METHODOLOGY FOR PRACTICE OF INFORMATION SECURITY IN SOFTWARE DEVELOPMENT COMPANIES

Edirisinhage Kasun Udara Jayasekara

(169111T)

Degree of Master of Business Administration in Information Technology

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2019

METHODOLOGY FOR PRACTICE OF INFORMATION SECURITY IN SOFTWARE DEVELOPMENT COMPANIES

Edirisinhage Kasun Udara Jayasekara

(169111T)

The dissertation was submitted to the Department of Computer Science and Engineering of the University of Moratuwa in partial fulfillment of the requirement for the Degree of Master of Business Administration in Information Technology.

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2019

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

……………………………….

Edirisinhage Kasun Udara Jayasekara

(Signature of the candidate) Date:

The above candidate has carried out research for the Masters thesis under my supervision.

……………………………….. ………………….

Dr Chandana Gamage Date

Signature of the Supervisor

COPYRIGHT STATEMENT

I hereby grant the University of Moratuwa the right to archive and to make available my thesis or dissertation in whole or part in the University Libraries in all forms of media, subject to the provisions of the current copyright act of Sri Lanka. I retain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

ABSTRACT

When modern organizations are considered, information is one of the most critical assets that need to be protected against external and internal threats. Since there is a massive increase in threats related to information technology applications, information security has become a significant factor. Moreover, information security ensures business continuity and reduce the risk of damage to an organization's reputation. Therefore, internal information security management is a critical factor. There are several factors which affect implementation of information security management. This research is focused on finding out a methodology for information security management in software development companies. To achieve objective information security governance, senior management support and organizational culture factors impact on information security management in software development companies are comprehensively studied. Furthermore, existing management models such as plan, do, check and act model, maturity models, etc., were analyzed to understand its applicability to information security management. An online questionnaire was developed based on three major factors identified during the literature review and shared with Associate technical leads, Technical leads, Software architects, Project managers, Delivery managers, Information Technology managers and Heads of IT in the software industry to represent the information security decision makers in an organization. Collected data was analyzed quantitatively using a statistical tool.

The research results have shown a strong positive relationship between information security governance and senior management support with information security management. Whereas Organizational culture has a very weak relationship with information security management. According to the research results, PDCA can be recommended to manage information security in Software development organizations.

Keywords: Information security, Information security governance, Information security management, Organizational culture, PDCA Model

ACKNOWLEDGEMENT

I wish to express my sincere gratefulness to Dr Chandana Gamage, for the great support, inspiration and guidance gave me to complete this research study as my research supervisor. This research study may not be possible unless his guidance and kindness offered to me. Then I have to express my sincere gratitude to Ms Jeeva Padmini for the support and the kindness offered to me throughout this study. I sincerely thank all the academic and non-academic staff of the University of Moratuwa who supported me throughout this time period.

I have to express my gratitude to all respondents from different IT organizations of Sri Lanka, for responding to my research questionnaire by spending their valuable time. Then I would like to be thankful to fellow students of my MBA program for great support offered me by sharing their knowledge.

Finally, I have to express my sincere thank to my parents and my loving wife Dr Upulsara Jayawardhana for helping me every way that they can.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	**Description**
BDIM	Business Driven Information technology Management
BSC	Balanced Scorecard framework
CMMI	Capability Maturity Model Integration
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and related Technologies
CSI	Crime Scene Investigation
FBI	Federal Bureau of Investigation
IDEAL	Initiating, Diagnosing, Establishment, Acting and Learning
ISG	Information Security Governance
ISM	Information Security Management
IT	Information Technology
NIST	National Institute of Standards and Technology
OC	Organizational Culture
OPM3	Organizational Project Management Maturity Model
PDCA	Plan, Do, Check and Act
QIP	Quality Improvement Paradigm
ROI	Return On Investment
SLASSCOM	Sri Lanka Association of Software and Service Companies
SMS	Seiner Management Support
SRE	Secure Requirement Engineering
SSE-CMM	System Security Engineering Maturity Model

1. INTRODUCTION

1.1. Background

When modern organizations are considered, information is one of the most critical assets that need to be protected from inside and outside threats. It is essential to ensure that correct information is made available to relevant people at the particular place and at the right time. That means it is necessary to ensure the confidentiality, availability and integrity of the information. If a particular organization cannot control the above-mentioned three factors, it could cause serious damage to the reputation of the company.

Due to the massive increase in the use of information technology applications, information security has become a major concern when starting to plan and manage a modern enterprise (Chang & Lin, 2007). Security of the information becomes a critical factor because of the value generated by the information related to the given organization. Due to this particular context, the information security management is one of the critical objectives to be concerned in present business domain (Kajava et al., 2006).

Strong security products or technology alone cannot protect an organization without a good management policy and implementation. Therefore, information security should not be considered only as a primarily technical subject area. Therefore, information security should primarily be considered as a management related issue and furthermore it cannot be restricted only for company internal factors (Chang & Chienta, 2006).

When some incidents related to information security are examined, it is evident that there are some internal organizational factors affected by these incidents. Information security management cannot be isolated from other business practices because it has a direct or indirect relationship between other business components inside the organization. Information security has a multifaceted nature. Due to that reason it directly interacts with multiple social and business functions (Anttila & Varonen, 2006). This fact was highlighted by Woodhouse (2008) when he stated "Information security culture is a part of the organizational culture and defines how an employee sees the organization".

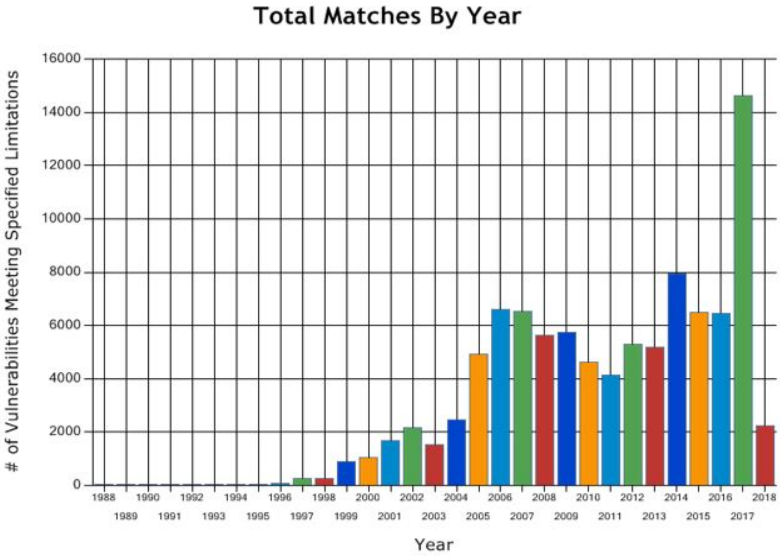
There is a direct relationship between business continuity management and information security management. Chang et al. (2006) stated that "information security management protects information from a wide range of threats in order to ensure business continuity, minimize business damage, and maximize return on investments". Finally the output of information security management ensures business continuity and minimizes the business damage. As a result it will maximize the return on investment.

There are several business segments listed under the domain of information technology. Such as,

- Software development
- Networking and telecommunications
- Hardware
- Maintenance and hosting
- Operational support
- Information security services

There are considerable deviations among these major categories. Every category has it’s own management structure, income generation model, technological model, daily activates, a category of employees etc. Software development is one of the major segments in the information technology industry. Moreover, software development has its own industry-specific behaviors than other segments in the IT industry. This research study focused on information security related to software development companies.

Many security vulnerabilities are caused unintentionally in design and development stage of software (Humphrey et al., 2004). According to a primary analysis conducted by the Computer Emergency Response Team Coordination Center (CERT/CC), most of the software-based vulnerabilities were occurred due to common reasons. Furthermore, Figure 1.1 NIST: US Department of Commerce analyzed and measured the information security vulnerability occurrence between the years of 1988 to 2018.



Source: Adapted from ENISA (2018)

Figure 1.1 Number of reported vulnerabilities between 1988 to 2018

According to these statistics, there is a massive increase of reported vulnerabilities. Thus, it automatically generates a greater requirement of information security as well as information security management.

1.1.1. Motivation

It is essential to avoid the internal information security management problems to obtain uninterrupted business continuity. Information security management frameworks/guidelines are playing a considerable role in certifying and managing organizational information security and these information security management guidelines are providing best practices required to modern organizations (Siponen & Willison, 2009).

Direct relationship between business continuity management and information security management could be one of the motivational factors for this study. Chang & Bruce (2006) highlighted that "ISM protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments". The final outcome of this research will be affected to the return on investment (ROI) of any software development company.

1.1.2. Research scope

It is essential to find how frameworks/guidelines are applicable to information security management. By integrating information security guidelines, organizations can illustrate their commitment to make their business environment secure (Siponen & Willison, 2009). Therefore firstly, the topic is narrowed down by investigating how information security management frameworks/guidelines use for software development.

Secondly, this investigation focuses in to,

- How PDCA (Plan-Do-Check-Act) model is related to information security management in software development companies.
- How Capability Maturity Model Integration (CMMI Model) is related to information security management in software development companies.

1.2. Problem Statement

There are three major problems being addressed through this research.

1. The initial problem is to find out how information security management is done in software development companies.
2. The second problem is to find out how to manage information security in software development companies. Therefore it is necessary to focus the direction of the research into information security management frameworks.

3. Finally, it is required to find out how to integrate information security management into a software development business by considering following questions.

- How is information security management done in software development companies?
- What aspects of the information security management strategy/framework/methodology are vulnerable to information security issues?
- How to integrate information security management into a software development business?

1.2.1. Research Objectives

Three main research objectives are given below.

- Find out how information security management is done in software development companies.
- Find out how information security management strategy/framework/methodology are vulnerable to information security issues.
- How to integrate information security management into a software development business.

1.2.2. Research significance

It is essential to identify how information security is used software development companies, and how it is managed within the organization to ensure business continuity. Ensuring business continuity is essential to provide uninterrupted service to the customer. Information security management frameworks and certain best practices are required to eliminate risks related to information security. It is also important to find out how information security management frameworks are vulnerable for information security issues. Therefore, the information security is one of the significant factors when we are managing an organization. Ultimately software development companies will be benefited by implementation of relevant information security management frameworks.

2. LITERATURE REVIEW

2.1 Introduction

Information security has become one of the critical factors to be concerned when administrating a modern business. It is very difficult to guarantee the long-term success of an organization without implementation of information security (Asri et al., 2011). Information security management activity safeguards information from both internal and external threats to guarantee and ensure business continuity in order to provide uninterrupted service to the customer. Finally it maximizes the return on investments (Chang & Ho, 2006). Therefore, a properly managed information security mechanism needs to be established in an organization.

Information security is not just a technical issue. Many non-technical factors such as social, business, regulatory, etc. are also related to information security management based on business context (Solms & Solms, 2004). According to the multidisciplinary nature of modern business, stakeholders related to the information security are expanding. In addition, external attackers are making use of mistakes created by the internal employees in their activities.

Information security management frameworks, standards, models and best practices play a major role in information security management of any organization. Information security management standards produce a common understanding of information security requirements. Finally it ensures and merges with globally accepted rules and guidelines (Aggeliki & Kokolakis, 2010). Developing a company-specific information security control mechanism is highly complicated and it requires specific knowledge and resources. Most of the companies do not have such capabilities inside their organizations. This context creates a greater demand for information security standards (Chang & Ho, 2006).

Through an analysis of existing studies related to information security in management literature, 15 major factors were identified, which affected to information security management. These factors are given in Table 2.1 with the frequency of appearance in literature referenced in this study.

Table 2.1 Identified factors related to information security management

No	Factors	Frequency
1	IT Competence of business managers	1
2	Environment uncertainty	2
3	Industry type	3
4	Organizational size	4
5	**Organizational culture**	8
6	Task Conflict	1
7	Ambiguity	1
8	Resistance to change	1

9	Lack of work instructions	1
10	Over-attention to performance compared to process improvement	2
11	**Information security governance**	3
12	Policies	3
13	Direction	2
14	Continuous Monitoring	4
15	**Seiner management support**	6

Among these 15 factors that affects to information security management, two major factors were selected based on frequency (Organizational culture and Senior management support). Information security governance is critical for the organizational wide effectiveness of information security (Ozkan & Karabacak, 2010). In addition to that information security governance contains policies, directions, continuous monitoring, etc. Considering that factor, information security governance was selected as the third factor. Based on above identified and selected factors, a conceptual framework was developed, having following independent variables:

- Organizational culture
- Information security governance
- Senior management support

2.2 Independent variables

2.2.1 Senior management support

A considerable number of significant factors affect the implementation of information security inside an organization. Although information security is a critical factor for an organization, the execution decision of the information security is in the hand of top-level management. Return on investment (ROI) is making a significant impact on that particular decision made by top-level management. One of the most significant problems related to information security is that it cannot directly exhibit the return on investment (ROI). In this context, IT managers are facing a difficult situation when a discussion requires to be take into the senior managerial level.

According to the most recent IT key metrics data from Gartner (2016), organizations spend an average of 5.6% of their total information technology budget specifically for information security related tasks. This fraction of the total information technology budget allocation is a significant amount of the total budget of the company. In this context, IT managers need to confine inside their margin on the way to implement information security.

Top-level management support is one of the critical factors for the successful implementation of the information security standards (Stambul & Razali, 2001). It has been noted that the information technology competency of the top-level management positively affects the implementation of proper information security management mechanism in an organization (Chang & Ho, 2006). "Risk-based thinking" is also one of the critical factors that top-level management should practice to cater for their strategic leadership and commitment to implement information security management standards (Barafort et al., 2016).

According to the research conducted by the Indian Institute of Foreign Trade, information security governances in IT outsourcing companies have a direct impact on the information security service quality (Bahl & Wali, 2014). Further, this research has pointed out that if information security governance considers as a part of the cooperate governance of the company then it will create a significant impact on the overall information security service quality. Finding information security governance as a part of the cooperate governance by senior management and obtaining their support is a crucial factor. On the other hand, it is essential to avoid internal problems related to information security and there should be a broad awareness among organizational hierarchy to identify what are the tasks and responsibilities related information security. Hence senior managerial support is necessary to accomplish that task.

2.2.2 Organizational culture

Kajava et al. (2006) state that "Information security is strongly a cultural issue". Organizational culture is considered as an intermediate factor between corporate management and employee behaviours. It has been noted that flexibility oriented organizational culture creates an unfavourable condition to information security management while control-oriented organizational culture creates a favourable condition to information security management implementations (Chang & Lin, 2007). To achieve information security corporate culture must be changed accordingly and employees must participate in the process (Ozkan & Karabacak, 2010).

Since information security has a multidisciplinary nature it can be divided into three significant categories called technical category, management category and organizational category (Solms, 2000). Corporate culture comes under the third category. Organizational culture reflects how human interaction affects the information security. Not withstanding how advanced the technical infrastructure plan to protect organizational assets and how committed the management to guarantee the implementation there is one additional factor remaining to make it realistic, which is organizational culture. That is because the organizational culture is an integral part of the plan designed and developed by management and technically related employees. To make information security implementation realistic, information security culture should be considered as a part of the organizational culture (Stambul & Razali, 2011).

Security awareness of the employees is a positive factor to improve information security culture. Furthermore, information culture comprises of social and ethical requirement to be addressed since it includes socio-ethical awareness related to information security (Eloff & Eloff, 2005). These conditions will produce the required platform for high quality information security management.

As information security culture is considered as a sub-part of the organizational culture and organizational culture means collections of learned things from experience (Woodhouse, 2008), a particular relationship can be identified between information security management and organizational culture.

2.2.3 Information security governance

Information security governance is a process of administrating an organization to achieve its business objectives and strategies by establishing, retaining and fine-tuning information security culture, learned from previous lessons and assigning roles and responsibilities to relevant peoples to perform required actions (Alves et al., 2006). Information security governance is a responsibility of operational and technical managers as stated by Williams & Andersen (2001). Furthermore, involvement of senior management is also a significant factor. Governance means that the board of directors understand the risk and identify relevant opportunities to mitigate and manages those risks.

According to Abu-Musa (2010), corporate information security governance contain a set of activities and responsibilities including,

- Complete responsibility for stakeholders
- Satisfying legal requirements related to information security
- Establishment of security policies
- Organization-wide information security awareness and education
- Assigning accountable roles and responsibilities related to information security within the organizational structure.
- Disaster recovery planning
- Establishing best practices and standards

Abu-Musa (2010) also stated that there are five expected primary outcomes from information security governance establishment.

1. Build up strategic alignment with information security and organizational business strategy to achieve overall business objectives.
2. Safeguarding critical information assets from potential threats.
3. Information security resources are managed by utilizing knowledge and resources.
4. Continuously observing to identify that organizational objectives are achieved by implementing information security governance.
5. Verify that expected outcome has been gained by implementing information security governance.

According to existing literature, information security governance is responsible for overall information security management in an organization. Existing IT governance frameworks can be used to guarantee smooth integration of information security governance with business strategies and objectives (Alves et al., 2006). The IT governance frameworks used widely in the industry are as follows:

- Balanced Scorecard (BSC) framework is responsible for integrating company vision and mission aligned with four major factors. They are financial, customer, Internal business management and learning/growth. BSC is a strategic planning and management system.
- Control Objectives for Information and Related Technologies (COBIT) is working as an intermediate glue between strategic planning and information technology solution implantation. Also, COBIT 5 is responsible for explicit policy creation and best practices.
- ISO/IEC 38500:2012 is a standard for corporate governance of information technology that provides a framework for top-level management to use it while valuating, directing and monitoring the organization (Alreemy et al., 2016).

2.3 Information security management models

Humphrey et al. (2004) stated that, "producing secure software requires several management actions". Therefore, information security models are essential to strengthen those management actions. In this study PDCA model and Maturity models were proposed to manage information security particularly in Software development companies.

2.3.1 PDCA Model

PDCA model (Plan, Do, Check and Act) was invented by W. Shewhart representing Bell Labs in 1930. Other than PDCA model, there are some well known process improvement methods exist such as IDEAL (Initiating, Diagnosing, Establishment, Acting and Learning) and QIP (Quality Improvement Paradigm) (Seong & Kim, 2004). PDCA is a classic quality management technique, which was promoted and practiced in Japan (Ning et al., 2010). PDCA model is currently used to achieve several industry-based objectives such as,

- Business-driven IT management (BDIM) practices
- Software quality improvement/management
- Information security management
- Continuous process improvement
- Organizational performance management

Kajava et al. (2006) stated that ISO/IEC 27001 recommended PDCA model for information security management with process management model, and ISO/IEC 27001 is explicitly referring PDCA model for information security management.

In a research conducted by University of Aegean and University of Piraeus, PDCA model has been used as a four-layer framework to interconnect existing information security standards, frameworks, guidelines, etc. (Tsohou et al., 2010). This framework is practically implemented to enhance, manage and consolidate information security related to a payroll system used by public servants in several government departments. Furthermore, PDCA model is useful for continuous process improvement in an organization.

Plan phase

Plan phase is responsible for information security policy establishment (Eloff & Eloff, 2005). According to Qing-ling et al. (2008), plan phase can be broken down into four major categories related to information security.

1. To analyze the current situation related to information security inside an organization and find out existing problems.
2. To find out the incidents behind information security problems.
3. To identify the information security factors related to those incidents.
4. To create a risk treatment plan according to identified factors related to information security incidents.

According to Tsohou & Kokolakis (2010), context establishment, risk assessment and risk treatment are the major segments of the plan phase.

1. Context establishment

System boundaries and limitations are determined in this particular phase. Under this system boundary identification, all the hardware, software, sub-systems, interconnection between external systems, human resources related with the system, legal frameworks, different types of data related with the system, etc. are recorded in detail.

2. Risk assessment plan

Risk assessment plan contains a detailed description of the identified risks, including risk evaluation criteria.

Table 2.2 Risk assessment plan

Risk	Possibility of occurrence	Level of vulnerability	Assets	Impact to the organization
Network failures	High	High	Organizational Servers	Temporary loss of availability
Unauthorized access to HRM system	Law	Medium	HRM Database and HRM System	Loss of availability/HRM management problems

Application software failures	Medium	High	Payroll application	Loss of availability/ Unwanted information reveal

Next step is a creation of risk treatment plan. This step include mechanisms to avoid identified information security threats.

3. Risk treatment plan

According to Tsohou & Kokolakis (2010) a risk treatment plan contains several controllers as listed below:

1. Organizational security policy
2. Assets management plan
3. Human resource security management plan
4. Physical working environment security management method
5. Communication and operational security management plan
6. Access control management policy
7. Incident management policy related to information security
8. Ensuring business continuity management
9. Compliance

After completion of the above listed three major steps, the plan phase of the PDCA model is completed. Overall, the plan phase is responsible for identifying all controllers and procedures required to implement information security policy.

Do phase

Do phase is responsible for implementation of identified procedures and controllers. According to Qing-ling et al. (2008), Do phase carries out the plan and measures which required to implement information security.

Check phase

Check phase is responsible for verify whether everything has happened according to the plan. Following two steps are required complete this particular phase.

1. Independent evaluation mechanism can be established based on the combination of user feedbacks.
2. Audit logs can be monitored periodically to check whether unusual situation is going on.

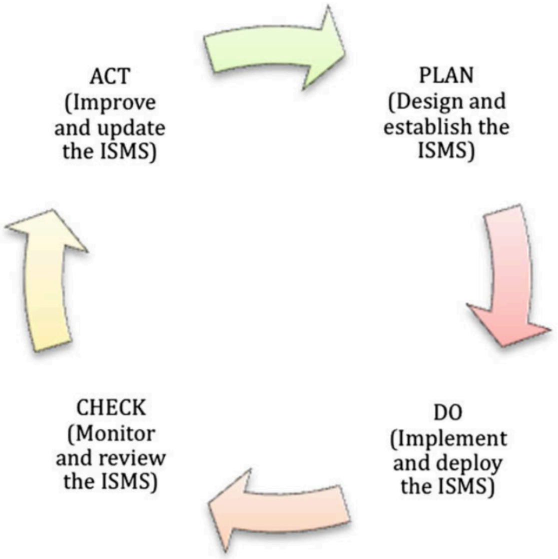
Act phase

The final phase of the PDCA model is responsible for maintaining information security management process by initiating corrective and preventive actions. It is required that IT Managers communicate those actions with all relevant stakeholders related to the organization to clarify whether their intended objectives are achieved

(Aggeliki & Kokolakis, 2010). In addition following two activities can be used as best practices.

1. Summarize the experience, and achievements related to PDCA round.
2. Put the remaining problems that have not been solved yet into a new PDCA cycle.

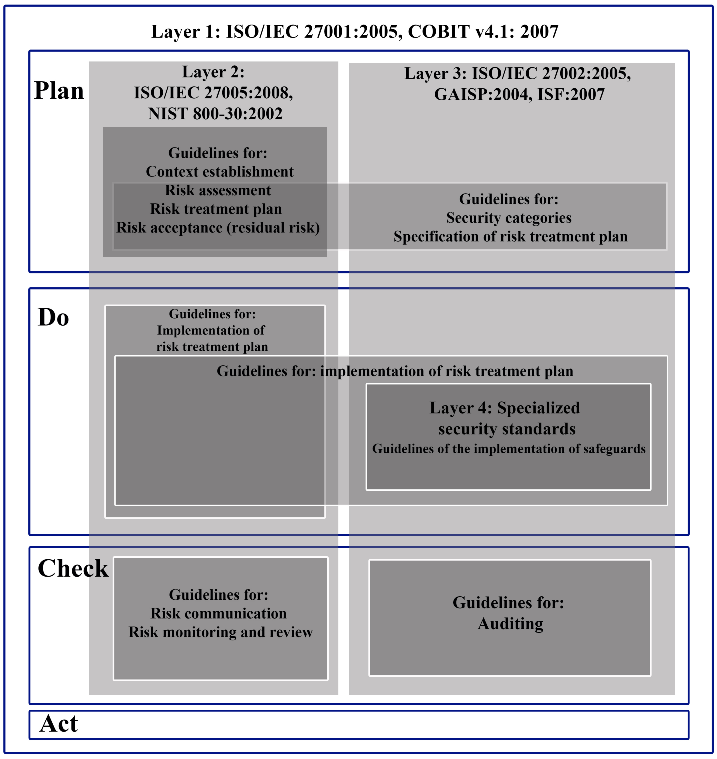
Formats of PDCA model



Source: Adopted from Humphreys (2008)

Figure 2.1 General implementation of PDCA model

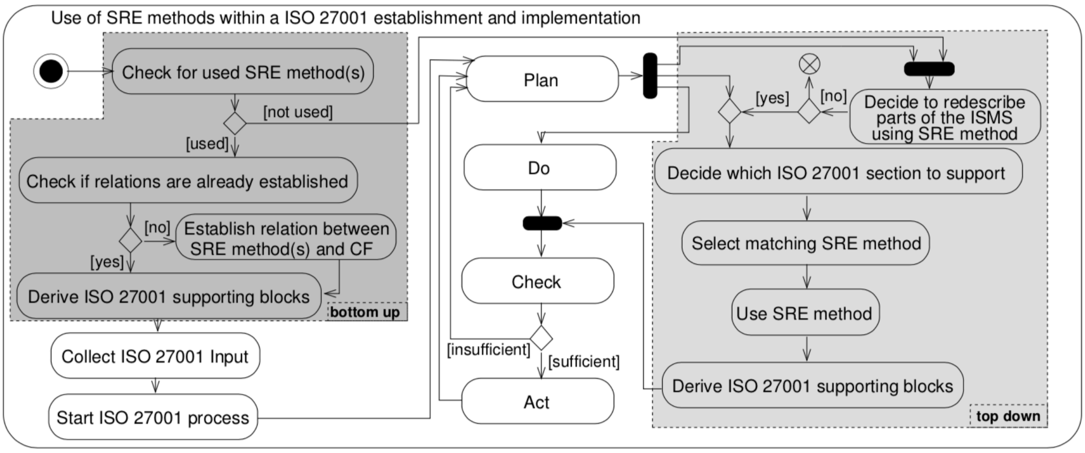
Figure 2.1 explains the general implementation of the PDCA model related to the information security. According to the Figure 2.1, PDCA model directly used without having any modification to the existing structure of the model.


Layer 1: ISO/IEC 27001:2005, COBIT v4.1: 2007
Plan
Layer 2: ISO/IEC 27005:2008, NIST 800-30:2002
Layer 3: ISO/IEC 27002:2005, GAISP:2004, ISF:2007
Guidelines for: Context establishment Risk assessment Risk treatment plan Risk acceptance (residual risk)
Guidelines for: Security categories Specification of risk treatment plan
Do
Guidelines for: Implementation of risk treatment plan
Guidelines for: implementation of risk treatment plan
Layer 4: Specialized security standards
Guidelines of the implementation of safeguards
Check
Guidelines for: Risk communication Risk monitoring and review
Guidelines for: Auditing
Act

Source: Adopted from Tsohou & Kokolakis(2010)

Figure 2.2 Four-layer model for information security management

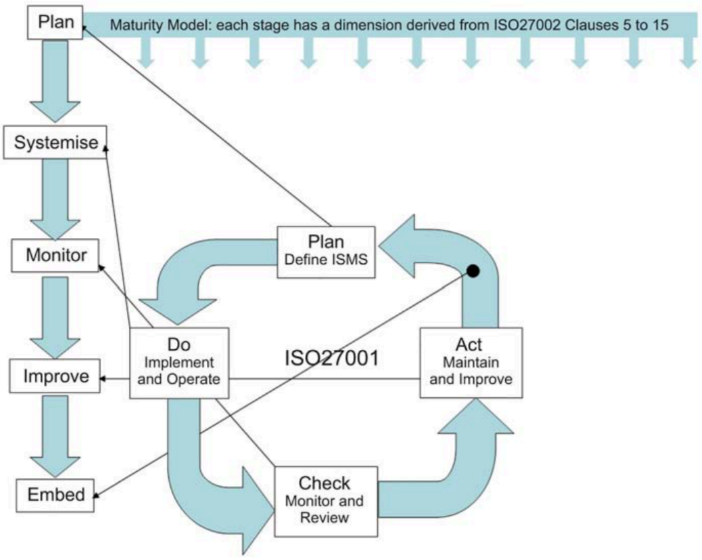
PDCA model is used to achieve different objectives related to management. As discussed earlier, this model can be used to manage overall information security inside an organization. Figure 2.2 shows a four-layer model used to manage overall information security related to information system. Given four layer model is practically used manage government payroll system in Greece.


Use of SRE methods within a ISO 27001 establishment and implementation
Check for used SRE method(s)
[not used]
[used]
Check if relations are already established
[no]
Establish relation between SRE method(s) and CF
[yes]
Derive ISO 27001 supporting blocks
bottom up
Collect ISO 27001 Input
Start ISO 27001 process
Plan
Do
Check
[insufficient]
[sufficient]
Act
[yes]
[no]
Decide to redescribe parts of the ISMS using SRE method
Decide which ISO 27001 section to support
Select matching SRE method
Use SRE method
Derive ISO 27001 supporting blocks
top down

Source: Adopted from Beckers & Heisel (2012)

Figure 2.3 IS0 27001 establishment using PDCA model

According to the Beckers & Heisel (2012), PDCA model can be applied to achieve ISO 27001 information security management standards. Figure 2.3 shows the relationship between ISO 27001-information security certification process and the PDCA model. In this particular diagram, white colour boxes represent the basic steps required to complete ISO 27001 process. The light-grey area located on the right-hand side represents the top-down use cases. As well as while the dark-grey area located on left-hand side represents the bottom up use cases. Here the top-down use cases support the most critical parts of ISO 27001-process. According to Beckers & Heisel (2012), bottom-up use-cases are for the existing/previous activities analyzing. For an example, under this approach if there is any previous documentation related to an information security management system, bottom-up use-cases are responsible for checking whether that documentation is compatible with the current mechanism.



Source: Adopted from Gillies (2011)

Figure 2.4 PDCA model for incremental approach

According to a research conducted by Gillies (2011), there is a five-stage model that is best suited for medium scale organization’s information security management. This model is called five stages of information security (5S2IS), and the purpose of this model is to encourage medium scale companies, which are not mature enough to implement ISO 27001-information security certifications.

According to Humphrey (1989), 5S2IS model is based on ISO 27001, ISO 27002 and CMM model, while CMM is supporting for improvements and evolutions. Figure 2.4 explains how 5S2IS model’s five stage of development is related to PDCA model. This particular approach provides benefits to medium scale organizations by,

- Motivating staff by successful achievement of milestones.
- Manage internal company conditions to create a clear pathway to obtain ISO 27001 information security certifications.

Newly established organizations can clear their pathway to adopt information security certification like ISO 27001 by using this model. This particular model is essential to this research study because it is a combination of both information security maturity levels and PDAC model.

2.3.2 Maturity models

Mayer & Fagundes (2009) stated that, “Maturity model works as a guide to the organization in such a way that the company is able to locate where it stands”. Also, maturity models provide an essential foundation and guidelines for continuous process improvement. Organizations allocate required budget and effort to establish policies and guidelines related to information security but security breaches are continuously happening. Therefore, organizational management needs to identify what is current level of information security that is being implemented. According to Mayer & Fagundes (2009) following maturity models are highlighted.

- Control Objectives for Information and related Technologies (COBIT)
- Organizational Project Management Maturity Model (OPM3)
- Capability Maturity Model (CMM)
- National Institute of Standards and Technology Maturity Model (NIST)
- System Security Engineering Maturity Model (SSE-CMM)

2.3.2.1 Capability Maturity Models

According to Humphrey et al. (2004), three major capability maturity models were highlighted as follows:

- Capability Maturity Integration (CMMI) is related to project management, process development, system engineering and software development.
- System Security Engineering Capability Maturity Model (SSE- CMM) is directly related to information security management in software systems.
- Integrated Capability Maturity Integration (iCMM) is responsible for supplier management and top to bottom enterprise-wide development. Also, iCMM is practically used by department of United States Federal Aviation.

2.3.2.2 Capability Maturity Model Integration (CMMI)

CMMI was developed by Carnegie Mellon University based on previous CMM (Capability Maturity Model) model. CMMI contains five major maturity levels as follows:

1. Initial	-	Situation is unpredictable
2. Repeatable	-	Basic Project Management
3. Defined	-	Process standardization
4. Quantitative	-	Quantitative management
5. Optimizing	-	Continuous process improvement

There is lack of evidence to prove Capability Maturity Model Integration (CMMI) is useful for information security management. It has been noted, there are other maturity models exist to manage information security. Therefore, in this study the close attention is paid to other maturity models that can be applied to information security management.

2.3.2.3 Relationship between maturity models and the information security

According to Asri et al. (2011) there are three major maturity models can be identified for information security management. These maturity models are described in Table 2.3.

Table 2.3 Maturity models required to information security management

Maturity model	Levels	Focus
SSE-CMM model	1.Conducted informal design 2. Planned and tracked 3. Well defined 4. Quantitatively controlled 5. Continuous improvement	Safety of the design engineering software
COBIT model	0. Non-existent 1. Initial/ad hoc 2. Repeatable but intuitive 3. Defined process 4. Managed and measurable 5. Optimized	Specific audit procedures

NIST model	1.Policy 2.Procedure 3.Implementation 4.Testing 5.Integration	Documentation

According to Asri et al. (2011), these three maturity models have a significant effect on information security management. Furthermore, SSE-CMM model is providing best practices and guidelines related to information security, but it doesn't offer a roadmap to achieve that objective. Also, this model provides the required support to develop secure software systems.

Control Objectives of Information Related Technology (COBIT) was designed and created by information system audit and control association. COBIT is responsible for auditing IT process, practices and controls (Mayer & Fagudes, 2009). COBIT was originally developed for targeting Information technology community. When COBIT model has become stable, general management concepts also added to this model (Sahibudin et al., 2008).

Computer security resource center (CSRC) also introduced a maturity model called NIST (National Institute of Standards and Technology) maturity model. It has been noted that, this model also contains five levels of maturity called policies, procedures, implementation approach, testing procedure and integration. This maturity model is supporting detail documentation related to information systems.

SSE-CMM model is responsible for security engineering and software design while COBIT model is responsible for software auditing procedures. Finally, NIST model is responsible for focusing on levels of documentation. Combination of these three major maturity models can do a quality information security management because there are three different areas covered by each particular model.

2.4 Summary

According to the reviewed literature, 15 major factors were identified, which affected to information security management. These factors are given in Table 2.1 with the frequency of appearance. According to previous studies, PDCA model is used to accomplish a wide variety of aspects such as performance management, software quality management, information security management, process management, etc. Information security management is one of the critical aspects among this set. There are several maturity models that can be applied for the context of information security management according to the previous studies. CMMI is not comprehensively used for the area of information security management. As it is stated, there are specific strengths and weakness related to each maturity model. As

Table 2.3 presented combination of maturity models will be the best practice for the overall information security management in any Software development company.

3. RESEARCH METHODOLOGY

3.1 Introduction

The research presented in this thesis has been conducted using a survey approach using quantitative research techniques. This study focuses on finding out answers to three main research questions. Research methodology is the pathway to find answers to these research questions. The particular research questions and the means of finding answers to these questions used in the research are given below.

1. Identify how information security management is done in software development companies.

To answer this question an online questionnaire based survey was conducted and the questionnaire was distributed among high ranked employees of the selected software development companies.

2. Find out what aspects of the information security management strategy/framework/methodology are vulnerable to information security issues.

The method adopted for finding answers to this particular question was a combination of an extensive literature review and analysis of the data obtained through the online questionnaire.

3. Identify how to integrate information security management into a software development business.

The answer to this question was based on the in-depth analysis of literature.

3.2 Research design

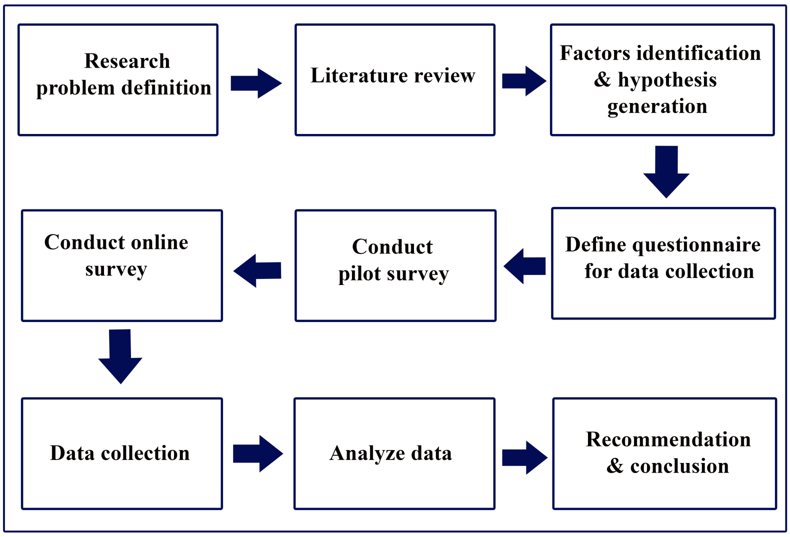

Research problem definition
Literature review
Factors identification & hypothesis generation
Define questionnaire for data collection
Conduct pilot survey
Conduct online survey
Data collection
Analyze data
Recommendation & conclusion

Figure 3.1 Research methodology

According to Figure 3.1, this research study initiated from problem definition by finding out the specific problems that need to be addressed. As a result of that, above mentioned three significant objectives have been defined.

The second phase of this approach is to conduct a comprehensive literature review. This helps to answer two major research questions. The comprehensive literature review is based on journals articles. Based on the results made by the comprehensive literature review, identified factors were categorized based on the frequency of appearance. According to the Table 2.1 among all these factors, three significant factors were selected based on frequency and relevance. Based on those identified factors research hypothesis were defined.

To validate research hypothesis there are 17 close-ended multiple-choice questions distributed among a sample of participants to collect required data for quantitative analysis. These questions are representing one dependent variable and three independent variables.

A pilot survey was conducted by sharing online questionnaire among a selected group of employees. After analyzing the results of the pilot survey, required modifications were done to the questionnaire. Then, the modified questionnaire was distributed among the target sample.

The final step of this process was to gather the required quantitative data from the target sample. With the gathered quantitative data a comprehensive statistical analysis has been done to validate the relevant research hypothesis.

3.3 Conceptual Framework

Through the literature review, 15 factors were identified, which has an impact on information technology management. Those factors and their frequency of appearing in literature is shown in Table 2.1.

As shown in Table 2.1, organization culture (8) and senior management support (6) are the most discussed factors out of 15 factors. Rest of the factors have low frequencies (Less than 5) of appearance. Moreover, since information security governance is critical for the organizational wide effectiveness of information security (Ozkan & Karabacak, 2010) and as information security governance contains policies, directions, continuous monitoring, etc. information security governance was selected as the third factor.

The conceptual framework was developed considering ‘Organization culture’, ‘Information security governance’, ‘Senior management support’ as the independent variables and Information security management as the dependent variable.

Thereafter, face-to-face discussions were conducted with subject matter experts and other industry experts to validate the identified three factors. Further, social media were used to understand the industry awareness of those three factors.

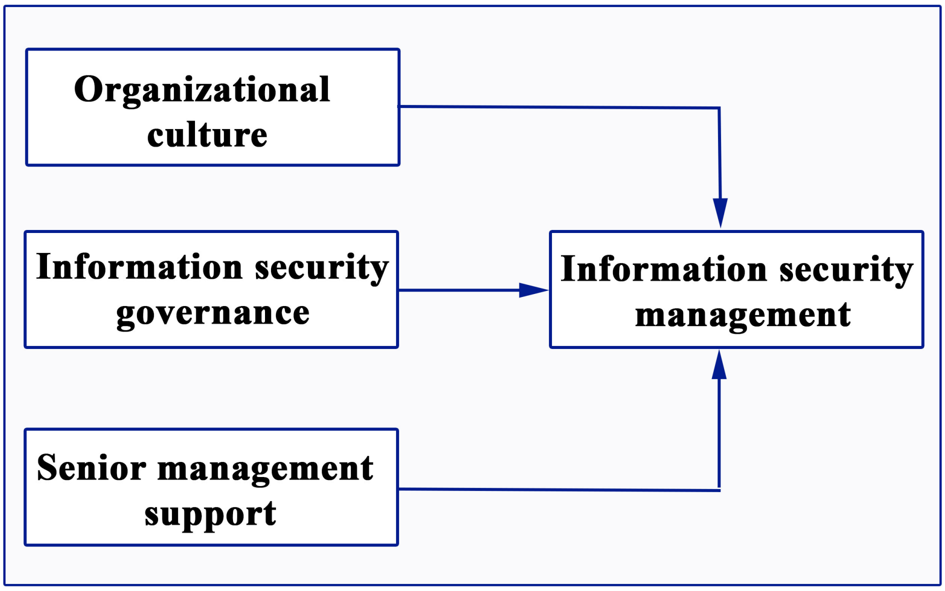

Organizational culture
Information security governance
Senior management support
Information security management

Figure 3.2 Conceptual framework

Table 3.1 Mapping table for objectives, factors and questions

Objective	Factors	Question number
1. Find out how information security management is done in software development companies.	Information security governance	10,11,12,13,14
	Information security management	8,9
2. Find out how information security management strategy/framework/methodology are vulnerable to information security issues.	Organizational culture	5,6,7
	Information security governance	10,11,12,13,14
	Information security management	8,9
3. Find out how to integrate information security management into a software development business	Information security governance	10,11,12,13,14
	Senior management support	15,16,17,18
	Information security management	8,9

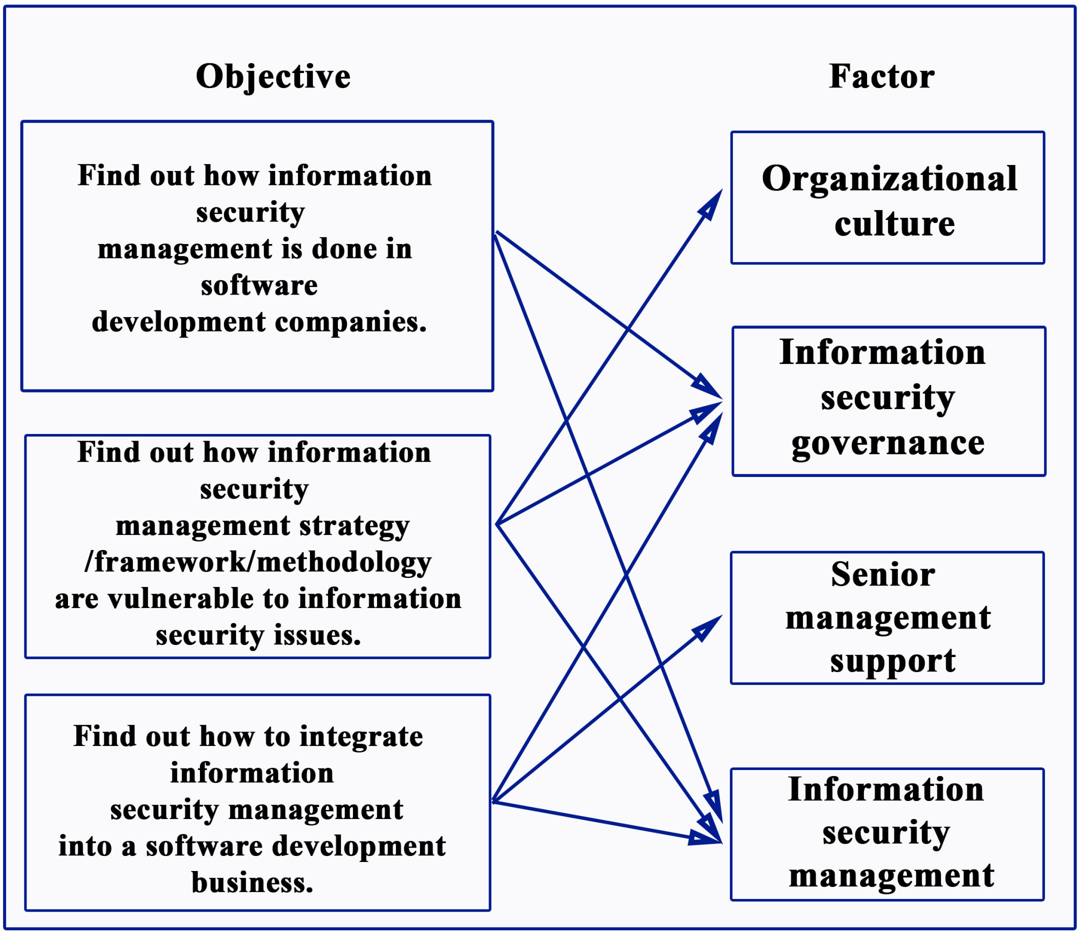

Objective
Factor
Find out how information security management is done in software development companies.
Find out how information security management strategy /framework/methodology are vulnerable to information security issues.
Find out how to integrate information security management into a software development business.
Organizational culture
Information security governance
Senior management support
Information security management

Figure 3.3 Mapping diagram

<u>Research hypothesis</u>

H1o - Organizational culture and ISM are positively correlated.

H1a – There is no relationship between Organizational culture and ISM.

H1o - Senior Management Support and ISM are positively correlated.

H1a - There is no relationship between Senior Management Support and ISM.

H1o - Information Security Governance and ISM are positively correlated.

H1a - There is no relationship between Information Security Governance and ISM.

3.4 Data collection

According to the national ICT workforce survey conducted in 2014, the estimated total ICT worker population in Sri Lanka was 33,918 in 2014. This ICT workforce contains all the software engineers, senior software engineers, technical leads, software architects, quality assurance engineers, project managers, business analysts, graphic designers, technical writers, etc. For this particular research, responses are calculated among following designations only. They are,

- Associate Technical Leads
- Technical Leads
- Software Architects
- Project Manages/ Delivery managers/IT managers
- Head of ITs

The reason for selecting above listed designations for this study was due to the assumption that these employees are directly involved with information security management related decision-making than lower designation holders in Software development companies.

The above-listed employee population was estimated to be 15% out of the total ICT population. According to the trend analysis, approximate total ICT population workforce will be around 40000 in 2017. Based on this particular situation our approximate target population size will be 6000 on 2017. These professionals are the target population of our research. The sample size for the above mentioned 6000 target population is 362 with a confidence level of 95% and an assumed error margin of 5%. These 362 employees were randomly selected from SLASSCOM registered software development companies for the quantitative data collection.

Above mentioned research questionnaire was created and distributed using Google forms. Before delivering the questionnaire among the target sample, a pilot survey was conducted. For the pilot survey, 11 employees were randomly selected from reputed Sri Lankan companies that included five technical leads, five information technology management position holders and one head of IT. These 11 selected employees were working in 8 different companies in Sri Lanka. Based on the responses received in the pilot study, required modifications were done to the questionnaire and redistributed among the selected sample randomly.

3.5 Summary

This research was conducted using a quantitative research approach. The study was conducted in a survey manner while considering a specific group of professionals in Sri Lankan IT sector as the population. Approximate target population size of this research is 6000, and the representative sample size is 362. There are three significant independent variables represent this study, they are 'Organizational culture', 'Senior Management Support' and 'Information Security Governance'. The dependent variable of this research is 'Information security management'. The data for the survey was collected through a self-administered survey questionnaire and the questionnaire was distributed as a Google form. The data analysis was conducted using IBM SPSS Version 24 by applying frequency, correlation and simple regression analysis.

4. DATA ANALYSIS

4.1 Introduction

Main purpose of this chapter is to provide comprehensive statistical analysis required to prove the hypotheses, which were previously introduced in section three. These hypotheses were validated and discussed in this chapter.

4.2 Data collection

4.2.1 Preliminary survey

An online questionnaire was distributed among the targeted audience to collect required data. To verify the reliability of the questionnaire, it is essential to conduct a preliminary survey. This particular survey was conducted within a very short period of time (two days). There were 11 responders who reacted to this questionnaire. These responses were collected from six different software development companies. Four technical leads, six management designation holders and one head of IT comprised the 11 employees. Based on the result of the preliminary survey, minor modifications were done to the questionnaire and redistributed to the main sample.

4.2.2 Research survey

The research survey was conducted targeting a random sample of 100 to 150 software development companies in Sri Lanka. Data collection was conducted 2017/12/17 between 2018/01/14. A total of 259 responses were collected during this time period.

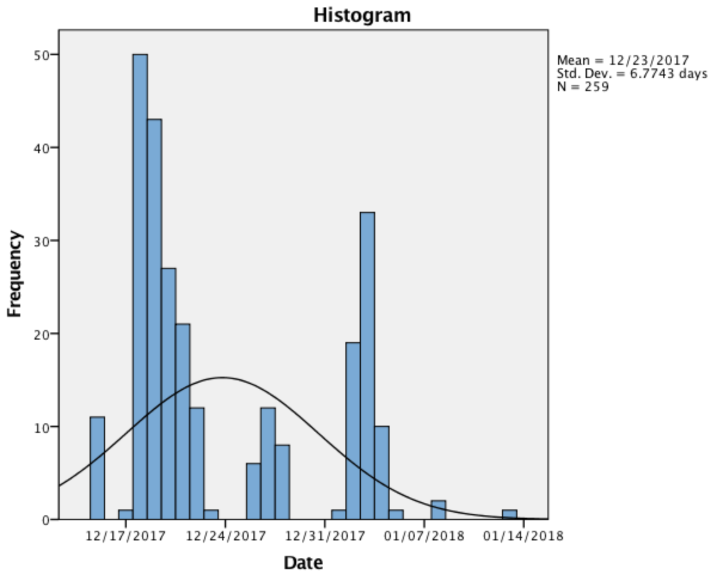


Figure 4.1 Response frequency distribution with the time

Figure 4.1 shows the frequency distribution of the responders (employees). For the data analysis only 191 responses are considered out of 259 responses, 63 responses were omitted because they were from Software Engineers. Five responses have been omitted due to incomplete answers. As it is mentioned in research methodology, for this research survey only the employees under the designation of Associate Technical leads, Technical lead, Software architect, Project Manager/Delivery Manager/IT Manage and Head of IT are considered. These selected 191 responses are compatible with this particular research purpose.

4.3 Reliability Analysis

It is required to test the validity and reliability of the data set before using them for hypothesis testing. To achieve this objective it is required to use Chronbach's alpha. Cronbach's alpha is a commonly utilized statistical mechanism to prove internal consistency/reliability of a dataset.

Table 4.1 Cronbach's alpha coefficient value representation

Cronbach's alpha	**Internal consistency**
X >= 0.9	Excellent
0.9 > X >= 0.7	Good
0.7 > X >= 0.6	Acceptable
0.6 > X >= 0.5	Poor
0.5 > X	Unacceptable

Table 4.1 shows the internal consistency levels related to Cronbach's alpha coefficient value.

4.3.1 Information security governance

4.3.1.1 Information security governance for employees

Table 4.2 Information security governance for employees

Question number	**Question**
10	There are specific roles and responsibilities assigned related to information security in my company
11	My company has already established information security management policies

Table 4.3 Case Processing summary for Information security governance for employees

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded[a]	**0**	**.0**
	Total	**191**	**100.0**

a. Listwise deletion based on all variables in the procedure.

Table 4.4 Reliability Statistics of Information security governance for employees

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.534	**.537**	**2**

Question number 10 and 11 are representing information security governance for employees. According to the data analysis information security governance for employees factor representing a poor internal consistency.

4.3.1.2 Information security governance for process

Table 4.5 Information security governance for process

Question number	Question
12	Weak information security service quality is negatively affecting the overall quality of the software produced by my company
13	Strong information security service quality is positively affecting the overall quality of the software produced by my company
14	Information security is directly affecting the brand identity of my company

Table 4.6 Case Processing Summary for Information security governance for process

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded[a]	**0**	**.0**
	Total	**191**	**100.0**

Table 4.7 Reliability Statistics of Information security governance for process

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.797	**.798**	**3**

Question number 12 and 13 and 14 are representing information security governance for process. According to the Table 4.7 information security governance for process factor representing a good internal consistency.

4.3.1.3 Information security governance reliability analysis

Here it is shown the overall Cronbach's alpha value related to the questions representing the information security governance.

Table 4.8 Case Processing Summary for information security governance

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded[a]	**0**	**.0**
	Total	**191**	**100.0**

a. Listwise deletion based on all variables in the procedure.

Table 4.9 Reliability Statistics for information security governance

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.826	**.832**	**5**

Table 4.9 presents the Cronbach's alpha values related to each question representing information security governance. These data indicate that information security governance representing a higher internal consistency/reliability.

Table 4.10 Information security governance

Question number	Question
10	There are specific roles and responsibilities assigned related to information security in my company
11	My company has already established information security management policies
12	Weak information security service quality is negatively affecting the overall quality of the software produced by my company
13	Strong information security service quality is positively affecting the overall quality of the software produced by my company
14	Information security is directly affecting the brand identity of my company

4.3.2 Senior management support

4.3.2.1 Operational support

Table 4.11 Operational support

Question number	Question
15	My company is allocating required budget for information security related tasks
16	Information security is part of the management activities of the top level management in my company

Table 4.12 Case Processing Summary of Operational support

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded[a]	**0**	**.0**
	Total	**191**	**100.0**

a. Listwise deletion based on all variables in the procedure.

Table 4.13 Reliability Statistics of Operational support

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.724	**.725**	**2**

Question number 15 and 16 are representing operational support. According to the Table 4.13 Operational support factor representing a good internal consistency value because Cronbach's Alpha value is 0.724.

4.3.2.2 Policy support

Table 4.14 Policy support

Question number	Question
17	Everyone is aware of information security related policies in my company
18	My company is investing on information security related certifications such as ISO 27001, BS7799, etc

Table 4.15 Case Processing Summary of Policy support

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded[a]	**0**	**.0**
	Total	**191**	**100.0**

a. Listwise deletion based on all variables in the procedure.

Table 4.16 Reliability Statistics of Policy support

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.632	**.635**	**2**

Question number 17 and 18 are representing policy support. According to the Table 4.16 policy support factor representing acceptable internal consistency.

4.3.2.3 Senior management support reliability analysis

Table 4.17 Case Processing Summary for senior management support

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded[a]	**0**	**.0**
	Total	**191**	**100.0**

a. Listwise deletion based on all variables in the procedure.

Table 4.18 Reliability Statistics for senior management support

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.793	**.800**	**4**

Table 4.19 Senior management support

Question number	Question
15	My company is allocating required budget for information security related tasks
16	Information security is part of the management activities of the top level management in my company
17	Everyone is aware of information security related policies in my company
18	My company is investing on information security related certifications such as ISO 27001, BS7799, etc

Table 4.18 presents the Cronbach's alpha values related to each question representing senior management support. These data indicate that senior management support representing a higher internal consistency/reliability because Cronbach's alpha value is 0.800.

4.3.3 Organizational culture

4.3.3.1 Empowerment

Table 4.20 Empowerment

Question number	Question
5	My company assigns me flexible working hours
6	Lower level management of my company has the power to take project-oriented decisions
7	My company is offering favourable conditions to teamwork and knowledge sharing

Table 4.21 Case Processing Summary for Empowerment

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded[a]	**0**	**.0**
	Total	**191**	**100.0**

a. Listwise deletion based on all variables in the procedure.

Table 4.22 Reliability Statistics for Empowerment

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.638	**.645**	**3**

Question number 5,6 and 7 are representing empowerment. According to the Table 4.22 empowerment factor representing acceptable internal consistency.

4.3.3.2 Resistance to change

Table 4.23 Resistance to change

Question number	Question
15	My company is allocating required budget for information security related tasks
16	Information security is part of the management activities of the top level management in my company
18	My company is investing on information security related certifications such as ISO 27001, BS7799, etc.

Table 4.24 Case Processing Summary for Resistance to change

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded^{a}	**0**	**.0**
	Total	**191**	**100.0**

a. Listwise deletion based on all variables in the procedure.

Table 4.25 Reliability Statistics for Resistance to change

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.716	**.728**	**3**

Question number 15,16 and 18 are representing resistance to change. According to the Table 4.25 resistance to change factor representing good internal consistency.

4.3.3.3 Organizational culture reliability analysis

Questions representing organizational culture do not indicate higher Cronbach’s alpha values like previous two independent variables, but it is inside the acceptable margin.

Table 4.26 Case Processing Summary for organizational

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded^{a}	**0**	**.0**
	Total	**191**	**100.0**

a. Listwise deletion based on all variables in the procedure.

Table 4.27 Reliability Statistics for organizational culture

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.566	**.575**	**6**

Table 4.28 Organizational culture

Question number	**Question**
5	My company assigns me flexible working hours
6	Lower level management of my company has the power to take project-oriented decisions
7	My company is offering favourable conditions to teamwork and knowledge sharing
15	My company is allocating required budget for information security related tasks
16	Information security is part of the management activities of the top level management in my company
18	My company is investing on information security related certifications such as ISO 27001, BS7799, etc.

4.3.4 Information security management

Questions representing dependent variable (Information security management) is also indicating higher internal consistency.

Table 4.29 Case Processing Summary for Information security management

Case Processing Summary

		N	%
Cases	Valid	**191**	**100.0**
	Excluded[a]	**0**	**.0**
	Total	**191**	**100.0**

a. Listwise deletion based on all variables in the procedure.

Table 4.30 Reliability Statistics for Information security management

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.801	**.801**	**2**

Table 4.31 Information security management

Question number	**Question**
8	My company has already identified information security as one of the critical factors for our business
9	My company has already established information security management mechanisms

Table 4.30 presents the Cronbach's alpha values related to each question representing information security management. These data indicate that information security management representing a higher internal consistency/reliability because Cronbach's alpha value is 0.801.

4.4 Demographic Analysis

4.4.1 Introduction

For this particular survey demographic information collected to identify the respondent's background. Only four questions represented in the demographic data.

4.4.2 Current designation of the employee

Table 4.32 Designations of the employees

I am currently working as a,

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Associate Technical Lead	**52**	**27.2**	**27.2**	**27.2**
	Technical Lead	**74**	**38.7**	**38.7**	**66.0**
	Software Architect	**16**	**8.4**	**8.4**	**74.3**
	Project Manager/Delivery Manager/IT	**41**	**21.5**	**21.5**	**95.8**
	Head of IT	**8**	**4.2**	**4.2**	**100.0**
	Total	**191**	**100.0**	**100.0**	

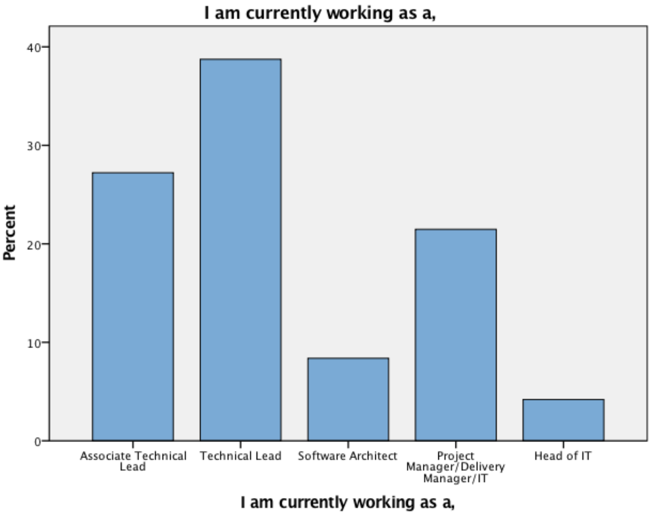


Figure 4.2 Designations of the employees

According to the Figure 4.2 and Table 4.32, 27.2 % responses are from associate technical lead position holders, and 38% of responses are from technical lead position holders. 8.4 %out of the total responses are from software architect position holders. This 8.4% is a very critical figure because software architects are the highest position holders in the technical hierarchy. Then management designation holders in software industry represent 21.5 %. Finally, 4.2% of people hold the position of Head of IT. The target population of this study is higher position holders in the software industry. It is required to verify the current designation of the employee before accepting the response for the data analysis.

4.4.3 Current working experience of the employee

Table 4.33 Current working experience of the employees

My current working experience is,

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3-5 years	**46**	**24.1**	**24.1**	**24.1**
	6-10 years	**104**	**54.5**	**54.5**	**78.5**
	11-15 years	**31**	**16.2**	**16.2**	**94.8**
	More than 15 years	**10**	**5.2**	**5.2**	**100.0**
	Total	**191**	**100.0**	**100.0**	

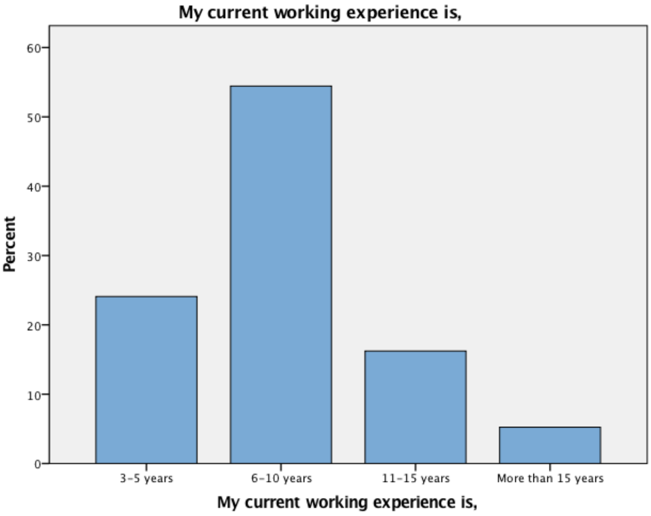


Figure 4.3 Current working experience of the employees

Table 4.33 and Figure 4.3 shows the current working experience of the employees. So 46 (24.1%) out of the 191 employees are representing the lower industry experience, which is 3-5 years. Majority of the employees 104 (54.5%) are under the category of 6 to 10 years. Then 31(16.2%) people are from the group of 11-15 years of experience. Finally, 10 people also had responded this questionnaire who got more than 15 years of experience. Verifying the working experience of the employee is essential. The most experienced employees make information security management related decisions in the organization. For this research study, the target population is most experienced employees in the industry.

4.4.4 Educational background of the employees

Table 4.34 Educational background of the employees

My highest educational qualification is,

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Diploma	**5**	**2.6**	**2.6**	**2.6**
	Bachelor's	**114**	**59.7**	**59.7**	**62.3**
	Postgraduate diploma	**13**	**6.8**	**6.8**	**69.1**
	Masters	**59**	**30.9**	**30.9**	**100.0**
	Total	**191**	**100.0**	**100.0**	

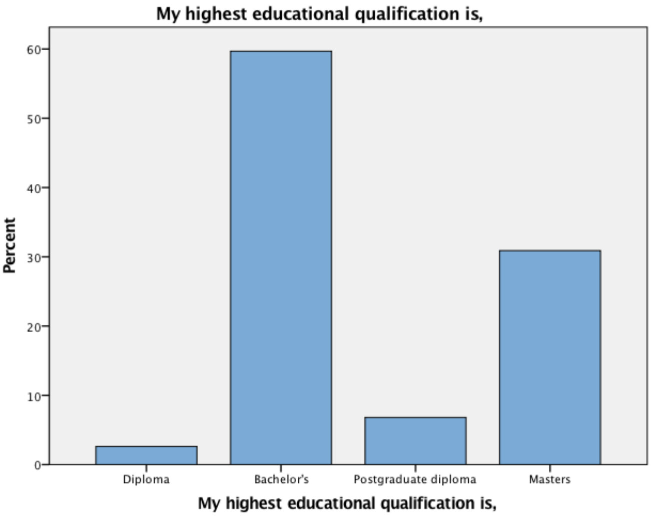


Figure 4.4 Educational background of the employees

Table 4.34 and Figure 4.4 represent the educational background of the employees. 2.6 % people are holding IT related diploma only. The majority of this category is holding bachelor's degree related to information technology that is 59.7 % of the total value. 6.8% of the peoples are holding postgraduate diploma. Finally the 59 (30.9%) total responses are from the master degree holders. Identify the educational background of the employee is essential to enhance the reliability of the sample.

4.4.5 Number of employees in the company

Table 4.35 Number of employees in the company

Total number of employees in my company,

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 50	**42**	**22.0**	**22.0**	**22.0**
	50 - 250	**69**	**36.1**	**36.1**	**58.1**
	Greater than 250	**80**	**41.9**	**41.9**	**100.0**
	Total	**191**	**100.0**	**100.0**	

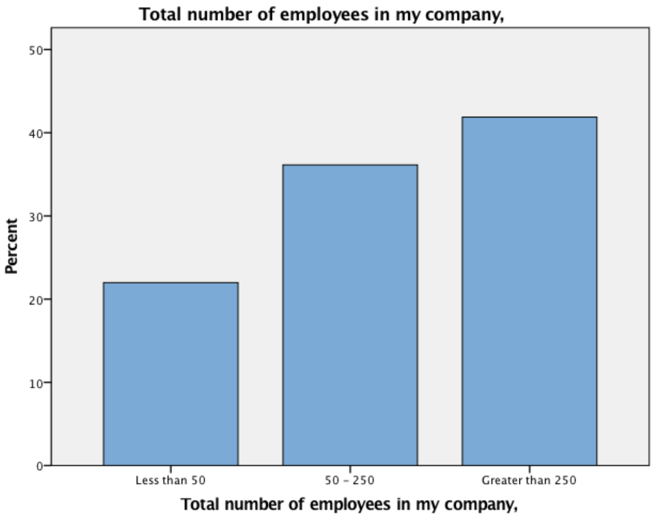


Figure 4.5 Number of employees in the company

According to the data populated in Table 4.35 and Figure 4.5, there are 42 responses from small-scale companies and 69 responses are from medium scale companies (50 – 250 employees). Finally, 80 responses are from large-scale companies.

4.5 Correlation Analysis

4.5.1 Pearson's correlation

Pearson's correlation was used to analyse the inter-item correlation of this particular research. And Pearson's correlation was considered as a statistical measure of linearity between two variables. If the Pearson's correlation value is close to 1 it is considered as the relationship is strong. And if it is close to 0, it is considered as a weak relationship between the variables.

Table 4.36 Pearson's correlation

"r" value	**Relationship**
0.80 to 1	Very strong
0.60 to 0.79	Strong
0.40 to 0.59	Moderate
0.20 to 0.39	Weak
0.00 to 0.19	Very weak

Table 4.36 is representing the level of correlation base on "r" value. As well as the significant value less than 0.01 was considered as extremely significant and significant value less than 0.05 was also considered a significant value as well.

According to the conceptual and theoretical framework there is one particular dependent variable that is called information security management, and it is essential to identify the relationship between the dependent variable and the independent variables. According to the conceptual and theoretical framework there are three independent variables called organizational culture, information security governance and senior management support. This chapter examines the relationship between the information security management and the above-mentioned independent variables. Calculated mean values are used to measure the overall relationship between dependent and independent variables.

4.5.1.1 Senior management support vs. Information security management

H_{1a} - Senior Management Support and ISM are positively correlated.

H_{1o} - There is no relationship between Senior Management Support and ISM.

Table 4.37 Correlation between information security management and the senior management support

Correlations

		ISM	SMS
ISM	Pearson Correlation	**1**	**.720**[**]
	Sig. (2-tailed)		**.000**
	N	**191**	**191**
SMS	Pearson Correlation	**.720**[**]	**1**
	Sig. (2-tailed)	**.000**	
	N	**191**	**191**

**. Correlation is significant at the 0.01 level (2-tailed).

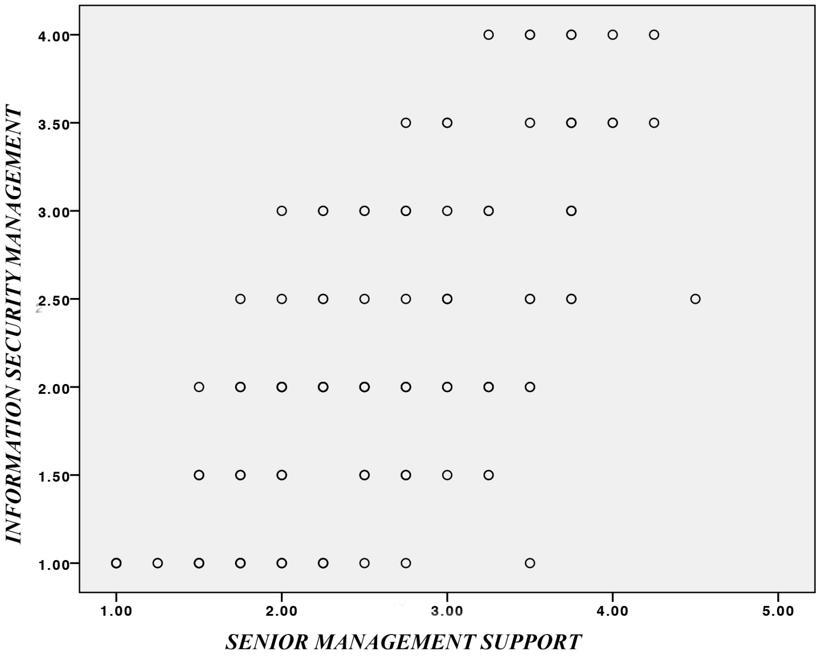


Figure 4.6 Direct comparison correlation between information security management and the senior management support.

According to the Table 4.37 and Figure 4.6, there is apparent linearity between these two variables. Significant value is 0.000, and it is considered as extremely significant. Pearson correlation value is 0.720, so it is a strong relationship.

4.5.1.2 Information security governance vs. Information security management

H2a - Information Security Governance and ISM are positively correlated.

H2o - There is no relationship between Information Security Governance and ISM.

Table 4.38 Correlation between information security management and the information security governance

Correlations

		ISM	ISG
ISM	Pearson Correlation	**1**	**.760****
	Sig. (2-tailed)		**.000**
	N	**190**	**190**
ISG	Pearson Correlation	**.760****	**1**
	Sig. (2-tailed)	**.000**	
	N	**190**	**191**

**. Correlation is significant at the 0.01 level (2-tailed).

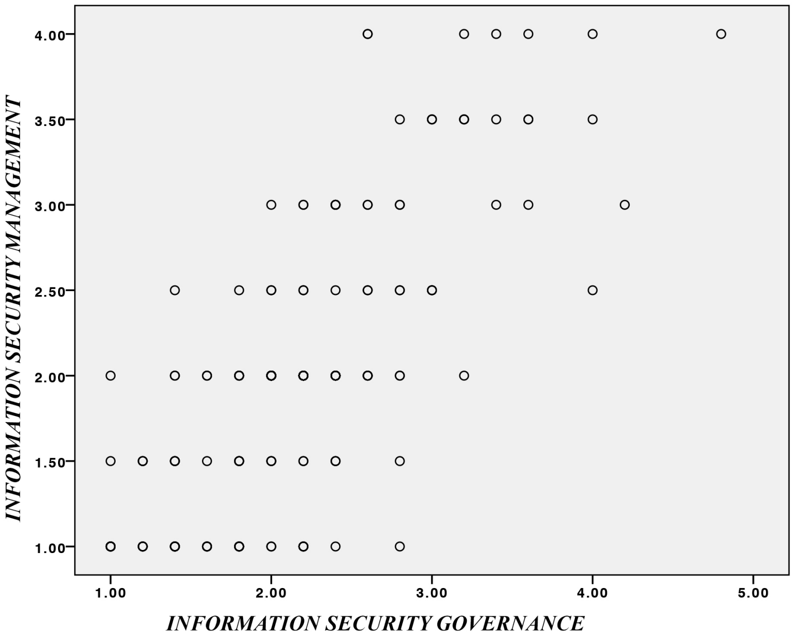


Figure 4.7 Direct comparison correlation between information security management and the information security governance.

According to the Table 4.38 and Figure 4.7, there is apparent linearity between these two variables as well. Here also significant value is 0.000, so it is considered as extremely significant. As Pearson correlation value is 0.760, it is a strong relationship.

4.5.1.3 Organizational culture vs. Information security management

H3a - Organizational culture and ISM are positively correlated.

H3o - There is no relationship between Organizational culture and ISM.

Table 4.39 Correlation between information security management and the Organizational culture

Correlations

		ISM	OC
ISM	Pearson Correlation	**1**	**.173***
	Sig. (2-tailed)		**.017**
	N	**191**	**191**
OC	Pearson Correlation	**.173***	**1**
	Sig. (2-tailed)	**.017**	
	N	**191**	**191**

*. Correlation is significant at the 0.05 level (2-tailed).

After illustrating the result of the Table 4.39 it is complicated to come to a conclusion as previous two figures. As the significant value of Pearson correlation is 0.017, the result of this data analysis is acceptable but Pearson correlation value is 0.173, so it has a weak relationship between the variables.

4.5.2 ANOVA Testing

ANOVA testing is used for this particular data analysis to further verify the correlations between given independent and dependent variables.

4.5.2.1 Senior management support vs. Information security management

Table 4.40 ANOVA results comparison between senior management support vs. Information security management

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	**63.862**	**1**	**63.862**	**203.469**	**.000**[b]
	Residual	**59.007**	**188**	**.314**		
	Total	**122.868**	**189**			

a. Dependent Variable: ISM

b. Predictors: (Constant), SMS

4.5.2.2 Information security governance vs. Information security management

Table 4.41 ANOVA results comparison between Information security governance vs. Information security management

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	**71.037**	**1**	**71.037**	**257.658**	**.000**[b]
	Residual	**51.832**	**188**	**.276**		
	Total	**122.868**	**189**			

a. Dependent Variable: ISM

b. Predictors: (Constant), ISG

4.5.2.3 Organizational culture vs. Information security management

Table 4.42 ANOVA results comparison between organizational culture vs. Information security management

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	**3.784**	**1**	**3.784**	**5.973**	**.015**[b]
	Residual	**119.085**	**188**	**.633**		
	Total	**122.868**	**189**			

a. Dependent Variable: ISM

b. Predictors: (Constant), OC

According to the results generated from Table 4.40, there is a linear relationship between senior management support vs information security management. According to the Table 4.41, there is a linear relationship between information security governance vs information security management. Because significant values related to both tables are 0.000 and this is lower than 0.05.

But when it comes to Table 4.42 significant value related to this particular table is 0.015 and this is not greater than 0.05, so we can accept the results and make a final discussion about that.

4.6 Regression Analysis

Regression analysis used to identify and estimate the relationship between the dependent variables and the independent variables in this research study. Regression analysis helps to determine how values of the dependent variable change according to the value change of the independent variable.

4.6.1 Senior management support vs. Information security management

H1a - Senior Management Support and ISM are positively correlated.

H1o - There is no relationship between Senior Management Support and ISM.

Table 4.43 Model Summary comparison between senior management support vs. Information security management

Model Summary

					Change Statistics				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1	**.721[a]**	**.520**	**.517**	**.56024**	**.520**	**203.469**	**1**	**188**	**.000**

a. Predictors: (Constant), SMS

Table 4.44 Coefficients results comparison between senior management support vs. Information security management

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	**.178**	**.132**		**1.345**	**.180**
	SMS	**.744**	**.052**	**.721**	**14.264**	**.000**

a. Dependent Variable: ISM

4.6.2 Information security governance vs. Information security management

H2a - Information Security Governance and ISM are positively correlated.

H2o - There is no relationship between Information Security Governance and ISM.

Table 4.45 Model Summary comparison between Information security governance vs. Information security management

Model Summary

					Change Statistics				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1	**.760**[a]	**.578**	**.576**	**.52507**	**.578**	**257.658**	**1**	**188**	**.000**

a. Predictors: (Constant), ISG

Table 4.46 Coefficients results comparison between information security governance vs. Information security management

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	**.092**	**.123**		**.745**	**.457**
	ISG	**.884**	**.055**	**.760**	**16.052**	**.000**

a. Dependent Variable: ISM

4.6.3 Organizational culture vs. Information security management

H3a - Organizational culture and ISM are positively correlated.
H3o - There is no relationship between Organizational culture and ISM.

Table 4.47 Model Summary comparison between organizational culture vs. Information security management

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	**.175[a]**	**.031**	**.026**	**.79588**	**.031**	**5.973**	**1**	**188**	**.015**

a. Predictors: (Constant), OC

Table 4.48 Coefficients results comparison between organizational culture vs. Information security management

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	**1.519**	**.195**		**7.807**	**.000**
	OC	**.221**	**.091**	**.175**	**2.444**	**.015**

a. Dependent Variable: ISM

According to coefficient Table 4.44, significant value is 0.000. This value is lower than 0.05. So there is a clear linear relationship between senior management support vs Information security management. Table 4.46 also exhibits the same situation. Significant value related to that is also 0.000. So there is a direct linear relationship between information security governance vs information security management, but coefficient Table 4.48 is not generating a positive result as previous. Significant value related to organizational culture vs information security management is 0.15, and this is higher than 0.05, so we cannot accept the result.

4.7 Summary

4.7.1 Reliability test summary (Cronbach's Alpha value)

Table 4.49 Reliability test summary

Independent variables	**Dependent variable (ISM)**
Organizational culture (OC)	**0.638**
Information security governance (ISG)	**0.826**
Senior management support (SMS)	**0.793**

According to Table 4.49, information security governance variables exhibited the highest internal consistency and reliability values. Senior management support is also presenting a higher internal consistency value. Furthermore, variables that represent Organizational culture under the questionable category. But that is also above the line of acceptability.

4.7.2 Inter item correlation analysis summary

4.7.2.1 Pearson Correlation summary

Table 4.50 Pearson Correlation summary

Independent variables		Dependent variable (ISM)
Organizational culture (OC)	Pearson Correlation Sig. (2-tailed)	0.173 0.017
Information security governance (ISG)	Pearson Correlation Sig. (2-tailed)	0.760 0.000
Senior management support (SMS)	Pearson Correlation Sig. (2-tailed)	0.720 0.000

Table 4.50 is representing the total mean summary of the Pearson Correlation statistics. According to above-given data, there are strong relationships between ISG and ISM as well as SMS and ISM. Sig values related to these variables are 0.000 so these test results are significant. But OC is exhibiting a very weak relationship with the dependent variable.

4.7.2.2 ANOVA table summary

Table 4.51 ANOVA table summary

Independent variable		Dependent variable (ISM)
Organizational culture (OC)	F Sig.	5.973 0.015
Information security governance (ISG)	F Sig.	257.65 0.000
Senior management support (SMS)	F Sig.	203.46 0.000

Table 4.51 is showing 0.000 significant values for ISG and SMS when comparing the relationship with ISM. OC is also showing a linear relationship with ISM according to this ANOVA test because it’s significant value is 0.015. According to ANOVA

test, all three independent variables are showing a linear relationship between dependent variables.

4.7.3 Linear Regression Analysis

Table 4.52 Coefficient table summary

Independent variables		**Dependent variable (ISM)**	
		Constant	**Productivity**
Organizational culture (OC)	**Sig.** **B**	**0.000** **1.519**	**0.015** **0.221**
Information security governance (ISG)	**Sig.** **B**	**0.457** **0.092**	**0.000** **0.884**
Senior management support (SMS)	**Sig.** **B.**	**0.180** **0.178**	**0.000** **0.744**

According to overall coefficient summary shows in Table 4.52 significant values related to both ISG and SMS are 0.000. For OC it is 0.015, but this is still acceptable because acceptable range should be under 0.05 ranges.

5. RECOMMENDATIONS AND CONCLUSION

5.1 Introduction

This research study was designed to achieve three major objectives as follows:

1. Find out how information security management is done in software development companies.
2. Find out how information security management strategies/frameworks/methodologies are vulnerable to information security issues.
3. Find out how to integrate information security management into a software development business.

This research focused on find out a methodology for practice information security in software development organizations. The first research objective focused on the factors of information security governance, senior management support and organizational culture impact on information security management in software development organizations. This objective has been achieved through an online questionnaire distributed among information technology professionals in Sri Lanka. After gathering required data, data analysis was performed to identify the relationship between these factors and information security management. The method adopted for finding answers to the second research objective was a combination of an extensive literature review and analysis of the data obtained through the online questionnaire. The third research objective was entirely based on the in-depth analysis of literature.

5.2 Discussion of the research findings

Data collection was conducted targeting 100 to 150 software development companies in Sri Lanka during one month. Within this time period, 259 responses have been collected. Furthermore, 68 responses were rejected and 191 responses were considered for the data analysis. These 191 responses were gathered from Associate technical leads, Technical leads, Software architects, Project managers/Delivery managers/IT managers and Head of ITs. Statistical analysis was performed based on collected data.

Table 4.48 shows the ultimate results of mean values related to Cronbach's Alpha. Furthermore, Table 4.49 represents the mean summary of the Pearson's correlations to check the inter-item correlations to identify the relationship between dependent and independent variables. Moreover, Table 4.50 and Table 4.51 represent means a summary of the ANOVA test results and Coefficient value results for linear regression analysis to analyze the relationship between dependent and independent variables further. It is required to test the validity and reliability of the data set before hypothesis testing. According to Table 4.48 each variable shows higher internal consistency/reliability. According to Table 4.49, information security governance and senior management support are showing strong relationship with information security management. Pearson's correlations 'r' value related organizational culture is 0.173, and organizational culture is not showing any relationship with information security management. As shown in Table 4.50 and Table 4.51 significance values related to each variable is below the significance level of 0.05.

According to the outcome of the data analysis, senior management support and information security governance are positively correlated to information security management. Moreover, it is difficult to identify a strong relationship between organizational culture and information security management according to the data analysis, but it shows a weak relationship with information security management.

The main objective of this research study is to find out a better methodology to practice information security in software development organizations. There are two major mechanisms were introduced to achieve that objective. The first mechanism is the PDCA model and the second mechanism is maturity models integration into information security management. Maturity models, which are more relevant in organizational culture context, because organizations achieve competence based on the way it works and thereafter it takes actions to check against maturity models. This context is suitable for the scenario that organizational culture and ISM are strongly correlated, but that is not accepted by the research results because organizational culture and ISM are weakly correlated. Furthermore, the research result shows senior management support and information security governance are strongly correlated with ISM which is driven by the management action PDCA model is the recommended model for practice information security management in software development organizations.

Main outcomes and recommendations of this research can be stated as follows:

- Information security governance and ISM are positively correlated. Software development organization should implement information security governance mechanism to achieve information security management.
- Senior Management Support and ISM are positively correlated. Without having the support of senior management, it is challenging to implement ISM mechanism in an organization. Therefore, senior management support is essential to implement information security management mechanism.
- According to the research outcome both Information security governance and Senior Management Support positively correlated with ISM. Therefore, the PDCA model can be recommend for managing information security in an organization because it requires management driven actions in implementation.
- Organizational culture and information security management are weakly correlated. Maturity models implementation required organizational culture driven actions. Therefore, according to the research results, maturity models are not accepted to manage information security.

5.3 Recommendations for future research

- Conduct a comprehensive study based on other same type models like IDEAL (Initiating, Diagnosing, Establishment, Acting, Learning) and QIP (Quality Improvement Paradigm) can be applicable to information security management.
- It is beneficial to identify new management areas that PDCA model can apply.

REFERENCES

Alfaraj, H. M., & Qin, S. (2011). Operationalising CMMI: integrating CMMI and CoBIT perspective. Journal of Engineering, Design and Technology, 9(3), 323-335. Emerald.

Bahl, S., & Wali, O. P. (2014). Perceived significance of information security governance to predict the information security service quality in software service industry: An empirical analysis. Information Management & Computer Security, 22(1), 2-23. Emerald.

Du, Q. L., Cao, S. M., Ba, L. L., & Cheng, J. M. (2008). Application of PDCA cycle in the performance management system. In 4th International Conference on Wireless Communications, Networking and Mobile Computing 2008 (WiCOM'08), pp. 1-4. IEEE.

Davis, N., Humphrey, W., Redwine, S. T., Zibulski, G., & McGraw, G. (2004). Processes for producing secure software. Security & Privacy, 2(3), 18-25.IEEE

Dey, M. (2007). Information security management-a practical approach. In AFRICON 2007 (pp. 1-6). IEEE.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. Computer Fraud & Security, 2005(11), 10-16. Elsevier.

Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345-361. Emerald.

Ernest Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458. Emerald.

Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., & Weippl, E. (2007). Information security fortification by ontological mapping of the ISO/IEC 27001 standard. In 13th Pacific Rim International Symposium on Dependable Computing, 2007 (PRDC 2007), pp. 381-388. IEEE.

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. The TQM Journal, 23(4), 367-376. Emerald.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information security technical report, 13(4), 247-255. Elsevier.

Kajava, J., Anttila, J., Varonen, R., Savola, R., & Roning, J. (2006). Information security standards and global business. In International Conference on Industrial Technology, 2006 (ICIT 2006), pp. 2091-2095. IEEE.

Labodová, A. (2004). Implementing integrated management systems using a risk analysis based approach. Journal of cleaner production, 12(6), 571-580. Elsevier.

Lee, J., Lee, J., Lee, S., & Choi, B. (2003). A CC-based security engineering process evaluation model. In 27th Annual International on Computer Software and Applications Conference, 2003 (COMPSAC 2003), pp. 130-135. IEEE.

Mellado, D., Fernández-Medina, E., & Piattini, M. (2007). A common criteria based security requirements engineering process for the development of secure information systems. Computer standards & interfaces, 29(2), 244-253. Elsevier.

Nunes, F. J. B., Belchior, A. D., & Albuquerque, A. B. (2010). Security engineering approach to support software security. In 6th World Congress on Services (SERVICES 2010), pp. 48-55. IEEE.

Nakatsu, R. T., & Iacovou, C. L. (2009). A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study. Information & Management, 46(1), 57-68. Elsevier.

Nguyen-Duc, A., Cruzes, D. S., & Conradi, R. (2015). The impact of global dispersion on coordination, team performance and software quality–A systematic literature review. Information and Software Technology, 57, 277-294. Elsevier.

Ning, J., Chen, Z., & Liu, G. (2010). PDCA process application in the continuous improvement of software quality. In International Conference on Computer, Mechatronics, Control and Electronic Engineering, 2010 (CMCE), pp. 61-65. IEEE.

Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. International Journal of Information Management, 30(6), 567-572. Elsevier.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In Second Asia International Conference on Modeling & Simulation, 2008 (AICMS 08), pp. 749-753. IEEE.

Seong Leem, C., & Kim, I. (2004). An integrated evaluation system based on the continuous improvement model of IS performance. Industrial Management & Data Systems, 104(2), 115-128. Emerald.

Sauvé, J., Moura, A., Sampaio, M., Jornada, J., & Radziuk, E. (2006). An introductory overview and survey of business-driven IT management. In The First IEEE/IFIP International Workshop on Business-Driven IT Management, 2006 (BDIM'06), pp. 1-10. IEEE.

Siponen, M. (2002). Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria. Information Management & Computer Security, 10(5), 210-224. Emerald.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270. Elsevier.

Stambul, M. A. M., & Razali, R. (2011). An assessment model of information security implementation levels. In International Conference on Electrical Engineering and Informatics,2011 (ICEEI), pp. 1-6. IEEE.

Staples, M., Niazi, M., Jeffery, R., Abrahams, A., Byatt, P., & Murphy, R. (2007). An exploratory study of why organizations do not adopt CMMI. Journal of systems and software, 80(6), 883-895. Elsevier.

Tan, T., He, M., Yang, Y., Wang, Q., & Li, M. (2008). An analysis to understand software trustworthiness. In the 9th International Conference for Young Computer Scientists, 2008 (ICYCS 2008), pp. 2366-2371.IEEE.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. Information Management & Computer Security, 18(5), 350-365. Emerald.

Wang, C. H., & Tsai, D. R. (2009). Integrated installing ISO 9000 and ISO 27000 management systems on an organization. In 43rd Annual 2009 International Carnahan Conference on Security Technology, 2009, pp. 265-267. IEEE.

Williams, P. (2008). A practical application of CMM to medical security capability. Information Management & Computer Security, 16(1), 58-73. Emerald.

Woodhouse, S. (2008). An isms (im)-maturity capability model. In IEEE 8th International Conference on Computer and Information Technology Workshops, 2008 (CIT Workshops 2008), pp. 242-247. IEEE.

Yang, Y. P. O., Shieh, H. M., & Tzeng, G. H. (2013). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. Information Sciences, 232, 482-500. Elsevier.

APPENDIX A

ONLINE SURVEY QUESTIONNAIRE

Methodology for practice of information security in software development companies

I am really grateful for every second you are investing for answering my survey questions. It will take around five to ten minutes of your time. Your responses are anonymous, will be confidential and used only for academic purpose.

* Required

1. I am currently working as a,

- ○ Software Engineer
- ○ Associate Technical Lead
- ○ Technical Lead
- ○ Software Architect
- ○ Project Manager/Delivery Manager/IT Manager
- ○ Head of IT

2. My current working experience is, *

- ○ 3-5 years
- ○ 6-10 years
- ○ 11-15 years
- ○ More than 15 years

3.My highest educational qualification is, *

- ○ Diploma
- ○ Bachelor's
- ○ Postgraduate diploma
- ○ Masters
- ○ PhD

4. Total number of employees in my company, *

- ○ Less than 50
- ○ 50 - 250
- ○ Greater than 250

5. My company assigns me flexible working hours, *

- ○ Strongly Agree
- ○ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

6. My company is offering favourable conditions to teamwork and knowledge sharing *

- o Strongly Agree
- o Agree
- o Neutral
- o Disagree
- o Strongly Disagree

7. Lower level management of my company has the power to take project-oriented decisions *

- o Strongly Agree
- o Agree
- o Neutral
- o Disagree
- o Strongly Disagree

8. My company has already identified information security as one of the critical factors for our business *

- o Strongly Agree
- o Agree
- o Neutral
- o Disagree
- o Strongly Disagree

9. My company has already established information security management mechanisms *

- o Strongly Agree
- o Agree
- o Neutral
- o Disagree
- o Strongly Disagree

10. There are specific roles and responsibilities assigned related to information security in my company *

- o Strongly Agree
- o Agree
- o Neutral
- o Disagree
- o Strongly Disagree

11. My company has already established information security management policies *

- o Strongly Agree
- o Agree

- Neutral
- Disagree
- Strongly Disagree

12. Weak information security service quality is negatively affecting the overall quality of the software produced by my company *

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

13. Strong information security service quality is positively affecting the overall quality of the software produced by my company *

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

14. Information security is directly affecting the brand identity of my company *

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

15. My company is allocating required budget for information security related tasks *

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

16. Information security is part of the management activities of the top level management in my company *

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

17. Everyone is aware of information security related policies in my company *

- o Strongly agree
- o Agree
- o Neutral
- o Disagree
- o Strongly disagree

18. My company is investing on information security related certifications such as ISO 27001, BS7799, etc *

- o Strongly agree
- o Agree
- o Neutral
- o Disagree
- o Strongly disagree