asset categorization for the enterprise in our model, shown in figure 4. There are six classes/categories of assets are:

Information Asset: this category describes information about the organization that has been collected, organized, classified and stored in any form, either printed on paper, shown in films or transmitted by post. It also covers electronically stored information on computers, servers, websites, mobile phones, USBs and electronically transmitted information by any means including email, databases and fax.

Software: this category can be divided into two sub-categories: 1) Application Software which implements organization business rules, a flaw in such software can have adverse impact on the image, reputation and business of the enterprise, hence the integrity of such application is vital. 2) System Software, like Operating Systems (OS), development tools and Database Management Systems (DBMS).

Physical Assets: this category describes hardware or visible equipments on which information can be manipulated; it include: a) Communication Equipments, including fixed and mobile telephones, fax machines, routers, EPABXs, modems est. b) Computer Equipments including desktops, laptops, servers, mainframe computers, PDAs, mobile phones est. c) technical Equipments, which include copper cables CAT 4 & 5 cables, fiber circuits est. d) Storage Media which include CD-ROMs, magnetic backup tapes, USB sticks, DATs est. e) fixtures and furniture.

Services: this category describes critical services on which computer systems depend. These include 1) Communication Services like Local Area Network (LAN), Wide Area Network (WAN) and value added services. 2) Computing Services like outsourced IT support and call centers. 3) Environmental Services which include general utilities like air-conditioning, lighting, power and water supplies.

People: this category describes human resources i.e. people with skill, qualification and experience that is vital to the organization.

Intangibles: this category describes organization brand image, corporate reputation and intellectual property.

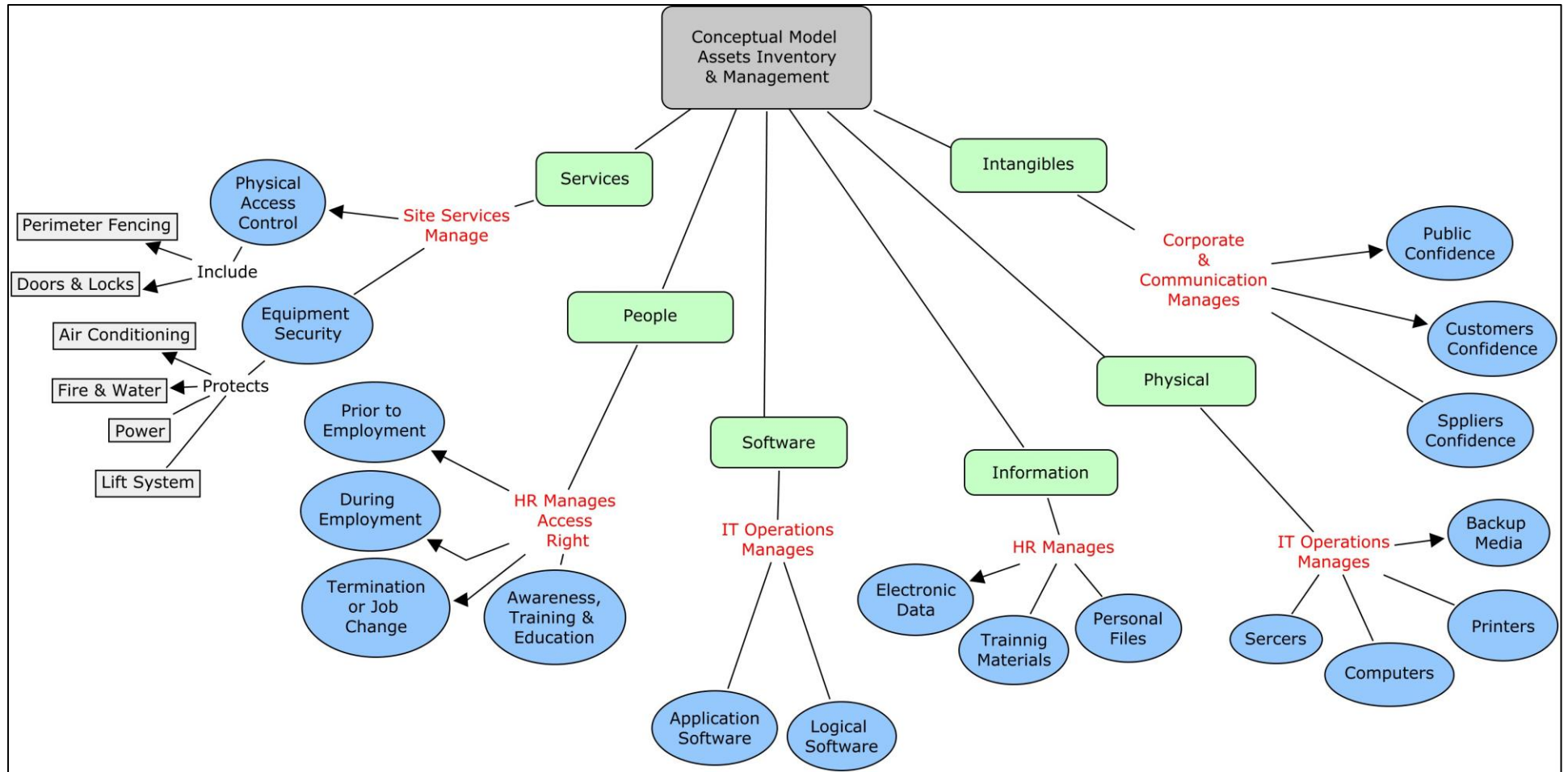


Figure 4: High level conceptual model diagram

Based on the high level description of asset classification in our model, we will briefly describe the low level information and asset interdependencies in our model as shown in figure 5. This is to allow the reader to appreciate asset evaluation and risk ranking, later on in the report.

- The enterprise in our case study has local ISDN which is connected to the local ISP provider. It uses fixed and mobile telephone networks for operational purposes. The fixed networks are comprised of series of multiple local access networks and are linked together through switches and hubs.
- Lighting Systems: the lighting system is connected to the central unit and it uses automated sensors, motion detectors and touch switches in different rooms and hallways.
- Intrusion Detection System: burglar alarms and physical locks are used throughout the premise. The main entrance is also secured with PIN access control system.
- Storage Devices: physical file cabinets and electronic storage systems are in use.
- Firewall: the internet gateway is protected by a corporate firewall.
- Servers: various services like email, student information and course material databases run on the server.
- Applications: various applications critical to teaching and financial accountings are in use e.g. Sage, MS Office suite est.
- Heat-Ventilation-Air condition-Cooling System: centralized heating and cooling systems are in use.
- Fire protection system in use is interfaced with other automated systems like security lock release under alarm conditions. Basically, the fire alarm system takes full advantage of other infrastructure systems through facility integration; for instance, HVAC system is integrated with fire alarms to automate the opening of exhaust dampers, shutting outdoor air and damping the fire floor if there is fire on the floor of the building.
- Security Monitoring and Access Control Systems: there are CCTVs within the building and around the perimeter protection to monitor activities of security concern.
- Lift and Transportation System: the lift system operates over two floors and it is manually controlled.

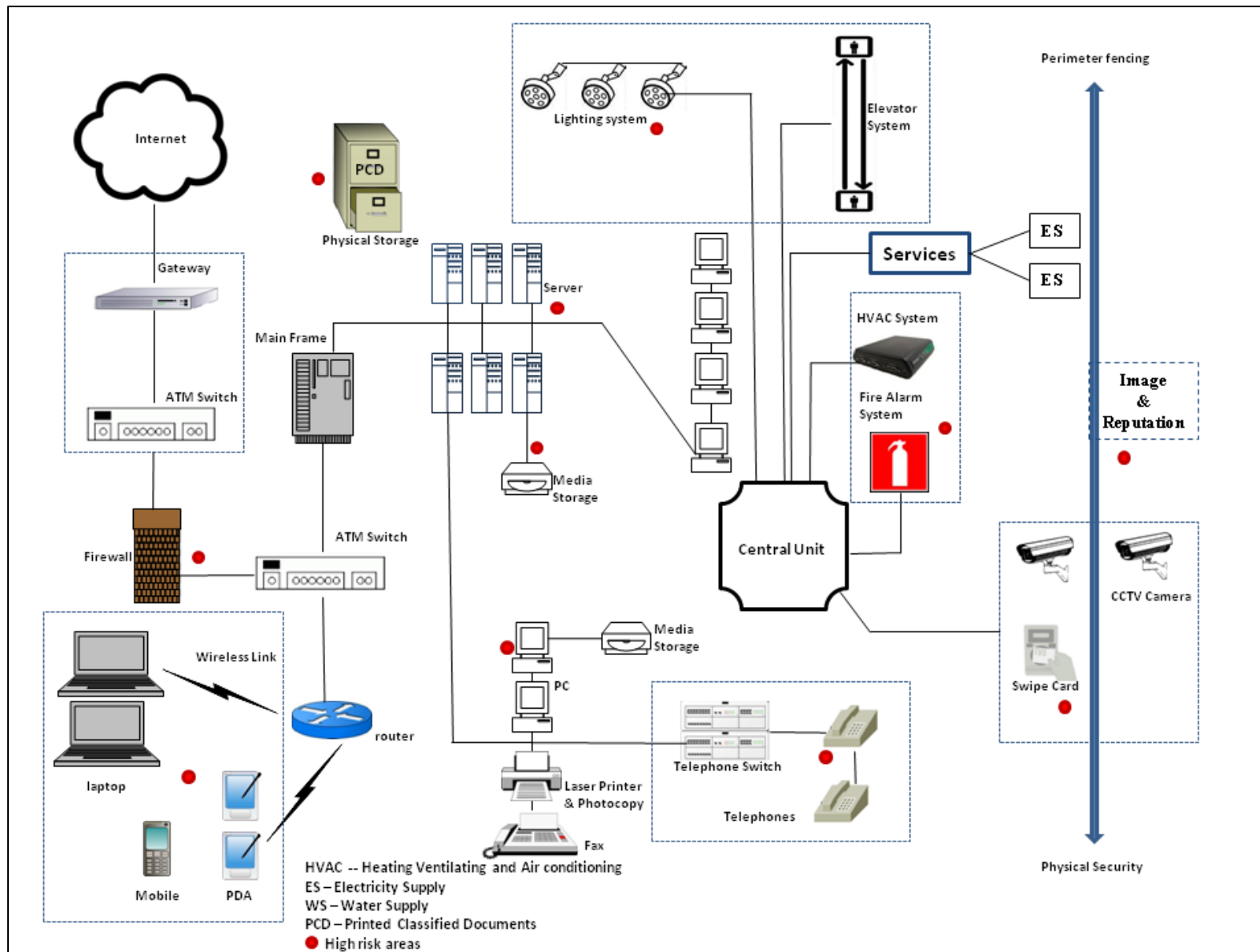


Figure 5: Low level conceptual model diagram

3.4 - Inventory of major Information Asset

This section presents different types of asset and asset group in our model, it can be seen as decomposing the asset classification described in section 3.3. The asset inventory shown in table 4 also lists the departments responsible for each asset (asset owners) and associated asset threats. The reader will need to refer to the catalogue of threats in table 5 in order to understand how threat reference numbers are mapped to each asset in our model. The catalogue of threats was compiled as proposed in [28] but through the process of the interview conducted, some threats were added or removed as appropriate to fit the requirements of our model.

Asset Group	Asset	Threats	Responsibility
Information	Personnel Files	1.16, 1.26, 1.28, 1.31, 1.35, 1.36, 1.39, 1.41, 1.47, 1.48	HR
	Bank Statements	1.16, 1.26, 1.28, 1.31, 1.35, 1.36, 1.39, 1.41, 1.47, 1.48	Finance
	Correspondence	1.12, 1.16, 1.26, 1.28, 1.31, 1.35, 1.36, 1.39, 1.41, 1.47, 1.48	HR
	Financial Statements	1.16, 1.26, 1.28, 1.31, 1.35, 1.36, 1.39, 1.41, 1.47, 1.48	Finance
	Training Materials	1.16, 1.26, 1.28, 1.31, 1.35, 1.36, 1.39, 1.41, 1.47, 1.48	HR
	Emails	1.9, 1.12, 1.16, 1.22, 1.28, 1.31, 1.35, 1.36, 1.17, 1.39, 1.41, 1.47, 1.48	ALL
	Electronic Data	1.16, 1.19, 1.28, 1.31, 1.35, 1.36, 1.17, 1.39, 1.41, 1.47, 1.48	ALL
Physical	Printers	1.1, 1.11, 1.14, 1.16, 1.17, 1.19, 1.25, 1.39, 1.44, 1.48	IT Operations
	Laptop Computers	1.1, 1.11, 1.16, 1.17, 1.19, 1.22, 1.25, 1.35, 1.37, 1.39, 1.44, 1.45, 1.48	IT Operations
	Desktop Computers	1.1, 1.11, 1.16, 1.17, 1.19, 1.22, 1.25, 1.35, 1.37, 1.39, 1.44, 1.45, 1.48	IT Operations
	Photocopy machines	1.1, 1.11, 1.14, 1.16, 1.17, 1.19, 1.25, 1.39, 1.44, 1.48	IT Operations
	Fax Machines	1.1, 1.11, 1.14, 1.16, 1.17, 1.19, 1.25, 1.39, 1.44, 1.48	IT Operations
	Fixed Telephones	1.1, 1.6, 1.11, 1.12, 1.14, 1.16, 1.17, 1.19, 1.25, 1.39, 1.44, 1.48	IT Operations
	Mobile Telephones	1.1, 1.6, 1.11, 1.12, 1.16, 1.17, 1.19, 1.25, 1.39, 1.44, 1.48	ALL
	PDA's	1.1, 1.11, 1.16, 1.17, 1.19, 1.22, 1.25, 1.37, 1.39, 1.44, 1.48	ALL

	Servers	1.1, 1.11, 1.14, 1.16, 1.17, 1.19, 1.22, 1.25, 1.35, 1.37, 1.39, 1.44, 1.45, 1.48	IT Operations
	Switches and Routers	1.1, 1.11, 1.14, 1.16, 1.17, 1.19, 1.37, 1.39, 1.44, 1.48	IT Operations
	Backup Media	1.1, 1.11, 1.14, 1.16, 1.17, 1.19, 1.37, 1.39, 1.44, 1.48	IT Operations
	USBs	1.1, 1.11, 1.16, 1.19, 1.37, 1.39, 1.44, 1.48	ALL
	Modems	1.1, 1.11, 1.14, 1.16, 1.17, 1.19, 1.22, 1.25, 1.35, 1.37, 1.39, 1.44, 1.45, 1.48	IT Operations
	Mainframe Computers	1.1, 1.11, 1.16, 1.17, 1.19, 1.22, 1.25, 1.35, 1.37, 1.39, 1.44, 1.45, 1.48	IT Operations
Software	Application Software	1.28, 1.37, 1.46, 1.48	IT Operations
	Logical Software	1.28, 1.37, 1.46, 1.48	IT Operations
People	People	1.18, 1.21, 1.22, 1.24, 1.31, 1.33, 1.35, 1.38, 1.39, 1.43, 1.45	HR
Services	Smoke detector	1.1, 1.3, 1.7, 1.13, 1.16, 1.18, , 1.48	Site Services
	Gas detectors	1.1, 1.3, 1.7, 1.13, 1.16, 1.18, , 1.48	Site Services
	Heating	1.1, 1.2, 1.3, 1.7, 1.9, 1.10, 1.13, 1.14, 1.16, 1.17, 1.27, 1.33, 1.34	Site Services
	Air Conditioning	1.1, 1.2, 1.3, 1.7, 1.10, 1.13, 1.14, 1.16, 1.17, 1.27, 1.33, 1.34, 1.48	Site Services
	LAN	1.3, 1.4, 1.6, 1.9, 1.12, 1.13, 1.14, 1.30, 1.40, 1.48	IT Operations
	Telephone System	1.1, 1.6, 1.11, 1.12, 1.14, 1.16, 1.17, 1.19, 1.25, 1.39, 1.44, 1.48	IT Operations
	Electricity Supply	1.3, 1.13, 1.14, 1.16,	Site Services
	Water Supply	1.1, 1.3, 1.10, 1.13, 1.15, 1.17, 1.48	Site Services
	UPSs	1.1, 1.3, 1.10, 1.13, 1.17, 1.48	IT Operations
	CCTV	1.3, 1.6, 1.13, 1.14, 1.16, 1.41, 1.48	Site Services
	Elevator	1.3, 1.6, 1.13, 1.14, 1.16, 1.40, 1.48	Site Services
Intangibles (Image & Reputation)	Public Confidence	1.3, 1.5, 1.10, 1.15, 1.18, 1.23, 1.33, 1.38, 1.39, 1.47, 1.48	Corporate & Communications
	Customers Confidence	1.3, 1.5, 1.10, 1.15, 1.18, 1.23, 1.33, 1.38, 1.39, 1.47, 1.48	Corporate & Communications
	Suppliers Confidence	1.3, 1.5, 1.10, 1.15, 1.18, 1.23, 1.33, 1.38, 1.39, 1.47, 1.48	Corporate & Communications

Table 5: Inventory of Assets

Ref	Threat	Ref	Threat
1.1	Airborne particles/dust	1.2	Air conditioning failure
1.3	Bomb Attack	1.4	Wireless communications infiltration
1.5	Cryptographic Compromise	1.6	Damage to communication lines
1.7	Deterioration of storage media	1.8	Earthquake
1.9	Eavesdropping	1.10	Environmental contamination (and other forms of natural or man-made disasters)
1.11	Extremes of temperature and humidity	1.12	Burglary
1.13	Failure of network components	1.14	Failure of power supply
1.15	Unauthorized email access	1.16	Fire
1.17	Flooding	1.18	Fraud/Embezzlement
1.19	Loss of data	1.20	Hurricane
1.21	Illegal import/export of software	1.22	Password Nabbing
1.23	Industrial action	1.24	IP Spoofing
1.25	Lightning	1.26	Logic Bomb
1.27	Unauthorized removal of equipment	1.28	Malicious software e.g. viruses, worms
1.29	Masquerading of user identity	1.30	Misrouting or rerouting of messages
1.31	Document Compromise	1.32	Unauthorized Network access
1.33	Operational support staff error	1.34	Power fluctuation
1.35	Personal computer misuse	1.36	Non-repudiation e.g. services, transactions
1.37	Software failure	1.38	Staff shortage
1.39	Theft	1.40	Traffic overloading
1.41	Transmission errors	1.42	Web page spoofing
1.43	Unauthorized use of storage media	1.44	Unauthorized use of network facilities
1.45	Use of software by unauthorized users	1.46	Use of software in an unauthorized way
1.47	User error	1.48	Willful damage

Table 6: Catalogue of threats

3.5 - Initial Risk Ranking Order

After identifying potential threats that constitute risk to the assets in our model, the next step is to rank the threats in order of importance as shown in table 7. This exercise was conducted with the system administrator who was able to identify and

select threats that constitute potential risk to the organization, and ranked the threats based on the management perception of threat exposure (relevant threats were selected from the catalogue of threats in table 6).

The ranking of risk exercise was combined with the risk assessment interview in order to understand the organization's current state of affair with respect to risk management. The questionnaire is structured to mirror general enterprise process flow. It is on this platform that we shall refine, asses and manage the organization ISMS by applying the two risk assessment methodologies discussed earlier (BS7799 and CRAMM Logic). Sample interview question form is included in appendix A, the interview questions were designed as proposed in [29], [30] and [31].

Ref	Threat	Initial Ranking
1.28	Malicious software e.g. viruses, worms	1
1.35	Personal computer misuse	2
1.37	Software failure	3
1.22	Password Nabbing	4
1.32	Unauthorized Network Access	5
1.39	Theft	6
1.47	User error	7
1.29	Masquerading of user identity	8
1.4	Wireless communications infiltration	9
1.13	Failure of network components	10
1.44	Unauthorized use of network facilities	11
1.31	Document Compromise	12
1.14	Failure of power supply	13
1.19	Loss of data	14
1.15	Unauthorized email access	15
1.6	Damage to communication lines	16
1.12	Burglary	17
1.43	Unauthorized use of storage media	18
1.24	IP Spoofing	19
1.48	Willful damage	20
1.2	Air conditioning failure	21
1.16	Fire	22
1.36	Non-repudiation e.g. services, transactions	23
1.27	Unauthorized removal of equipment	24
1.17	Flooding	25
1.18	Fraud/Embezzlement	26

Table 7: Initial risk ranking table

3.6 - Summery

In this chapter, we have been able map the assets in our case study to design our conceptual model. We have been able to understand what constitutes asset and how assets are categorized. Most importantly, we have been able to show asset grouping, interdependencies and owners (responsibilities) in our conceptual model; including the enterprise perception of risk and the ranking of threats. Through the interview process, we have been able to establish the initial risk ranking, according to the management priorities. In the next chapter, we shall carry out risk assessment of our model (smart infrastructure) based on the 26 identified initial risks.

Chapter 4

Implementation of Threat Assessment

4.1 - Introduction

All the work described so far in this thesis has been a subtle guide to this chapter where our two threat assessment methodologies are implemented. This chapter focuses on mitigating only the high risk areas identified in our model and the initial risk ranking order discussed in the last chapter. Two assumptions are of key importance here so that time is not wasted dealing with what has been covered previously and our reader can follow this report appropriately. The two risk assessment methodologies required that we start with: 1) the scope of the organization, 2) identify key asset and risks; all of these requirements have been largely addressed in section 3.2, section 3.4 and section 3.5 respectively.

4.2 - Applying BS7799-2:2002 Methodology

Based on the procedure outlined in the British Standard [21] and at section 2.5.1 of this report, this section shows how we apply BS7799-2 control subject to mitigate the risks shown in the initial risk ranking order on table 7. The aim of applying BS7799 methodology is to mitigate those risks either by avoidance (A), detection & recovery (D), reduction of threat (R), transfer (T), reduction of vulnerability (V). Since Standards only provide outlines of what should be achieved rather than showing how things should be done, we will assume that the technologies chosen to accomplish the control strategies in the standards are appropriate for our expected outcomes/results.

Table 8 shows how each risk is addressed by applying the appropriate clause and control object of BS7799-2. For each risk identified on the initial risk ranking table, the control subject is mapped with the strategy use to mitigate the risk, i.e. the actions taken; technology or policy wise as well as values showing risk control expected outcomes. Expected outcome for each strategy depends on individual organization risk acceptance level, rather than the risk the strategy mitigates. Based on the interview conducted in our case study, the expected outcomes shown on table 8 were considered appropriate for the college.

After applying selected BS7799 control strategies, we are required to adhere to the PCDA model cycle of activities by documenting, reinforcing and improving the enterprise security with time. By applying these control strategies, we will assume that the effectiveness of the applied controls is always checked. If there is any significant change in the scope of the enterprise, effectiveness of the controls can change as well, and the process has to be repeated.

Risk	BS7799-2:2002 Clause	BS7799-2:2002 Control Subject	Strategy	Expected Outcome
Malicious software e.g. viruses, worms	A.8.3.1	<i>Controls against malicious software</i>	<i>Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.</i>	A, R
Personal computer misuse	A.12.1.5	<i>Prevention of misuse of information processing facilities</i>	<i>Management shall authorize the use of information processing facilities and controls shall be applied to prevent the misuse of such facilities.</i>	A
Software failure	A.6.3.3	<i>Reporting software malfunctions</i>	<i>Procedures shall be established for reporting software malfunctions.</i>	D, R, V
Password Nabbing	A.9.3.1	<i>Password use</i>	<i>Users shall be required to follow good security practices in the selection and use of passwords.</i>	A
Unauthorized Network Access	A.9.4.9	<i>Security of network services</i>	<i>A clear description of the security attributes of all network services used by the organization shall be provided.</i>	A, R
Theft	A.7.1.3	<i>Securing offices, rooms and facilities</i>	<i>Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.</i>	A
User error	A.10.2.1	<i>Input data validation</i>	<i>Data input to application systems shall be validated to ensure that it is correct and appropriate.</i>	A, R
Masquerading of user identity	A.9.5.3	<i>User identification and authentication</i>	<i>All users shall have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual. A suitable authentication technique shall be chosen to substantiate the claimed identity of a user.</i>	A, R, V

Wireless communications infiltration	A.9.8.1	<i>Mobile computing</i>	<i>A formal policy shall be in place and appropriate controls shall be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments.</i>	A, R, V
Failure of network components	A.8.4.3	<i>Fault logging</i>	<i>Faults shall be reported and corrective action taken.</i>	R, V
Unauthorized use of network facilities	A.9.4.8	<i>Network routing control</i>	<i>Shared networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.</i>	A, R, V
Document Compromise	A.12.1.4	<i>Data protection and privacy of personal information</i>	<i>Controls shall be applied to protect personal information in accordance with relevant legislation.</i>	A, R, V, D
Failure of power supply	A.7.2.2	<i>Power supplies</i>	<i>Equipment shall be protected from power failures and other electrical anomalies.</i>	A, R
Loss of data	A.8.4.1	<i>Information back-up</i>	<i>Back-up copies of essential business information and software shall be taken and tested regularly.</i>	A, R, V, D
Unauthorized email access	A.8.7.4	<i>Security of electronic mail</i>	<i>A policy for the use of electronic mail shall be developed and controls put in place to reduce security risks created by electronic mail.</i>	A, R, V
Damage to communication lines	A.7.2.3	<i>Cabling security</i>	<i>Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.</i>	A, R, V, T
Burglary	A.7.1.1	<i>Physical security perimeter</i>	<i>Organizations shall use security perimeters to protect areas that contain information processing facilities.</i>	A, R
Unauthorized use of	A.8.6.1	<i>Management of</i>	<i>The management of removable computer media, such</i>	A, R

storage media		<i>removable computer media</i>	<i>as tapes, disks, cassettes and printed reports shall be controlled.</i>	
IP Spoofing	A.9.4.3	<i>User authentication for external connections</i>	<i>Access by remote users shall be subject to authentication.</i>	A, R, V
Willful damage	A.7.2.1	<i>Equipment siting and protection</i>	<i>Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.</i>	A, R, V
Air conditioning failure	A.6.3.4	<i>Learning from incidents</i>	<i>Mechanisms shall be put in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.</i>	A
Fire	A.7.2.1	<i>Equipment siting and protection</i>	<i>Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access</i>	A, T
Non-repudiation e.g. services, transactions	A.10.3.4	<i>Non-repudiation services</i>	<i>Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event or action.</i>	A, R, V
Unauthorized removal of equipment	A.7.3.2	<i>Removal of property</i>	<i>Equipment, information or software belonging to the organization shall not be removed without authorization of the management.</i>	A, R, V, D
Flooding	A.7.2.1	<i>Equipment siting and protection</i>	<i>Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.</i>	A, R, V, D
Fraud/Embezzlement	A.6.1.3	<i>Confidentiality agreements</i>	<i>Employees shall sign a confidentiality agreement as part of their initial terms and conditions of employment.</i>	A, R

Table 8: BS7799 Controls

4.3 - Applying CRAMM Logic Methodology

Applying CRAMM logic to our model involves a 4-phase approach: the first phase is the scope i.e. information gathering and business process which has been described in section 3.2.

The second phase is to identify and prioritize the high-risk business areas and evaluate the business impact, this will be based on the initial risk ranking discussed section 3.5, table 7. Using the risk scoring matrix process described in section 2.5.2.2, we calculate the measure of risk for each threat ranked in table 7 and re-order the risks (or prioritize the risk) based on the risk scoring matrix. The reader need to recall that, likelihood of risk and severity of risk values are obtained as part of the risk assessment interview process. Table 9 Show the final ranking of threat by measure of risks, after the risk scoring process. Based on the new ranking of risk (the gross risk), we now select the risks with high scoring ration, which require immediate action. We assume that these are the risks that are clearly above the organization risk acceptance level. The reader can recall that it was explained in section 1.2 that it is not every risk that is worth the time and resources to control; it could be more economically viable to leave controlled or manageable risks if they are below organization risk acceptance level and cannot be of any significant harm.

Next in phase three, we shall apply mitigating controls or countermeasures to the 10 identified high risk areas in our model (prioritized gross risk), table 9 shows the highlighted top 10 risk area, while table 10 shows selected countermeasures and the effectiveness of each risk mitigating controls (measure of risks after implementing controls). The method of applying precise CRAMM countermeasure is a 3 step process: a) asset classes associated with countermeasures are compared to the asset classes to which individual component of an asset depends b) if a match is identified, the next step is to ascertain that recommendations of the countermeasure are sufficient enough to justify the asset measure of risk c) for each pairing of relevant threat/asset, the CRAMM software then compares the threat/asset pairing associated with the measure of risk to the maximum security level associated with each countermeasure that protects against the threat. As stated earlier, CRAMM software comes with over 3000 library of detailed countermeasures organized into over 70 logical grouping. However, since we do not have access to the CRAMM software, which could have automated the process of risk scoring and countermeasure recommendations, we had to rely on CRAMM 5.1 user guide and brainstorming for the risk mitigation controls identification process. It is important to point out here that CRAMM v5.1 user guide [32] contains detailed threat/countermeasure group table that shows which threat each countermeasure group combats.

The forth phase (in a real world situation) is to include recommendation of countermeasures in the enterprise business continuity plan (BCA), but it is not within the context of this work. It is apparent from the risk analysis with CRAMM Logic that effective measurement of ISMS is an onerous task, which requires an honest and realistic approach. There must be a balanced assessment of the likelihood and significance of threat based on recommended risk mitigating controls [33].

Ref	Risk	Initial Threat Ranking	Likelihood (Value of L) 1 - 5	Severity (Value of S) 1 - 15	Measure of Risk (L * S)	Risk Classification	Final Threat Ranking
1.35	Personal computer misuse	2	5	10	50	High Risk	1
1.47	User error	7	3	15	45	High Risk	2
1.28	Malicious software e.g. viruses, worms	1	4	10	40	High Risk	3
1.16	Fire	22	3	10	30	Moderate Risk	4
1.44	Unauthorized use of network facilities	11	3	10	30	Moderate Risk	5
1.32	Unauthorized Network Access	5	3	10	30	Moderate Risk	6
1.37	Software failure	3	2	15	30	Moderate Risk	7
1.19	Loss of data	13	2	10	20	Moderate Risk	8
1.22	Password Nabbing	4	2	10	20	Moderate Risk	9
1.27	Unauthorized removal of equipment	24	3	5	15	Moderate Risk	10
1.12	Burglary	17	2	5	10	Low Risk	11
1.39	Theft	6	2	5	10	Low Risk	12
1.29	Masquerading of user identity	8	1	10	10	Low Risk	13
1.24	IP Spoofing	19	2	5	10	Low Risk	14
1.31	Document Compromise	12	1	10	10	Low Risk	15
1.15	Unauthorized email access	15	2	5	10	Low Risk	16
1.48	Willful damage	20	2	5	10	Low Risk	17
1.4	Wireless communications infiltration	9	1	10	10	Low Risk	18
1.36	Non-repudiation e.g. services, transact	23	3	2	6	Low Risk	19
1.2	Air conditioning failure	21	1	5	5	Low Risk	20
1.18	Fraud/Embezzlement	26	1	5	5	Low Risk	21
1.43	Unauthorized use of storage media	18	2	2	4	Very Low Risk	22
1.6	Damage to communication lines	16	2	2	4	Very Low Risk	23
1.14	Failure of power supply	13	2	2	4	Very Low Risk	24
1.13	Failure of network components	10	1	2	2	Very Low Risk	25
1.18	Flood	25	1	2	2	Very Low Risk	26

Table 9: Measure of risk and final threat ranking

Ref	Risk	Countermeasures	Pre-Control implementation (Likelihood 1-5)	Post-Control implementation (Likelihood 1-5)	Post-Control implementation (Severity 1-15)	Measure of Risk (L * S)	Risk Classification
1.35	Personal computer misuse	Identification and Authentication Logical Access Control System Administration Controls Security Education and Training Security Policy Compliance Checks	5	3	10	30	Moderate Risk
1.47	User error	Logical Access Control User Control Application Input/output Controls Back-up of Data	3	2	15	30	Moderate Risk
1.28	Malicious software e.g. viruses, worms	Protection Against Malicious Software Detection of Malicious Software Removal of Malicious Software Network Access Controls Mobile Code Protection	4	3	10	30	Moderate Risk
1.16	Fire	Fire Detection Fire Evacuation Fire Prevention Suppression and Control	3	1	10	10	Low Risk

		<i>Insurance Back-up of Data</i>					
1.44	Unauthorized use of network facilities	<i>Diagnostic and Control Equipment Distribution and Termination Equipment Protecting Cabling against Physical Damage Authenticating Wireless Devices Encryption of Wireless Traffic</i>	3	1	10	10	Low Risk
1.32	Unauthorized Network Access	<i>Authenticating Wireless Devices Encryption of Wireless Traffic Application Authentication Node Authentication Remote Diagnostic Port Protection Network Connection Control Gateway/Firewall Policy and Procedures</i>	3	2	10	20	Moderate Risk
1.37	Software failure	<i>Software Integrity Software Maintenance Controls Back-up of Data</i>	2	1	15	15	Moderate Risk

1.19	Loss of data	<i>Recovery Option for Hosts</i> <i>Recovery Options for Network Services</i> <i>Back-up of Data</i> <i>Equipment Failure Protection</i> <i>Data Protection</i> <i>Management Structure</i>	2	1	10	10	Low Risk
1.22	Password Nabbing	<i>Identification of a User by Token or Biometric Devices</i> <i>Frequency of Password Change</i> <i>Workstation Identification</i> <i>User Authentication for External Connections</i> <i>Password Length</i> <i>Password Storage</i> <i>Password Generation</i>	2	1	10	10	Low Risk
1.27	Unauthorized removal of equipment	<i>Back-up of Data</i> <i>Room / Zone Physical Security</i> <i>Theft Protection</i> <i>Physical Equipment Protection</i> <i>Incident Handling</i> <i>Compliance Checks</i>	3	1	5	5	Very Low Risk

Table 10: CRAMM Controls

Chapter 5

Results and Analysis

This section discusses our findings based on the application of both risk assessment methodologies to our model.

BS7799: It can be said that relevant control subjects have been applied as specified in the Standard; input to loss of confidentiality, integrity and availability on all assets were collectively considered for each risk, rather than treating each risk based on confidentiality, integrity or availability. However, the Standard did not include any specific technology needed to apply the control subjects. We assumed that selected technology (based on management decisions) will be appropriate enough to mitigate identified risk; if found to be ineffective, then the process is repeated.

CRAMM: by applying CRAMM Logic, we can see the efficiency and measurability of risk mitigating controls from the differences in gross risk and net risk maps shown in figure 6 and figure 8 respectively. We had to consider some important metrics i.e. measure of risk before and after applying countermeasures; based on this information, we will be able to create a net risk map showing the net risk exposure for the organization [34]. It can be seen from the risk management chart shown in figure 7, that there is a considerable drop in the likelihood of each instance of risk after applying controls to mitigate the risk. We also assumed that after applying controls to each risk, it is not possible to measure any considerable change in the significance of each risk, hence the metric for risk significance is constant. Any change in the metric of likelihood of risk, affects the overall measure of risk for that particular instance of risk.

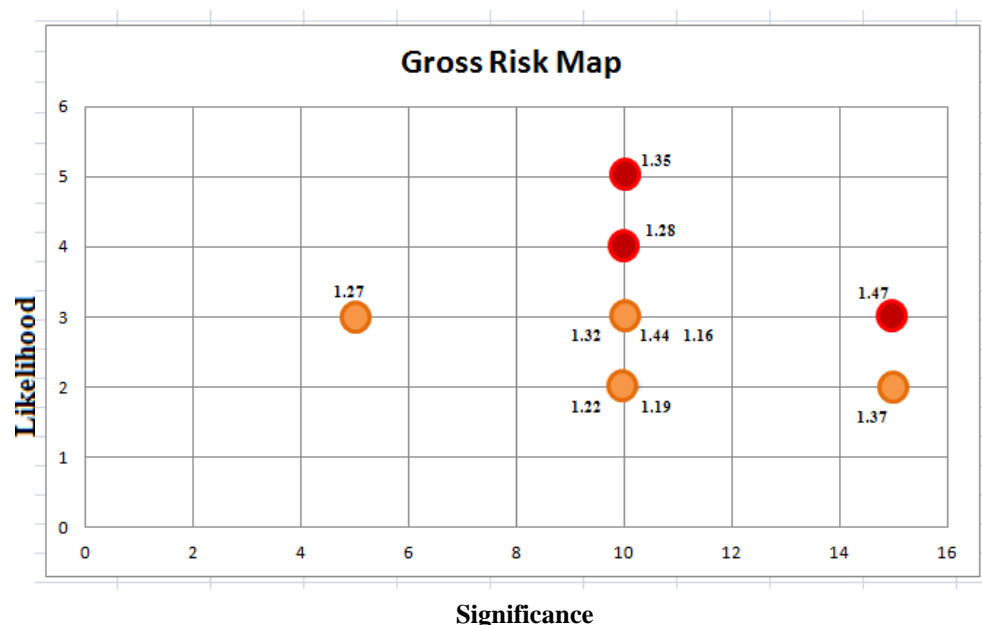


Figure 6: Gross Risk Map

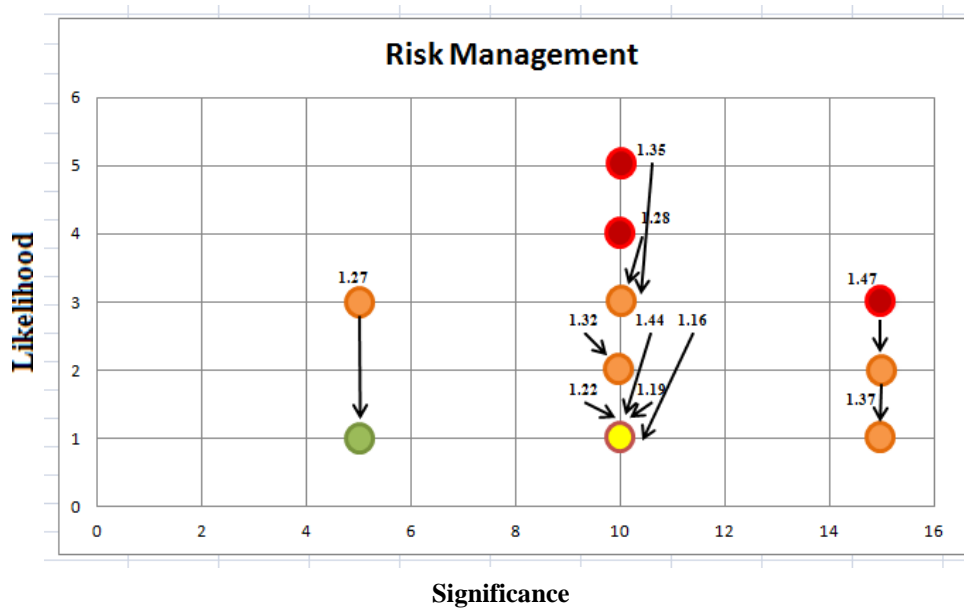


Figure 7: Risk Management

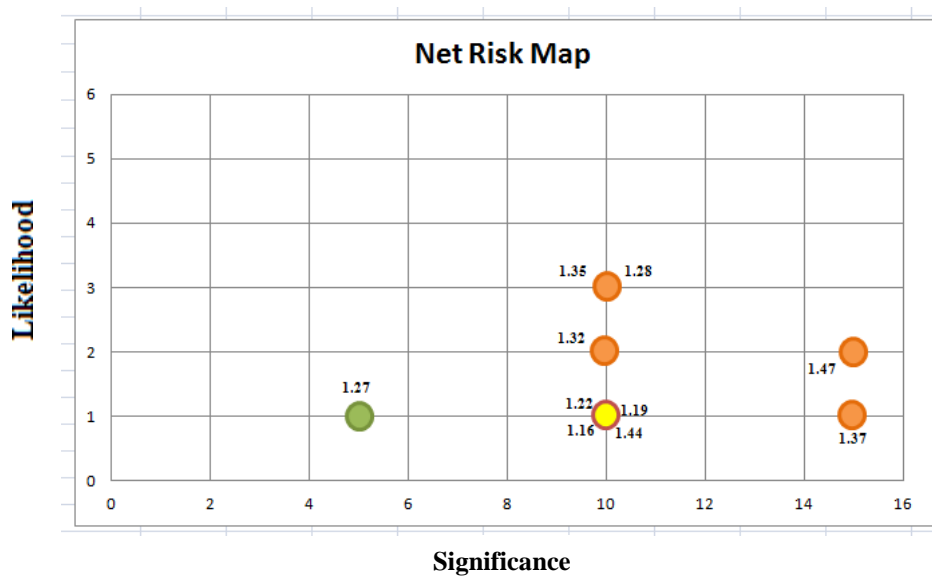


Figure 8: Net Risk Map

After the implementation of CRAMM Logic risk mitigating controls, the total percentage of risks classified as 'High Risk', based on the measure of risk was reduced by 30%, this represents a drop from 30% in the pre-implementation stage to 0% in the post implementation stage. Similarly, the total percentage of risks classified as 'Moderate Risk' was also reduced by 20%, this represents a drop from 70% in the pre-implementation stage to 50% in the post implementation stage. However, there was a 50% increase in the lower categories of risk (i.e. 'Low Risk' and

'Very Low Risk'), which were not present at all in the selected gross risks before applying risk countermeasures. This represents 40% and 10% of risks classified as 'Low Risk' and 'Very Low Risk' respectively. See the pre-implementation and post-implementation charts shown in figure 9 and figure 10 respectively. It was considered that severity of risk either before or after countermeasures remain unchanged, since any significant improvement to the likelihood of risk results in a more acceptable gross or residual risk.

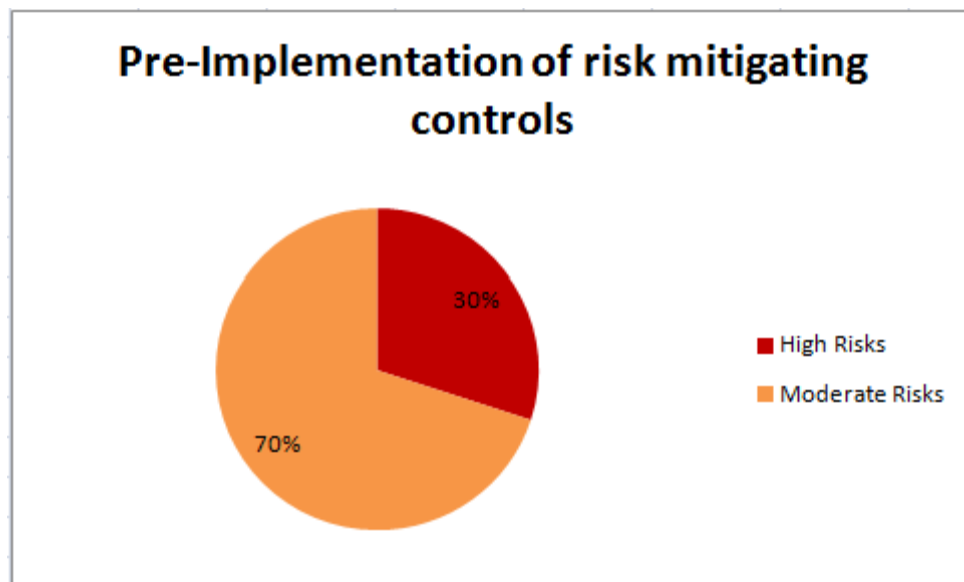


Figure 9: Pre mitigation risk ratio

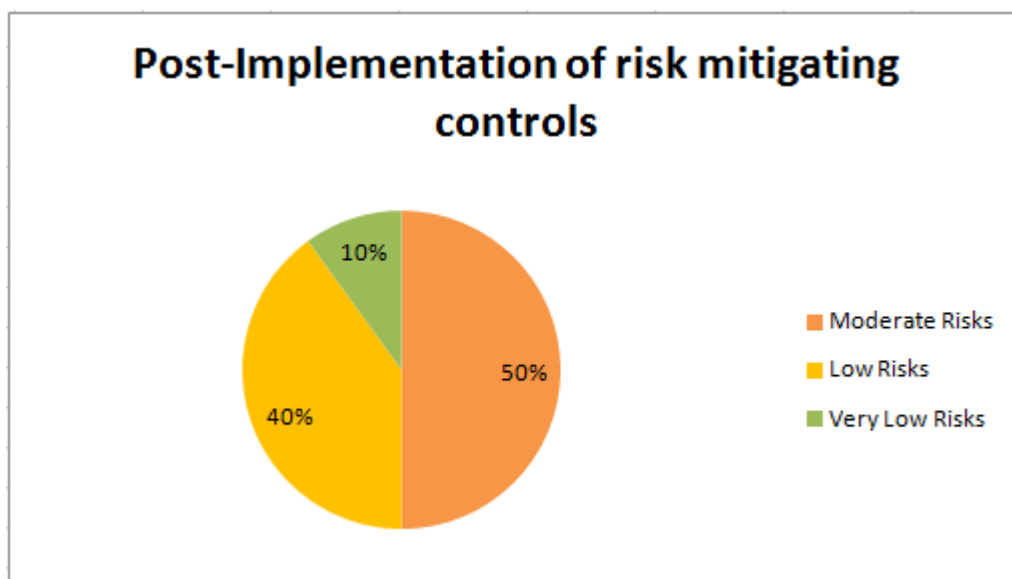


Figure 10: Post mitigation risk ratio

Chapter 6

Conclusion and Discussion

Generally speaking, risk is inevitable in any organization and to a larger extent; risk is a constant feature of any business process. However only manageable risk should be allowed and this can only be measured through risk analysis. Risk analysis and management provide organizations with a clearer picture of the impact of risk and the cost of avoiding such risk. It prevents imbalance in the amount of time and resources expended on avoiding risks of minor potential impact or ignoring risks all together in the hope that they never happen.

Arguably, the most significant potential impact to organizations would be the ability to measure the effectiveness of selected controls in BS7799. Achieving compliance with security Standard BS7799 is a substantially daunting task and operationally intensive process. It is clear from the scope of the conceptual model we worked on that, establishing the current compliance position of every information system within the scope is a painstaking process; it is actually much harder if the same approach is extended to a larger organization. Again, application of security Standard is too generic, since Standards are designed to be applicable to any organization irrespective of sizes, type and nature of operation or business.

BS7799 is a risk management methodology that produces relative result without any relationship for comparing the results; it is basically geared towards ranking of risks. The metric (or measurement) with regards to the BS7799 Standard is just to ascertain whether an organization is compliant with a Standard or an organization meets the specifications defined in a Standard. A BS7799 Standard is not necessarily concerned about the security of organization asset in the same sense as CRAMM assessment tool. The Standard is simply providing broad guidelines, for instance, encryption of portable devices – However, whether the encryption is successful or not is not really addressed. A device may be encrypted to fulfill the requirement of the guidelines by using lower key length encryption like '00000000', which may be broken easily with the simplest form of brute force attack; or in the case of password, the same password may be used across all the devices, which implies that breaking the security scheme on one device is as good as having access to the rest of the devices. The bottom line is that, BS7799 does not account for the scale of security controls and it is difficult to measure the effectiveness of security guidelines in the Standard.

Even more, in situations where there is available expertise to implement the best technology in line with BS7799 security controls and as appropriate for the right platform with the best security principle, problem still exists because such technology is not embedded in Standards (which cannot be) as a result of changes in technology over the years. Standards are meant to be something that is enduring but as technology changes, the guideline used to encrypt all the devices will still be the

same (since guidelines are not review at the same rate of technology change) whether what is used is Triple Des, AES or simply applying Higher key sizes.

Risk assessment tools on the other hand have the tendency to be tailored to the security and applicable regulatory requirement of each organization. Based on the analysis of our results, the most efficient and capital effective approach to achieving compliance is through a database software product, in our case; CRAMM. It became quickly obvious that achieving full compliance can be realized with minimum pain and simplified assessment process. It is possible to quickly identify areas of risk and resources required to mitigate the risks as well as providing a strong business case to justify and maximize the effectiveness of expenditure in information security. CRAMM takes into account the peculiarity of each organization security requirement and provide appropriate countermeasure to mitigate the risk. CRAMM, unlike BS7799, produces results that are both measureable and comparable. It provides a calculation-based approach to comparing how much greater one risk is over the other.

More often there are usually appreciable levels of security controls already adopted by most organizations like good physical security or anti-virus procedures. However, when the probe on justifying selected controls or how the risk such controls mitigate is being measured, then we hit the bricks. In this current era of escalating identity fraud, corporate scandal and IT costs; the driver behind risk management should transcend beyond identification and implementation of controls to mitigate risks but it should also be about the measurement of each control, relative to risks. After all, if controls cannot be measured, how possible is it to demonstrate that any improvement has been made or the controls are working effectively.

One key and important recommendation of this report is that; even if the organization modeled in this project already holds certification to BS7799 or ISO 27001, it is suggested that proceedings should be commenced on establishing a clearly defined set of security control measurements.

Chapter 7

Future Work

The risk assessment procedure has been completed in line with the objectives set out at the beginning of this project; however, due to unavailability of some specific resources, time constraints, supervisor's advice and the interim report feedback, there have been few modifications to the project objectives. Outlined below are some of the areas that can be included as part of future work for this project:

- Develop a larger conceptual model: the conceptual model used for this work is a bit narrow. It would be more interesting to see a complex model which can reflect a more in-depth IT infrastructure and information systems.
- Security Management Standards: the Standard considered for this work is BS7799, but as stated in the report, there are more that can be used. As part of the future work for this project, it would be better if more information security Standards are used or compared as part of requirement guidelines to secure our model.
- Risk assessment tools: there are also a lot more software based risk assessment tools other than CRAMM, as part of the future work, more than one software tool could be used for risk assessment of our model. Likewise, it would be interesting to see the output of CRAMM automated process rather than relying on calculations by hand (CRAMM Logic).
- Case Study: as part of future work, it would be nice if the risk assessment can actually be carried out on the enterprise used as a case study. In addition, the work can eliminate unsuitable methodologies and propose recommendation to organizations facing the daunting task of determining appropriate methodology.

References

- [1] Eloff, J. H. P., Labuschagne, L. and Badenhorst, K. P. A Comparative Framework for Risk Analysis Methods. *Computer Security*, 12, 6 1993), 597-603.
- [2] Rossouw von, S. Information Security Management (3): the Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security*, 6, 5 1998), 224-225.
- [3] Corporation, L. Regulatory Compliance and Critical System Protection: The Role of Mission-Critical Power and Cooling in Data Integrity and Availability. *Emerson Network Power*2005), 1-20.
- [4] Kissel, R. Glossary of information Security Terms. National Institute of Standard and Technology. NIST IR 7298 Revision 1, 2011), 4-211.
- [5] Geric, S. and Hutinski, Z. Information System Security Threats Classifications. *Journal of information and organizational sciences*, Volume 31, Number 1 (2007)
- [6] Alhabeeb, M., Almuhaideb, A., Dung, P. and Srinivasan B. Information Security Threats Classification Pyramid. *IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*, 2010.
- [7] Bonnette, A. C. Assessing Threats to Information Security in Financial Institutions. *SANS Institute InfoSec Reading Room*2003).
- [8] Lihong, Z., Ana, V. and Miguel, N. Supporting decision making in risk management through an evidence-based information systems project risk checklist. *Information Management & Computer Security*, 16, 2 2008), 166-186.
- [9] Elky, S. An Introduction to Information System Risk Management. *SANS Institute InfoSec Reading Room*2006).
- [10] deRu, W. G. and Eloff, J. H. P. Risk analysis modelling with the use of fuzzy logic. *Comput Secur*, 15, 3 1996), 239-248.
- [11] Straub, D. W. and Welke, R. J. Coping with systems risk: security planning models for management decision making. *MIS Q.*, 22, 4 1998), 441-469.
- [12] ASYCUNDA, Risk Management. UNCTAD 2000 [online], available at www.asycuda.org/slideshows/risk.ppt [accessed on] 10/August/2011
- [13] Calder, A. and GWatkins, S. Information Security Risk Management for ISO270001-270002, IT Governance Publishing, Cambridgeshire 2010.
- [14] General Accounting Office (GOA). Information Security Risk Assessment - Practices of Leading Organizations: A Supplement to GAO's May 1998 Executive Guide on Information Security Management. GAO/AIMD-00-33) 1999

- [15] Carey, P. Data Protection: A Practical Guide to UK and EU Law, Third Edition, Oxford University Press, 2009.
- [16] Vassilis, T. and Theodore, T. From risk analysis to effective security management: towards an automated approach. Information Management & Computer Security, 12, 1 (2004), 91-101.
- [17] Information Technology Governance, Information Security and ISO27001 – An Introduction. IT Governance Ltd 1.1) 2006.
- [18] CRAMM 5 Case Study Datasheet. Risk Analysis Consultants) 2010.
- [19] Business Link, Understanding BS7799. Department of Trade and Industry [online], available at <http://www.connectingsomerset.co.uk/tips/e-business/Understanding%20BS%207799.pdf> [accessed on] 3/August/2011.
- [20] Siponen, M. and Willison, R. Information Security Management Standards: Problems and solutions. Information & Management, 46, 5 (2009), 267-270.
- [21] British Standard 7799 Part 2 (September 2002), Information Technology – Specification for Information Security Management System, BSI, London.
- [22] Spinellis, D., Kokolakis, S. and Gritzalis, S. Security requirements, risks and recommendations for small enterprise and home-office environments. Information Management & Computer Security, 7, 3 (1999), 121-128.
- [23] Siemens Enterprise. CRAMM v5.1 Information Security Toolkit (Datasheet). 2005.
- [24] Yazar, Z. A Qualitative Risk Analysis and Management Tool - CRAMM. SANS Institute InfoSec Reading Room (2002), 1-15.
- [25] Siemens Enterprise. The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures. Siemens Enterprise, City, 2005.
- [26] West Essex PCT -Risk Assessment Procedure and Guideline Version 2, February 2010
- [27] Humphreys, E. Information Security Management Standards: Compliance, governance and risk management. Information Security Technical Report, 13, 4 (2008), 247-255.
- [28] Risk Assessment Manual v1.4 [online], available at <https://www.igt.connectingforhealth.nhs.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf> [accessed on] 22/August/2011.
- [29] PCI Security Standards Council LLC. Self-Assessment Questionnaire D and Attestation of Compliance, v2.0) 2010.

[30] Open Information Systems Security Group. Information Systems Security Assessment Framework (ISSAF) Draft 0.2) 2006.

[31] AIG Net Advantage Modular Edition. Information Security and Privacy Self-Assessment, Version 4.1. AIG Executive Liability) 2009.

[32] CRAMM v5.1 User's Guide [online], available at
http://dtps.unipi.gr/files/notes/2007-2008/eksamino_5/politikes_kai_diaxeirish_asfaleias/egxeiridio_cramm.pdf
[accessed on] 2/September/2011

[33] Wright, S. White Paper - Measuring the Effectiveness of Security using ISO27001 Version 1.8) 2006.

[34] Lowendahl J., Antonsen M., Everbrand J. And Lidros J. A Successful Tool to Create Positive Change: Results of an I.T Risk Assessment and Benchmark. Transcendent Group (2005).

Appendix A

Questionnaire

Risk Assessment Questionnaire				
Ref		Y/Comments	N/Comments	N/A
1	Do you have information retention policy			
2	Do you have security awareness and training program in place			
3	Do you have password management policy in place			
4	Do you have access control policy to sensitive resources			
5	Do you secure connections to the college network from wireless/mobile devices			
6	Do you have established firewall and router configuration standards			
7	Do you outsource any security management programme to a third party			
8	Do you have virus protection programme in place			
9	Do you maintain a policy that addresses information security for all personnel			
10	Do you have information security and privacy policy			
11	Do you have physical security policy in place			
12	Do you have policies in place to comply with privacy requirement of your standard regulatory body			