INFORMATION SECURITY CHALLENGES IN RELATION TO ENTERPRISE SECURITY POLICIES IN THE FINANCIAL SECTOR IN SRI LANKA

BY

B.A.R.L. JAYAWARDANA

(2009/MISM/16)

submitted in accordance with the requirements for the degree of

MASTERS IN INFORMATION SYSTEMS MANAGEMENT

at the

UNIVERSITY OF COLOMBO

SUPERVISOR: DR. KAPILA PONNAMPERUMA

NOVEMBER 2011

DECLARATION

I certify that this Dissertation does not incorporate without acknowledgement any material previously submitted for the Degree or Diploma in any University, and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text

Date: ....

B.A.R.L. Jayawardana

The undersigned, have supervised the dissertation entitled **Information Security Challenges in relation to Enterprise Security Policies in the Financial sector in Sri Lanka** presented by B.A.R.L. Jayawardana, a candidate for the degree of Masters in Information Systems Management, and hereby certify that, in my opinion, it is worthy of submission for examination.

Date: ....

Dr. Kapila Ponnamperuma
Supervisor

While mathematics is logical; people are erratic, capricious and barely comprehensive

Schneier (2000, Preface)

Contents

List of Figures

Acknowledgement

This thesis was written for the Masters Degree in Information Systems Management, at the 'Faculty of Graduate Studies', 'University of Colombo', Sri Lanka. It is my pleasure to take the opportunity to express my thanks to the people who helped me during the writing process of the thesis.

Firstly, my thanks go to the supervisor, Dr. Kapila Ponnamperuma, for his effectual supervision, fruitful discussions, constructive suggestions and valuable comments.

Then I would like to extend my sincere gratitude to Dr. Chaminda C. Jayasundara, the coordinator of MISM, for his inspiring encouragement, illuminating instructions and various kinds of help. Besides, I am grateful to Prof. K.A.P. Siddhisena and Mr. Rushan Abegunawardene for their kind help in many aspects.

A very special thank goes to the gentlemen who helped me from the selected banks during my interview process by spending their valuable time during busy hours.

Finally, I would like to thank my family members and colleagues for giving me the opportunity to complete my studies and make this thesis a success.

B.A.R.L. Jayawardana

Abstract

Information is becoming the lifeblood of the twenty-first century enterprises. Most of the top management teams have already identified that information should be treated as other assets. However, some are still not much aware about the value of corporate information. Nevertheless, members of these two groups have still not found a comfortable solution to protect information and make their lives easy. Technology is developing rapidly, parallel to that information security solutions are also becoming cutting-edge. However, unfortunately technology advancements are also with accessible to the hands of hackers and other vulnerable people. So the top management or information security managers cannot successfully complete their job only by providing cutting edge solution in place. Information security is very crucial nowadays. Information security alone is not a technical exercise anymore. It's hybrid. A better information security is only when proper management blends with cutting-edge technology.

In the Sri Lanka's context, most enterprises are moving towards securing their corporate information assets. This study focuses on Information Security Challenges in relation to Enterprise Security Policies in the financial sector.

The research will be carryout on registered private commercial banks which are listed in Colombo Stock Market (Public Listed Companies) and having Fitch Rating above 'A'.

Throughout this research, the selected business entities will be checked on whether they have identified corporate information as an asset to secure, possible risks, threats and vulnerabilities for information security, measures taken to minimize shortfalls and vulnerabilities and explore the obstructions to improve information security. These areas will be check by a framework developed based on ISO 27001:2005 standard for Information Security Management System (ISMS)

Chapter 1 Introduction

The consent for enterprise IT relies on how it facilitates transformation of the business or share in its ultimate goals. By all means, organizations must fully embrace IT not only as a way to achieve greater performance and reduce costs, but also differentiate themselves by offering customers a diverse range of compelling and increasingly sophisticated services. New innovative technologies are emerging and it is important to successfully integrate them to achieve limitations, which ultimately increase the speed of the business and keep abreast with the rapidly moving world which gains ultimate competitive advantage among rivals.

While the business is running on information technology, it generates a huge amount of information, which relates to the business. Most of the information contains critical business information that is very confidential and sensitive. Getting this kind of information to competitor's or unsafe hands, would cause huge damage to the business.

If information does not carry any value, no one will care about it and protection of information treats and security will not be in the scene. But, information plays a crucial role in today's organizations. It is seen as a valuable component, but few organizations have actually realized the full potential of their information assets. Information located in different parts of the organizations is often believed to be of enormous value, although they actually don’t have any measurable financial attributes. Knowing the actual value of the information assets within organizations can lead to a better understanding of the more valuable and less valuable information. If a company does not know the value of the information and the other assets they are trying to protect, they do not know how much money and time should be spent on protecting them.

No matter the size of an enterprise, whether it is a public or private enterprise or whether it is a single or multicounty enterprise, there is a need for an information security in the organization.

Security in enterprise information systems is also not simply a matter of technology and cannot be addressed satisfactorily with hardware and software alone. It is also a matter of managing people, establishing and enforcing strong accurate policies, implementing procedures that strengthen security, and periodically reviewing the effectiveness of the security architecture and making necessary changes. The provision of security in any enterprise must also be customized to that particular organization. While the principles of information security and common understanding in the IT field are important, the actual application of such principles depend largely on a number of factors that often vary from enterprise to enterprise (e.g., confidentiality needs for data, customers, access requirements, volatility of data value, etc).

The responsible personnel of the organization for enterprise security must balance the need for security against the need for access to their systems. The other important factor is the cost of the security measures. Once everything is in place, the overall strength of the security architecture is constructed.

For an organization to successfully secure, protect trusted information system, it is necessary to have information systems security, with the required tools and direction.

Through the evaluation of information system security, the fundamental principals are confidentiality, integrity and availability and primary objectives should be in the above three areas. Confidentiality is the objective that information is not disclosed to unauthorized persons, processes or devices. Integrity is the objective that supports sameness of information. Availability focuses timely, reliable access to information for authorized users. These are referred to as the CIA triad. The level of security required to accomplish these principals differs per company because their security goals and requirements may be different.

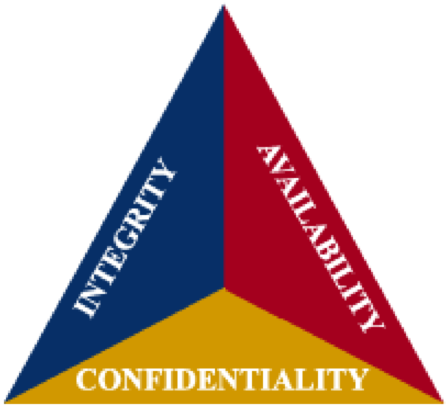


Figure 1: CIA triad

Security objectives are the core of all information system security. All information system security policies, controls, safeguards, countermeasures, and even threats, vulnerabilities and security processes can and should be considered within the framework of the security objective.

Prior to implementation or thinking about a protection system, it’s necessary to have an idea about what type of treats or attacks are possible for the targeted enterprise. The steps taken towards the protection, without having sound idea on the risks would not make much sense.

In the majority of organizations the words “threat”, “vulnerability”, “risk” and “exposure” are used to represent the same thing, even though they have different meanings and relationship to each other. It is important to understand the definition of each word, but more importantly, one should understand its relationship to the other concepts.

Vulnerability usually refers to a weakness in software, hardware, control or procedure that provide a chance for an attacker enter or accesses unauthorized resources. This could happen by even breaking or misusing a control that has been applied for safeguarding the resources. Eg. a service running on a server, unrestricted modem dial-in access, an open port on a firewall, negligent physical security that allows anyone to enter a server room, or non-enforced password management

A threat is any possible danger to information asset. It is normally defines as a vulnerability which is already identified and used against. The person who is taking the benefit of this is referred to as the threat agent. A threat agent is an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy or an employee making an unintentional mistake that could expose or destroy the integrity of confidential information.

A risk is the possibility of a threat agent taking advantage of vulnerability. A risk is the possibility and probability that a threat agent will exploit vulnerability. If a firewall has several ports open, there is a higher risk that an intruder will use one to access the network in an unauthorized method. If users are not educated on processes and procedures, there is a higher risk that an employee will make an intentional or unintentional mistake that may reveal information. If an intruder detection system is not implemented in a network, there is a higher risk that an attack will go unnoticed until it is too late. Reducing the vulnerability or the threat reduces the risk.

An exposure is an instance of being exposed to losses from a threat agent. Vulnerability can cause an organization to be exposed to possible damages. If password management is negligent and password rules are not enforced, the company can be exposed to the possibility of having users' passwords captured and used in an unauthorized manner. If a company does not have its wiring inspected and does not put proactive fire prevention steps into place, it can expose itself to potential devastating fires.

A countermeasure, or safeguard, mitigates the possible risk. A countermeasure is a software configuration, hardware, control or procedure that eliminates vulnerability or reduces the risk of a threat agent from being able to exploit a vulnerability. Countermeasures can be strong password management, a security guard, access control mechanisms within an operating system.

If a company has antivirus software and the virus signatures are not kept up-to-date, this is a vulnerability. The company is vulnerable to virus attacks. The threat is virus showing up in the environment and disrupting productivity. The possibility of a virus showing up in the environment and causing damage is the risk. If a virus creeps into the company's environment, then it has exposure. The countermeasures in this situation are to update the virus signature databases and install the virus software on all computers. Applying the right countermeasures can eliminate the vulnerability and exposures and reduce the risk. The company cannot eliminate the threat, but it can protect itself and prevent this treat agent from exploiting vulnerabilities within the environment.

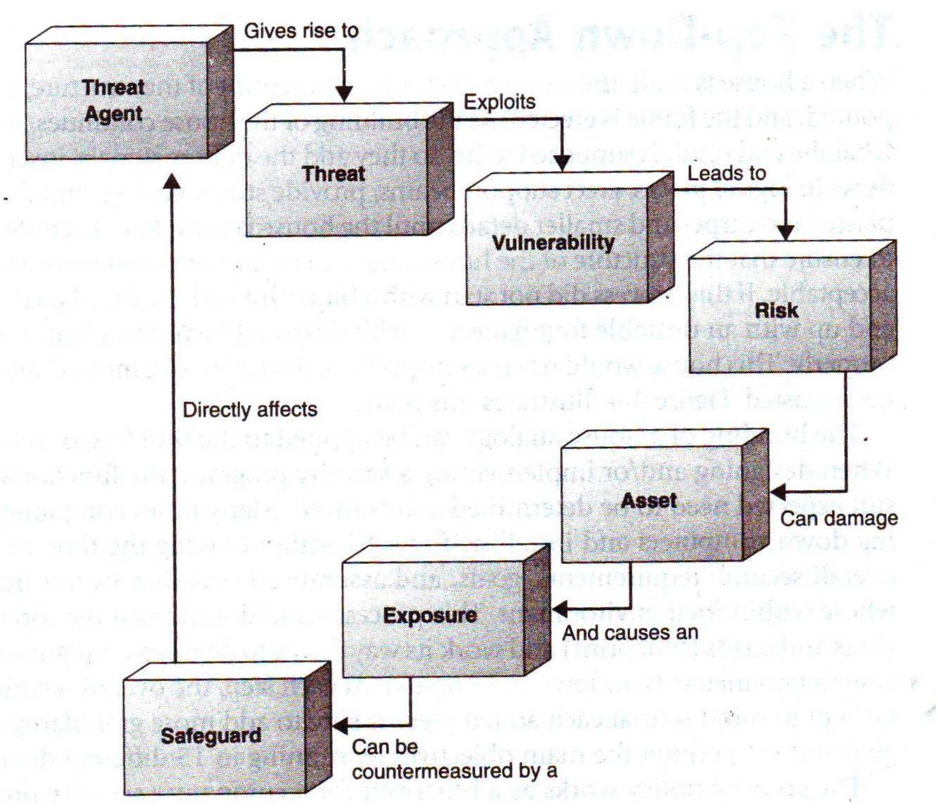


Figure 2: Relationship among the different security components.

(Harris, 2004, p.57)

1.1 Problem Statement

Though information security is a critical and high prioritized subject in other countries, in Sri Lanka it is still a developing story. In order to get the security in place there should be something to protect and to protect something it should have a considerable value. But without seeing a value, people will not invest on security. There are two main categories in this domain. The first group identify the value of the information and try to do something to protect them. The second groups do not see any value of the information and think investment for information security is useless. The information security of an organization relies on the hands of people belong to these two types. Doing nothing is critical and meanwhile doing something is also vulnerable. When attacked and information goes to unsafe hand, it cannot be undone and precautions do not make much sense. The most important thing is that these two groups do not have a clear idea what they are playing with. Sometimes it could be highly confidential personal data or it could be some financial information which is the lifeblood of an organization. Most of the cases, they are playing around with these critical information and they really do not know what type of disaster could happen? Therefore, it should be "better safe than sorry".

The aim of this research is to identify the information security challenges faced by the financial sector in Sri Lanka.

In order to gain a better understand of the information security challenges faced by financial sector of Sri Lanka, four dimensions will be discussed in the thesis. Accordingly, the following research questions are developed for this thesis:

- Whether the banks have identified information as an asset to secure?
- What possible risks, threats and vulnerabilities for information security?
- What measures taken to minimize the impact of shortfalls and vulnerabilities?
- Are there any obstructions to improve information security?

1.2 Objectives

This research attempts to:

- Identify whether the banks have identified information as an asset to secure
- Identify possible risks, threats and vulnerabilities for information security and measures taken to minimize the impact of those
- Examine whether there are any obstruction to improve information security

Chapter 2 Literature Review

In the current world, rapidly changing risks and vulnerabilities, cross-organization collaboration, e-commerce and information security has become a critical requirement of the business than ever before. There are many new and developing researches, standards, tools and technologies in place to help enterprises secure their business transactions, infrastructure and valuable information.

Unfortunately enterprises still struggle to meet the regulatory requirement, economic conditions and risk management. Many organizations still do not clearly understand the scope of information security and some hesitant to justify ROI in information security and they still see information security as a cost centre. While the true story is somewhat different and it's actually information security can be used as a good instrument to help the enterprise improve efficiency to meet their business goals and objectives. (ISACA, 2010, p.5)

Another concern in Information security is that some believe information security as purely a technical control. Though IT provides the technical backing for information security, it should not be considered as a complete solution for information security at anytime. Information security can only be guaranteed through information security policies including standards, procedures and guidelines to protect information. An enterprise should also provide guidance for information security programs and expectations of the enterprise and the way the information is to be used, shared, transmitted and destroyed. These policies and guidance should have a proper balance with the enterprise culture and the human behaviors in order to have 100% effectiveness that is expected. Many enterprises develop their policies for technology, policy, process and standards without having proper understanding on organizational culture which impacts the effectiveness of the program. Security controls that are developed without considering human behaviors are not very effective and it is difficult to gain planed benefits. Information security programs should consider non-technical areas like employees, interact of technologies in processes and most importantly organizational governance, culture and human factor and whether they support or obstruct the journey to protect the information of the organization.

It's important to create information security programs to align with the organization's goals and priorities, which bring value and controlling risks at the same time to the organization at the end of the day. But most of the information security managers fail to do so. Without having a proper framework in place it's difficult to integrate security program with the goals, objectives, strategies and activities of the business. An effective security program includes its functionality and how it works with the organization's priorities. Normally the missing part is a descriptive model for managers in other business units to consider information security for business rather than a technical subject. In every business unit information is stored, updated or retrieved. Most of the organizations use a virtual world which spread across data centres, networks, serves, applications and databases to store their business information. Corporate information is very crucial for the business and normally it's a collection of electronic information related to business transactions. And at every level there is a risk of losing or manipulating information. The problem that the enterprises are facing is that even though business managers understand the importance of securing the information they are not flexible to support security policies and guidelines.

Organizations must put their best effort to safeguards this information by implementing policies, procedures and technology. However, information security is not a straightforward topic though it is treated as a very simple thing by most of the people. In the past, boards of directors and corporate executives were also disinterested in matters pertaining to information security. This disinterest increased considering revenue-side focus and an ignorance of the costs associated with aggregated risk and actual loss. Time has changed the situation, whereby top management teams and boards are now very interested in the controls and procedures in place to prevent fraud, minimize loss and keep operations going. Their focus is now on how to make clear how they develop and roll-out internal controls for all systems related to information.

2.1 Information security and corporate governance

(ISACA, 2010, p.7) Information security is an area which is continually developing. Throughout history, the importance of information protection has been addressed in many places. Introduction of cryptography is an early example of a control created by understanding information is a valuable asset. The relatively recent businesses depend on computers to support business operations which lead to the development of technology-based information security solutions that are mainly focused on protecting the enterprise's information infrastructures from threats. While business has seen the business information as a valuable asset, at the same time it has come to transport and depend on public networks.

The current landscape is puzzled with challenges. While external issues such as rapidly changing regulatory requirements and continually shifting risks constitute primary concerns, they do not stand alone. Internal issues can prove just as tricky. For example, although security managers and business managers are working toward the same goal, they often seem to be speaking a different language. Information security managers strive to ensure that their program helps the enterprise meet its organizational goals; this can be a difficult task. However, they address specific threats, risks, controls and technologies, while business managers are focused on cost, productivity and return on investment (ROI).

(Solms, 2001), explains the strong relationship between corporate governance and information security. He has also emphasized that top management in a company has no choice but to be committed and responsible for information security, simply because by law they are committed, responsible to enforce good corporate governance of their companies. There is no doubt anymore that information security is the control to ensure the confidentiality, integrity and availability of electronic assets, and it is today an extremely important aspect in the strategic management of any company.

It is also a known fact that the important strategic role of information security is only being established in a company once senior management gives it full support and commitment. Information security has long ago moved away from being only a technical issue, and has really today become a management issue.

However, the problem is that in many companies senior management does not have enough tone and responsibility towards information security, which makes it a very challenging job for an information security officer to roll-out information security across the company.

This is mainly because in many cases senior management, especially at the Board level, view information security as a technical issue, which must be solely handled by the IT section. Without the management support, information security managers fight a very difficult, and often losing, battle in implementing and rolling out an enterprise-wide information security plan in the company.

2.2 Information assets

Information is an asset, which like any other asset owned by the organization, has significant value to the stakeholders of it. Information security is a critical component that is required to enable and ensure the availability, integrity and confidentiality of data, network and processing resources required for the organization to perform its business and operational practices.

By ISO/IEC 27001:2005 standard, asset is defined as 'anything that has value to an organization' (Calder, 2009). In many ways information assets are different from other assets. It has a unique posture among others. Threats to information assets also differ from others. It is exposed to a wide range of threats, both external and internal.

As per (Calder & Watkins, 2006) information is right at the heart of the modern organizations. Information's availability, confidanciality and integrity are directly efects to the existance of the 21st- century organization. If the organization fails to take a systematic and comprehensive approch to protect availability, confidanciality and integrity of information, the organisation is surely valnurable to a wide range of possible threats. So the danger is clear and the strategic responsibility of safegurding organization's information asset is no longer a job of only chief information officer (CIO).

The risks faced by the organizations due to lack of adequate information security systems fall under three categories: damage to operations, damage to reputation and legal damage. Damage in any of these three categories could be a severe damage to the organization, both in the short and long term.

As per the information security survey carried out by Ernst & Young in 2004, among 1,300 executives across 51 countries, only 20 percent have strongly agreed that they belive infomation security is CEO-level pririty subject. This clearly shows the people's intension on information security, which they still belive is a technical matter for the CIO and his subordinates.

Access to information from anyware, anytime is becoming a trend in the modern world. Along with this, it changes the face of business environment. It removes physical boundaries in the traditional business environement. In most of the cases there's no difference in accessible to information from home as in the normal office environment. Social networks are becoming major advertising media for corporates. No doubte these movements definitly gaining significant benefits to organizations.

However, new technology also means new risks. It's very difficult to find physical boundaries for information in today's businesses. This rising of risk levels are also noticed by many.

Ernst & Young's 2010 global information security survey report (1600 organizations across 56 countries have participated in this survey) provides evidence on how information assets are getting more valuable to corporations day by day. Out of those participants, 60 percent have agreed that new technology and new business trends increase the level of risk to information. Only 37 percent believe that risk levels remain unchanged and a very few (about 3 percent) believe risks are decreasing.

Relative to the increase of threats, corporate have increase their expenditures for information security. The same survey indicates that among the participants of the survey, 46 percent have increased their investment on information security, while 48 percent remain unchanged and 6 percent decrease their expenditure on information security.

At the same time, due to recession and various other financial difficulties faced by organizations, they have limited the financial and human resources allocated for information security. All these factors ultimately causes increase in risks and vulnerabilities to information which badly affects the corporate image in the long run.

2.3 Cost of a data breach

Data breach cost is very difficult to estimate because there can be so many effects from a data breach which make it difficult to identify all costs associated with the loss. Data breaches are very common in the modern word. Day by day it increases the number of incidents and costs and the impact attached to it.

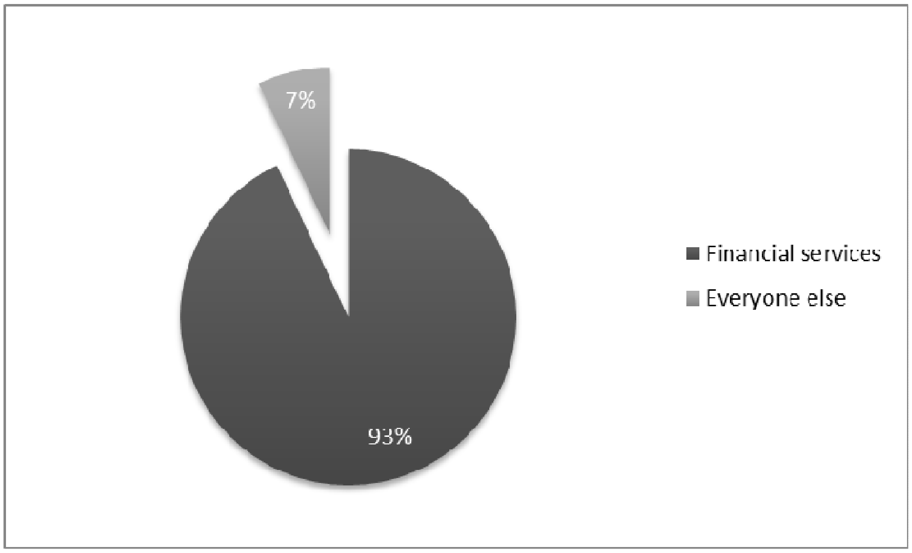


Figure 3: Industries represented by percent of records

(Verizon Business, 2009)

As identified in the Data breach investigations report-2009 by Verison Business, 93 percent of records are breached in the financial service sector. It's very clear the potential for financial sector when considering data braches.

As per the same report, it stated that the majority of breaches still occur due to basic controls that are not in place or not consistently implemented across the organization. If obvious weaknesses are left exposed, attacker will exploit them.

The graph below from http://datalossdb.org shows the increase of incidents along with time.

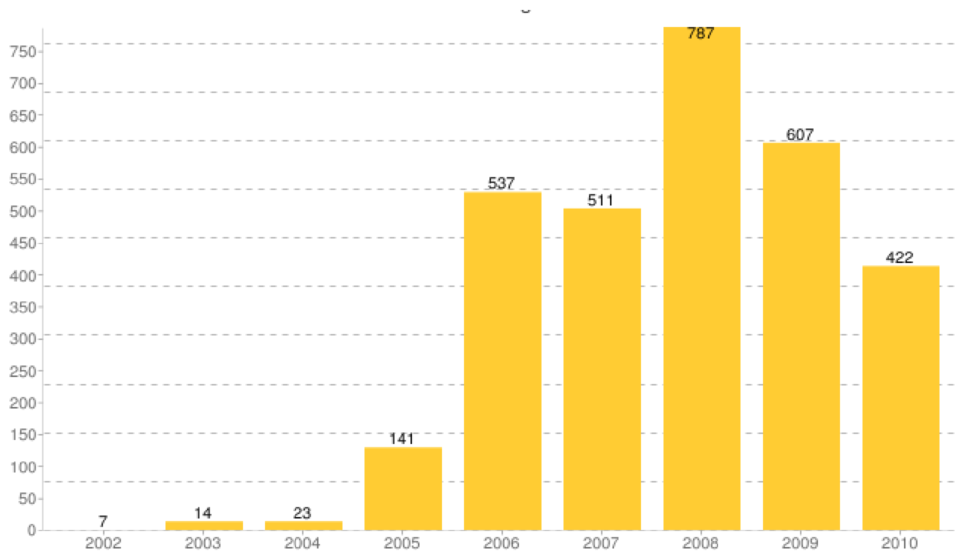


Figure 4: Incidents over Time

(OSF DataLossDB, 2011)

It's identified that at a high-level, security incidents originate from an external, internal or partner source. External threats originate from sources outside the organization. Examples include hackers, organized crime groups, and government entities, as well as environmental events such as weather and earthquakes.

Internal threats are those originating from within the organization. This includes human assets like company management, temporary and permanent employees, as well as other assets such as physical facilities and information processing systems. Most insiders are trusted to a certain degree and some employees like IT administrators have high levels of access and privilege to sensitive areas of the organization.

Partners include any third party sharing a business relationship with the organization. This value chain of partners, vendors, suppliers, contractors, and customers are known as the extended enterprise. Information exchange is the lifeblood of the extended enterprise and, for this reason, some level of trust and privilege is usually implied between business partners.

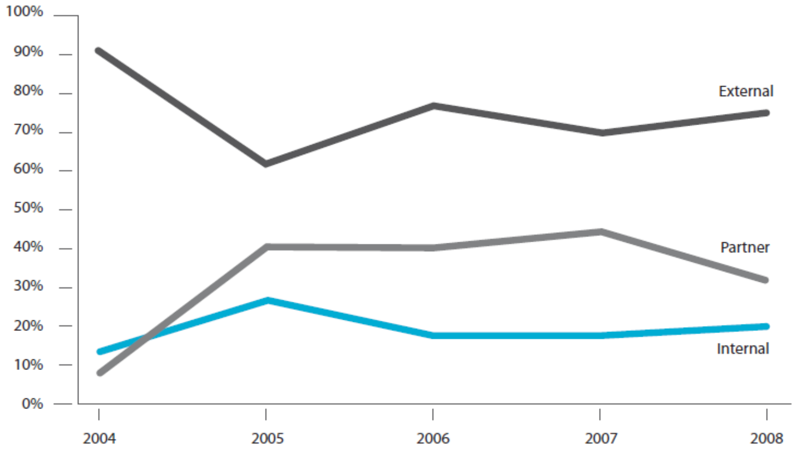


Figure 5: Breach sources over time by percent of breaches

(Verizon Business, 2009)

The majority of data breaches originated from outside sources. The statistic remains notably consistent over the five-year period of this study. Based on these results, it seems unwise to downplay the threat posed by outsiders.

Insiders, on the other hand, are behind the lowest percentage (20 percent) of breaches for four years running.

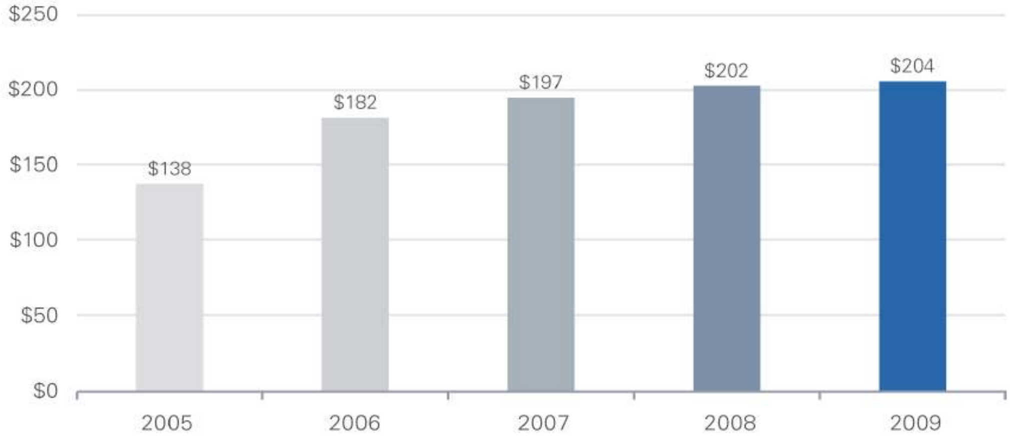


Figure 6: The rising cost of security breaches
(Ponemon Institute, 2010, p.13)

Data breaches and their assocoated costs are increasing every year. The above graph shows the variation of the cost on a per record basis. (Ponemon Institute, 2010, p.13)

2.4 Information Security Policy

Information security policy of the organization is the crucial point for setting up and conveying security requirement and sets the goals for information security practices within an organization, defining appropriate behavior and setting the stage for the security program. It's required to have a strong policy development framework to guide formulation, implementation, awareness and compliance. Top management of the organization is thoroughly responsible for setting up and enforcing a proper, well documented information security policy, including standards, procedures, guidelines and rules of use.

A comprehensive policy document addresses importance of information security in the organization. It also indicates what to be protected, possible risks and threats and how to deal with them and continues reviewing, monitoring and actions to ensure that the policies are properly applied and performed. The policy document also need to go through continues review and update process to be in line with the business needs and practices.

The roles and responsibilities of the all information systems users are also addressed in the policy document in order to ensure the protection of confidentiality, availability and integrity of information assets of the organization. The policy must mention management's objectives and expectations for information security clearly, in detail along with the implications of noncompliance.

The existence of the policy documents heavily depend on the management’s dedication and adherence to information security. Application and relevance of the policy document need to be reviewed and updated in pre-set time lapses. In most of the organizations reviewing is done once a year, while other organizations concerned about information security do it in more frequently. Failure to keep the policy up to date reflects lack of management's commitment or the failures in processes to organizational governance.

2.5 Information security standards

ISO/IEC 27001:2005 is known as the best Information Security Management Systems standard. This standard is published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). ISO/IEC 27001 was born as BS 7799 (British standard) in 1999. It was revised by BSI (British Standard Institute) in 2002, explicitly incorporating Plan-Do-Check-Act cyclic process concept, and was adopted by ISO/IEC in 2005.

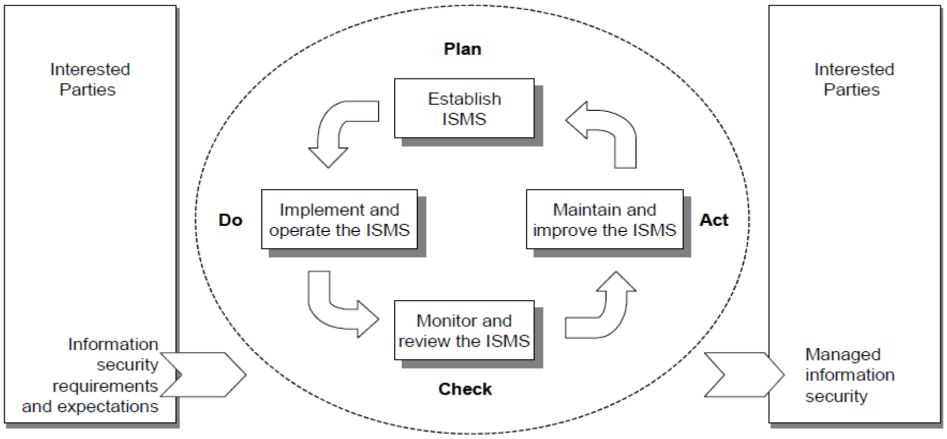

Interested Parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested Parties
Managed information security

Figure 7: PDCA Model applied to ISMS processes

(International Standard Organization, 2005)

ISO/IEC 27001 standard is getting rapidly popular among organizations worldwide and as per http://www.iso27001security.com (2011) there are over 7,000 organizations worldwide that have already been certified compliant with ISO/IEC 27001 or equivalent national variants and about 1000 new certificates are added to this number every year.

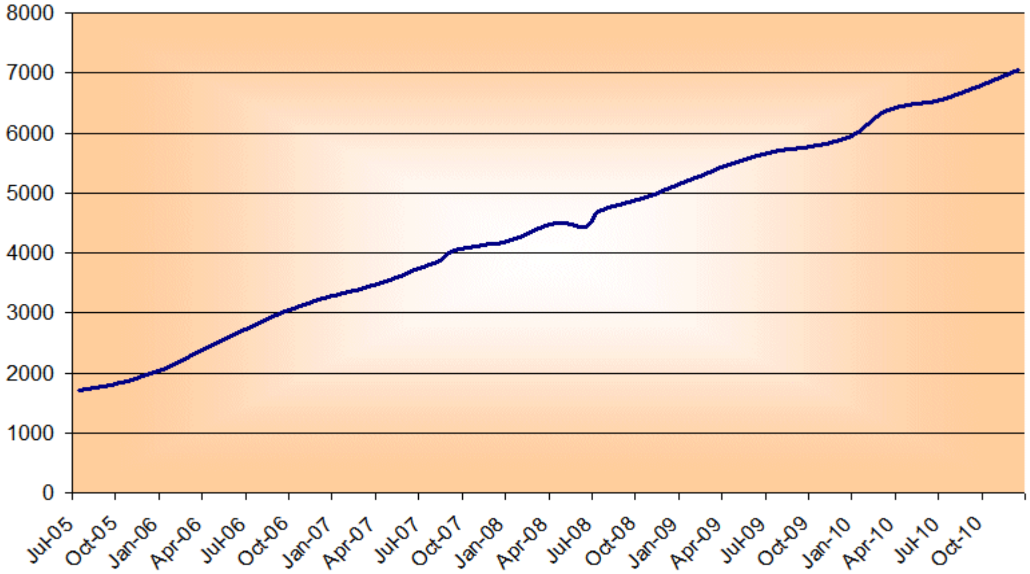


Figure 8: Number of ISO/IEC 27001 certificates

(ISO27k infosec management standards, 2011)

2.6 Culture

One of the most important areas of security based on each individual's action is the organizational culture (Johnson & Goetz, 2007 p. 22). The organizational culture can be considered a personality of the organization and is connecting the organization members together. This culture is developed based on the activities like the management vision, as well as employee behavior, both performed individually, by a group or at an organizational level.

2.7 Information Security Culture

It is according to (Johnson & Goetz, 2007, p.22) important to set “the right tone at the top” making executive leaders and the senior level aware of and engage in security issues, strategies and policies. They are responsible for emphasis employees as it is a vital part of the business. When emphasizing employee one of the most important areas is executive education, since top managers often make decisions within outsourcing and joint ventures where the right decisions are based on security risk elements (Johnson & Goetz, 2007). Is the top management aware of threats and their impact in this company? This has been investigated closer?

In order to create a security culture, awareness is very important and it must penetrate all hierarchy levels in the organization. It should address the value of protecting the information, explaining risk and impact of losing or compromising the information causes (Johnson & Goetz, 2007). According to Johnson & Goetz (2007), an officer named Chumbley at Dell introduced a strategic initiative on how to do this effectively. Initiatives promoting good security behavior are also important and people should be rewarded for practice proper security practices. The information security behavior by employees develops an information security culture similar to the organizational culture does with the employees. It consists of attitudes, assumptions, beliefs, values and knowledge possessed by the employees, as well as the stakeholders and their interference with the systems and procedures in the organization.

Awareness campaigns can consist of general information security awareness activities and targeted educational sessions for specific audiences. These sessions are highly effective to educate departments regarding their information security responsibilities. The human resources or administration functions are mainly responsible for the initial awareness training for new employees, and its more advantageous if this awareness provides training materials indicating information security's importance for the enterprise.

Information security steering committees is an example of different functional area which overlooks on improve the enterprise's overall security posture. This includes risks assessments as well. Apart from this, the human resources division plays a major role in access control policies, most importantly changing and termination of employment policies. Most if the information steering committees are made of cross-functional teams from different functional groups to encourage communication and teamwork and reduces departmental isolation and duplicated efforts, reducing costs and improving profitability.

The organization's culture acts a major role in this model. Culture basically constitutes the processes behind the method by which things get done. If the top management does not genuinely support the information security program, it could discourage other employee's sense of responsibility to information security in lower hierarchies. Therefore, it is important for the organization's senior management team, including the board of directors and all executives, to treat information security as their sole liability and genuinely support to it.

The information security culture mostly focuses on the enterprise's governance needs and common needs. Alignment of information security and business objectives enables the information security program aligns with the enterprise from the boardroom to end users, and requires information security controls to be practical and provide real, measurable risk reduction.

Frequently, information security controls are implemented with little or no assessment of the actual risks and threats to the enterprise, resulting in damaging under protection or wasteful overprotection. Information security managers must understand the business and its objectives, operating and regulatory environment, potential threats, risk impacts, operational flexibility, and resilience. Only then they can select appropriate controls to mitigate risk effectively.

Risk management is a crucial area and it requires organizational support from top to bottom, skilled people, well-organized processes and selection of proper technology. Each element is interconnected and depends on impacts and supports the other elements. Regularly this relationship is complex and it is crucial to achieve a balance among these elements. If one element is weak, information security is in danger.

Well aligned security functions, especially on information and physical security, maximize the return of investment of the project and also support each other as well. Nonaligned functions are wasteful and delay the identification and mitigation of cross-functional risks.

2.8 Business Model for Information Security

There's common believe that, in order to handle a critical area like information security, the exercise should be backed with a proven model to be successful. The Business Model for Information Security discussed here was a model for systemic security management, created by Dr. Laree Kiely and Terry Benzel at the USC Marshall School of Business Institute for Critical Information Infrastructure Protection. (ISACA, 2010, p.14)

The model takes a business-oriented approach to managing information security. It approaches information security dynamically within the context of business and shows the enterprise that information security can be both predictive and proactive.

The model can be adopted regardless of the size of the organization or the current information security framework of the organization in place. Moreover, it does not depend on any particular technology or technological change over time. The model is applicable across industries, geographies, and regulatory and any legal system. It includes traditional information security as well as privacy, linkages to risk, physical security and compliance.

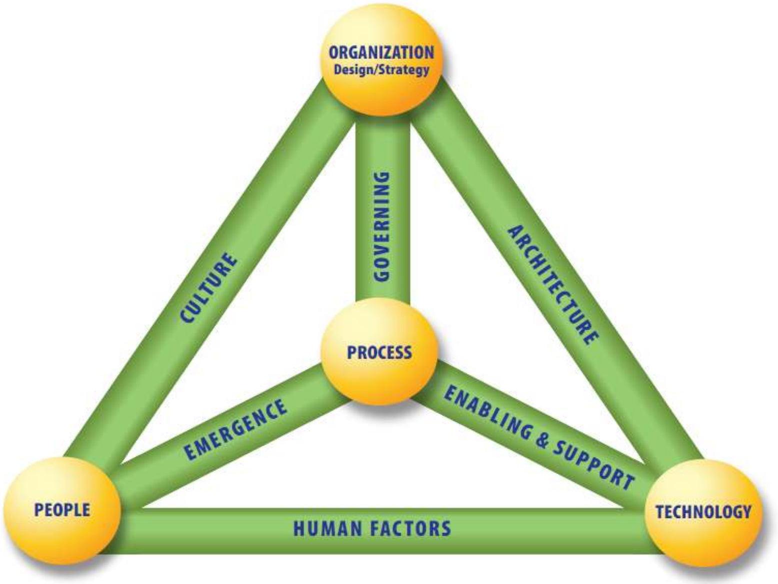


Figure 9: The Business Model for Information Security
(ISACA, 2010, p.14)

The model consists of four main elements to represent organization strategy, people, process and technology which are the key areas of the organization and there are a set of dynamic connectors which creates link in between key components.

An organization consists of group of people working together, assets and processes interacting with each other in defined roles and working toward a common goal. An organization's strategy specifies its business goals and the objectives to be achieved, as well as its values and missions to be pursued. The strategy should adapt to external and internal factors. Different types of resources like people, equipment, knowledge and experience are the primary material to design the strategy. Design also describes how the organization implements its strategy. Processes, culture and architecture are also important to determining the design of strategy.

The people element represents the human resources and the security issues that bind it. It contains the responsibilities, strategy, values, behaviors and biases. The information security manager of the organization is responsible to corporate with the human resources and legal departments to address issues such as:

- Recruitment strategies which address access control of the staff, background checks, interviews and roles and responsibilities assigned to them.
- Employment issues like location of office which they are physically based, access and rights to application tools and data, employee training and awareness, changes of the employment within the enterprise
- Termination of employment also address reasons for leaving, revoke of roles and responsibilities, access to systems, access to other employees as much as possible

External parties related to organization like customers, suppliers, media, stakeholders and others can have a strong influence on the information security of the enterprise and need to be critically considered within the security posture.

Process includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all the dynamic interconnections. Processes recognize measure, manage and control risks, availability, integrity and confidentiality for information and they also ensure accountability. They originate from the organization's strategy and implement the operational part of the organization element.

To get the most out to the enterprise, processes must align with:

- Meet business requirements and align with policy
- Consider emergence and be adaptable to changing requirements
- Be well documented and communicated to appropriate human resources
- Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

The technology element is composed of the tools, applications and infrastructure that make the processes more efficient. As a developing component that experiences frequent changes, it has its own dynamic risks. It gives a typical enterprise's dependence on technology and technology make up a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.

Usually organization's management team sees technology is a way to resolve surety threats and risks, but in actual, technology is a method to mitigate some types of risks and it's not an information security solution as whole.

The efficiency and performance of technology greatly depend on users and organizational culture. Some users still do not trust technology or do not have enough competence to use it. Sometimes users think technology reduces their performance or try to avoid or override technical controls. But information security managers should be well aware about these rumors and threats.

There are dynamic interconnections that link the elements together and apply a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to stability.

Governing is the navigation of the enterprise, while having good strategic leadership in place. Governing of the organization demarcate limits an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance, while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms shared by all people who have a common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures are to make processes usable and easy.

Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively.

Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Emergence, which implies surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

The human factor of dynamic interconnection represents the interaction and gap between technology and people and as such, is critical to an information security program. If people do not understand how to use technology, unfamiliar with technology or unable to follow applicable policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection.

Human factors may also be considered because of age, experience level and exposure to culture. Since human factors play a critical role in maintaining balance within the model, it is important to be aware all of the enterprise's human resources on related skills.

The security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. Strong business information architecture is essential to understanding the need for security and designing the security architecture.

It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. Enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

Given the pace of business today, enterprises need to understand the issues at any given time and be able to design solutions quickly and effectively. By applying systems thinking concepts, the model allows for a life-cycle approach to information security management throughout the enterprise. The model focuses on security, but once it is fully embraced, it can positively impact other functional processes as well.

The model will benefit a range of stakeholders by reducing costs, improving performance, fostering a better understanding of organizational risks, increasing collaboration and reducing duplication of effort. Diligent utilization of the model will equip enterprises to deal with current and future issues such as:

- Regulatory requirements
- Globalization
- Growth and scalability
- Organizational synergies
- Evolving technology
- Economic markets
- Human resources
- Competition
- Ever-changing threats
- Innovation

Practically all enterprises have areas the model can help to manage more efficiently. Methods espoused in the model such as creating a culture that intentionally accepts information security, providing awareness and training so employees understand thoroughly what information security is and how it relates to them, and considering social and psychological issues will help to improve any enterprise’s security management.

2.9 Outcomes of information security

For an enterprise Information security is one of the most important areas to be focused on. It is the gatekeeper of the enterprise's information assets. That creates the requirement of the information security programme to protect organizational data, while enabling the enterprise to pursue its business objectives and to tolerate an acceptable level of risk in doing so.

This tension between entrepreneurial risk and protection can be difficult to manage, but it is a critical part of a security professional's job. Providing information to those who should have it, is as significant as protecting it from those who should not have it. Security must enable the business and support its objectives rather than becoming self-serving.

From a governance perspective, there are six major outcomes that the security programme should work towards achieve as stated in the publication on information security: governance.

- Strategic alignment
- Risk management
- Value delivery
- Resource management
- Performance management
- Assurance process integration

There are a number of indicators for integration of diverse security-related functions. Most important, there should be no gaps in the level or information asset protection. Overlaps in areas of security planning or management should be minimized. Another indicator is the level of integration for information assurance activities with security. Roles and responsibilities should be clearly defined for specific functions. This includes the relationships between various internal and external providers of information assurance. All assurance functions should be identified and considered in the overall organizational strategy.

It is fair to say that the Technology element contains exceptional capability for addressing security weaknesses. Many information security concerns can be satisfied by the implementation of technology-based controls including those concerns related to human error or deliberate attack and the impact of natural or man-made disruptive incidents.

Once a tool is used mainly for perimeter protection, technology has advanced through the years to provide protection not only for the perimeter, but also to areas such as data loss prevention, encryption methodologies, event correlation, access control and information management. While there are many options for the tools, enterprise risk and business process risk are the driving forces behind the security programme. Technology selection should, therefore, always address the utility, efficiency and productivity of the overall enterprise. Once the technology is selected and implemented, training must be given to those who use the tools and monitoring will be needed to verify that the technology is functioning appropriately. There have been many recent and well-publicized breaches from enterprises with loads of technology in place to prevent security events. While technology is an important piece of the puzzle, if it is implemented and ignored, it can give the enterprise a false sense of security.

Chapter 3 Methodology

3.1 Introduction

This chapter presents the methods and data analysis techniques used for the study. It describes in detail, areas considered in the evaluation, how the framework was set for the study and how the questionnaire was prepared based on the framework. Also it gives some literature related to international standards considered for preparation of the framework. Finally it discusses data collection methods and data analysis techniques.

3.2 Research model

Considering the sample size available for this research and the research area, the research will be conducted as a qualitative approach. Structured in-depth interviews will be carried out with the selected sample.

3.3 Study area

Information Security Challenges in relation to Enterprise Security Policies in the Financial sector in Sri Lanka. The research will look into Information security challenges faced by the financial sector in Sri Lanka with regard to enterprise security policies.

3.4 Framework

Information is the currency of the information age. Information is the most valuable asset possessed by an organization in many cases. Though the truth is that, information has not been treated as valuable asset by most of the organizations. Information Technology governance is the discipline which coordinates with hierarchies, standards and processes and manage and protect the organization's information assets.

An asset as defined in ISO 27001 (ISO 27001) is an Information Security Management System (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). Its full name is ISO/IEC 27001:2005) as 'anything that has value to an organization'. Information assets are subject to a wide range of threats, both external and internal, ranging from the random to the highly specific. Risks include acts of nature, fraud and other criminal activity, user error and system failure. Information risks can affect one or more of the three fundamental attributes of an information asset:

- availability
- confidentiality
- integrity

These three attributes are defined in ISO 27001 as follows:

- Availability - the property of being accessible and usable upon demand by an authorized entity, which allows for the possibility that information has to be accessed by software programs, as well as human users.
- Confidentiality - the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity - the property of safeguarding the accuracy and completeness of assets.

ISO 27001 defines information security as the preservation of confidentiality, integrity and availability of information: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

Information Security Management System (ISMS), as part of the overall management system, is based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources. An ISMS exists to preserve confidentiality, integrity and availability. The ISMS secures the confidentiality, availability and integrity of the organization's information and information assets, and its most critical information assets are those for which all three attributes are important.

An ISMS - which the Standard is clear includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources. It is a structured, logical management approach to information security which is designed to ensure the effective interaction of the three key components of implementing an information security policy:

- process (or procedure)
- technology
- user behavior

The Standard's requirement is that the design and implementation of ISMS should be directly influenced by each organization's needs and objectives, security requirements, the processes employed and the size and structure of the organization.

3.4.1 Overview of ISO 27001 standard

ISO/IEC 27001 is the formal set of specifications against which organizations may evaluate their Information Security Management System (ISMS). ISO/IEC 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system - an overall management and control framework - for managing an organization’s information security risks.

Information is the lifeblood of an organization. Identifying and protecting that information is the essence of ISO27001. Information Assets exist in many forms:

- Content, container, carrier
- Databases, applications, registries & IT systems
- Legal, Board & Organizational records
- Intellectual property
- Reputation
- People

The security of the information fall under above categories will be considered in three aspects:

Confidentiality- Protecting information from unauthorized disclosure

Integrity- Protecting information from unauthorized modification and ensuring accuracy and completeness.

Availability- Ensuring information is available when you need it

In order to evaluate Information Security Management Systems of an organization for this research, ISO 27001 standards and its domains will be used as the framework.

The study of Information Security Challenges will be carried out focusing on 11 domains of ISO 27001:

1. Information Security Policy

   This domain mainly indicates management direction and support for information security and whether it is in accordance with the organization's business requirements and applicable laws and regulations. Under this domain it will evaluate the existence of a proper information security policy and whether it provides clear-cut directions for all the relevant information security related areas. Proper frequent review of the information security policy and making significant changes to it accordingly is also a major area covered under this domain. It will decide the continuity, suitability, adequacy and effectiveness of the policy. Because having an information security policy just for the sake of having it also a vulnerability for the organization. It should be always up-to-date and aligned with the business processes and objectives.

2. Organization Information Security

   Organization Information Security basically discusses about the management framework to initiate and control the implementation of Information Security in the organization. The corporate management should always take the lead in the exercise of information security. It accounts for a major half of the success of the project. Management commitment that can be measured in different areas. Their support, clear-cut direction, demonstrated commitment, assignment and acceptance of their information security responsibility are accountable for it. Apart from those areas, coordination between different business units of the organization, delegation of responsibilities, authorization for new information processing facilities, sign confidentiality and non-disclosure agreements with relevant parties, maintaining contact with relevant authorizes and special interest groups in order get their aid in an emergency are also important factors of the journey toward information security. Most importantly, management should initiate and execute regular independent information security audits in order to check the validity of objectives, controls, policies processes and procedures in planed intervals and make significant changes appropriately

.

3. Asset Management

The current domain addresses the issues related to assets. Assets are very important to an organization. In this scope, it address information assets which include assets containing organization's critical business information. Proper management of assets promotes business success. Apart from asset management, asset classification and acceptable use of assets will also be covered in this research.

4. Human Resources security

Human resource element is another important item in an organization's information security project, because every control, policy has to be implemented and practiced by the employees of the organization. Without the proper support of the human resource element, information security is a failure. Here human resources entity represents all the permanent employees, contract employees and any third party working for the establishment. This domain will enquire about the information security roles and responsibilities, terms and conditions of the employment, awareness about information security, disciplinary process and revoke assets and access rights upon termination or change of employment

.

5. Physical & Environmental security

The objective of this area is to check whether organizations have taken necessary steps to prevent unauthorized physical access, damage or obstruction to the organization's information infrastructure. Also to check if the equipment related to information are well maintained and properly disposed after usage.

6. Communication & Operational Management

Operational procedures and responsibilities ensure smooth flow of operations of the organization. By documenting operating procedures up-to-date procedures are made available to relevant users. Even when there is a sudden change of responsibilities it would not cause much effect to the operations.

It is very important to practice proper change management procedure. When the organization expands its size and business, it is difficult to be managed by a few people. The best practice is to document proper procedure before the change appears in the production environment.

Segregation of duties also makes life easier. It reduces the risk of dependence the business on a few people. When a task is completed by a group people rather than doing it oneself reduces the possibility for mistakes, errors, unauthorized access or changes to the production environment.

When a business depends on a third party, there is a risk bound to it. In order to minimize this risk, relevant agreement is signed with the service providers to ensure their service quality to create awareness about an organization’s security controls and procedures. It’s also important to review those agreements to check their deliveries are in line with the conditions applied in the agreements.

Apart to the paper based agreements, it is important to apply proper technical controls in a suitable way to protect the information and its infrastructure from threats.

Organization's business information, security system documentation and any other critical documents containing business critical information should be properly handled, stored and transferred to avoid unauthorized disclosure and misuse.

If the organization is open to the internet and if it allows its customers to carryout business online, there are many risks and threats bound to it. Most of the organizations are internet enabled these days. Therefore, it's required to check whether the information security manager is aware and ready for those threats.

Audit logging, monitoring and reviewing are important to track unauthorized access and processing activities. Therefore this will check on audit logging, in addition to monitoring of mission critical applications and services.

The above controls will ensure whether the organization practices correct and secure operation of information processing facilities.

7. Access Control

The main objective of this domain is to check whether the organization has taken necessary steps to control access to information assets. Access to information will be evaluated under physical access and logical access categories. In general, the availability of proper access control policy will be evaluated. Physical access control will focus on steps taken to control access and secure the organization's premises and information processing facility from unauthorized access and threats. Under logical access control category, it will evaluate access to logical information assets and the management of user accounts, passwords, privilege management, user registration and revoke rights and proper review of user rights in pre-planned intervals. Segregation of sensitive information and their processing facilities from normal user environment will also be discussed under this domain.

8. Information Systems acquisition, development & maintenance

This domain will enquire the compatibility of security of information systems of the organization. Under this it will go in detail to check whether cryptography controls have been properly applied to protect authenticity or integrity of information. The protection provided for information system's source codes and the process follow for control changes to information systems will also check under this domain. Apart from that, if the organization outsources their development work to third parties, the controls applied for that process will also evaluate.

9. Information security incident management

   Once organization has implemented an information security management system, it is important to check events and weakness occurred related to it. So there should be a proper mechanism to track and log those events and weakness and attend to those timely and correct. Employees of the organization should be well aware about this practice, in order to report properly, when they see a security breach or weakness of the controls. Under this domain it will check the organization has complied with the above controls and procedures.

10. Business continuity management

    Hassle-free smooth continuity of the business is a dream of boards and top management teams of every organization. Because any damage to the smooth flow of the business would cause damage to organization’s reputation and it will badly affected in the short term, as well as in the long run. Therefore, all the management team members are responsible for implementing a proper documented business continuity plan. Implementation is not only sufficient, and they are responsible for the assessment of new risks and review the plan in predefined intervals and make significant changes appropriately to keep the policy up to date. Under the business continuity management domain the above mentioned areas will be checked.

11. Compliance

Depending on the organization's business criticalness, a set of legal requirements should be fulfilled by the organization. Normally these enforcements are regulated by the government or its authorized independent body in order to maintain the smooth flow of business of the organization, as well as to protect the rights of the consumers. It will check whether the organization is in line with the security policies and standards enforced to practice.

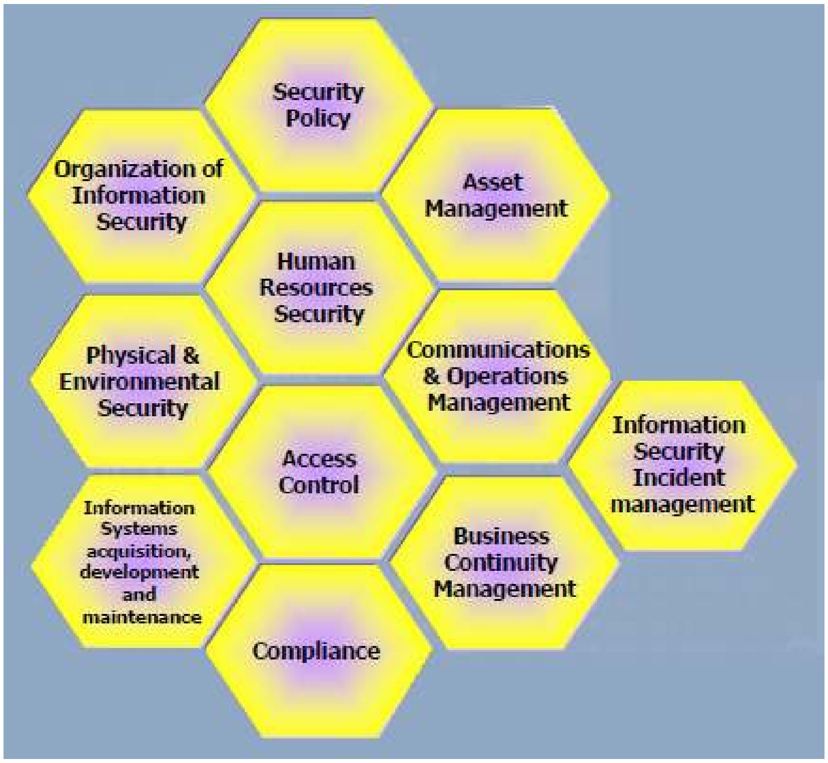

Security Policy
Organization of Information Security
Asset Management
Human Resources Security
Physical & Environmental Security
Communications & Operations Management
Information Security Incident management
Access Control
Information Systems acquisition, development and maintenance
Business Continuity Management
Compliance

Figure 10: Framework at a glance

3.5 Population

Sri Lankan financial sector consist of 72 institutes registered as financial institutes in the Central Bank of Sri Lanka as at 31st March 2010. Those 72 institutes contain 22 commercial banks, 14 specialized banks and 36 other types of finance companies. As per the feasibility study shows that most of the small scale finance companies and specialized banks are not heavily dependent on information technology. Therefore, it is decided to use only the registered commercial banks as the population of this research.

3.6 Limitations

Due to limitations like reluctance to disclose information security related data of the institutes and since the research is case-based research, the sample size is limited to five. The sample selection criteria out of the total population of 22 commercial banks are given below.

3.7 Sample selection

In the process of selecting the sample of the research, two main factors were considered. Number one is the usage and dependability of the business on information technology. As per the initial study carried out, it was found that the private banks have more potential in information security approach. State-owned banks are still behind and they were not willing to talk about their information security much.

Especially, important areas like top to bottom approach for information security are found in most of the private banks. As per (Mizzi, 2008) adopting a strategic information security approach is a top-down approach. He also emphasizes that information security is no longer an IT issue and has become “a priority in boardrooms”. Moreover, the CEO owns the information security program and top management server as information security leaders. The experience had on the initial study and considering the above facts, it was decided to consider only the private commercial banks listed in the Colombo Stock Market (PLC)

The second factor is the financial strength to invest in information technology and most importantly information security. As per (Mizzi, 2008), information security is considered an essential corporate investment. He moreover states that information security is not an item of the corporate budget and measuring ROI for information security is not enough. It gives an indication that an organization should have considerable financial strength to invest on a complete information security project and then only it could be a business enabler for the organization. The Fitch Rating system is considered to short list institutes based on their financial strength. The Fitch Rating system is a common, independent rating system for enterprises, especially for financial institutes to indicate their financial strength. For this research, only the banks having Fitch Rating “A” or above were considered.

The table below gives the commercial banks that are registered at the Central Bank of Sri Lanka and other parameters considered in the sample selection.

	Bank Name	Private	PLC	Fitch Rating (LKA)
1	Bank of Ceylon	No	No	AA
2	Citibank NA	Yes	No	AAA
3	Commercial Bank of Ceylon PLC	Yes	Yes	AA
4	Deutsche Bank AG	Yes	No	-
5	DFCC Vardhana Bank Ltd	Yes	No	AA-
6	Habib Bank Ltd	Yes	No	-
7	Hatton National Bank PLC	Yes	Yes	AA-
8	ICICI Bank Ltd	Yes	No	-
9	Indian Bank	Yes	No	-
10	Indian Overseas Bank	Yes	No	-
11	MCB Bank Ltd	Yes	No	-
12	National Development Bank PLC	Yes	Yes	AA
13	Nations Trust Bank PLC	Yes	Yes	A
14	Pan Asia Banking Corporation PLC	Yes	Yes	BBB
15	People’s Bank	No	No	AA-
16	Public Bank Berhad	Yes	No	-
17	Sampath Bank PLC	Yes	Yes	AA-
18	Seylan Bank PLC	Yes	Yes	BBB+
19	Standard Chartered Bank	Yes	No	AAA
20	State Bank of India	Yes	No	-
21	The Hongkong & Shanghai Banking Corporation Ltd	Yes	No	AAA
22	Union Bank of Colombo Ltd	Yes	No	BB+

3.7.1 'A' or Higher Fitch rated companies

Institute	Rating
Citibank N.A.- Colombo Branch	AAA(lka)
Dialog Axiata PLC	AAA(lka)
HSBC Sri Lanka Branch	AAA(lka)
John Keells Holdings PLC	AAA(lka)
National Savings Bank	AAA(lka)
Sri Lanka Telecom PLC	AAA(lka)
Standard Chartered Bank, Sri Lanka Branch	AAA(lka)
Bank of Ceylon	AA(lka)
Commercial Bank of Ceylon PLC	AA(lka)
DFCC Bank	AA(lka)
National Development Bank PLC	AA(lka)
DFCC Vardhana Bank	AA-(lka)
Hatton National Bank PLC	AA-(lka)
Hayleys PLC	AA-(lka)
People's Bank	AA-(lka)
Sampath Bank PLC	AA-(lka)
Sri Lanka Insurance Corporation Ltd	AA-(lka)
Central Finance Company PLC	A+(lka)
HNB Assurance PLC	A(lka)
Lanka Orix Leasing Company PLC	A(lka)
Nations Trust Bank PLC	A(lka)
People's Leasing Company Limited	A(lka)
Abans (Pvt) Limited	A-(lka)
Commercial Leasing Company Limited	A-(lka)
DSI Holdings Limited	A-(lka)
Lanka Orix Finance Company Limited	A-(lka)

(Fitch Ratings Lanka Ltd, 2011)

Since the information security area is very sensitive and support privacy of the information provided by the respondent, the author has kept the names of respondents anonymous and called them as respondents B1, B2, B3, B4 and B5 so that they could feel free to provide detailed information.

According to above criteria, the following banks have been short listed for this research:

- Commercial Bank of Ceylon PLC
- National Development Bank PLC
- Hatton National Bank PLC
- Sampath Bank PLC
- Nations Trust Bank PLC

3.8 Outline of the interview

The interview is conducted based on the 11 domains developed for the evaluation of information security management system (ISMS). In order to gain proper evaluation information security policies, procedures and controls, the 11 domains have been separated in smaller areas. The following detailed areas will be covered in the structure of the interview. The interview will be conducted with people who are responsible to overlook the information security of the organization. If he does not have proper idea on some areas, he will get other unit's manager support and assistance to provide required feedback.

1. Designation of the participant

   The designation is very important here. It indicates whether the top management or the board of directors has clearly identified the importance of information security domain and they have appointed a suitable and capable person to look after the information security of the enterprise. Also it will get an idea about respondent's background as well.

2. Does your organization use Information Technology for business?

   The specific enterprise should have the Information Technology exposure as it is the basic requirement to have information security in the scene. Therefore, it will check whether the enterprise use information technology for their business.

3. What is your initial reaction to the word "Information Security"?

   In this interview, the respondent is the key person in the organization for information security. So the information security itself should be in the cache. This will check at a glance when the person hears the word information security, what gets in the mindset at once.

4. Is your organization's concern Information Security a major area?

   If the information security is treated as major area by an organization, the top management should identify it as a critical areas and the real value of the information. Only if they have identified information as a critical area, the journey information security would be successful.

5. Does your organization treat its information as a valuable asset?

   In general terms if somebody uses to secure something, definitely there should be some sort of value on it. In simple terms, enterprise definitely should see the value of information before introducing information security. Because ROI of information security investments cannot be figured out easily in numbers. Usually, finance and top management would not allow for spending on information security without seeing the proper value of it to the organization. Therefore, the every effort put by management for information security, from policy making to implementation and sustainability is purely because they have identified the value of the information. In order to check if they have identified information as an asset is needed to be clarified before proceeding to information security in detail.

6. Number of employee, computer users and computers?

   This information will help to get an overview about organization's size and its capacity.

7. Does your organization have a documented Information Security Policy?

   The first step to have information security in a formal way is having an information security policy in place. If there is an updated security policy in place, it covers things like organization's culture such as how the top management's direction & support to success of information security is in accordance with organization's business objectives and relevant laws and regulations enforced to follow. The answer for this question gives a good idea about the organization's culture and its governance.

8. Does your Information Security Policy address all the necessary areas and provide clear-cut directions to all the processors related to information security?

   In addition to having a updated information security policy in place, it's required to check whether the policy address all the relevant areas a proper security policy should address and whether it provides clear-cut directions.

9. How frequently do you review your Information Security Policy?

   Information security policy should be reviewed in pre-planned intervals to make significant changes and recommended measures to ensure its effectiveness and suitability. Policy review is normally done after having a proper audit. By checking this area, it will indicate whether an organization needs an independent audit and review the information security policy in recommended frequencies.

10. Is there Confidential Agreements / Non-Disclosure agreements (NDA) / Service Level Agreements (SLA) with related parties?

Most organizations use third parties for day to day activities and services. Data/ voice/ internet Service providers, labour supply companies, third party maintenance staffs coming for A/C, generator, etc maintenance belong to this category. Even though they are not direct employed under the organization, sometimes they work in the same premises and have access to most of the areas the company employee use that normal employees do not have access to like server rooms, etc and they see most of the business transactions / discussions of the organization. Even though they do not reside in the premises, they have access to critical information of the organization. So it is vitally important to address this category in the information security policy. Otherwise without knowing anyone, the corporate information would be disclosed outside. The preliminary step that can be taken regarding these third parties is to sign a non-disclosure or confidential agreement with them or their company by enforcing them to sign NDA's with their employees. Sometimes there are legal enforcements by which an organization is bound, such as data protection and privacy of customer information, etc. Apart from that, it's required to ensure these services are timely. The continuity of the business relies on many direct and indirect parties. So it is important to ensure their service levels. Therefore, smooth flow and minimize risk of business continuity is required to sign service level agreements with critical service providers and third parties.

11. When did you carry out the last business risk analysis?

This will check if the organization has taken necessary steps to carryout independent review of information security policy in regular intervals and get an idea. What are the possible risks to the business and change the policy suite to identified risks and vulnerabilities.

12. Does your organization maintain an updated list of assets with their ownerships?

    It is important to have a comprehensive list of assets with their unique identification with their owners in order to provide appropriate protection and smooth running. Most importantly, this should be identified for information processing facilities in order to control proper maintenance, development and security.

13. Does your organization practice information classification, labeling and handling according to their criticalness?

    In order to guarantee that information assets get necessary protection and attention depending on their criticalness, it is required practice a proper labeling mechanism.

14. Is there a practice to sign a confidentiality agreement with all employees including permanent, contract and temporary?

    The employees of the organization are exposed to much information of the organization. The only way to minimize information discloser to outsiders is to make them aware about information security control and make necessary legal enforcements like signing confidentiality agreements with different employees.

15. Does your organization organize regular awareness sessions to employees to educate them on information security, practices, policies and guidelines?

    User training is very important to succeed any project. Because users should be aware what is actually happening and have a clear idea about their roles and responsibilities. In information security too, user awareness is a very important aspect for the success of the project. This basically should be at the beginning whenever employee joins the organization (induction program) and in regular intervals or when there a significant change in policies or procedures. And it is important to have easy access to policies and procedures they are enforced to practice.

16. Does your organization take disciplinary actions against employees for violation of information security procedures, after a proper investigation?

    Whenever there is a security breach, it should be treated as an important incident; the suspects should be identified and after having proper inquiry, there should a disciplinary process at the end. It will definitely be an example for others and very important to maintain information security.

17. Is there a pre-defined practice to revoke all relevant responsibilities, access rights and returning assets when there’s a termination or change of employment?

Whenever there is a change or termination of an employment, there should be a proper procedure to revoke all responsibilities, logical and physical access rights and returning assets. This should happen immediately the change or termination happens.

18. Is there a documented procedure for management of removable media?

    Removable media plays an important role in information security. Due to their physical factors, they can be taken out easily without any extra effort. Most of the time these removable medias contain very critical information like database backups, system backups which are intend to sending off-site which is also an requirement. The only way to minimize unnecessary information leakages, losses is having proper policy and procedure in place which address about handling removable media.

19. Is there a documented procedure for disposal of media containing organization's information?

    There should be a proper procedure and practice for proper disposal of storage media which contains corporate information. Especially when there is a warranty replacement or returning assets back there should be a proper mechanism to remove all the corporate information and other information assets like licensed software, etc and also ensure that the dispose or deleted information cannot be retrieved in any form. If the information contains on hard media such as paper, it should be properly disposed by shredding.

20. Is there a documented procedure for exchange of an organization's information like agreements, physical media, electronic messaging, business information, etc?

    There should be proper produce for exchange of all kind of organization's information like agreements, physical media, electronic messaging, and business information, within an organization and with any external party. There can be exchange agreements or any other legal enforcement to protect the privacy of information exchange.

21. Does your organization practice e-commerce service / internet enabled banking?

    Most of the organizations are now using electronic commerce. There are many advantages to customers by enabling E-commerce; at the same time there are threat and vulnerabilities as well. Therefore, if the organization is into e-commerce and other internet enabled service like online payment transactions or their basic banking need, the organization needs to practice a set of control to minimize inherent threats and vulnerabilities of having open access to internet.

22. Does your organization maintain a proper log of all the transactions and events and review those accordingly?

    In order to maintain integrity and security of information processing facilities, it is necessary to keep a proper tract of all the transactions. In technical terms, the track of transactions is called audit logging. Audit logs are basically recording user activities, exceptions and security events; specially user's and special user's successful and failed logins and activities are retained for a pre-agreed time period for further monitoring and investigation. It helps to detect unauthorized information processing activities, exceptional events, actions and further developments of procedures and policies. These logs should be protected to avoid tampering and unauthorized access. There should be a proper documented procedure to practice, maintain and analyze audit logs properly.

23. Is there an access control policy in practice which address user registration, privilege management, password management, session management and application access management? How frequently does your organization review user access rights?

Proper access management is very important in information security domain which covers physical and logical access control for information. There should be a properly documented access control policy which addresses user registration, privilege management, password management and review of user rights in pre-defined intervals. Revoke rights also very important immediately there is a change or termination in employment or change in operational procedures.

24. Are users aware of proper use of passwords and access rights?

    Proper use of passwords is very important to avoid unauthorized user access or compromise information and information processing facilities. These types of thing could happen due to various reasons. Mainly it could be due to the lack of proper password management practices. Systems should force users to change their password frequently and prompt for complex password which cannot guess or use brute-force easily. Even though password policy exists with these controls, users may share their password among others. That's also a critical violation of password policy and a threat to information security. Therefore user awareness should discourage users on those practices.

25. Does your organization practice Network Access Control?

    Network Access Control is a type of access control mechanism used to control access to corporate network. It authenticates user or device before granting access to resources on the network. Sometimes it checks the device's health before granting access like whether the anti-virus is installed and up-to-date, firewall is enabled, etc in order ensure more protection of network and resources on it. There should a proper procedure to address network access control area.

26. Is there a segregation of network / sensitive system isolation depending on their criticalness?

    In a corporate network, there are different types of information resides. Some are very critical to business. When considering users groups, there are different categories for different purposes. So if everything puts in the same segment of the network it would create a threat. Therefore, it is required identify information and user groups separately and segregate accordingly in order to ensure protection of everyone as well as organization.

27. Does your organization use cryptographic controls for information?

    Cryptography is used to protect confidentiality, authenticity or integrity of information. Organizations need to use cryptographic controls whenever it seems required.

28. Is there proper access control/protection to business applications source libraries?

    If the organization keeps its application's source code in the network, it is very important to look after its security. By getting source libraries to unauthorized hand could lead to unauthorized access to production environment without any difficulty. Therefore, there should be a proper procedure to control access to source libraries and as much as possible segregation between production and development and testing environments.

29. Is there a documented change management procedure?

    Change management is very critical to organization. Not only in information systems and processing facilities, but change management is important in other areas as well. It controls changes to information processing facilities and systems and all the changes will go through a proper flow with necessary approvals in order to ensure the smooth flow of information systems and processing facilities.

30. Does your organization outsource system development work?

    By out sourcing application development work to the third party, the organization discloses a lot of business logics and operational secrets to the third party. Therefore outsource software development exercise should be overlooked and monitored by the responsible people of the organization.

31. Does your organization use licensed copies of software applications?

    Using licensed software application will keep the organization safe side in legislative, regulatory and contractual requirements with regard to intellectual property rights.

32. Is there a documented procedure to report and evaluate information security events, weaknesses, incidents and improvements?

    In order to maintain proper information security in the organization, the support of all hierarchies is very important. Due to some change in a process or an operation, there could be a newly created threat. The responsibility of other users is to inform regarding such thing to the relevant authorities in right manner. It will allow information security manager or whoever responsible to act accordingly and make necessary arrangements. In order to do this, users should know the reporting path of such incident. As well as there should be a proper procedure to log such information correctly and attend to it timely and make necessary improvements to procedures.

33. Does your organization have business continuity / disaster recovery plan is place? How frequently is it reviewing, testing, re-assessing?

    Every organization should have a proper business continuity / disaster recovery plan in order to ensure smooth flow of the business. It increases the comfortability of employees, as well as credibility on organization of customers. Because failure in a critical business processes are due to failure of information systems or natural disaster will create bad impact in corporate image, short-term as well as in the long run. Organization should be ready to face any kind of disaster and carry out a business continuity plan accordingly to minimize the failures of business. For the use of such an accidental incident, it is required get the disaster recovery plan standby which is allowed only by proper frequent reviewing, testing and update accordingly.

34. How do you describe top management's support to organization's information security? (Financial & attitude backing towards information security)

    This question helps to get a good idea about the organization governance and how the top management team understands information security subject and the value of information to them. Sometimes their attitude is okay, but they are not willing to spend on information security much and since it is difficult to justify ROI in numbers. Most of the finance people put pressure on information security managers or the requesting party for information security expenses asking ROI of the investments. Only by setting big tone and power from the very top only normal way to get information security project a success. Even though the initial steps get success, maintaining security practices are also a hard task. That is why it needs continues support of top management by financially and attitude.

35. How do you define the context of information security in your organization?

Context of information security in the organization is very important for a successful information security exercise in the organization. Specially intention and respect to information security of the organization of different hierarchies in different business units. Because without align people's mind towards one vision in implementation of information security would drive the project to a failure. If employees in other business units other than information technology sometimes think that information security is IT unit's business which should in their minds under any circumstances. Ultimately information security is everyone's business and it should be in everyone's hearts and minds.

36. Do you see any obstructions to improve information security in your organization?

How successful the information security in an organization, there could be sometimes minor obstructions which put some sort of resistance on information security. Sometimes those minor things could do a big damage.

Therefore the best thing is to address even small things also as soon as possible and clear it off.

3.9 Relationship between questioned areas and 11 domains

Questioned area	Covered domain(s)	Sub Domain
1. Does your organization use Information Technology for business?	General	
2. What do you think of when you hear the word "information security"?	General	
3. Does your organization concerned about Information Security as a major area?	Organization of Information Security	Management commitment to information security
4. Does your organization treat its information as a valuable asset?	Organization of Information Security	Management commitment to information security
5. Number of employees of the company?	General	

6. Number of computer users of the company?	General	
7. Number of computers of the company?	General	
8. Does your organization have a documented Information Security Policy?	Security Policy / Organization of Information Security	Information Security Policy
9. Does your Information Security Policy address all the necessary areas and provide clear-cut directions to all the processors related to information security?	Security Policy / Organization of Information Security	Information Security Policy
10. How frequently do you review your Information Security Policy?	Security Policy / Organization of Information Security	Review of the information security policy
11. Is there Confidential Agreements /Non-Disclosure agreements (NDA) / Service Level Agreements (SLA) with related parties?	Internal Organization / Communication and operations management / Compliance with legal	Confidentiality Agreements / Security of network services / Data protection

	requirements	and privacy of personal information
12. When did you carry out the last business risk analysis?	Business continuity management	Business continuity and risk assessment
13. Does your organization maintain an updated list of assets with their ownership?	Asset Management	Inventory of assets/ ownership of assets
14. Does your organization practice information classification, labeling and handling according to their criticalness?	Asset Management	Information Classification
15. Is there a practice to sign a confidentiality agreement with all employees including permanent, contract and temporary?	Human Resources Security	

16. Does your organization organize regular awareness sessions for a employees to educate them on information security, practices, policies and guidelines?	Human Resources Security	Information security awareness, education and training
17. Does your organization take disciplinary actions against employees for violation of information security procedures, after a proper investigation?	Human Resources Security	Disciplinary process
18. Is there a pre-defined practice to revoke all the relevant responsibilities, access rights and returning assets when there’s a termination or change of employment?	Human Resources Security	Termination or change of employment
19. Is there a documented procedure for management of removable media?	Communications and operations management	Media handling / Management of removable media

20. Is there a documented procedure for disposal of media containing organization's information?	Communications and operations management	Media handling / Disposal of media
21. Is there a procedure to address handling information and critical documentation?	Communications and operations management	Media handling / Information handling procedures
22. Is there a documented procedure for exchange of all kind of organization's information like agreements, physical media, electronic messaging, business information, etc?	Communications and operations management	Exchange of information

23. Does your organization practice e-commerce service / internet enabled banking?	Communications and operations management	Electronic commerce services
24. Does your organization maintain proper log of all the transactions?	Communications and operations management	Audit logging
25. Is there a defined security procedure for monitoring and reviewing logs?	Communications and operations management	Monitoring system use
26. Is there an access control policy in practice which address, user registration, privilege management, password management, session management and application access management?	Access control	User registration/ Privilege management
27. How frequently does your organization review user access rights?	Access control	Review of user access rights
28. Are users aware of proper use of passwords and access rights?	Access control	User password management

29. Does your organization practice Network Access Control?	Access control	Network access control
30. Is there a segregation of network / sensitive system isolation depending on their criticalness?	Access control	Segregation in networks
31. Does your organization use cryptographic controls for information?	Information systems acquisition, development and maintenance	Cryptographic controls
32. Is there proper access control/protection to business applications source libraries?	Information systems acquisition, development and maintenance	Security of system files / Access control to program source code
33. Is there a documented change management procedure?	Information systems acquisition, development and maintenance	Security in development and support processes / Change control procedures

34. Does your organization outsource system development work?	Information systems acquisition, development and maintenance	Outsourced software development
35. Does your organization use licensed copies of software applications?	Compliance with legal requirements	Intellectual property rights
36. Is there a documented procedure to report and evaluate information security events, weaknesses, incidents and improvements?	Information security incident management	Reporting information security events and weaknesses
37. Does your organization have business continuity / disaster recovery plan is place?	Business continuity management	Information security aspects of business continuity management
38. How frequently is it reviewing, testing, re-assessing?	Business continuity management	Testing, maintaining and reassessing

		business continuity plans
39. How do you describe top management’s support to organization’s information security? (Financial & attitude backing towards information security)	Internal Organization	Management Commitment to information security
40. How do you define context of information security in your organization?	Internal Organization	
41. Do you see any obstructions to improve information security in your organization?	Internal Organization	

3.10 Data Collection

The data collection of this research was done through in-depth structured interviews with the respondents. It was conducted on 11 domains introduced in the framework. These 11 domains were separated into small areas in order obtain more information.

3.11 Data analysis

The collected data will be analyzed by studying multiple cases by comparing the cases in a cross-case analysis.

Chapter 4 Data Presentation

The collected data through in-depth interviews under 11 domains are given below. This is a very high level comparison.

4.1 *A High level comparison of collected data*

B3 bank avoids answering some questions due to privacy of the information. Those are marked as “Avoid”

Questioned area	**Respondent B1**	**Respondent B2**	**Respondent B3**	**Respondent B4**	**Respondent B5**
Designation of the participant	Executive officer – IT security	Manager – Networks and communications	Asst. Manager – IT security	Information Security Administrator	Senior Communication Engineer – Network Security
42. Does your organization use Information Technology for business?	Yes	Yes	Yes	Yes	Yes
43. What do you think of when you hear the word “information security”?	Information Security is	The protection of	Protecting CIA of	It is basically about	Essential thing in today’s

	everyone job. Practicing IS will definitely boost up the organization benefits.	data against unauthorized access	information	protecting information and avoid unauthorized access and confidentiality, integrity and availability of information. A threat to Information security can make big	world. It's important to business continuity

				impact on business short and long term basis.	
44. Does your organization concern Information Security as a major area?	Yes	Yes	Yes	Yes	Yes
45. Does your organization treat its information as a valuable asset?	Yes	Yes	Yes	Yes	Yes
46. Number of employees of the company?	1001-5000	1001-5000	1001-5000	1001-5000	1001-5000
47. Number of computer users of the company?	1001-5000	1001-5000	1001-5000	1001-5000	1001-5000
48. Number of computers of the company?	1001-5000	1001-5000	1001-5000	1001-5000	1001-5000

49. Does your organization have a documented Information Security Policy?	Yes	Yes	Yes	Yes	Yes
50. Does your Information Security Policy address all the necessary areas and provide clear-cut directions to all the processors related to information security?	Yes	Yes	Avoid	partially	Yes
51. How frequently do you review your Information Security Policy?	Once a year	Once a year	Once a year	Once a year	Once in three months
52. Is there Confidential Agreements /Non-Disclosure agreements (NDA) / Service Level Agreements (SLA) with related	Yes	Yes	Avoid	Some	Some

parties?					
53. When did you carry out the last business risk analysis?	Within the last year	Within the last year	Avoid	Within the last year	Within last year
54. Does your organization maintain an updated list of assets with their ownerships?	Yes	Yes	Yes Without the ownership	Yes Without ownership	Yes
55. Does your organization practice information classification, labeling and handling according to their criticalness?	Yes	No	Avoid	Some 50%	Yes 80%
56. Is there a practice to sign a confidentiality agreement with all employees including permanent,	Yes	Yes	Avoid	Yes	Yes

contract and temporary?					
57. Does your organization organize regular awareness sessions to employees to educate them on information security, practices, policies and guidelines?	Yes	No	Avoid	No	Yes
58. Does your organization take disciplinary actions against employees for violation of information security procedures, after a proper investigation?	Yes	Yes	Avoid	Yes	Yes
59. Is there a pre-defined practice to revoke all the relevant responsibilities, access	Yes	Yes	Avoid	Yes	Yes

rights and returning assets when there’s a termination or change of employment?					
60. Is there a documented procedure for management of removable media?	Yes	Yes	Avoid	No Practice only	Yes
61. Is there a documented procedure for disposal of media containing organization’s information?	Yes	Yes	Avoid	Yes	Yes
62. Is there a procedure to address handling information and critical documentation?	Yes	Yes	Avoid	Yes	Yes

63. Is there a documented procedure for exchange of all kind of organization's information like agreements, physical media, electronic messaging, business information, etc?	Yes	Yes	Avoid	Yes	Yes
64. Does your organization practice e-commerce service / internet enabled banking?	Yes Online banking	Yes Payment gateway, internet banking	Yes Internet banking, B2B applications	Yes Online banking	Yes Online banking, B2B applications
65. Does your organization maintain proper log of all the transactions?	Yes	Yes	Avoid	Yes	Yes

66. Is there a defined security procedure for monitoring and reviewing logs?	Yes	Yes	Avoid	Yes	Yes
67. Is there an access control policy in practice which address, user registration, privilege management, password management, session management and application access management?	Yes	Yes	Avoid	Yes	Yes
68. How frequently does your organization review user access rights?	Once in three months	Once in six months	Avoid	Once a year	Once in three months, high level users once a month

69. Are users aware of proper use of passwords and access rights?	Yes	Yes	Avoid	Yes	Yes Well documented
70. Does your organization practice Network Access Control?	Yes	No	Avoid	Yes	Yes
71. Is there a segregation of network / sensitive system isolation depending on their criticalness?	Yes	Yes	Avoid	Yes	Yes
72. Does your organization use cryptographic controls for information?	Yes	Yes	Avoid	Yes	Yes
73. Is there proper access control/protection to business	Yes	Yes	Avoid	Yes	Yes

applications source libraries?					
74. Is there a documented change management procedure?	Yes	Yes	Avoid	Partially	Yes
75. Does your organization outsource system development work?	No	No	Avoid	Partially	Partially
76. Does your organization use licensed copies of software applications?	Yes	Yes	Avoid	Yes	Yes
77. Is there a documented procedure to report and evaluate information security events, weaknesses, incidents and improvements?	Yes	Yes	Avoid	No	Yes

78. Does your organization have business continuity / disaster recovery plan is place?	Yes	Yes	Yes	Yes	Yes
79. How frequently is it reviewing, testing, re-assessing?	Once a year	Once in six months	Once a year	Once a year	Once in three months
80. How do you describe top management's support to organization's information security? (Financial & attitude backing towards information security)	Excellent	Corporate management's support and attitude has changed for the positive in the near past	Policies & procedures from top to bottom. Info Sec is required. Financial budgets okay	Attitude wise okay, they encourage too. Financial baking also good. Some units managers	Attitude excellent, need to improve financials

				think InfoSec is IT's job.	
81. How do you define context of information security in your organization?	We are ISO 27001 compliant	Information security has become a critical necessity and has high priority	It's under IT div and given high priority.	Top management set the tone. But does nto get much support from middle management and users.	Info Sec is under IT, but directly report to MD monthly
82. Do you see any obstructions to improve information security in your	No	No, as information	User awareness is	Resistance to change in	Resistance to change in

organization?		security has become high priority concern	not sufficient	users mindsets. When users losing some facilities (eg. USB) due to InfoSec controls, they resist a lot. User awareness not sufficient.	users mindsets. Length procument and financial processes. Difficult to justify ROI
83. Additional comments:	ISO 27001	-	Management	-	Salifiable

	certified and have successfully sustained for the first year		commitment is good. There’s a steering committee to overlook Info Sec. Info Sec can act independently		approach to InfoSec.

Chapter 5 Data Analysis

In this chapter the data obtained during the interviews are analyzed using the cross-case method analysis.

5.1 Cross-case analysis

In this section the data was examined through a cross-case analysis, where the five cases are compared with each other. The similarities and differences were identified and discussed by comparing the data from five case studies.

The structured in-depth interviews were carried out with the key personnel responsible for information security of the selected banks. In order to keep the privacy of the respondent's institutes, here B1, B2, B3, B4 and B5 are used as respondents, instead of their actual identity and affiliation.

The respondents (B1 - Executive Officer, IT Security of the bank; B2 –Manager, Networks and Communications; B3 - Assistant Manager, IT Security; B4 - Security Administrator; B5 -Senior Communication Engineer, Network Security) participated in the interviews.

Respondent B3 avoided answering some questions, since he felt the questions too sensitive and it could harm the information security of the bank.

The first question asked at the interview was whether the bank uses information technology for business. Everyone's answer was similar. Most respondents stressed that they were heavily depending on information technology and they cannot even think how to run the operations without the support of information technology. The responses show the banks' dependability on information technology (Hagsten, 2009; Haider; Abbas et al, 2011) and the requirement for information security in these firms.

Then it was to clarify how these key information security people actually use information security. The second question was "what do you think of when you hear the word information security"? The intension of this question was to ascertain their thoughts at a glance when they hear information security. Almost everyone was having information security in their minds. As soon as the question was asked, they responded immediately, and stated the importance of information security.

Respondent B1 mentioned that information security is everyone's job. Even though some people think that it is the responsibility of IT solely, it is not the truth. He also emphasized that information security is not a cost centre and it will definitely gain advantages to the company by boosting up the organization's benefits. Their bank sees information as a valuable asset and they treat its information security as a major area (Hall, 2011).

B2 replied that in general information security is protection of information against unauthorized access. When information goes to unauthorized unsafe hand it could cause major damage to the company (Alshboul, 2010; Kumar et al, 2008). So information security ultimately protects information from getting into unauthorized hands in order to ensure the smooth run of the business. Moreover, they think information security as a high priority area. Recently the mindsets of their top management were changed drastically on information security. His own words it explains as "the top management of the bank identified information as a valuable asset to the bank in the recent past and now they exert pressure and set the targets to strengthen the information security of the bank"

Responded B3 tackled the question technically. He stated that information security is about protecting confidentiality, integrity and availability of information. When it loses the balance of information on confidentiality, integrity and availability, there is a significant risk to the organization. Therefore, information security is basically about balancing the three factors according to bank's business objectives and controls (Chen, 2006; Alshboul, 2010). Then he talks about the banks perception on information and information security. Their top management also is highly involved in information security not only by setting vision but also committed to it. There's doubt that respondents view on information security was that it was a high priority area and they had already identified the value of information correctly.

Respondent B4 responded that information security is about restricting unauthorized access to information. He also mentioned that though restricting unauthorized access is important, t not all about information security. It also should protect the integrity and availability of information as well for it to become information security (Chen, 2006; Alshboul, 2010). Different to other respondents, he mentioned the impact of information security breaches to the business. According to him, it could make a negative impact on the bank short term, as well as in the long run too (Alshboul, 2010; Kumar et al, 2008). Their bank is highly dependent on information technology and treats information as a valuable asset and securing them is also seen as a major concern.

B5 viewed information security as an essential thing in today's world. The protection provided for information will help business to flow smoothly. In other words, information security is about business continuity as explained by Savage (2002); "a business continuity plan, which is part of an organization's IT- and information security program". B5's bank also treats information as a valuable asset and security of it also as a major area and allocated investment, resource and efforts to maintain a proper information security environment.

Question/ Area	B1	B2	B3	B4	B5
1. Does your organization use Information Technology for business?	Yes	Yes	Yes	Yes	Yes
2. What do you think of when you hear the word "information security"?	Everyone's job	Protect information	CIA of information	CIA of information	Essential thing
3. Does your organization concern Information Security as a major area?	Yes	Yes	Yes	Yes	Yes
4. Does your organization treat its information as a valuable asset?	Yes	Yes	Yes	Yes	Yes

Then there were a few questions to get an idea about the scale of the organizations participating in this research. The scale described here using the number of employees, number of computer users and number of computes of each organization. By analyzing the responses, all the five respondents' replies were in a similar category; the number of employee, number of computer users and number of computers fall in the range of 1001-5000 category. It indicates that the five organizations selected for this research are more or less in similar capacity and scale organizations, which could be used as a positive point to analyze and compare data.

	B1	B2	B3	B4	B5
No. of Employees	1001-5000	1001-5000	1001-5000	1001-5000	1001-5000
No. of Users	1001-5000	1001-5000	1001-5000	1001-5000	1001-5000
No. of Computers	1001-5000	1001-5000	1001-5000	1001-5000	1001-5000

Then the respondents were asked about the presence of a documented information security policy and their contents. All five respondents confirmed that there was a documented information security policy in place.

In B1's case, it is well documented by addressing all the areas relevant to information security. They have not found anything in their day-to-day life which is not covered by this. As per him it is a complete policy, which gives them expert guidance throughout the information security journey document which is true statement as per the explanation given for information security policy by Hone and Eloff (2002). Moreover, it was the most important component of an information security policy: frequent review: they normally review their information security policy once a year as a practice.

B2 also stated having a documented information security policy which addresses most necessary areas. He stated frankly that their top management recognizes the value of information in recent past and are engaged in the development of information security currently. They also review the entire information security policy annually.

B3 also confirmed having a well documented information security policy in place. Unfortunately he avoided disclosing its contents and coved areas due to fears on possible risk to their information security. Though he did not provide any details about the information security policy, he stated that the policy is reviewed every year and significant changes implemented in order to keep it up to date.

Respondent B4 stated that their bank was having a documented information security policy to direct the organization on information security domain. He drilled down to their information security policy and stated the areas addressed in the document. Their information security policy does not provide clear cut directions to the Access Control domain. They have a good practice in place and they need a formal approval to obtain access right. Anyhow it is not included in the security policy. As per him asset management is well documented in the policy and it provides good direction. Business continuity which bank needs a lot of attention is also covered in their information security policy. Areas related to human resources in information security are also clearly mentioned in their document. But their information security policy does not provide directions to information security incident management, which could play a major role in information security project. Other areas are also covered in the document. They review information security policy every year as per the directions provided by the policy itself.

Responded B5 stated satisfaction with their information security policy. He sees the information security policy as the core of the information security of the bank. As per him, it provides good guidance in all areas related information security domain. They believe that the current policy is more effective as it is reviewed monthly and discussed. If they identified anything which requires urgent attention, it is corrected immediately right there. Otherwise, decisions are taken in the monthly meetings appear in the information security policy document once in three month time.

Respondents were enquired about the legal enforcements taken to prevent information leakages from third parties and the steps to ensure their service level for the smooth run of the business. Here the considered third parties as direct and indirect service or manpower providers (Hagen et al, 2008). Eg. Data, Internet service providers, Maintenance companies for A/C, Generators etc, labour supply companies for security, cleaning services etc.

The B1 and B2 said that they comply with these criteria. As per B1, they have already signed confidential, non-discloser and service level agreements as per the relevancy with all third parties involvement with the bank’s information infrastructure, directly and indirectly. B3 did not disclose information related to agreements due to the privacy of the bank. Respondents B4 and B5 had a more or less same idea. They have agreements only with directly affecting parties like data/internet service providers, A/C and generator maintenance companies. They do not see any requirement to sign these types of agreements with indirectly involvement parties like labour supply companies for security tea and cleaning services. Respondent B5 specially stated that why they do not see the requirement for binding with indirect parties, because the bank staff always guides the third parties and spends time with them, whenever they access the bank, and do not allow them to be alone under any circumstances.

The next question was “when did you carry out the last business risk analysis?” Respondents B1, B2 and B4 replied that they had carried out their last business risk analysis during the last year and as per their bank’s regulations it is carried out every year. B5 stated that they had their last business risk analysis last year and they normally carry out two business risk analysis per year and most probably in June and December. B3 did not respond to this question.

Then the respondents were interviewed on the controls for having asset management. Respondents B1, B2, B3, B4 and B5 confirmed that banks maintain updated list of assets. B1, B2 and B5 stated that they also maintain the ownership or the responsible user against assets. B3 and B4 mentioned that though they have updated asset list with the unique identification number, they do not log the owner or responsible user of the asset in the list.

Classify assets on their criticality and labeling it is practiced more or less by almost everyone in the sample, except B3. Respondent B3 did not respond to the question. B1 and B2 have practices asset classification and labeling in every business unit across the bank. B4 does only for critical information processing facilities and critical hard documents. Information systems and client PC’s are not included under this exercise. Respondent B5 believes they comply 80% on this. Most of the identified information assets are classified under this exercise, but not fully implemented in the bank.

The respondents were next interviewed on human resources related control for information security of the bank. They were asked whether they have confidentiality or non-discloser agreements with the employees, including permanent and temporary. Except B3, others responded positively to having such practice in place. Furthermore, B5 stated that it is a requirement in their bank, and already incorporated in the employment letter. B4 told that though the employees have to sign a confidentiality agreement with the company, it is effective only they are employees of the bank, and once they leave the bank it would not be effective.

Then they were asked about the user awareness sessions on information security and its practices, policies and guide lines. Except B3, other responded positively. Respondents B1 and B5 agreed that awareness is very important to keep the information security project running lively and they all conduct user awareness session on bank's information security. B1 drilled down to their user awareness practices. He stated that starting from the induction program for new-comers, they conduct regular user awareness sessions specially when there is a major change in their information security procedure or control. B5 responded that they published all the information security policies and procedures in their intranet for easy access of users and authorized users can read policy documents right there. He added that new comers are educated at the induction program, inclusive of monthly training session on information technology and information security awareness included.. Respondent B2 and B4 stated that, since they are new to information security implementations they do not conducting a proper user awareness sessions and there is no proper mechanism to it. Users do it as a mutual practice.

Human resources are another related task in order to enforce disciplinary actions against violation of company rules and regulations. They were questioned whether they take disciplinary action against an employee after a proper investigation violates information security. Except B3, others responded were having such practice in place. B1 and B2 stressed that they are very strict on employees who violate information security practices and they have past experiences when many employees were fired for information security violations after having a proper investigation. The disciplinary actions set the example to other and it was very effective for the benefit of the information security approach of the bank. B2 and B4 revealed that even though there is a disciplinary procedure, they do not see as a significant and they have not seen any incidents where employees lose their jobs due to information security breaches.

In information security too there are many factors that trigger those events. The respondents were questioned about the existence of policy to revoke all the relevant responsibilities, access rights and returning assets when there is a change or termination in the employment. Except for B3, others responded were having a procedure in place for enforcement. B5 mentioned that if they miss to revoke rights, assets at the point of change or termination of employment, they could tackle it at the rights review process carried out in every three months.

Then there were questioned about their practices and procedures of handling and exchanging of media containing critical corporate information. B1, B2 and B5 were having such procedure to handle removable media and exchange critical information. B1 stressed that they were extra cautious on removable media, because a small mistake could do major damage. B1 and B5 specifically stated that they do not allow normal users to use removable media like USB memory sticks in the corporate network. Because banks are responsible for the protection of privacy of information of customers under their custody. Furthermore B5 stated that not only handling removable media, but also the proper disposal of media containing corporate information was very important. They were not used to returning a faulty hard disk drive used in a server or a critical PC to the supplier as warranty replacement. This kind of action could make blunders. B4 responded that they do not have a proper procedure to take over handling removable media.. But they have a proper practice to handle areas like backup tapes and other removable media having critical information. B3 did not respond to this question.

Then all were asked about their presence in internet banking and e-commerce. All the banks, including respondent B3, responded that they were open to the internet. When considering the services offered by these banks, more or less all the banks provide customers online banking facility to carry out normal baking functionalities like account balance check, fund transfer, utility bill payments, etc.

All respondents were questioned about maintaining transactions logs and reviewing them accordingly. Except B3, others responded that maintaining a proper log of all transactions is compulsory for banks as per the regulations for them to follow. When it comes to log review part, all the banks take samples out of the logs and analyze check for any attacks or unusual activities. Moreover, B5 told that in their setup, process owner who is responsible to look after a specific part of the information processing facilities is responsible to carry out log review process.

Next respondents were questioned about access control policy, which addresses user registration, privilege management, session management and the regular review of them. Except B3, others confirmed that they were having such policy even though the contents may be little different. B1, B2, B4, B5 stressed that since this a high priority area, password policies, enforcement to use complex passwords, session timed out, automatic inactivity when there is no transaction for a long period are applied not only for internal users, but also to external users, normally the customers who use internet banking. Apart from access management, the respondents stated that they review user rights in pre defined time periods. B1 and B4 stated that their banks run user review exercise once a year, while B2 stated having reviews every six months. B5 implements in two stages, for normal users once every three months and for special users having high level privileges, monthly. Furthermore, B1, B2, B4, B5 stressed that they educate their users, including external users, on the proper use of passwords and access rights. B5 stressed that they have well documented and published, which is easily accessible by users. B4 emphasized that technical control were in place to enforce users to use proper password behaviors, but the lower level users share passwords among their peers, which he sees views as an unavoidable challenge.

Then they were questioned about the security of their internal networks. For the question “does your organization practice Network Access Control”, B1, B4 and B5 responded “yes”, while B2 responded with “No” and B3 with no answer. However, B1, B2, B4 and B5 stated that they were isolated sensitive critical systems from normal users in their networks in order to benefit of security of those critical systems.

The next question was on the cryptographic control used. In this question too, B1, B2, B4 and B5 responded by “Yes”, while B3 did not response.

Then they were asked about information systems development. Except B3, others actively answered the questioned areas. Firstly they were asked whether they have provided enough protection to business application source libraries. The answer of B1, B2, B4 and B5 was “yes”. B1 and B2 stressed that since they do not outsource development work outside, and the source libraries are only with their development team who are employees of the bank and they are solely responsible for the protection of source libraries. B4 and B5 stated that though they out sourced their development work partially, they have their own development teams and they play a major role in system development. The spirit of their answers was though they outsource development work, the major critical systems are developed by the internal development team and they are responsible for the protection of those source libraries.

Then they were questioned about change management procedures which is very important in system development and other areas as well. As per the answers of B1, B2, B4 and B5 more or less they are having some control on change management procedures. B5 stressed the importance of having a change management process for systems development. When the user originates the request, it is evaluated by relevant authorities and forwarded to the development team. Depending on the urgency of the change it is prioritized. After the development work is completed, quality assurance process is carried out by the same unit and then it is sent to the audit department to check the change before it is applied in the production environment, then only it goes to the implementation stage. Once implemented, the change management system notifies the requested user, as well as the development team, on this change and it is on live. In B4's case it is not 100% complete change management procedure. Up to some level it addresses change management, especially on application development.

Then they were enquired about the use of licensed software applications. Except B3, others confirmed that they use only licensed software in their banks in order to protect the intellectual property rights and get rid of unnecessary risks by using pirated copies of software.

After that they were asked about the procedure they practice to report and evaluate information security events, weakness, incidents and improvements. Respondents B1, B2 and B5 confirmed having such procedure documented in place. B4 responded that they do not have such procedure documented and the users report information security units when they see such event or anything related to information security. Once they receive such a call, the unit itself logs it in the system and it is difficult to take action taken against those incidents. B3 did not response to the question.

They respondents were enquired about the very crucial area for any business, especially for banks, regarding business continuity, disaster recovery, reviewing, testing and reassessing. All the respondents, including B3, confirmed firmly that have a very strong business continuity plan in place for the use in an emergency or disaster. Respondents B1, B3 and B4 stated that they review test and reassess the plan once a year, while B2 reviews it every six months. B5 stated that to comply with the regulations of the Central Bank of Sri Lanka, they carry out reviewing, testing and reassessing business continuity plan once in every three months.

In order to get an overall idea about their culture and governance, they were asked about the support from their top management teams, especially on financial and attitude backing towards information security project.

The respondent B1 replied with “Excellent”. Moreover, he stressed that they received good attitude support, as well as necessary resources like human and financial extended from top management in order to succeed in the information security project. As per him, their top management sees information security is a very important area to the bank and set the tone and encourage the information security unit and other business units to certify in ISO 27001 standard, which is for information security management systems.

B2 stated that the corporate management's perception on information security has changed for the positive in the near past. Now he sees considerable increase in support and change in their attitudes to succeed in information security project.

B3 sees that their bank having good motivation from top management towards information security. He thinks that setting the tone and example from top to bottom is a unique feature of their bank. Policies from top hierarchies also obey and adhere to those policies set by them; which is a very good measure of the continuity of information security project. This enthusiasm is there from right at the top to very bottom level user. Financial backing for information security is also satisfied, he finally stated.

The respondent B4's case is different. He receives excellent support from the top management from their attitude, as well as financial resources, and they encourage them to register independent professional bodies like "techcert" in order to strengthen information security of the banks. Though the top management set policies right from the very top, the middle management and bottom level employees of other business units view information security as a business of information technology division and do not lend their support much to information security.

The respondent B5 also agreed that their top management's attitude support was excellent. Their support to provide human and financial is also considerably satisfactory. But he sees the need for financial funding to be improved.

As the answer for the question asked about the reporting hierarchy of the information security unit in the bank, all the respondents stated that they kept under information technology division, but they have direct access to top level like managing director or chief information officer for regular updates regarding information security project of the bank, which denotes the top management's requirement to isolate and independent the information security unit.

Finally all were questioned about the obstructions faced by them to improve information security of the bank.

Respondent B1 stressed that he does not see any obstructions existing to resist improvement of information security. Since they are ISO 27001 certified bank. And he added more, the most difficult thing is not obtaining the certificate, but to maintaining it. They have sustained for the first year after having the certification, he sees it is an achievement and it is also evident that it is not an obstruction for information security.

B2 stated that since they are onto information security in the recent past, now information security is becoming a critical necessity and has become a high priority area. In order to expedite the information security rollout across the bank, user awareness is very important. He sees lack of user awareness making some resistance in information security implementations and need to pay more attention to it.

B3 also stated that regular user awareness plays major role in the proper flow of information security, especially when it comes to the implementation of policies and procedures. They are having a steering committee in place to handle the smooth flow of information security of the bank. He sees only user awareness needing more attention and other respondents that he does not see any considerable obstructions to the improvement of information security.

B4 has identified some obstructions to improve information security of their bank. He mentioned two main areas which he sees as real obstruction to information security and needing more attention. The first area he highlighted is support of middle management and users of other business units. He gave an example as evidence for this. Recently they have applied some controls on restricting access of USB memory devices in end user computers. After this exercise they got requests from other divisions asking for this facility. He sees this resistance because users see information security as a disturbance and it is solely information technology's business. The second point he mentioned is lack of user awareness on information security. After the inductions programs, the information security unit does not get proper time to address users on information security on a regular basis. The current practice is to include any information security awareness in information technology training sessions, which is not adequate. There should be a proper awareness program arrangement dedicated for information security.

Respondent B5 sees obstructions for information security as resistant to change user mindsets and difficulties faced in financial approvals in the procurement process. Users and middle managers of other business units are very reluctant see information security as a benefit to the bank, as well as them. It is very difficult to change the mindsets to understand the benefits of information security and treat as positively. He sees the increase of user awareness could change the mind sets of users from negative to positive on information security. On the other hand, he emphasized that the lengthy processes in procurement would delay information security implementations. Moreover, it is difficult to justify some investments, since finance managers ask ROI in numbers which is bit difficult give. Due to these conditions, responsible personnel for information security project get more pressure and are discouraged. In addition, he does not see any major obstructions for information security in their bank and plan to certify it in ISO 27001 in future.

Chapter 6 Conclusions

The purpose of this thesis is to gain a better understanding of the information security challenges faced by the financial sector in Sri Lanka. In order to fulfill the purpose, four research questions were proposed at the beginning. After research and analysis, the four research questions are answered as following:

- Whether the banks have identified information as an asset to secure?

  In the security domain the first step is to identify the valuable assets to security. As per Schou and Shoemaker (2006) “Information is like no other asset: it is intangible; therefore, it cannot be accounted for like car parts or soapboxes. It is valuable: yet it is hard to establish a precise dollar value for knowledge. These two characteristics, lack of tangibility and ambiguous worth, pose a fundamental dilemma for the assurance process because it creates a situation where you are unsure of what to protect”. Therefore without proper knowledge of the actual values of assets, providing security is pointless. Similarly in order to implement information security, firstly the organization should understand its actual value and dependability of the business on information. If the organization is to succeed in this evaluation, definitely they have done the very first step in achieving information security and they could end up with a good information security project in place.

After the research, it was revealed that all the banks used for the sample survey had identified information as an asset to secure and gradually they are achieving good information security. Most banks have placed information at the most critical category in the list of assets which the most valuable to the bank (Schou and Shoemaker, 2006). Favorable actions like top management's tone setting and commitment, investments, allocate necessary resources for information security could be seen from everyone interviewed which is an indication of the identification of actual, intangible value of information.

- What possible risks, threats and vulnerabilities for information security?

The study highlighted some areas which could be vulnerable to the bank's operations as follows:

Some banks are not having a proper information security policy. An effective security policy should be developed based on based practices by addressing all relevant areas, easily accessible through various methods, read, understood and agreed by all employees and enforced by relevant authorities (Whitman & Mattord, 2008). Actually the bank already has a documented information security policy, but it does not address all the areas which should be addressed by an information security policy.

Two banks do not have properly signed NDA’s or confidentiality agreements with all the relevant parties. They see only directly involving parties require these agreements. As per Hagen et al (2008), signing non-disclosure agreements (NDA) with related parties of both internal and external is a necessity. It will be helpful when taking disciplinary action against especially outsourced activities, which could ultimately be vulnerable.

Again one bank does not practice information classification according to their criticalness or confidentialities. Schou and Shoemaker (2006) explains that the, protection for assets can be enabled by classifying and tagging which gives a tangible representation of the items to be secured. Without having a proper classification, running a large scale business is a risk.

Four out of five banks discussed about their weakest arm on information security, which is the lack of user awareness. All of them view this as the major obstruction to improve information security. According to Chen and et al (2006) also it is true: Organizations with lack of awareness could easily be open to security threats and also the lack of awareness can render the sophisticated technological countermeasures useless, which is ultimately vulnerable to the organization.

One bank highlighted the absence of the documented procedure for handling removable media, which could be a threat to banks and its customer’s information. Bragg (2011) explains, having such document will prevent unauthorized disclosure, modification, removal, or destruction of assets. In addition he says there is a widespread lack of any formal procedures for media handling and media disposal, which most of smaller organizations do not have and most of large organizations having such policy, but no proper procedure in place to meet the requirement.

The frequency of user rights reviewing process is low in one bank compared to others, which could be vulnerable by having unnecessary rights to users due to the lack of proper review. Bragg (2011) also shows the purposeless of such practice without having formal across-the-organization review of rights in frequent manner.

One bank does not have a proper change management procedure a bank should have in place due to its criticalness of the business.

Report and evaluate security events, incidents, weakness and improvements are very important in a successful information security project, which one bank does not comply with. A qualitative study within users' experience of information security by Albrechtsen (2007) shows that in general most employees have a low degree of information security awareness since they admitted they contributed with very few actions to strengthen their security. They were not aware of what incidents may cause, did not see what own improvements contribute or their value of their security actions for the organization.

- What measures taken to minimize the impact of shortfalls and vulnerabilities?

The collected data shows that all the banks are already implementing information security. Though they are at different levels of information security practices, all of them attempt to get good information security project in place. The areas like having at least some kind of information security policy and reviewing it, carrying out business risk analysis, signing NDA or confidentiality agreements with employees and other third parties, management and review of user rights, user awareness, usage of licensed software applications and having a business continuity plan and reviewing it frequently shows the readiness of the organizations to minimize and bear the impact of information security vulnerability or a shortfall. As Saint-Germain (2005) explained in his article on ‘Information Security Management best practices’, in order to address all aspects of information security, it is required to implement a more comprehensive approach using methodical compliance framework. Moreover, he mentioned that compliance is not always straightforward. Compliance to government regulatory requirements or framework does not mean that an organization is secured. There should be an approach to go beyond regulation and frameworks and implement security controls appropriate for the specific organization.

- Are there any obstructions to improve information security?

The findings in this study indicate that there are obstructions to improve information security in the interviewed banks. Except one bank, the other four banks talked about the lack of user awareness as an obstruction to improve information security which proves information security cannot succeed only by using technology; it requires hearts and minds of stakeholders to succeed. This is found in the case study of Chen et al (2006), that improving security awareness helps knowledge and correct judgment help prevent human errors and carelessness.

Bibliography

- Abbas H., Magnusson C., Yngstrom L., Hemani A.. (2011). Addressing dynamic issues in information security management. *Information Management & Computer Security*. 19 (1), p5-24.

- Albrechtsen, E., (2007). A qualitative study of users' view on information security. *Computers & Security*. 26 (4), p276-289.

- Alshboul A., (2010). Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks. *Communications of the IBIMA*. 2010 (486878).

- Blyth A., and Kovacich G., (2006). *Information Assurance (security in the information environment)*. 2nd ed. London: Springer-Verlag Ltd.

- Bragg, B., (2011). Common ISO 27001 Gaps. *ISSA Journal*. January (1), p37-40.

- Calder, A., (2009). *Information Security Based on ISO 27001/ISO 27002: A Management Guide.* USA: Van Haren Publishing.

- Calder, A., & Watkins, S. (2006). *International IT Governance: An Executive Guide to ISO 17799/ISO 27001.* USA: Kogan Page.

- Central Bank of Sri Lanka. (2010, 12 25). *http://www.cbsl.gov.lk/*. Retrieved 12 25, 2010, from http://www.cbsl.gov.lk/: http://www.cbsl.gov.lk/

- Chen, C. C., Shaw, R. S., Yang, S.C. (2006). Mitigating information security risks By increasing user awareness: A case study of information security awareness system. *Information Technology, Learning & Performance Journal*. 24 (1), p1-14.

- Commercial Bank of Ceylon PLC. (2011, 02 20). *http://www.combank.net/*. Retrieved 02 20, 2011, from http://www.combank.net/: http://www.combank.net/

- Ernst & Young. (2010). *Global Information Security Survey.* USA: Ernst & Young.

- Fitch Ratings Lanka Ltd. (2011, 02 20). *http://www.fitchratings.lk/*. Retrieved 02 20, 2011, from Fitch Ratings: http://www.fitchratings.lk/

- Gupta, J. N., & Sharma, S. K. (2009). *Handbook of research on information security and assurance.* Hershey, PA: Information Science Reference.

- Hagen J. M., Albrechtsen E. and Hovden J.. (2008). Implementation and effectiveness of organizational information security measures.*Information Management & Computer Security*. 16 (4), p377-397.

- Hagsten, E., (2009). Human capital, information technology and productivity. *In Statistics Sweden, Investments in the Future 2, International Statistical Conference*. Prague, 14-15 September.

- Hall J. H., Sarkani S., Mazzuchi T. A.. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*. 19 (3), p155 -176.

- Harris, S., (2004). *CISSP Certification.* USA: Edinburgh Osborne/McGraw Hill.

- Hatton National Bank PLC . (2011, 02 20). *http://www.hnb.net/*. Retrieved 02 20, 2011, from http://www.hnb.net/: http://www.hnb.net/

- Hone K., Eloff J.H.P. (2002). What makes an effective information security policy. *Network Security*. 2002 (6), p14-16.

- International Standard Organization. (2005). *ISO/IEC 27001:2005 Standard.* USA: International Standard Organization.

- ISACA. (2010). *The Business Model for Information Securit.* USA: ISACA.

- ISO27k infosec management standards. 2011. ISO27k infosec management standards. [ONLINE] Available at: http://www.iso27001security.com. [Accessed 10 February 2011].

- Johnson, M., & Goetz, E. (2007). *Embedding Information Security into the Organization.* USA: Dartmouth Coll.

- Kumar, R. L., Park, S., Subramaniam, C. (2008). Understanding the value of countermeasures portfolios in information systems security.*Journal on Management Information Systems*. 25 (1), p241-279.

- Mizzi, A., (2008). *Return on Information Security Investment.* USA: Lulu.

- National Development Bank PLC. (2011, 02 20). *http://www.ndbbank.com/*. Retrieved 02 20, 2011, from http://www.ndbbank.com/: http://www.ndbbank.com/

- Nations Trust Bank. (2011, 02 20). *http://www.nationstrust.com/*. Retrieved 02 20, 2011, from http://www.nationstrust.com/: http://www.nationstrust.com/

- OSF DataLossDB | Data Loss News, Statistics, and Research. 2011. OSF DataLossDB | Data Loss News, Statistics, and Research. [ONLINE] Available at: http://datalossdb.org. [Accessed 10 February 2011].

- Ponemon Institute. (2010, 01 01). *http://www.ponemon.org.* Retrieved 02 20, 2011, from http://www.ponemon.org: http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf

- Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *The Information Management Journal*. 4 (1), p60-66.

- Sampath Bank PLC. (2011, 02 20). *http://www.sampath.lk/.* Retrieved 02 20, 2011, from http://www.sampath.lk/: http://www.sampath.lk/

- Savage M., (2002). Business continuity planning. *Work Study* . 51 (5), p254-261.

- Schneier, B., (2000). *Secrets and Lies: Digital Security in a Networked World.* USA: John Wiley & Sons.

- Schou, C., Shoemaker, D (2006). *Information assurance for the enterprise: A roadmap to information security*. NY: McGraw-Hill .

- Solms, P. B., (2001). Corporate Governance and Information Security. *Computers & Security* .

- Sullivan, D., (2009). *The Shortcut Guide to Prioritizing Security Spending.* USA: Realtime Publishers.

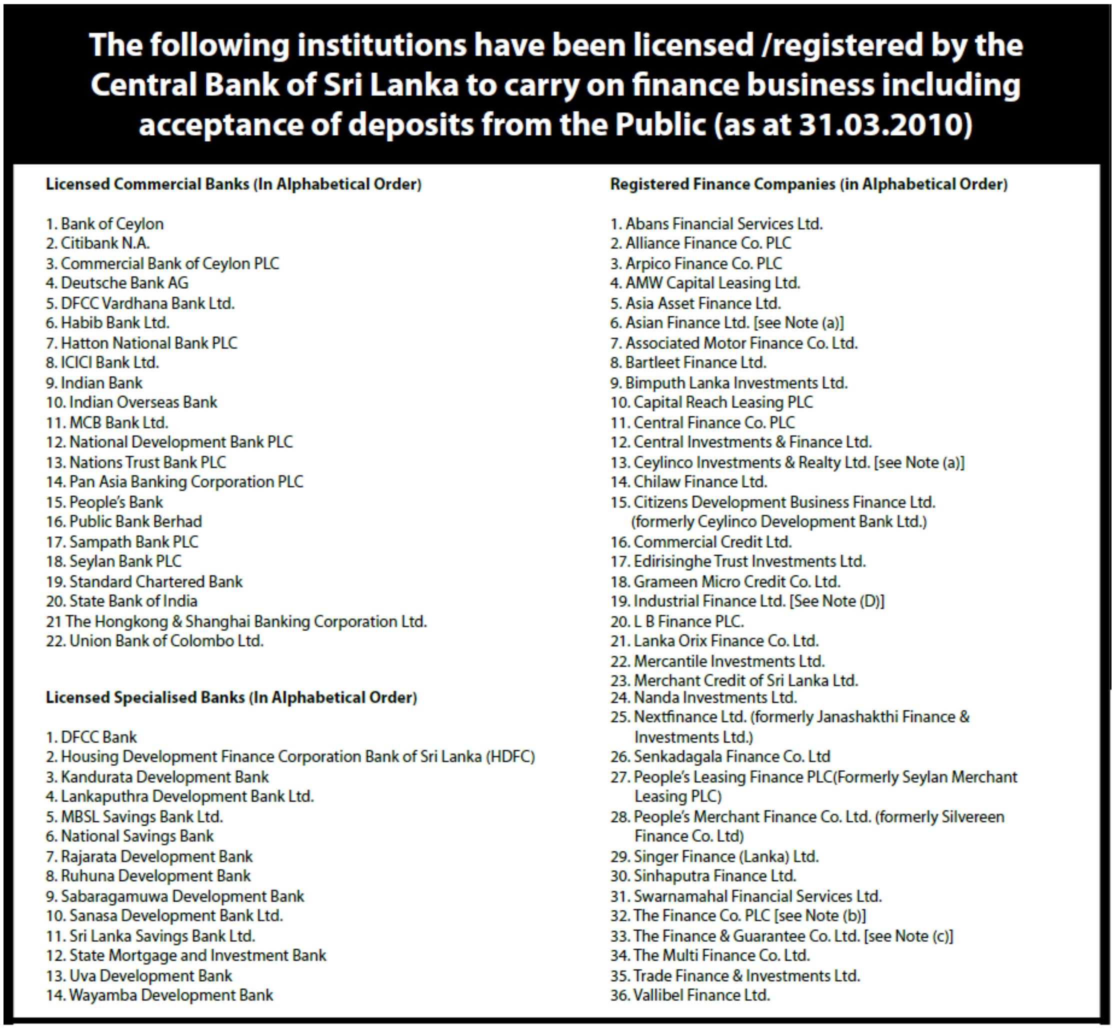
- Verizon Business. (2009). *Data Breach Investigations Report.* USA: Verizon Business.

- Warkentin, M., & Vaughn, R. (2006). *Enterprise information systems assurance and system security: managerial and technical issues.* Hershey: Idea Group Pub.

- Whitman, M. E. and Mattord, H., (2010). *Management of Information Security*. 3rd ed. Boston: Course Technology.

Annexure

List of Banks / financial institutes



The following institutions have been licensed /registered by the Central Bank of Sri Lanka to carry on finance business including acceptance of deposits from the Public (as at 31.03.2010)

Licensed Commercial Banks (In Alphabetical Order)

1. Bank of Ceylon
2. Citibank N.A.
3. Commercial Bank of Ceylon PLC
4. Deutsche Bank AG
5. DFCC Vardhana Bank Ltd.
6. Habib Bank Ltd.
7. Hatton National Bank PLC
8. ICICI Bank Ltd.
9. Indian Bank
10. Indian Overseas Bank
11. MCB Bank Ltd.
12. National Development Bank PLC
13. Nations Trust Bank PLC
14. Pan Asia Banking Corporation PLC
15. People's Bank
16. Public Bank Berhad
17. Sampath Bank PLC
18. Seylan Bank PLC
19. Standard Chartered Bank
20. State Bank of India

21 The Hongkong & Shanghai Banking Corporation Ltd.

22. Union Bank of Colombo Ltd.

Licensed Specialised Banks (In Alphabetical Order)

1. DFCC Bank
2. Housing Development Finance Corporation Bank of Sri Lanka (HDFC)
3. Kandurata Development Bank
4. Lankaputhra Development Bank Ltd.
5. MBSL Savings Bank Ltd.
6. National Savings Bank
7. Rajarata Development Bank
8. Ruhuna Development Bank
9. Sabaragamuwa Development Bank
10. Sanasa Development Bank Ltd.
11. Sri Lanka Savings Bank Ltd.
12. State Mortgage and Investment Bank
13. Uva Development Bank
14. Wayamba Development Bank

Registered Finance Companies (in Alphabetical Order)

1. Abans Financial Services Ltd.
2. Alliance Finance Co. PLC
3. Arpico Finance Co. PLC
4. AMW Capital Leasing Ltd.
5. Asia Asset Finance Ltd.
6. Asian Finance Ltd. [see Note (a)]
7. Associated Motor Finance Co. Ltd.
8. Bartleet Finance Ltd.
9. Bimputh Lanka Investments Ltd.
10. Capital Reach Leasing PLC
11. Central Finance Co. PLC
12. Central Investments & Finance Ltd.
13. Ceylinco Investments & Realty Ltd. [see Note (a)]
14. Chilaw Finance Ltd.
15. Citizens Development Business Finance Ltd. (formerly Ceylinco Development Bank Ltd.)
16. Commercial Credit Ltd.
17. Edirisinghe Trust Investments Ltd.
18. Grameen Micro Credit Co. Ltd.
19. Industrial Finance Ltd. [See Note (D)]
20. L B Finance PLC.
21. Lanka Orix Finance Co. Ltd.
22. Mercantile Investments Ltd.
23. Merchant Credit of Sri Lanka Ltd.
24. Nanda Investments Ltd.
25. Nextfinance Ltd. (formerly Janashakthi Finance & Investments Ltd.)
26. Senkadagala Finance Co. Ltd
27. People's Leasing Finance PLC(Formerly Seylan Merchant Leasing PLC)
28. People's Merchant Finance Co. Ltd. (formerly Silvereen Finance Co. Ltd)
29. Singer Finance (Lanka) Ltd.
30. Sinhaputra Finance Ltd.
31. Swarnamahal Financial Services Ltd.
32. The Finance Co. PLC [see Note (b)]
33. The Finance & Guarantee Co. Ltd. [see Note (c)]
34. The Multi Finance Co. Ltd.
35. Trade Finance & Investments Ltd.
36. Vallibel Finance Ltd.

(Central Bank of Sri Lanka, 2010)