THE STUDY OF INFORMATION SYSTEM SECURITY AUDIT GUIDED PRACTICES FOR BANK BY USING BANK OF THAILAND GUIDELINE

SASITORN SILAMANOTHUM

A THEMATIC PAPER SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE (TECHNOLOGY OF INFORMATION SYSTEM MANAGEMENT) FACULTY OF GRADUATE STUDIES MAHIDOL UNIVERSITY 2014

Thematic Paper
entitled

THE STUDY OF INFORMATION SYSTEM SECURITY AUDIT GUIDED PRACTICES FOR BANK BY USING BANK OF THAILAND GUIDELINE

……
Miss Sasitorn Silamanothum
Candidate

……
Asst. Prof. Bunlur Emaruchi, Ph.D.
Major advisor

……
Asst. Prof. Supaporn Kiattisin, Ph.D.
Co-advisor

……
Prof. Banchong Mahaisavariya,
M.D., Dip Thai Board of Orthopedics
Dean
Faculty of Graduate Studies
Mahidol University

……...
Asst. Prof. Supaporn Kiattisin,
Ph.D. (Electrical and Computer Engineering)
Program Director
Master of Science Program in
Technology of Information System
Management
Faculty of Engineering
Mahidol University

Thematic Paper
entitled

THE STUDY OF INFORMATION SYSTEM SECURITY AUDIT GUIDED PRACTICES FOR BANK BY USING BANK OF THAILAND GUIDELINE

was submitted to the Faculty of Graduate Studies, Mahidol University
for the degree of Master of Science
(Technology of Information System Management)
on
March 10, 2014

……
Miss Sasitorn Silamanothum
Candidate

……
Lect. Sotarat Thammaboosadee, Ph.D.
Chair

……..…...
Asst. Prof. Bunlur Emaruchi, Ph.D.
Member

……
Lect. Surapong Pongyupinpanich
Member

……....……
Asst. Prof. Supaporn Kiattisin, Ph.D.
Member

…… ……
Prof. Banchong Mahaisavariya,
M.D., Dip Thai Board of Orthopedics
Dean
Faculty of Graduate Studies
Mahidol University

……
Lect. Worawit Israngkul,
M.S.(Technical Management)
Dean
Faculty of Engineering,
Mahidol University

ACKNOWLEDGEMENTS

The study of information system security audit guided practices for bank by using bank of Thailand guideline would like completely. I thanks to my thematic advisor team, Bunlur Emaruchi, Ph.D. (Major advisor) and Supaporn Kiattisin, Ph.D. (Co-advisor) for invaluable suggest, help and recommend throughout the course of this research

I also thank employee and manager of bank for help to answer questionnaire and suggest design questionnaire to complete.

I thank Technology information system management officer for suggest and coordinate operation of this research.

I gratefully encouragement my parent, my friend and my co-worker for support of this research.

Sasitorn Silamanothum

THE STUDY OF INFORMATION SYSTEM SECURITY AUDIT GUIDED PRACTICES FOR BANK BY USING BANK OF THAILAND GUIDELINE

SASITORN SILAMANOTHUM 5336480 EGTI / M

M.Sc. (TEACHNOLOGY OF INFORMATION SYSTEM MANAGEMENT)

THEMATIC PAPER ADVISORY COMMITTEE: BUNLUR EMARUCHI, Ph.D., SUPAPORN KIATTISIN, Ph.D.

ABSTRACT

A information security systems audit, using the Bank of Thailand guidelines ensures reliable operations and the use of proper techniques. Information systems are considered business processes established for the purpose of confidentiality, integrity, accuracy and completeness of data for use in effective resource allocation and regulation compliance.

This research is quantitative, using three methodologies: documentary research, questionnaires and interviews.

The results confirm successful research because the IT officer and IT manager were cooperating in answering the questionnaire and suggesting information security for the bank. The information security system of the bank complies with Bank of Thailand guidelines, but some processes should be improved such as Access control, Physical Security Control, Logging and Data Collection. There are better information security methods.

KEY WORDS: INFORMATION SYSTEM SECURITY / AUDIT / BANK OF THAILAND

124 pages

การศึกษาแนวทางการตรวจสอบด้านความปลอดภัยระบบสารสนเทศของธนาคารตามแนวทางของธนาคารแห่งประเทศไทย

THE STUDY OF INFORMATION SYSTEM SECURITY AUDIT GUIDED PRACTICES FOR BANK BY USING BANK OF THAILAND GUIDELINE

ศศิธร ศิระมโนธรรม 5336480 EGTI / M

วท.ม. (เทคโนโลยีการจัดการระบบสารสนเทศ)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์ : บันลือ เอมะรุจิ, Ph.D., สุภาภรณ์ เกียรติสิน, Ph.D.

บทคัดย่อ

การตรวจสอบด้านความปลอดภัยของระบบสารสนเทศของธนาคารตามแนวทางของธนาคารแห่งประเทศไทยเป็นกระบวนการที่จะต้องพิจารณาถึงระบบสารสนเทศมีความสามารถครอบคลุมไปถึงวัตถุประสงค์ในด้านของความมีประสิทธิภาพของสารสนเทศที่เกี่ยวข้องกับกระบวนการทางธุรกิจ ความมีประสิทธิผลในการใช้ทรัพยากร การรักษาความลับของข้อมูลสารสนเทศ ความสมบูรณ์ถูกต้องครบถ้วนถูกต้องของข้อมูล ความน่าเชื่อถือของข้อมูล สภาพความพร้อมใช้งาน และการปฏิบัติตามระเบียบของธนาคาร จากการวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณโดยใช้วิธีการค้นคว้าวิจัยจากเอกสาร, แบบสอบถาม และการสัมภาษณ์เจ้าหน้าด้านเทคโนโลยีสารสนเทศในการเก็บข้อมูล

ผลการวิจัยพบว่า การวิจัยนี้ประสบผลสำเร็จเพราะความร่วมมือกันเป็นอย่างดีจากเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศของธนาคารในการตอบแบบสอบถามและให้คำแนะนำเกี่ยวกับความปลอดภัยสารสารสนเทศ โดยระบบสารสนเทศของธนาคารมีความปลอดภัยเป็นไปตามแนวทางของธนาคารแห่งประเทศไทยที่ได้กำหนดไว้ แต่มีบางกระบวนการที่ควรปรับปรุงคือ การควบคุมการเข้าถึง, การรักษาความปลอดภัยทางกายภาพ และการจัดเก็บและรวบรวมข้อมูลของการทำธุรกรรมให้มีความปลอดภัยในสารสนเทศยิ่งขึ้น

124 หน้า

CONTENTS

CONTENTS (cont.)

CONTENTS (cont.)

CONTENTS (cont.)

LIST OF TABLES

LIST OF TABLES (cont.)

LIST OF TABLES (cont.)

LIST OF TABLES (cont.)

LIST OF FIGURES

CHAPTER I
INTRODUCTION

Information is vital to the banks. Preventive and detective information is essential for reliability and maintaining customer confidence to ensure that necessary decisions can be made for customers. If information is disclosed to or exchanged with unauthorized persons, the bank will suffer the impact in the form of negative reputation and payment of damages to customers.

Information security is an operating process that secures systems, devices and equipment critical to the operation. Banks need to maintain stability and protect the privacy of customer information. Furthermore, business continuity plans should be made for circumstances where businesses are unable to operate or systems do not work such as during system errors, blackouts and floods, etc.

The information security systems of banks ensure reliable operations and proper techniques. Information systems are considered business processes established for the purpose of confidentiality, integrity, accuracy and completeness of data for use in effective resource allocation and regulation compliance. Checking the security of information systems focused on the system can be run as scheduled for safety and preventing unwanted and potentially harmful compromise to banking systems. Banks are under obligation to manage and prevent information systems for less vulnerability and negative impact.

Risk assessment is the process of identifying vulnerabilities, threats and impact. Organizations that follow appropriate policy or comply with information systems gain adequate security. Accordingly personnel are ensured of understanding policy with skilled practice.

Banks need to control systems and security in order to prevent customer from refusing to make financial transactions and denying liability. Taking into account integrity and reflecting on responsibility helps banks reduce fraud and corruption for both customers and banks.

1.1. Significance of the Problem

Information security is critical to banks because banks have important customer data and sensitive information. Banks need instill confidence and reliability in customers regarding security. Information is not disclosed without permission and accurately. Today's threats are varied. For example, hackers can disrupt computer operations, gather sensitive information, gain access to private computer systems or modify data files to perform some type of harmful activity on the information systems of banks. Because natural disasters or protests might affect bank operations and require banks to halt services, banks should have business continuity plans (BCP). Weaknesses may result in operation vulnerability for systems and employees. For example, bank employees might engage in corrupt practice by modifying the transactions of customers, even though the bank should train employees regarding information systems and the penalties involved. However, banks should also prevent threats and weaknesses by managing risks with feasibility studies, risk assessment, problem-solving and follow-up. Therefore, the study of information system security audit-guided practices for banks by using the Bank of Thailand Guideline to help secure information by covering risks applicable to standards such as ISO 27001 and GTAG, etc. Help is available to ensure the effectiveness and efficiency of information security systems for banks.

1.2. Objectives

1.2.1. To know risks affecting the operations and information systems of banks.

1.2.2. To create information security guidelines for banks.

1.2.3. To ensure that IT officers have knowledge, understanding and awareness about information security.

1.3. Expected Outcomes/Benefits of Study

1.3.1. Reduced IT risks for banks.

1.3.2. Application of information security guidelines.

1.3.3. Knowledge, understanding and awareness of information security for IT officers.

1.4. Scope

The scope of this research was aimed at studying the risk for information systems and information security guidelines then creating an information security manual for banks by applying the Bank of Thailand Guidelines for information security.

1.5. Duration of Study

Table1.1. Duration of Study

Details	Month								
	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014
Feasibility of Study	←	→							
Data Collection			←	→					
Creation and Testing of Questionnaire					←	—	→		
Survey by Using Questionnaire							←	→	
Summary and Analysis									← →

1.6. Research Methodology

1.6.1. To study information system security audit-guided practices by using the Bank of Thailand Guidelines, framework and standards.

1.6.2. Analysis to determine whether or not the operations follow policy, compliance, framework and standards.

1.6.3. Creation of questionnaires for information technology employees and managers.

1.6.4. Improvement and survey of questionnaires.

1.6.5. Analysis of the results in order to define the risks and vulnerability, including suggested information security for banks.

1.6.6. Summary and recommendations suggested by findings.

1.7. Definitions

1.7.1. Access

With respect to privacy, an individual's ability to view, modify, and contest the accuracy and completeness of personally identifiable information collected about him or her. (*Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, Appendix 7, 7.8 Glossary of Terms, page 32)*

1.7.2. Authentication

The act of verifying the identity of a system entity (e.g., user, system, network node) and the entity's eligibility to access computerized information. Designed to protect against fraudulent log on activity. Authentication can also refer to the verification of the correctness of a piece of data. (*Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, Appendix 7, 7.8 Glossary of Terms, page 32)*

1.7.3. Authorization

The act of verifying the identity of a user and the user's eligibility to access computerized information

Scope Note: Assurance: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data. *(COBIT 5 Framework, Appendix H Glossary, page 89)*

1.7.4. Availability

Availability is one of the information quality goals under the accessibility and security heading. *(COBIT 5 Framework, Appendix H Glossary, page 89)*

1.7.5. Business continuity

Preventing, mitigating and recovering from disruption. The terms 'business resumption planning', 'disaster recovery planning' and 'contingency planning' also may be used in this context; they focus on recovery aspects of continuity, and for that reason the 'resilience' aspect should also be taken into account. *(COBIT 5 Framework, Appendix H Glossary, page 89)*

1.7.6. Business process control

The policies, procedures, practices and organizational structures designed to provide reasonable assurance that a business process will achieve its objectives *(COBIT 5 Framework, Appendix H Glossary, page 89)*

1.7.7. Compliance

Compliance in the sense that information must conform to specifications is covered by any of the information quality goals, depending on the requirements. Compliance to regulations is most often a goal or requirement of the use of the information, not so much an inherent quality of information. *(COBIT 5 Framework, Appendix F Comparison between the COBIT 5 Information Model and COBIT 4.1 Information Criteria, page 63)*

1.7.8. Confidentiality

Confidentiality corresponds to the restricted access information quality goal. (COBIT 5 Framework, *Appendix F Comparison between the COBIT 5 Information Model and COBIT 4.1 Information Criteria*, page 63)

1.7.9. Control

The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management or legal nature. Also used as a synonym for safeguard or countermeasure. *(COBIT 5 Framework, Appendix H Glossary, page 91)*

1.7.9. Data controller

Organizations or functions that control access and processing of personal information. (*Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, Appendix 7, 7.8* Glossary of Terms, page 32)

1.7.10. Data security

Protection of data from accidental or unauthorized modification, destruction, or disclosure through policies, organizational structure, procedures, awareness training, software, or hardware that ensure data is accurate, available, and accessed only by those authorized. Maintenance of confidentiality, integrity, and availability of information. (*Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, Appendix 7,* 7.8 Glossary of Terms, page 33)

1.7.11. Effectiveness

Information is effective if it meets the needs of the information consumer who uses the information for a specific task. If the information consumer can perform the task with the information, then the information is effective. This corresponds to the following information quality goals: appropriate amount, relevance, understandability, interpretability, objectivity. (*COBIT 5 Framework, Appendix F Comparison between the COBIT 5 Information Model and COBIT 4.1 Information Criteria*, page 63)

1.7.12. Efficiency

Whereas effectiveness considers the information as a product, efficiency relates more to the process of obtaining and using information, so it aligns to the ‘information as a service’ view. If information that meets the needs of the information consumer is obtained and used in an easy way (i.e., it takes few resources—physical

effort, cognitive effort, time, money), then the use of information is efficient. This corresponds to the following information quality goals: believability, accessibility, ease of operation, reputation. (*COBIT 5 Framework, Appendix F Comparison between the COBIT 5 Information Model and COBIT 4.1 Information Criteria*, page 63)

1.7.13. GTAG

Global technology audit guide (*Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, Appendix 7*, 7.9 Glossary of Acronyms, page 36)

1.7.14. Identification

The relating of personal information to identifiable individual. (*Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, Appendix 7*, 7.8Glossary of Terms, page 33)

1.7.15. Information

An asset that, like other important business assets, is essential to an enterprise's business. It can exist in many forms: printed or written on paper, stored electronically, transmitted by post or electronically, shown on films, or spoken in conversation. *(COBIT 5 Framework, Appendix H Glossary, page 91)*

1.7.16. Integrity

If information has integrity, then it is free of error and complete. It corresponds to the following information quality goals: completeness, accuracy. *(COBIT 5 Framework, Appendix F Comparison between the COBIT 5 Information Model and COBIT 4.1 Information Criteria, page 63)*

1.7.17. Inputs and outputs

The process work products/artifacts considered necessary to support operation of the process. They enable key decisions, provide a record and audit trail of process activities, and enable follow-up in the event of an incident. They are defined at the key management practice level, may include some work products used only within

the process and are often essential inputs to other processes. The illustrative COBIT 5 inputs and outputs should not be regarded as an exhaustive list since additional information flows could be defined depending on a particular enterprise's environment and process framework. *(COBIT 5 Framework, Appendix H Glossary, page 91)*

1.7.18. Policy

Overall intention and direction as formally expressed by management. *(COBIT 5 Framework, Appendix H Glossary, page 92)*

1.7.19. Process

Generally, a collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g., products, services)

Scope note: Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance. *(COBIT 5 Framework, Appendix H Glossary, page 92)*

1.7.20. Reliability

Reliability is often seen as a synonym of accuracy; however, it can also be said that information is reliable if it is regarded as true and credible. Compared to integrity, reliability is more subjective, more related to perception, and not just factual. It corresponds to the following information quality goals: believability, reputation, objectivity. *(COBIT 5 Framework, Appendix F Comparison between the COBIT 5 Information Model and COBIT 4.1 Information Criteria, page 63)*

1.7.21. Risk

The combination of the probability of an event and its consequence *(COBIT 5 Framework, Appendix H Glossary, page 93)*

1.7.22. Security

The protection of data from unauthorized access, misuse, or abuse and destruction or corruption of data. *(Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, Appendix 7, 7.8 Glossary of Terms, page 34)*

1.7.23. Sensitive personal information

Personal information that requires an extra level of protection and a higher duty of care *(Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, Appendix 7, 7.8 Glossary of Terms, page 35)*

1.7.24. System

A system consists of five key principles organized to achieve a specified objective. The five principles are: infrastructure (facilities, equipment, and networks); software (systems, applications, and utilities); people (developers, operators, users, and managers); procedures (automated and manual); and data (transaction streams, files, databases, and tables). *(Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, Appendix 7, 7.8 Glossary of Terms, page 35)*

1.7.25. System of internal control

The policies, standards, plans and procedures, and organizational structures designed to provide reasonable assurance that enterprise objectives will be achieved and undesired events will be prevented or detected and corrected *(COBIT 5 Framework, Appendix H Glossary, page 93)*

1.7.26. Vulnerability

Any weakness or exposure of IT asset that could lead to a compromise of the asset's confidentiality, integrity, or availability. (*Global Technology Audit Guide 6: Managing and Auditing IT Vulnerabilities, Appendix 5,5.5 Glossary of Terms, page 15)*

CHAPTER II
LITERATURE REVIEW

2.1. Risk Assessment

2.1.1. Risk Definition

Risk has many interpretations, and is often used to describe dangers or threats to a particular person, environment, or business. The following are some of the definitions of risk:

Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization (PCI DSS Risk Assessment Guidelines November 2012, page 3).

Risk is a function of the combination of the probability of an event and its consequence (COBIT 5 Framework, Appendix H Glossary, page 93).

2.1.2. Defining Risk Assessment

Risk assessment is a systematic process for identifying and evaluating events (i.e., possible risks and opportunities) potentially affecting the achievement of objectives either positively or negatively. Such events can be identified in the external environment (e.g., economic trends, regulatory landscape and competition) and within an organization's internal environment (e.g., people, process, and infrastructure). When these events intersect with an organization's objectives—or can be predicted to do so—they become risks. Risk is, therefore, defined as "the possibility that an event will occur and adversely affect the achievement of objectives" (Committee of Sponsoring Organizations, Enterprise Risk Management—Integrated Framework (2004), p.16.).

2.1.3. Selection of Risk Assessment Methodology

2.1.3.1. There are many risk assessment methodologies available from which the IS auditor may choose. These range from simple classifications of high, medium and low, based on the IS auditor's judgments, to complex and apparently

scientific calculations to provide a numeric risk rating. IS auditors should consider the level of complexity and detail appropriate for the organization being audited.

2.1.3.2. IS auditors should include, at a minimum, an analysis, within the methodology of the risks to the enterprise resulting from the loss of and controls supporting system availability, data integrity and business information confidentiality.

2.1.3.3. All risk assessment methodologies rely on subjective judgments at some point in the process (e.g., for assigning weightings to the various parameters). The IS auditor should identify the subjective decisions required to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy.

2.1.3.4. In deciding which is the most appropriate risk assessment methodology, IS auditors should consider as the following:

2.1.3.4.1. The type of information required to be collected (some systems use financial effects as the only measure - this is not always appropriate for IS audits).

2.1.3.4.2. The cost of software or other licenses required to use the methodology.

2.1.3.4.3. The extent to which the information required is already available.

2.1.3.4.4. The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise).

2.1.3.4.5. The opinions of other users of the methodology, and their views on how well the methodology has assisted them in improving the efficiency or effectiveness of their audits.

2.1.3.4.6. The willingness of management to accept the methodology as the means of determining the type and level of audit work carried out.

2.1.3.5. No single risk assessment methodology can be expected to be appropriate in all situations. Conditions affecting audits may change over time. Periodically, the IS auditor should re-evaluate the suitability of the chosen risk assessment methodologies.

2.1.4. Use of Risk Assessment

2.1.4.1. IS auditors should use the selected risk assessment techniques in developing the overall audit plan and in planning specific audits. Risk assessment, in combination with other audit techniques, should be considered in making planning decisions such as the following:

2.1.4.1.1. The nature, extent and timing of audit procedures.

2.1.4.1.2. The areas or business functions to be audited.

2.1.4.1.3. The amount of time and resources to be allocated to an audit.

2.1.4.2. The IS auditor should consider each of the following types of risk to determine their overall level:

2.1.4.2.1. Inherent risk

Inherent risk is the susceptibility of an audit area to error in a way that could be material, individual or in combination with other errors, assuming that there were no related internal controls. For example, the inherent risk associated with operating system security is ordinarily high, since changes to, or even disclosure of, data or programs through operating system security weaknesses could result in false management information or competitive disadvantage. By contrast, the inherent risk associated with security for a stand-alone PC, when a proper analysis demonstrates it is not used for business-critical purposes, is ordinarily low.

Inherent risk for most IS audit areas is ordinarily high since the potential effects of errors ordinarily span several business systems and many users.

In assessing the inherent risk, the IS auditor should consider both pervasive and detailed IS controls. This does not apply to circumstances where the IS auditor's assignment is related to pervasive IS controls only. At the pervasive IS control level, the IS auditor should consider to the level appropriate for the audit area in question:

- The integrity of IS management and IS management experience and knowledge
- Changes in IS management

- Pressures on IS management that may predispose them to conceal or misstate information (e.g., large business-critical project overruns hacker activity).

- The nature of the organization's business and systems (e.g., the plans for e-commerce, the complexity of the systems, the lack of integrated systems).

- Factors affecting the organization's industry as a whole (e.g., changes in technology, IS staff availability).

- The level of third-party influence on the control of the systems being audited (e.g., because of supply chain integration, outsourced IS processes, joint business ventures, and direct access by customers).

- Findings from and dates of previous audits.

At the detailed IS control level, the IS auditor should consider the level appropriate for the audit area in question:

- The findings from and dates of previous audits in this area.

- The complexity of the systems involved.

- The level of manual intervention required.

- The susceptibility to loss or misappropriation of the assets controlled by the system (e.g., inventory, payroll).

- The likelihood of activity peaks at certain times during the audit period.

- Activities outside the day-to-day routine of IS processing (e.g., the use of operating system utilities to amend data).

- The integrity, experience and skills of management and staff involved in applying the IS controls.

2.1.4.2.2. Control Risk

Control risk is the risk that a potential error in an audit area that could be material, individual or in combination with other errors will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed owing to the volume

of logged information. The control risk associated with computerized data validation procedures is ordinarily low because the processes are consistently applied.

The IS auditor should assess the control risk as high unless relevant internal controls are:

- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

2.1.4.2.3. Detection Risk

Detection risk is the risk that the IS auditor's substantive procedures will not detect an error that could be material, individual or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with identifying a lack of disaster recovery plans is ordinarily low, since existence is verified easily.

In determining the level of substantive testing required, IS auditors should consider both of the following:

-Assessment of inherent risk
- Conclusions on control risk post-compliance testing

The higher the assessment of inherent and control risks, the more audit evidence IS auditors should normally obtain from the performance of substantive audit procedures (ISACA, IS Audit guideline, G13 Use of Risk Assessment in Audit Planning. 2008; p.4).

2.1.5. Degree of Risk

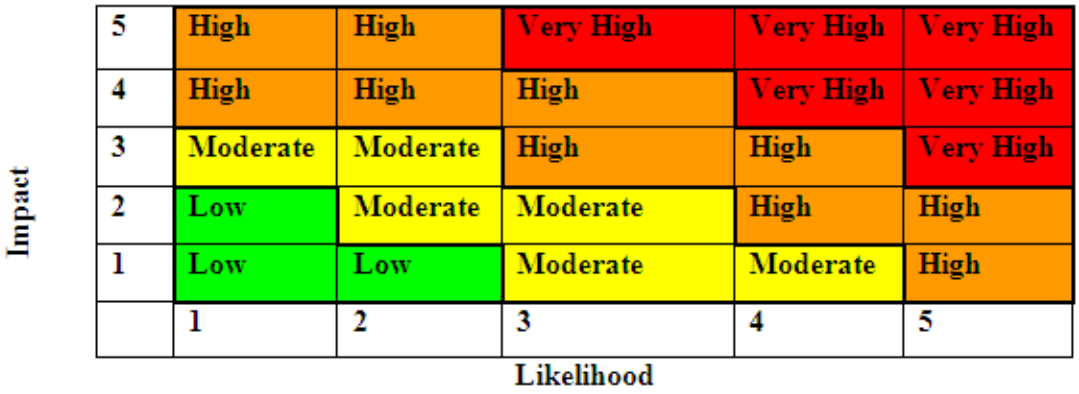

Figure 2.1 risk assessment

Table 2.1 definition of risk

Level of Risk	**Definition**
Extreme	Risk tolerance; improve process within 1 month.
High	Risk tolerance; improve process within 3 months.
Medium	Risk appetite; improve process within 6 months.
Low	Risk appetite; improve process within 1 year.

2.2. IT Risks

The definition of 'IT Risk' becomes important at this stage. There is a common misperception in the industry that IT risks include only security-related IT risks. The ISACA's Risk IT Framework defines IT risks as "the business risks associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise".

The Risk IT Framework covers all IT-related risks as follows:

2.2.1. Not achieving IT value

2.2.2. Late project delivery

2.2.3. Compliance issues

2.2.4. Misalignment with business objectives

2.2.5. Obsolete or inflexible IT architecture

2.2.6. IT service delivery problems

2.2.7. IT skills shortage

(IT risk management: Drivers, challenges and enablers for Australian organizations @ 2013, ISACA Sydney Chapter and ISACA Melbourne Chapter)

2.3. Security Controls Implementation Using Bank of Thailand Standards

2.3.1. Logical Administrative Access Control

2.3.1.1. Access Rights Administration

Financial institutions should have effective access rights to information and systems.

-. Access rights to resources in the system. User is compliant with appropriate individual duties.

- Access rights to improving immediate modifications.

- A review of access rights to set periods related to risks of applications and systems.

- Users should sign acceptable-use policies.

2.3.1.2. Authentication

Authentication is identifying the rights by using unique credentials with entitlements for individuals by evidence-specific persons such as shared secrets, tokens and biometrics. Financial institutions may also use multi-factor authentication. Multi-factor authentication makes security stronger than using a single method. Authentication maintains the confidentiality of data and makes a clear responsibility in systems for identity of the transaction.

Financial institutions should have efficiency authentication with the level of risk that financial institutions are experiencing. The procedures are as follows:

- Selecting actual authentication mechanisms considered appropriate in conjunction with programs, services and systems.

- Determining the suitability of using multi-factor authentication that should be identified as a significant increase in services and electronic payments.

- Encryption is used for authentication, e.g. passwords, PIN codes, digital certificates and biometric templates etc. during transmission and storage on the network.

2.3.1.3. Network Access

Financial institutions should provide security by accessing control to various network hierarchies to prevent unauthorized access as follows:

- Grouping network servers, programs and information in terms of who is entitled access to security domains such as untrustworthy external networks, third-party providers or users).

- Properly establishing requirements for internal access and among security domains by covering access control, software permission, dedicated lines, filtering routers, firewalls, remote access servers and virtual private networks, etc.

- Properly using control measures in order to comply with regularly access.

Financial institutions reduce the vulnerability of the network by reducing less-trusted domains and less secure connections whereby financial institutions should determine how to use protocols, filtering routers, firewalls, gateways and demilitarized zones (DMZ).

2.3.1.4 Operating System Access

Financial institutions provide reliable security for access to devices on operating systems.

- Accessing control systems to assist system utilities.

- Restricting and monitoring access right authentication or privilege access.

- Logging and monitoring access right authentication. If programs access sensitive data, the access should be an alert event when violation is a security event.

-. Improving operating systems by using security patches.

- Securing physical and logical devices which can be connected to the operating system.

2.3.1.5. Application Access

Financial institutions should access control to applications by the following methods:

- Selecting authentication and authorization methods by transactions appropriate with the risks of the system.
- Monitoring and accessing rights to ensure limited access on a need-to-know basis to ensure that users are required to enable their effective and protected use in such a way that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.
- Using time of day to allow users to use.
- Keeping access logs, event logs and recording security events.
- Selecting a rapid analysis of user activities at once.

2.3.1.6. Remote Access

Financial institutions should secure remote access, then access to the system by giving consideration to the following:

- Blocking remote access when business is unnecessary.
- Requiring prior approval for remote access by management with a mandatory process for monitoring compliance in the future.
- Installing appropriate control systems in order to prevent incorrect use of the system.
- Logging and monitoring for remote access.
- Security for remote access devices.
- Using strict authentication and encryption to enhance communication security.

2.3.2. Physical Security

Financial institutions should define demilitarized zones (DMZ) by considering priority and risk. Control and measure are installed for appropriate preventive and detective demilitarized zones (DMZ) in order to prevent risks by taking the following into consideration:

- Unauthorized persons
- Damage of external environment

- Interference of electromagnetic waves

If physical security is not strong, it cannot maintain the confidentiality, integrity and availability of information to ensure that financial institutions reduce risks by installing program or providing policy for demilitarized zones (DMZ).

Demilitarized zones (DMZ) are defined as physical division by providing security policy depending on the importance of information and electronic equipment. An example of a demilitarized zone of the financial institutions requires most stringent security but the location of the branch may have lower security. Financial institutions set different demilitarized zones whether demilitarized zones are located in the same building or computer system.

2.3.2.1. Data Center Security

The important objective is to select the location of the data center. Financial institutions limit risks from internal and external factors by considering locations with the least risk for disasters such as fires, floods, explosions and other natural disasters. In addition, measures are required to prevent or deter intruders from external organizations such as security fences, barricades, motion detectors and other devices.

2.3.2.2. Cabinet and Vault Security.

Cabinet and vault security is required to protect from fire and theft to meet standards and must have the ability to show a level of protection placed on lockers and safes. Therefore, organizations should use safes in relation to the level of importance of the data stored.

2.3.2.3. Physical security for distributed computer systems

Financial institutions consider the importance of the location on computers, data and systems such as the computers located in the front lobby at branches by giving consideration to the following:

- Set the counter to prevent access to personal computers.
- Set keyboard locks on personal computers.
- Removing the disk drives of personal computers.
- Use screensaver passwords.
- Use automated cut-off systems.

Financial institutions should establish policies to protect personal computer from risks.

- Power fluctuations may cause damage to data and personal computers.

- Using personal computers causes a release of static electricity. There are effects on the components of personal computers or damage to memory on personal computers.

- Security of equipment, data stored on file serverd and media can be moved.

- To prevent unauthorized access to networks, systems or data transmission, banks should secure the following if personal computers are used for fund transfers:

- Lock personal computers.

- Protect failed electricity.

- Provide security guards.

- Use magnetic card readers to prove user identity.

- Control access to network devices such as data files, file systems and applications. Financial institutions should be allowed to use personal computers only as necessary.

- Control work stations by using passwords and monitoring activity.

- Insulate communication lines to prevent wiring exposure to publicly accessible places and too close to power grids.

- Prevent malicious users from capturing data and compromising networks.

- Prevent capture of data from the distribution of the spectrum. Walls must be covered in aluminum plate attached to the back room and windows closed with insulation.

2.3.3. Encryption

Financial institutions should use encryption to reduce the risk of data stored and transmission data. Data may be disclosed and changed. The following factors must be taken into consideration when using the encryption method:

- Sufficient strength of encryption in protecting disclosed data.
- Effectiveness and efficiency of key management.
- System reliability.
- Properly encrypted security for data transmission.

2.3.4. Malicious Code Security Control

Financial institutions should be able to prevent the risk of malicious code by implementing the following:

2.3.4.1. Antivirus software should be installed on both the client and host computers.

2.3.4.2. Determine the scope of network communication to protect the strategic plan as necessary.

2.3.4.3. Filter and allow specific information to be passed into the application system.

2.3.4.4. Train employees.

2.3.4.5. Enforce appropriate policies.

2.3.5. System Development, Acquisition and Maintenance

Financial institutions should secure the development of new systems, improve existing systems and supply new systems from third parties.

2.3.5.1. Banks need to establish security measures before development and procurement of a new system.

2.3.5.2. Use security standard guidelines.

2.3.5.3. Use security control, audit trails and logs of input data and processing in addition to changing control processes for effectiveness as follows:

2.3.5.4. Customize parameters or patch programs and help strengthen the security system before the system is actually used.

2.3.5.5. Update installed patch program processes to support new risks.

2.3.5.6. Control software vendors to protect the integrity, accuracy and confidentiality of the source code.

2.3.6. Personnel Security Control

Financial institutions should reduce risks caused by internal users by giving consideration to the following:

2.3.6.1. Check the backgrounds of new employees by considering both crimes and financial history in relation to the importance of the task and the level of access to the system. Generally, the financial institution should consider character references as well as work, education and identity documents issued by the government. Financial institutions should monitor employees because environmental changes may affect employees in the organization, thereby making the system invalid or corrupt.

2.3.6.2. Hiring contracts should cover the responsibilities of the staff such as confidentiality, nondisclosure and authorized use. Financial institutions have a duty to protect confidential customer information and organizational structures. If financial institutions cannot keep secrets, the following consequences will ensure:

- Disclosure to competitors.
- Increasing risk of fraud.
- Damage to corporate reputation.
- Data breach of customer rights.
- Violation of the law.

Therefore, financial institutions must define confidentiality in contracts to inform new employees and contractors. Contracts should also be drafted before access to the system by new employees and contractors.

2.3.6.3. Determine employee responsibilities, accountability of security in job descriptions, employment contracts and training.

2.3.6.4. Provide training to ensure that employees are aware of and observe operations in compliance with policy.

2.3.7. Electronic and Paper-Based Media Handling.

Financial institutions should control and protect access to all types of storage media, including paper, film or any other media. Methods for prevents damage or loss to information are as follows:

2.3.7.1. Set policy and manage the storage of data.

2.3.7.2. Ensure protection and disposal of sensitive information.

2.3.7.3. Monitor the security of data on media in transit and the transfer of information to third parties.

2.3.8. Logging and Data Collection

In the process of collecting and gathering transaction data, financial institutions should perform the following:

2.3.8.1. Determine system components to ensure logging in complete transactions.

2.3.8.2. Consider the level of data logged in each element.

2.3.8.3. Establish security policy.

2.3.8.4. Analyze log files.

2.3.9. Business Continuity Management

Financial institutions should consider the significant problems in preparing business continuity planning.

2.3.9.1. Define the key personnel who will serve in the implementation of business continuity plans, including the training of personnel with such functions.

2.3.9.2. Secure back-up sites and alternative communication networks.

2.3.10. Data Security

Financial institutions must control and protect access to storage media such as all types of paper, tape and other media to prevent damage or loss of data as follows:

2.3.10.1. Establish policies and controls for the management and storage of data.

2.3.10.2. Establish a system to ensure protection and security. Dispose of sensitive media.

2.3.10.3. Secure information in transit and transfers of information to third parties.

2.3.11. Service Provider Oversight

Financial institutions should govern and control outsourced operations or service providers related to security issues as follows:

2.3.11.1. Exercise measures of analysis find service providers (due diligence).

2.3.11.2. Service providers must make a contractual assurance to guarantee security responsibility in operations control and reporting.

2.3.11.3. Contracts must define non-disclosure agreements on systems and information.

2.3.11.4. Third-party reviews must assess the security systems of service providers with appropriate audit processes and testing.

2.3.11.5. Incident response policies and contractual notification requirements should be consistent.

2.3.12. Insurance

Financial institutions should consider scope and coverage to obtain compensation for all risk types and risk reduction by taking advantage of protection under insurance policy.

2.4. COBIT5 for Information Security

Drivers

In COBIT 5, the processes APO13 Manage security, DSS04 Manage continuity and DSS05 Manage security services provide basic guidance on how to define, operate and monitor a system for general security management. However, the assumption made in this publication is that information security is pervasive throughout the entire enterprise, with information security aspects in every activity and process performed. Therefore, COBIT 5 for Information Security provides the next generation of ISACA's guidance on the enterprise governance and management of information security. The major drivers for the development of COBIT 5 for Information Security include:

1. The need to describe information security in an enterprise context including:

– The full end-to-end business and IT functional responsibilities of information security

– All aspects that lead to effective governance and management of information security, such as organisational structures ,policies and culture

– The relationship and link of information security to enterprise objectives

2. An ever-increasing need for the enterprise to:

– Maintain information risk at an acceptable level and to protect information against unauthorised disclosure, unauthorised or inadvertent modifications, and possible intrusions.

– Ensure that services and systems are continuously available to internal and external stakeholders, leading to user satisfaction with IT engagement and services.

– Comply with the growing number of relevant laws and regulations as well as contractual requirements and internal policies on information and systems security and protection, and provide transparency on the level of compliance.

– Achieve all of the above while containing the cost of IT services and technology protection.

Enterprise Enablers

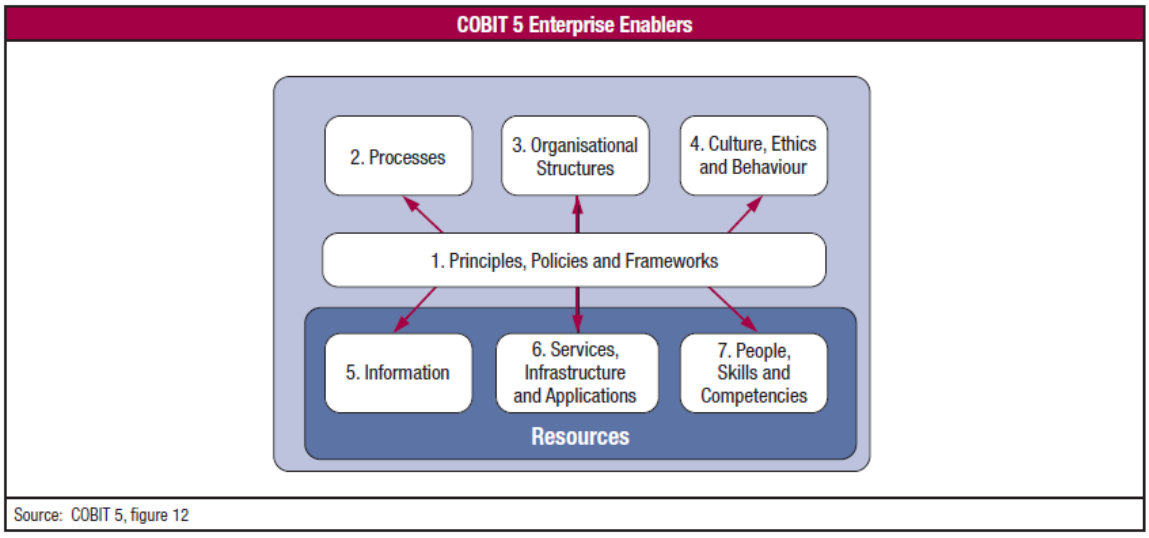

Figure 2.2 COBIT 5 Enterprise Enablers

COBIT 5 for Information Security provides specific guidance related to all enablers.

2.4.1. Principles, Policies and Frameworks

Principles, policies and frameworks refer to the communication mechanisms put in place to convey the direction and instructions of the governing bodies and management, including:

- Principles, policies and framework model
- Information security principles
- Information security policies
- Adapting policies to the enterprises environment
- Policy life cycle

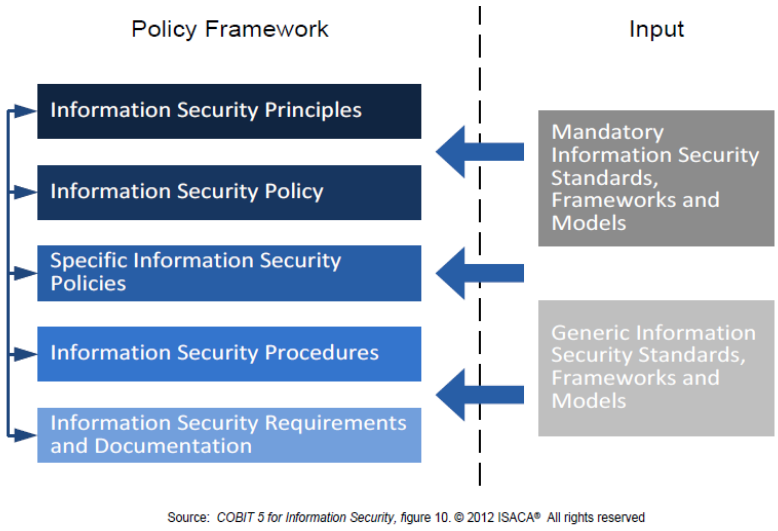

Figure 2.3 COBIT 5 Policy Framework

Policies provide more detailed guidance on how to put principles into practice. Some enterprises may include policies such as:

- Information security policy
- Access control policy
- Personnel information security policy
- Incident management policy
- Asset management policy

2.4.2. Processes

Processes including information security-specific details and activities The COBIT 5 process reference model subdivides the IT-related practices and activities of the

enterprise into two main areas governance and management with management further divided into domains of processes:

-The Governance domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined.

-The four Management domains are in line with the responsibility areas of plan, build, run and monitor (PBRM).

2.4.3. Organisational structures

COBIT 5 examines the organisational structures model from an information security perspective. It defines information security roles and structures and also examines accountability over information security, providing examples of specific roles and structures and what their mandate is, and also looks at potential paths for information security reporting and the different advantages and disadvantages of each possibility.

2.4.4. Culture, ethics and behaviour

In terms of culture, ethics and behaviour, factors determining the success of information security governance and management

Examines the culture, ethics and behaviour model from an information security perspective providing detailed security specific examples of:

2.4.4.1. The Culture Life Cycle measuring behaviours over time to benchmark the security culture some behaviours may include:

- Strength of passwords
- Lack of approach to security
- Adherence to change management practices

2.4.4.2. Leadership and Champions need these people to set examples and help influence culture:

- Risk managers
- Security professionals
- C-level executives

2.4.4.3. Desirable Behaviour; a number of behaviours have been identified that will help positively influence security culture:

- Information security is practiced in daily operations.
- Stakeholders are aware of how to respond to threats.
- Executive management recognises the business value of security.

2.4.5. Information

Information is not only the main subject of information security but is also a key enabler.

2.4.5.1. Information types are examined and reveal types of relevant security information which can include:

- Information security strategy
- Information security budget
- Policies
- Awareness material
- Etc.

2.4.5.2. Information stakeholders as well as the information life cycle are also identified and detailed from a security perspective. Details specific to security such as information storage, sharing, use and disposal are all discussed.

2.4.6. Service capabilities

The services, infrastructure and applications model identifies the services capabilities that are required to provide information security and related functions to an enterprise. The following list contains examples of potential security-related services that could appear in a security service catalogue:

- Provide security architecture.
- Provide security awareness.
- Provide security assessments.
- Provide adequate incident response.
- Provide adequate protection against malware, external attacks and intrusion attempts.

- Provide monitoring and alert services for security related events.

2.4.7. People, skills and competencies

To effectively operate an information security function within an enterprise, individuals with appropriate knowledge and experience must exercise that function. Some typical security-related skills and competencies listed are:

- Information security governance
- Information risk management
- Information security operations

COBIT 5 for Information Security defines the following attributes for each of the skills and competencies:

- Skill definition
- Goals
- Related enablers

2.5. ISO27001 Information Security

2.5.1. Security policy

2.5.1.1. Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

-Information security policy document, an information security policy document shall be approved by management and published and communicated to all employees and relevant external parties.

-Review of the information security policy, the information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

2.5.2. Organization of information security

2.5.2.1. Internal organization

Objective: To manage information security within the organization.

-Management commitment to information security, management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

-Information security coordination, information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.

-Allocation of information security responsibilities, all information security responsibilities shall be clearly defined.

-Authorization process for information processing facilities, a management authorization process for new information processing facilities shall be defined and implemented.

-Confidentiality agreements, requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.

-Contact with authorities, appropriate contacts with relevant authorities shall be maintained.

-Contact with special interest groups, appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

-Independent review of information security, the organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

2.5.2.2. External parties

Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

-Identification of risks related to external parties. The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.

-Addressing security when dealing with customers. All identified security requirements shall be addressed before giving customers access to the organization's information or assets.

-Addressing security in third party agreements, agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

2.5.3. Asset management

2.5.3.1. Responsibility for assets

Objective: To achieve and maintain appropriate protection of organizational assets.

-Inventory of assets, all assets shall be clearly identified and an inventory of all important assets drawn up and maintained.

-Ownership of assets, all information and assets associated with information processing facilities shall be owned by a designated part of the organization.

-Acceptable use of assets, rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

2.5.3.2. Information classification

Objective: To ensure that information receives an appropriate level of protection.

-Classification guidelines, information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.

-Information labeling and handling, an appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.

2.5.4. Human resources security

2.5.4.1. Prior to employment

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

-Roles and responsibilities, security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

-Screening Control, background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations, ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

- Terms and conditions of employment, as part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.

2.5.4.2. During employment

Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities, liabilities and are equipped to support organizational security policy in the course of their normal work and to reduce the risk of human error.

-Management responsibilities, management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

- Information security awareness, education and training; all employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

-Disciplinary process, there shall be a formal disciplinary process for employees who have committed a security breach.

2.5.4.3. Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

-Termination responsibilities, responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.

-Return of assets; all employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

-Removal of access rights; the access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

2.5.5. Physical and environmental security

2.5.5.1. Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

-Physical security perimeter, security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.

-Physical entry controls, secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

-Securing offices, rooms and facilities; physical security for offices, rooms, and facilities shall be designed and applied.

- Protecting against external and environmental threats; physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster shall be designed and applied.

-Working in secure areas, Physical protection and guidelines for working in secure areas shall be designed and applied.

- Public access, delivery and loading areas; access points such as delivery and loading areas and other points where unauthorized persons may enter

the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

2.5.5.2. Equipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

-Equipment siting and protection, equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

-Supporting utilities, Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

-Cabling security, power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

-Equipment maintenance; equipment shall be correctly maintained to ensure its continued availability and integrity.

-Security of equipment off premises, security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.

-Secure disposal or re-use of equipment, all items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

-Removal of property; equipment, information or software shall not be taken off-site without prior authorization.

2.5.6. Communications and operations management

2.5.6.1. Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

-Documented operating procedures; operating procedures shall be documented, maintained, and made available to all users who need them.

-Change management, changes to information processing facilities and systems shall be controlled.

-Segregation of duties, duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

- Separation of development, test and operational facilities; development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.

2.5.6.2. Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

-Service delivery; it shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party.

-Monitoring and review of third party services; the services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.

-Managing changes to third party services; changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

2.5.6.3. System planning and acceptance

Objective: To minimize the risk of systems failures.

-Capacity management; the use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

-System acceptance; acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

2.5.6.4. Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

- Controls against malicious code; detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

- Controls against mobile code; where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.

2.5.6.5. Back-up

Objective: To maintain the integrity and availability of information and information processing facilities.

-Information back-up; back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

2.5.6.6. Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

-Network controls; networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

-Security of network services; security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

2.5.6.7. Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

-Management of removable media, there shall be procedures in place for the management of removable media.

-Disposal of media; media shall be disposed of securely and safely when no longer required, using formal procedures.

-Information handling procedures, Procedures for the handling and storage of information shall be established to protect this
information from unauthorized disclosure or misuse.

-Security of system documentation, system documentation shall be protected against unauthorized access.

2.5.6.8 Exchange of information

Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

-Information exchange policies and procedures; formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.

-Exchange agreements, agreements shall be established for the exchange of information and software between the organization and external parties.

-Physical media in transit; media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

-Electronic messaging, information involved in electronic messaging shall be appropriately protected.

-Business information systems; policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

2.5.6.9. Electronic commerce services

Objective: To ensure the security of electronic commerce services, and their secure use.

-Electronic commerce; information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

-On-line transactions; information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

-Publicly available information, the integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.

2.5.6.10. Monitoring

Objective: To detect unauthorized information processing activities.

-Audit logging; audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

-Monitoring system use, procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.

-Protection of log information, logging facilities and log information shall be protected against tampering and unauthorized access.

-Administrator and operator logs, system administrator and system operator activities shall be logged.

-Fault logging; faults shall be logged, analyzed, and appropriate action taken.

-Clock synchronization, the clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.

2.5.7. Access control

2.5.7.1. Business requirement for access control

Objective: To control access to information.

-Access control policy shall be established, documented, and reviewed based on business and security requirements for access.

2.5.7.2. User access management

Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

-User registration, there shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

-Privilege management, the allocation and use of privileges shall be restricted and controlled.

-User password management, the allocation of passwords shall be controlled through a formal management process.

-Review of user access rights, management shall review users access rights at regular intervals using a formal process.

2.5.7.3. User responsibilities

Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

-Users shall be required to follow good security practices in the selection and use of passwords.

-Unattended user equipment, users shall ensure that unattended equipment has appropriate protection.

-A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

2.5.7.4. Network access control

Objective: To prevent unauthorized access to networked services.

-Policy on use of network services, users shall only be provided with access to the services that they have been specifically authorized to use.

-User authentication for external connections, appropriate authentication methods shall be used to control access by remote users.

-Equipment identification in networks, automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.

-Remote diagnostic and configuration port protection; physical and logical access to diagnostic and configuration ports shall be controlled.

-Segregation in networks; groups of information services, users, and information systems shall be segregated on networks.

-Network connection control; for shared networks, especially those extending across the organization’s boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications

-Network routing control shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

2.5.7.5. Operating system access control

Objective: To prevent unauthorized access to operating systems.

-Secure log-on procedures, access to operating systems shall be controlled by a secure log-on procedure.

-User identification and authentication; all users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

-Systems for managing passwords shall be interactive and shall ensure quality passwords.

-The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

-Session time-out, inactive sessions shall shut down after a defined period of inactivity.

-Restrictions on connection times shall be used to provide additional security for high-risk applications.

2.5.7.6. Application and information access control

Objective: To prevent unauthorized access to information held in application systems.

-Information access restriction, access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

-Sensitive systems shall have a dedicated (isolated) computing environment.

2.5.7.7. Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

-Mobile computing and communications; a formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

-Teleworking; a policy, operational plans and procedures shall be developed and implemented for teleworking activities.

2.5.8. Information systems acquisition, development and maintenance

2.5.8.1. Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

-Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

2.5.8.2. Correct processing in applications

Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications.

-Input data validation; data input to applications shall be validated to ensure that this data is correct and appropriate.

-Control of internal processing; validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

-Message integrity; requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

-Output data validation; data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

2.5.8.3. Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

-A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

-Key management shall be in place to support the organization’s use of cryptographic techniques.

2.5.8.4. Security of system files

Objective: To ensure the security of system files.

-Control of operational software; there shall be procedures in place to control the installation of software on operational systems.

-Protection of system test data; test data shall be selected carefully, and protected and controlled.

-Access to program source code shall be restricted.

2.5.8.5. Security in development and support processes

Objective: To maintain the security of application system software and information.

-Change control procedures; the implementation of changes shall be controlled by the use of formal change control procedures.

-Technical review of applications after operating system changes. When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

-Restrictions on changes to software packages; modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

-Information leakage; opportunities for information leakage shall be prevented.

-Outsourced software development shall be supervised and monitored by the organization.

2.5.8.6. Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

-Control of technical vulnerabilities; timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

2.5.9. Information security incident management

2.5.9.1. Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

-Information security events shall be reported through appropriate management channels as quickly as possible.

-Reporting security weaknesses; all employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

2.5.9.2. Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

-Responsibilities and procedures; management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.

-Learning from information security incidents; there shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

-Collection of evidence; where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

2.5.10. Business continuity management

2.5.10.1. Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

-Including information security in the business continuity management process, a managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

-Business continuity and risk assessment; events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

-Developing and implementing continuity plans including information security; plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

-Business continuity planning framework; a single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

-Testing, maintaining and reassessing business continuity plans; business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

2.5.11. Compliance

2.5.11.1. Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations and of any security requirements.

-Identification of applicable legislation; all relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.

-Intellectual property rights (IPR); appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

-Protection of organizational records; important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

-Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

-Prevention of misuse of information processing facilities; users shall be deterred from using information processing facilities for unauthorized purposes.

-Regulation of cryptographic controls; cryptographic controls shall be used in compliance with all relevant agreements, laws and regulations.

2.5.11.2. Compliance with security policies and standards, and technical compliance

Objective: To ensure compliance of systems with organizational security policies and standards.

-Compliance with security policies and standards; managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

-Technical compliance checking; information systems shall be regularly checked for compliance with security implementation standards.

2.5.11.3. Information systems audit considerations

Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

-Information systems audit controls, audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.

-Protection of information systems audit tools, access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

2.6. Information System Components

Hardware: The term hardware refers to machinery. This category includes the computer itself, which is often referred to as the central processing unit (CPU), and all of its support equipments. Among the support equipments are input and output devices, storage devices and communications devices.

Software: The term software refers to computer programs and the manuals (if any) that support them. Computer programs are machine-readable instructions that direct the circuitry within the hardware parts of the system to function in ways that produce useful information from data. Programs are generally stored on some input / output medium, often a disk or tape.

Peopleware: Every system needs people if it is to be useful. Often the most over-looked element of the system are the people, probably the component that most influence the success or failure of information systems.

Data: Data are facts that are used by programs to produce useful information. Like programs, data are generally stored in machine-readable form on disk or tape until the computer needs them.

Procedures: Procedures are the policies that govern the operation of a computer system. "Procedures are to people what software is to hardware" is a common analogy that is used to illustrate the role of procedures in a system.

2.7. Theory Classified by Information System Components

2.7.1. Hardware

Table 2.2 Theory classified by hardware

COBIT5	ISO 27001	Security Control Implementation using Bank of Thailand Guidelines
- Service capability	- Security policy - Physical and environmental security - Communications and operations management	- Physical Security Control

Hardware security compares three theories in which COBIT 5 focuses on corporate governance and management, including services, infrastructure and application enablers covering security architecture, adequate security and configured systems aligned with security requirements, security architecture, monitoring and alert services for security-related events.

ISO27001 focuses on security policy as well as physical and environmental security with communications and operations management.

Security controls implementation using Bank of Thailand guidelines focuses on physical security control.

2.7.2. Software

Table 2.3 Theory classified by software

COBIT5	ISO 27001	Security Controls Implementation Using Bank of Thailand Guidelines
- Service capability	- Security policy - Communications and operations management - Access Control - Information systems acquisition, development and maintenance; information security incident management	- Access control - Encryption - Malicious code security Control - System development, Acquisition and maintenance

Software security compares three theories in which COBIT 5 focuses on corporate governance and management, including secure development, adequate security and configured systems aligned with security requirements and security architecture, user access and access rights in line with business requirements, adequate protection against malware, external attacks and intrusion attempts, adequate incident response, security testing and monitoring and alert services for security-related events.

ISO27001 focuses on security policy, physical security, environmental security, communications operations management and operations management.

Security controls implementation uses Bank of Thailand guidelines focused on physical security control.

2.7.3. Peopleware

Table 2.4 Theory classified by peopleware

COBIT5	ISO 27001	Security Controls Implementation Using Bank of Thailand Guidelines
- Principles, policies and frameworks - Organizational structures - Processes - Culture, ethics and behavior - People, skills and competencies	- Security policy - Internal organization - Human resources security - Communications and operations management	- Personal security control

Peopleware security compares three theories in which COBIT 5 focuses on corporate governance and management, including principles, policies and frameworks; organizational structures; APO13 management security processes, DSS04 management continuity and DSS05 Management security services; culture, ethics and behavior; people, skills and competency.

ISO27001 focuses on security policy, internal organization, human resources security, communications and operations management.

Security controls implementation uses Bank of Thailand guidelines focused on personal security control.

2.7.4. Data

Table 2.5 Theory classified by data

COBIT5	ISO 27001	Security Controls Implementation Using Bank of Thailand Guidelines
- Information security	- Security policy - Asset management - Communications and operations management	- Electronic and paper-based media handing - Logging and data collection - Data security

Data security compares three theories in which COBIT 5 focuses on corporate governance and management, including information security strategy, budget, planning, policies, requirements, awareness material, review reports and dashboard.

ISO27001 focuses on security policy, asset management, communications management and operations management.

Security controls implementation uses Bank of Thailand guidelines focused on electronic and paper-based media handing, data security, logging and data collection.

2.7.5. Procedures

Table 2.6 Theory classified by procedure

COBIT5	ISO 27001	Security Controls Implementation Using Bank of Thailand Guidelines
- Principles, policies and frameworks	- Security policy - Communications and	- Service provider oversight

Table 2.6 Theory classified by procedure (cont.)

COBIT5	ISO 27001	Security Controls Implementation Using Bank of Thailand Guidelines
- People, skills and competencies	operations management - Business continuity management - Compliance	- Business continuity management - Insurance

Procedures compares three theory in which COBIT 5 focuses on corporate governance and management, including principles, policies and frameworks; people, skills and competencies.

2.8. Benefits

2.8.1. Benefits of COBIT 5

Using COBIT 5 for information security brings a number of information security-related capabilities to the enterprise which can result in a number of enterprise benefits such as the following:

- Reduced complexity and increased cost-effectiveness due to improved and easier integration of information security standards, good practices and/or sector-specific guidelines.
- Increased user satisfaction with information security arrangements and outcomes.
- Improved integration of information security in the enterprise.
- Informed risk decisions and risk awareness.
- Improved prevention, detection and recovery.
- Reduced (impact of) information security incidents.
- Enhanced support for innovation and competitiveness.
- Improved management of costs related to the information security function.

- Better understanding of information security.

2.8.2. Benefits of ISO 27000 Information Security

ISO 27001 is the only auditable international standard that defines the requirements for an information security management system (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls. ISO 27001 helps protect information assets and gives confidence to interested parties, including an organization's customers. The standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

- Fewer incidents.
- Fewer disruptions.
- Less time spent in responding to accidents and incidents.
- More time to spend on proactive measures.
- Lower client audit requirements.
- Less negative press meaning less time and money spent on damage limitation measures.
- Fewer resources spent on finding new customers and investors.
- Opportunities for positive PR.
- Greater productivity.
- Less time and money spent in responding to incidents.
- Understanding of business information processes.
- Better ability to reassure customers and internal parties.

2.8.3. Benefits of security controls implementation using Bank of Thailand Guidelines

- Improved integration of information security in the enterprise.
- Improved information technology governance in the enterprise.
- Suggestions for information security.
- Less time and money spent in responding to incidents.
- Use of information security audits.
- Customer assurance.
- Reduced information security risks.

CHAPTER III
MATERIALS AND METHODS

3.1. Population Sampling

The population for the present study was composed of information technology officers and managers as follows:

3.1.1. IT Developers responsible for the following:

- Development and maintenance of computerized systems for requirements in analyses related to business needs.
- Development and improvement of computerized systems used on the job.
- Planning, resource management, monitoring and control of implementing plans.
- Offering advice to users in checking computer systems (UAT).
- Training users to use computerized systems in related departments.
- Making and preparing user manuals.
- Preparing documentation for delivery systems.
- Joining in the development of operations with vendors for education on the requirements for analysis of systems related to bank compliance.
- Applying version control and document control.
- Maintaining storage controllers such as applications and documents of computer systems for enhancing the operations of the organization.
- Reviewing project plans and information systems development of banks and consultation.
- Tracking and reporting on the implementation of project plans or system development.
- Analyzing the problems and risks in project implementation.

- Evaluating the of use information systems by users.

3.1.2. Network administrators responsible for the following:

- Supervising the processing of data by computers at data centers and disaster recovery centers to ensure continuous and efficient work flow.
- Maintaining computers and devices to work normally; controlling information and reporting to authorities.
- Supporting and studying information processes on computers at data centers and disaster recovery centers.
- Monitoring, analyzing and troubleshooting programs for continuous and efficient operations.
- Maintaining information systems.
- Creating, removing and changing branches on systems.

3.1.3. Security administrators responsible for the following:

- Governing the operations of various departments to ensure compliance with security policies.
- Assessing risks and reviewing security policy, including suggestions to prevent and reduce risks.
- Considering system development concerning information security.
- Assessing systems and information technology equipment concerned with information security.
- Managing bank accounts.
- Monitoring, conducting surveillance and analyzing events when information security is breached.
- Managing logs.
- Designing and installing antivirus programs, controlling systems, and protecting against computer viruses.
- Analyzing and fixing problems caused by viruses.

3.1.4. IT Operation administrators responsible for the following:

- Analysis, design, installation, maintenance and troubleshooting software on host computers.

- Monitoring and evaluation of the efficiency of using resources on host computers.

The roles of the population compared to 12 criteria used in the research that each population will focus on information security as follows:

1. Information technology officers

- IT developers will focus on information security and access control, system development, acquisition and maintenance, encryption, personal security control, insurance, service provider oversight, electronic and paper-based media handing and personal security control.

- Network administrators will focus on information security access control, physical security control, business continuity management and data security.

- Security administrators will focus on information security access control, malicious code security control, logging and data collection and data security.

- IT operation administrators will focus on the information security access control, electronic and paper-based media handing, logging and data collection and data security.

2. Information technology managers will focus on security information as follows:

- Access control
- Physical security control
- Encryption
- Malicious code security control
- System development, acquisition and maintenance
- Personal security control
- Electronic and paper-based media handing

- Logging and data collection
- Data security
- Service provider oversight
- Business continuity management
- Insurance

3.2. Sample Size

The sample size for IT officers was calculated based on Yamane's formula (Yamane, 1967) as follows:

$$n = \frac{N}{1+Ne^2}$$

where n = the sample size

N = population size

e= 5 percentage point error

Case 1: IT Departments using a fail system; (N = 42; e = 0.05)

$$n = \frac{N}{1+Ne^2}$$

$$= \frac{42}{1+42(0.05)^2} = 38$$

Case 2: IT Department under normal circumstances. (N = 148; e = 0.05)

$$= \frac{148}{1+42(0.05)^2} = 108$$

3.3. Sampling

Purposive sampling was employed for selecting the sample based on appropriate inclusion criteria for study. In the present study, the researcher considered officers using the information technology of banks. Hence, the information is reliable, consistent with facts and can be used for benefit. The researcher will collect data from IT officers and managers of banks.

3.4. Research Criteria

The study of concepts, theories and research make it possible to set independent variables. The category of security controls implementation from information system security audit-guided practices by using Bank of Thailand Guideline involves the following 12 categories:

- Access control
- Physical security control
- Encryption
- Malicious code security control
- System development, acquisition and maintenance
- Personal security control
- Electronic and paper-based media handing
- Logging and data collection
- Data security
- Service provider oversight
- Business continuity management
- Insurance

3.5. Research Instrumentation

3.5.1. Questionnaire

This research will use a questionnaire containing a survey opinion sample. The sample is information technology officers and managers. The questionnaire is divided into the following three parts:

Part 1 - Background of respondents

- Gender
- Age
- Education
- Occupation
- Position

Part 2 - Opinions of users divided into 12 categories according to the research criteria. Each criterion will consist of 5 questions. The findings are discussed in terms of the 12 categories as follows:

1. Access Control

1.1. Do you think priority rights to access and improvements access rights should be periodically changed? If so, how often?

Table 3.1 Question 1 of access control

Frequency	Score
Immediately	5
Monthly	4
Every 3 months	3
Every 6 months	2
Over one year	1

1.2.How often your friends show or share user names and passwords?

Table 3.2 Question 2 of access control

Frequency	Score
Never	5
About 1-5 times per month	4
About 5-10 times per month	3
About 10-15 times per month	2
Always	1

1.3.How often do you change the password on your system?

Table 3.3 Question 3 of access control

Frequency	Score
Monthly	5
Every 3 months	4

Table 3.3 Question 3 of access control (cont.)

Frequency	Score
Every 6 months	3
Over one year	2
Never	1

1.4. How long did you wait to change your default password after receiving it?

Table 3.4 Question 4 of access control

Frequency	Score
Immediately	5
1 month	4
3 months	3
6 months	2
Over one year	1

1.5. Do you have operation access control to your bank? (More than one choice possible)

1.5.1. Restricted authority

1.5.2. Tracking and monitoring

1.5.3. Granting privilege access

1.5.4. Logging

1.5.5. Security Patches

Table 3.5 Question 5 of access control

Number of Control Types	Score
5 types	5
4 types	4
3 types	3
2 types	2
1 or no types	1

2. Physical Security Control

2.1. What security controls does the bank use at the datacenter? (More than one choice possible)

2.1.1. A security guard before entering the building.

2.1.2. ID card exchange before entering the building.

2.1.3. Log building entries and exits.

2.1.4. Submit written application forms before entering the data center.

2.1.5. Place a security guard before entering the data center.

2.1.6. Exchange cards before entering the data center.

2.1.7. Log data center entries and exits.

Table 3.6 Question 1 of physical security control

Number of Control Types	Score
7 types	5
5-6 types	4
4 types	3
2-3 types	2
1 or no types	1

2.2. To what kinds of disaster has your bank data center been exposed? (More than one choice possible)

2.2.1. Fire

2.2.2. Flood

2.2.3. Earthquake

2.2.4. Explosion

2.2.5. Propagation of electromagnetic waves

2.2.6. Power interruption

2.2.7. Plane crash

2.2.8. Chemical hazard

Table 3.7 Question 2 of physical security control

Number of Disaster Types	Score
None	5
1-3 types	4
4 types	3
5-7 types	2
All types	1

2.3. What kinds of warnings and information are provided during data center emergencies? (More than one choice possible)

2.3.1.Auto warning switch when the circuit is cut off

2.3.2. Detection equipment lighting

2.3.3. Radar equipment to record video images of the perpetrator

2.3.4. CCTV

2.3.5. Gas Fire

2.3.6. Smoke detectors

2.3.7. Elevated floor computer room

2.3.8. Heat detectors

Table 3.8 Question 3 of physical security control

Number of Control Types	Score
8 types	5
5-7 types	4
4 types	3
1-3 types	2
No control	1

2.4.What safety or cabinet features are provided for information security? (More than one choice possible)

2.4.1. At least 1 hour of heat prevention

2.4.2. Theft prevention or difficult movement

2.4.3. Moisture prevention

2.4.4. Shock absorption

2.4.5. Passwords and locks

Table 3.9 Question 4 of physical security control

Number of Control Types	Score
5 types	5
4 types	4
3 types	3
2 types	2
1 types	1

2.5. How are physical security measures or settings established for the distributed computing system? (More than one choice possible)

2.5.1. Demarcation of work.

2.5.2. PC key locks.

2.5.3. Screensaver passwords for monitors.

2.5.4. Automated system cut-off.

2.5.5. UPS protected power outage to prevent data corruption.

2.5.6. PC user names and passwords.

2.5.7. Are there security settings to prevent unauthorized access to files such as set passwords, limited rights and others?

Table 3.10 Question 5 of physical security control

Number of Security Settings	Score
7 security settings	5
5-6 security settings	4
4 security settings	3
2-3 security settings	2
1 or no security settings	1

3. Encryption

3.1. What parts of the information technology environment are encrypted? (More than one choice possible)

3.1.1. Operation system

3.1.1. Middleware or equipment

3.1.1. Applications

3.1.1. File system

3.1.1. Protocol

Table 3.11 Question 1 of encryption

Number of Encryption Types	Score
5 types	5
4 types	4
3 types	3
2 types	2
1 or no types	1

3.2. How many strong encryption techniques are used to protect disclosure of information to other organizations?

Table 3.12 Question 2 of encryption

Number of Disclosures Protected	Score
No disclosures	5
One disclosure per year	4
4 disclosures per year	3
12 disclosures per year	2
12 disclosures per year	1

3.3. Did you think the banking system is reliable in protecting things such as customer information, financial information, etc? (More than one choice possible)

3.3.1. Information is non-disclosed.

3.3.2. Information integrity is maintained and completely protected.

3.3.3. System authentication is employed.

Table 3.13 Question 3 of encryption

Number of Reliable Protection Types	Score
3 types	5
2 types	3
1 type or no types	1

3.4. What encryption management does the bank use? (More than one choice possible)

3.4.1. Data Handing

3.4.2. Key Management

3.4.3. Actual Encryption

Table 3.14 Question 4 of encryption

Number of Encryption Management Types	Score
3 types	5
2 types	3
1 or no types	1

3.5. Do you think encryption techniques are effective when intruders attempt to change information?

Table 3.15 Question 5 of encryption

Frequency of Information Changes with Permission	Score
Never	5
Once per year	4
4 times per year	3
12 times per year	2
More than 12 times per year	1

4.Malicious Code Security Control

4.1. Do you think malicious code protection is important for banks?

Table 3.16 Question 1 of malicious code security control

Frequency	Score
Very important	5
Important	4
Moderately important	3
Slightly important	2
Least important	1

4.2.Do you have an anti-virus program installed on your computer?

Table 3.17 Question 2 of malicious code security control

Response	Score
Yes	5
No	1

4.3. How often do you update the anti-virus software on your computer?

Table 3.18 Question 3 of malicious code security control

Anti-Virus Update Frequency	Score
Weekly	5
Monthly	4
Every 3 months	3
Every 6 months	2
Over a year or never	1

4.4. Do you think malicious code surveillance is necessary?

Table 3.19 Question 4 of malicious code security control

Response	Score
Yes	5
No	1

4.5. Do you have bank channels for employee awareness of information security? (More than one choice possible)

4.5.1. Training

4.5.2. Bank magazine

4.5.3. Intranet/Internet

4.5.4. Information security activities

4.5.5. Bank advertisements

4.5.6. E-mails

4.5.7. Social networks

Table 3.20 Question 5 of malicious code security control

Number of Bank Channels for IT Awareness	Score
7 channels	5
5-6 channels	4
4 channels	3
2-3 channels	2
1 or no channels	1

5.System Development, Acquisition and Maintenance

5.1. Do you use information security policy for application development? If so, how? (More than one choice possible)

5.1.1. Define security measures before developing or procuring new systems.

5.1.2. Documented approval for using system.

5.1.3. Store development of document writing

5.1.4. Use of international standards for information security

5.1.5. Use of audit trails.

5.1.6. Logging.

5.1.7. Patch programs to help strengthen security when there are system changes.

Table 3.21 Question 1 of system development, acquisition and maintenance

Number of IT Policies for Application Development	Score
7 policies	5
5-6 policies	4
4 policies	3
2-3 policies	2
1 or no policies	1

5.2. Do you have information security standards for data input to the system? (More than one choice possible)

5.2.1. Controlling access to input and change data.

5.2.2. Checking errors in input data.

5.2.3. Verifying unusual or suspicious activity.

5.2.4. Reviewing and approving for sensitive data.

Table 3.22 Question 2 of system development, acquisition and maintenance

Number of Information Security Controls for Input	Score
4 controls	5
3 controls	4
2 controls	3
1 controls	2
No control	1

5.3. Do you have information security standards for processing data in the system? (More than one choice possible)

5.3.1. Batch control totals

5.3.2. Hashing data after processing data

5.3.3. Information is changed that it should show information.

5.3.4. Check process in order

Table 3.23 Question 3 of system development, acquisition and maintenance

Number of Data Processing Control Types	Score
4 controls	5
3 controls	4
2 controls	3
1 control	2
No control	1

5.4. Is approval required before program changes?

Table 3.24 Question 4 of system development, acquisition and maintenance

Response	Score
Yes	5
No	1

5.5. Do you have version control when changing programs?

Table 3.25 Question 5 of system development, acquisition and maintenance

Response	Score
Yes	5
No	1

6. Personal Security Control

6.1. Do you have a bank that checks new employee backgrounds? If so, how? (More than one choice possible)

6.1.1. History of old organization

6.1.2. Criminal history

6.1.3. Financial history

6.1.4. Family background

6.1.5. Educational history

Table 3.26 Question 1 of personal security control

Number of Checks Applied	Score
5 checks	5
4 checks	4
3 checks	3
2 checks	2
1 checks	1

6.2.What is the definition of contract significance? (More than one choice possible)

6.2.1. Non-disclosure of sensitive information

6.2.2. No violation of customer information and rights

6.2.3. No violation of the organization

6.2.4. No damage to bank's reputation

6.2.5. No criminal violation of the law.

6.2.6. Prohibition of fraud in the work.

Table 3.27 Question 2 of personal security control

Number of Control Types	Score
6 types	5
4-5 types	4
3 types	3
1-2 types	2
No control	1

6.3. Do you have policy awareness acknowledgements for your bank?

Table 3.28 Question 3 of personal security control

Response	Score
Yes	5
No	1

6.4. Does your bank hold training for awareness of information security policy or law?

Table 3.29 Question 4 of personal security control

Response	Score
Yes	5
No	1

6.5. How can information security training be described? (More than one choice possible)

6.5.1. Acceptable use of policy

6.5.2. Desktop security

6.5.3. Log-on requirements

6.5.4. Password administration guidelines

6.5.5. Social engineering guidelines

Table 3.30 Question 5 of personal security control

Number of Information Security Training Control Types	Score
5 types	5
4 types	4
3 types	3
2 types	2
1 or no types	1

7.Electronic and Paper-Based Media Handing

7.1. How should the bank's sensitive data be stored? (More than one choice possible)

7.1.1. Paper documents

7.1.2. Back-up tapes

7.1.3. Disks

7.1.4. Cassettes

7.1.5. Optical storage

Table 3.31 Question 1 of electronic and paper-based media handing

Number of Sensitive Data Storage Control Types	Score
5 types	5
4 types	4
3 types	3
2 types	2
1 or no types	1

7.2. Has your bank ever been able to access storage media from an intruder? (More than one choice possible)

7.2.1. Exposure of corporate secrets

7.2.2. Breaches in customer confidentiality

7.2.3. Alteration of data

7.2.4. Disruption of business activities

7.2.5. Intruder damage storage media

Table 3.32 Question 2 of electronic and paper-based media handing

Number of Intrusion Types	Score
1 or no intrusion types	5
2 types	4
3 types	3
4 types	2
5 types	1

7.3. How often does the bank review policy and storage media procedures?

Table 3.33 Question 3 of electronic and paper-based media handing

Frequency of Policy Review & Storage Media Procedures	Score
Monthly	5
Every 3 months	4
Every 6 months	3
Annually	2
No reviews	1

7.4. How does your bank protect handling and storage? (More than one choice possible)

7.4.1. Fire protection

7.4.2. Flood protection

7.4.3. Limited access

7.4.4. Tracking

7.4.5. Logging

Table 3.34 Question 4 of electronic and paper-based media handing

Handling & Storage Protection Control Types	Score
5 types	5
4 types	4
3 types	3
2 types	2
1 or no types	1

7.5. How does your bank security control storage media for transit data? (More than one choice possible)

7.5.1. Strict selection of company or personnel for supplying storage media

7.5.2. Verification of storage media

7.5.3. Establishment of storage media methods

7.5.4. Use of encryption for transit sensitive data

7.5.5. Establishment of non-disclosure agreements with transit data personal

Table 3.35 Question 5 of electronic and paper-based media handing

Number of Storage Media Control Types	Score
5 types	5
4 types	4
3 types	3
2 types	2
1 or not types	1

8. Logging and Data Collection

8.1. What benefits do you think bank data storage security will yield? (More than one choice possible)

8.1.1. Identification of responsible parties

8.1.2. Response to security

8.1.3. System monitoring

8.1.4. Enforcing employee, customer and partner compliance with information security policies.

8.1.5. Review and analysis of unauthorized system access

8.1.6. Report support to human resource management

8.1.7. Awareness of security violations

8.1.8. Assistance in compromised system reconstruction

Table 3.36 Question 1 of logging and data collection

Number of Data Security Benefits	Score
7-8 benefits	5
5-6 benefits	4
4 benefits	3
2-3 benefits	2

Table 3.36 Question 1 of logging and data collection (cont.)

Number of Data Security Benefits	Score
0-1 benefits	1

8.2. What logs does your bank keep? (More than one choice possible)

8.2.1. Transaction by internet channels

8.2.2. Firewall logs

8.2.3. Event logs

8.2.4. Operation system logs

8.2.5. Access logs

8.2.6. Remote access logs

Table 3.37 Question 2 of logging and data collection

Number of Log Types	Score
6 types	5
4-5 types	4
3 types	3
1-2 types	2
No logs	1

8.3. Do you have log details? (More than one choice possible)

8.3.1. Transaction ID

8.3.2. Terminal ID

8.3.3. Date and time

8.3.4. Access system behavior

8.3.5. Request service

8.3.6. Transaction

Table 3.38 Question 3 of logging and data collection

Number of Log Details	Score
6 details	5
4-5 details	4
3 details	3
1-2 details	2
No details	1

8.4. How do you think your bank controls and monitors logs? (More than one choice possible)

8.4.1. Log encryption

8.4.2. Log integrity

8.4.3. Log back-up and disposal

8.4.5. Log storage independently and separately from other computers.

8.4.6. Writable log storage media (not once, but multiple times).

8.4.7. Centralized logging

8.4.8. Parameter configuration that cannot be edited.

Table 3.39 Question 4 of logging and data collection

Number of Log Control and Monitoring Types	Score
7-8 types	5
5-6 types	4
4 types	3
2-3 types	2
0-1 types	1

8.5. Do you have your bank monitor violations on security systems for analysis and response to events?

Table 3.40 Question 5 of logging and data collection

Response	Score
Yes	5
No	1

9. Data Security

9.1. Do you have a bank with established data security policy?

Table 3.41 Question 1 of data security

Response	Score
Yes	5
No	1

9.2. Do you have a bank that focuses on protection and disposal of storage media?

Table 3.42 Question 2 of data security

Response	Score
Yes	5
No	1

9.3. Do you think your bank focuses on security of transport and transfers of information between organizations?

Table 3.43 Question 3 of data security

Response	Score
Yes	5
No	1

9.4. Does your bank focus on classified information, defining the use of data file protection and setting priority of information?

Table 3.44 Question 4 of data security

Response	Score
Yes	5
No	1

9.5. Does your bank limit employee rights?

Table 3.45 Question 5 of data security

Response	Score
Yes	5
No	1

10. Service Provider Oversight

10.1. Do you think your bank has analyzed the procurement and selection of service providers?

Table 3.46 Question 1 of service provider oversight

Response	Score
Yes	5
No	1

10.2. Do you think banks focus on confidentiality and integrity of information by contracts with service providers?

Table 3.47 Question 2 of service provider oversight

Response	Score
Yes	5
No	1

10.3. Does you banks verify by external auditors in order to assess the security of the services?

Table 3.48 Question 3 of service provider oversight

Response	Score
Yes	5
No	1

10.4. Is your bank consistent in terms of response policies with service provider compliance in order to provide service alerts regarding violation events?

Table 3.49 Question 4 of service provider oversight

Response	Score
Yes	5
No	1

10.5. Does your bank gain verification from external audits?

Table 3.50 Question 5 of service provider oversight

Response	Score
Yes	5
No	1

11. Business Continuity Management

11.1. How important does your bank consider having sufficient computers and printers for use?

Table 3.51 Question 1 of business continuity management

Response	Score
Very important	5
Important	4
Moderately important	3
Slightly important	2
Least important	1

11.2. Does your bank use efficient computers and printers compared to usage?

Table 3.52 Question 2 of business continuity management

Frequency of Computer/Printer Failures	Score
Over a year to never	5
Every 6 months	4
Every 3 months	3
Monthly	2
Weekly	1

11.3. Do you think business continuity planning is important to business?

Table 3.53 Question 3 of business continuity management

Response	Score
Very important	5
Important	4
Moderately important	3
Slightly important	2
Least important	1

11.4. How often does your bank prepare business continuity planning by department?

Table 3.54 Question 4 of business continuity management

Response	Score
Every 3 months	5
Every 6 months	4
Annually	3
Every 2 years	2
Never	1

11.5. Is your bank aware of business continuity planning?

Table 3.55 Question 5 of business continuity management

Response	Score
Yes	5
No	1

12. Insurance

12.1. Does your bank's insurance cover system risks?

Table 3.56 Question 1 of insurance

Response	Score
Yes	5
No	1

12.2. Do you have additional insurance coverage when new system risks occur?

Table 3.57 Question 2 of insurance

Response	Score
Yes	5
No	1

12.3. What risks do you think insurance covers? (More than one choice possible)

12.3.1. Editing text on website.

12.3.2. Denial of service attacks.

12.3.3. Loss of income

12.3.4. Information theft

12.3.5. Violation of customer confidentiality

12.3.6. Data destruction or changes by intrusion

12.3.7. Counterfeited customer information

Table 3.58 Question 3 of insurance

Number of Risks Covered by Insurance	Score
7 risks	5
5-6 risks	4
4 risks	3
2-3 risks	2
0-1 risks	1

12.4. Do you think insurance offers sufficient coverage for reputation risks?

Table 3.59 Question 4 of insurance

Response	Score
Yes	5
No	1

12.5. Do you think insurance offers sufficient coverage for customer confidentiality risks?

Table 3.60 Question 5 of insurance

Response	Score
Yes	5
No	1

Discussion of research findings from questionnaire use of interval scale

Interval scale = (Maximum – Minimum) / Range

= (5-1)/5

= 0.80

4.21 – 5.00 means Excellent

3.41 – 4.20 means Good

2.61 – 3.40 means Normal

1.81 – 2.60 means Few

1.00 – 1.80 means Poor

Interval scale = (Maximum – Minimum) / Range
= (5-1)/3
= 1.33

3.67 – 5.00 means Excellent

2.33 – 3.66 means Normal

0.99 – 2.32 means Poor

Interval scale = (Maximum – Minimum) / Range
= (5-1)/2
= 2

3.00 – 5.00 means Excellent

0.99 – 2.99 means Poor

Part 3 - Opinions of managers divided into 12 categories according to the research criteria. Priority was ranked by scores of 1-5 points (High =1; Low = 5).

- Access control
- Physical security control
- Encryption
- Malicious code security control
- System development, acquisition and maintenance
- Personal security control
- Electronic and paper-based media handing
- Logging and data collection
- Data security
- Service provider oversight
- Business continuity management
- Insurance

3.5. Research Methodology

3.5.1. Review of information system security audit guide practices for the Bank of Thailand and other theories.

3.5.2. Collection of theories to prepare research criteria by using the criteria of information system security audit guide practices for the Bank of Thailand.

3.5.3. Creation of a questionnaire for officers and managers separated into the following three parts.

Part 1 - Background of respondents

- Gender
- Age
- Education
- Occupation
- Position

Part 2 - Opinions of users divided into 12 categories according to the research criteria. Each criterion will consist of 5 questions. The findings will be discussed in terms of each of the 12 categories as follows:

Part 3 - Opinions of managers divide into 12 categories according to the research criteria with priority ranked by scores of 1-5 points (High =1; Low = 5).

3.5.4. The questionnaires were tested with approximately ten sets of IT officers and IT managers. The IT officers and IT managers were able to understand the questionnaires. Accordingly, the questionnaires were involved with information system security audit guide practices for the Bank of Thailand. The questionnaires were then improved.

3.5.5. The questionnaires were used to ask the samples as follows:

3.5.5.1. IT Department had caused system failures.

3.5.5.2. IT Department had caused system success.

3.5.5.3. IT Manager concerned with the research criteria from failure of the IT department and the IT department in general.

3.5.6. The questionnaires concluded as internal benchmarking with a comparison of the findings on the IT Department in general and on IT department failure. The bank is aware of IT operational ability.

3.5.7. The research findings were analyzed.

3.5.7.1. Bank operations information security strengths and weaknesses were determined.

3.5.7.2. Information security risk protection guidelines were established.

3.6. Data Collection

3.6.1. Study of theories.

Study of the Information System Security Audit Guide Practices for Bank of Thailand then information systems completely ensure security.

3.6.2. Collection

3.6.2.1. Information System Security Audit Guide Practices for Bank of Thailand

3.6.2.2. ISO 27001 Information Security Management Systems

3.6.2.3. Benchmarking

CHAPTER IV
RESULTS

Survey Results of Sample Population Characteristics

1.Classified by Gender

1.1. Population of Successful Project

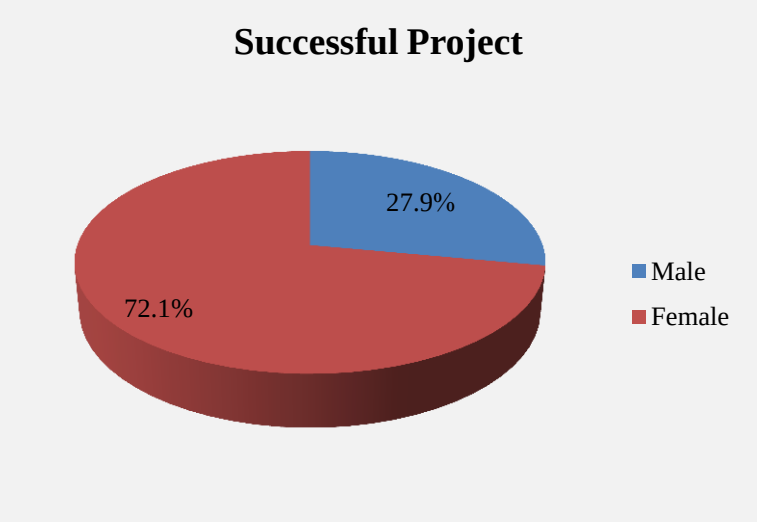

Figure 4.1 Population of Successful Project

Figure can be described as follows:

Table 4.1 Population of successful project details classified by gender

Gender	Sample Number	Percentage
Male	43	27.9
Female	111	72.1
Total	**154**	**100**

1.2. Population of Failed Project

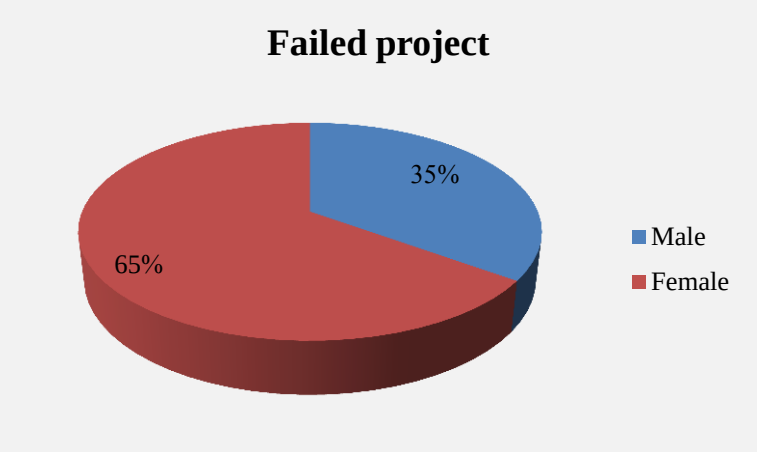

Figure 4.2 Population of Failed Project

Figure can be described as follows:

Table 4.2 Population of failed project details classified by gender

Gender	Sample Number	Percentage
Male	14	35
Female	26	65
Total	**40**	**100**

2.Classified by Age and Education

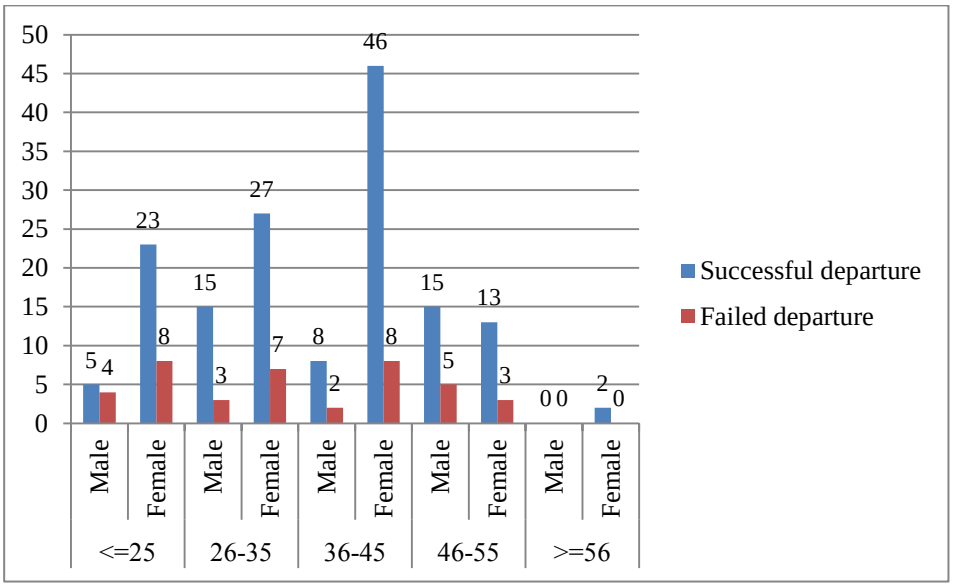

Figure 4.3 Classified by Age

Figure can be described as follows:

Table 4.3 Population of successful project and failed details classified by age and education

Age	Gender/ Education	Successful Project		Failed Project	
		Number	Percentage	Number	Percentage
<=25	**Male**				
	-Bachelor	3	10.71	2	16.67
	-Master	2	7.14	2	16.67
	Female				
	-Bachelor	11	39.29	3	25.00
	-Master	12	42.86	5	41.67
		28	**100**	**12**	**100**
26-35	**Male**				
	-Bachelor	14	33.33	1	10.00
	-Master	1	2.38	2	20.00
	Female				
	-Bachelor	9	21.43	3	30.00
	-Master	18	42.86	4	40.00
		42	**100**	**10**	**100**
36-45	**Male**				
	-Bachelor	7	12.96	2	20.00
	-Master	1	1.85	0	0.00
	Female				
	-Bachelor	33	61.11	8	80.00
	-Master	13	24.07	0	0.00
		54	**100**	**10**	**100**
46-55	**Male**				
	-Bachelor	10	35.71	2	25.00
	-Master	5	17.86	3	37.50
	Female				
	-Bachelor	9	32.14	2	25.00

Table 4.3 Population of successful project and failed details classified by age and education (cont)

Age	Gender/ Education	Successful Project		Failed Project	
		Number	Percentage	Number	Percentage
	-Master	4	14.29	1	12.50
		28	**100**	**8**	**100**
>=56	**Male**				
	-Bachelor	0	0	0	0
	-Master	0	0	0	0
	Female				
	-Bachelor	2	100	0	0
	-Master	0	0	0	0
		2	**100**	**0**	**0**

3.Classified by position

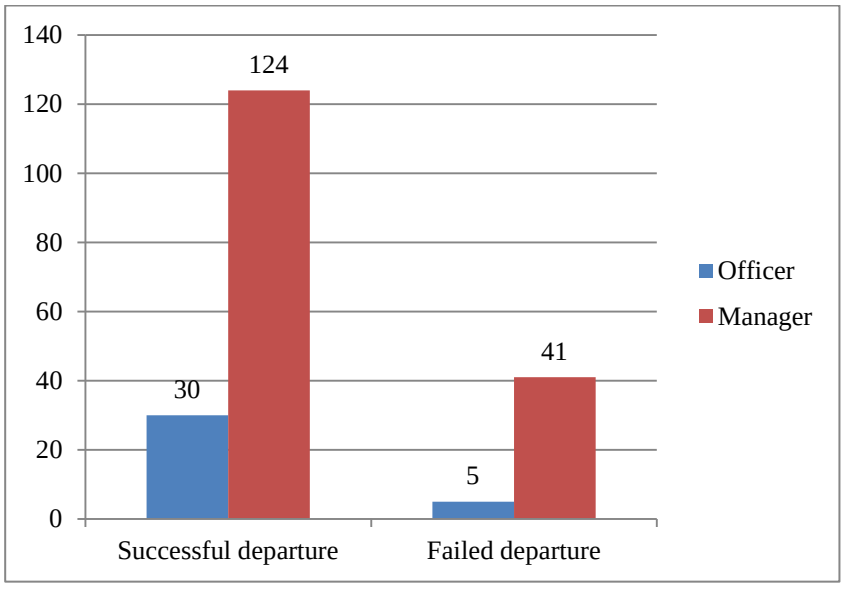

Figure 4.4 Classified by position

Figure can be described as follows:

Table 4.4 Population of successful project and failed details classified by position

Position	Success departure	Failure departure
Officer	30	5
Manager	124	41

4. Classified by departure

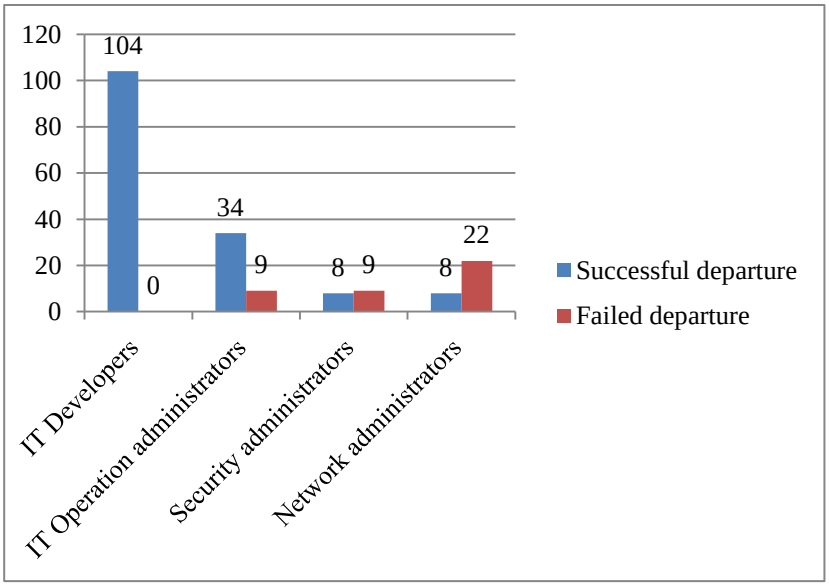

Figure 4.5 Classified by departure

Figure can be described as follows:

Table 4.5 Population of successful project and failed details classified by departure

Position	Success departure	Failure departure
IT Developers	104	0
IT Operation administrators	34	9
Security administrators	8	9
Network administrators	8	22

Survey results

The questionnaires were used to add data to Microsoft Excel in two separate projects, one of which was a success project and the other a failure. The successful project contained 154 samples. The failed project contained 40 samples as in the following samples:

Table 4.6 background of respondents

No. App.	Gender	Age	Educate	Work Period	Position	Departure
T1	Female	26-35	MASTER	<=5	OFFICER	IT Development
T2	Female	36-45	BACHELOR	16-20	OFFICER	IT Development
T3	Female	26-35	MASTER	6-10	OFFICER	IT Development
T4	Male	26-35	BACHELOR	<=5	OFFICER	IT Development
T5	Female	36-45	BACHELOR	11-15	OFFICER	IT Development
T6	Female	<=25	MASTER	21-25	OFFICER	IT Development
T7	Female	36-45	BACHELOR	11-15	OFFICER	IT Development
T8	Female	<=25	BACHELOR	<=5	OFFICER	IT Development
T9	Female	36-45	MASTER	11-15	OFFICER	IT Development
T10	Female	46-55	BACHELOR	21-25	MANAGER	IT Development

Table 4.6 can be described background of respondents such as number questionnaire, gender, age, education, work period, position and departure

Table 4.7 Example Data in Objective 1-2

No. App.	1. Access Control					2. Physical Security Control				
	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	2.4	2.5
T1	2	5	3	5	3	2	5	4	3	1
T2	1	4	1	1	3	2	4	4	2	2
T3	4	5	1	1	1	2	4	2	2	2
T4	3	4	4	5	3	5	5	2	1	2
T5	4	2	2	5	3	2	5	2	1	1
T6	3	5	3	3	1	2	5	2	3	2
T7	4	5	3	5	3	5	5	4	5	4
T8	4	4	2	1	4	2	5	4	3	4
T9	5	4	2	5	3	2	4	3	4	3
T10	4	5	1	5	1	5	4	2	3	2
Total	505	673	336	546	364	434	714	434	420	350
Questionnaires Set	154	154	154	154	154	154	154	154	154	154
Total Amount	**3.28**	**4.37**	**2.18**	**3.55**	**2.36**	**2.82**	**4.64**	**2.82**	**2.73**	**2.27**

Table 4.8 Example Data in Objective 3-4

No.App	3.Encryption					4.Malicious Code Security Control				
	3.1	**3.2**	**3.3**	**3.4**	**3.5**	**4.1**	**4.2**	**4.3**	**4.4**	**4.5**
T1	2	5	5	3	5	4	5	4	5	4
T2	1	4	1	1	4	4	4	1	4	4
T3	1	4	1	3	4	4	5	1	5	2
T4	2	5	5	1	4	5	5	5	5	3
T5	1	5	3	1	5	5	5	5	5	3
T6	3	5	1	1	3	5	5	5	5	3
T7	1	5	5	3	5	5	5	3	5	2
T8	4	5	3	3	4	5	5	5	5	1
T9	1	5	5	1	5	5	5	5	5	4
T10	2	5	1	1	5	4	5	3	5	5
Total	294	742	434	266	658	662	717	521	748	396
Questionnaires Set	154	154	154	154	154	154	154	154	154	154
Total Amount	**1.91**	**4.82**	**2.82**	**1.73**	**4.27**	**4.30**	**4.66**	**3.38**	**4.86**	**2.57**

Table 4.9 Example Data in Objective 5-6

No.App	5.System development, Acquisition and Maintenance					6.Personal Security Control				
	5.1	**5.2**	**5.3**	**5.4**	**5.5**	**6.1**	**6.2**	**6.3**	**6.4**	**6.5**
T1	4	5	4	5	5	5	4	5	5	1
T2	2	3	1	4	4	1	1	4	4	4
T3	2	3	3	5	5	2	2	5	5	2
T4	3	1	2	5	5	4	5	5	5	5
T5	2	2	3	5	5	3	5	5	5	1
T6	4	1	1	5	5	2	4	5	5	1
T7	2	3	5	5	5	2	5	5	5	5
T8	4	5	2	5	5	5	4	5	5	1
T9	3	3	3	5	5	2	5	5	5	4
T10	1	2	2	5	5	2	5	5	5	2
Total	409	381	756	756	420	616	756	756	482	662
Questionnaires Set	154	154	154	154	154	154	154	154	154	154
Total Amount	**2.66**	**2.47**	**4.91**	**4.91**	**2.73**	**4.00**	**4.91**	**4.91**	**3.13**	**4.30**

Table 4.10 Example Data in Objective 7-8

No.App	7.Electronic and paper-based media handing					8.Logging and Data Collection				
	7.1	**7.2**	**7.3**	**7.4**	**7.5**	**8.1**	**8.2**	**8.3**	**8.4**	**8.5**
T1	5	3	1	3	2	4	5	2	1	5
T2	2	4	1	1	1	3	3	2	1	1
T3	1	4	4	2	2	2	2	2	2	5
T4	1	5	5	4	1	4	4	3	1	5
T5	2	5	4	1	1	2	4	4	1	5
T6	1	1	1	1	1	1	1	1	1	1
T7	3	5	2	3	5	2	4	5	3	5
T8	3	3	3	3	2	3	0	3	5	5
T9	2	5	2	3	3	2	3	4	2	5
T10	4	5	2	2	1	4	2	2	2	5
Total	350	588	364	336	294	392	406	406	280	602
Questionnaires set	154	154	154	154	154	154	154	154	154	154
Total amount	**2.27**	**3.82**	**2.36**	**2.18**	**1.91**	**2.55**	**2.64**	**2.64**	**1.82**	**3.91**

Table 4.11 Example Data in Objective 9

No.App	9.Data Security				
	9.1	**9.2**	**9.3**	**9.4**	**9.5**
T1	5	5	5	5	5
T2	4	1	1	1	4
T3	5	5	5	5	5
T4	5	5	5	5	5
T5	5	5	5	5	5
T6	1	1	1	1	1
T7	5	5	5	5	5
T8	5	5	5	5	5
T9	5	5	5	5	5
T10	5	5	5	5	5
Total	644	602	602	602	644
Questionnaires set	154	154	154	154	154
Total amount	**4.18**	**3.91**	**3.91**	**3.91**	**4.18**

Table 4.12 Example Data in Objective 10-11

No.App	10.Service Provider Oversight					11.Business Continuity Management				
	10.1	**10.2**	**10.3**	**10.4**	**10.5**	**11.1**	**11.2**	**11.3**	**11.4**	**11.5**
T1	5	5	5	5	5	4	5	4	3	5
T2	1	4	4	4	1	2	4	4	4	1
T3	5	5	5	5	5	3	4	3	2	1
T4	5	5	5	5	5	5	5	5	3	5
T5	5	5	5	5	5	4	5	3	3	5
T6	1	1	1	1	1	1	1	1	1	1
T7	5	5	5	5	5	5	5	5	3	5
T8	5	5	5	5	5	4	4	4	5	5
T9	5	5	5	5	5	3	4	5	1	5
T10	1	5	5	5	1	3	4	4	3	5
Total	546	644	658	644	546	490	602	546	406	546
Questionnaires set	154	154	154	154	154	154	154	154	154	154
Total amount	**3.55**	**4.18**	**4.27**	**4.18**	**3.55**	**3.18**	**3.91**	**3.55**	**2.64**	**3.55**

Table 4.13 Example Data in Objective 12 and summary

No.App	12.Insurance					Summary	sum/60
	12.1	**12.2**	**12.3**	**12.4**	**12.5**		
T1	5	5	5	5	5	245	4.08
T2	1	1	3	1	1	146	2.43
T3	5	5	2	5	5	199	3.32
T4	1	5	4	1	5	236	3.93
T5	5	5	2	5	5	222	3.70
T6	1	5	1	5	5	140	2.33
T7	5	5	5	5	5	259	4.32
T8	5	5	5	5	5	241	4.02
T9	5	5	4	5	5	239	3.98
T10	5	5	5	1	1	209	3.48
Total	546	700	518	546	658		
Questionnaires set	154	154	154	154	154		
Total amount	**3.55**	**4.55**	**3.36**	**3.55**	**4.27**		

Table 4.8

Table 4.7 - Table 4.13 can be described. Researcher inputs data from questionnaire to Microsoft excel including information security objective 12 categories and each category has 5 questions.

After using result by totaling the score of the objectives

Total/Questionnaire Set = Total Number

Total Number of Objectives / 5 = Result

Table 4.14 Summary of Successful departure and failed departure

Objective	Successful departure	Failed departure
1.Access Control	3.15	2.51
2.Physical Security Control	3.05	2.70
3.Encryption	3.11	2.50
4.Malicious Code Security Control	3.95	3.15
5.System development, Acquisition and Maintenance	3.55	3.20
6.Personal Security Control	3.94	3.20
7.Electronic and paper-based media handing	2.51	1.70
8.Logging and Data Collection	2.71	1.65
9.Data Security	4.02	2.30
10.Service Provider Oversight	3.95	2.50
11.Business Continuity Management	3.36	1.95
12.Insurance	3.85	2.90

Survey result concerned about manager

Table 4.15 Survey result concerned about manager

Objective	Successful departure	Failed departure
1.Access Control	3.15	2.51
2.Physical Security Control	3.05	2.70
3.Malicious Code Security Control	3.95	3.15
4.Personal Security Control	3.94	3.20

Table 4.15 Survey result concerned about manager (cont.)

Objective	Successful departure	Failed departure
5.Logging and Data Collection	2.71	1.65

Research result of successful department and failed departure

The analysis of sample towards implementation of information security. Summary of the sample average reviews on Information System Security Audit Guide Practices for Bank of Thailand.

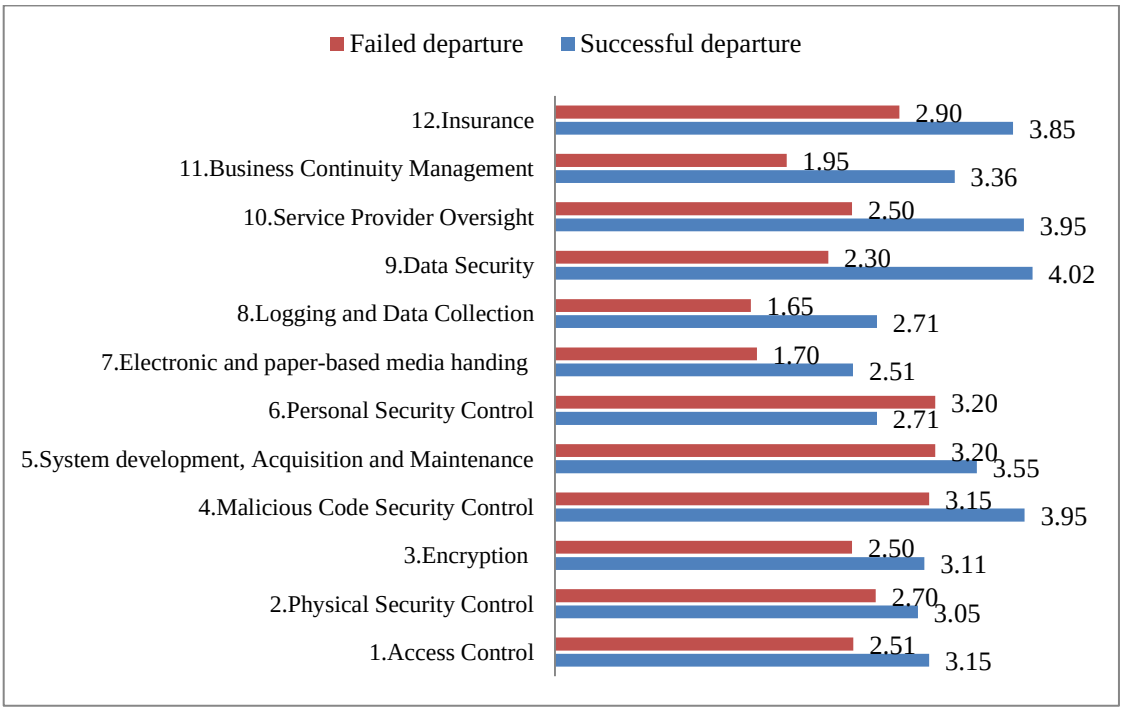

Figure 4.6 Compare result of successful department and failed departure

Figure 4.6 can be described most information security of successful departure has data security 4.02 score and least information security has Electronic and paper-based media handing 2.51 score. Then most information security of failed departure has personal security control 3.20 score and least information security has logging and data collection 1.65 score. Information security of two departures compared then there are appear personal security control of failed departure more successful departure. It should be improve process by increase checks new employee backgrounds, definition of contract significance and information security training for new employee.

Table 4.16 Survey result details

Security control objective	Objective	Successful Departure			Failed Departure		
Access Control	Do you think priority rights to access and improvements access rights should be periodically changed?	3.28	Total	3.15	2.53	Total	2.51
	How often your friends show or share user names and passwords?	4.37			4.78		
	How often do you change the password on your system?	2.18			1.75		
	How long did you wait to change your default password after receiving it?	3.55			2.00		
	Do you have operation access control to your bank?	2.36			1.50		
Physical Security Control	What security controls does the bank use at the datacenter?	2.82	Total	3.05	2.00	Total	2.70
	To what kinds of disaster has your bank data center been exposed?	4.64			4.50		
	What kinds of warnings and information are provided during data center emergencies?	2.82			2.50		
	What safety or cabinet features are provided for information security?	2.73			2.50		
	How are physical security measures or settings established for the distributed computing system?	2.27			2.00		
Encryption	What parts of the information technology environment are encrypted?	1.91	Total	3.11	2.00	Total	2.50
	How many strong encryption techniques are used to protect disclosure of information to other organizations?	4.82			4.50		

Table 4.16 Survey result details (cont.)

Security control objective	Objective	Successful Departure			Failed Departure		
	Did you think the banking system is reliable in protecting things such as customer information, financial information, etc?	2.82			1.00		
	What encryption management does the bank use?	1.73			1.50		
	Do you think encryption techniques are effective when intruders attempt to change information?	4.27			3.50		
Malicious Code Security Control	Do you think malicious code protection is important for banks?	4.30	Total	3.95	3.50	Total	3.15
	Do you have an anti-virus program installed on your computer?	4.66			4.00		
	How often do you update the anti-virus software on your computer?	3.38			2.50		
	Do you think malicious code surveillance is necessary?	4.86			3.75		
	Do you have bank channels for employee awareness of information security?	2.57			2.00		
System development, Acquisition and Maintenance	Do you use information security policy for application development?	2.82	Total	3.55	3.00	Total	3.20
	Do you have information security standards for data input to the system?	2.66			2.00		
	Do you have information security standards for processing data in the system?	2.47			1.50		
	Is approval required before program changes?	4.91			4.75		
	Do you have version control when changing programs?	4.91			4.75		

Table 4.16 Survey result details (cont.)

Security control objective	Objective	Successful Departure			Failed Departure		
Personal Security Control	Do you have a bank that checks new employee backgrounds?	2.73	Total	3.94	1.75	Total	3.20
	What is the definition of contract significance?	4.00			2.75		
	Do you have policy awareness acknowledgements for your bank?	4.91			4.75		
	Does your bank hold training for awareness of information security policy or law?	4.91			4.75		
	How can information security training be described?	3.13			2.00		
Electronic and paper-based media handing	How should the bank's sensitive data be stored?	2.27	Total	2.51	1.25	Total	1.70
	Has your bank ever been able to access storage media from an intruder?	3.82			2.75		
	How often does the bank review policy and storage media procedures?	2.36			1.75		
	How does your bank protect handling and storage?	2.18			1.25		
	How does your bank security control storage media for transit data?	1.91			1.50		
Logging and Data Collection	What benefits do you think bank data storage security will yield?	2.55	Total	2.71	1.75	Total	1.65
	What logs does your bank keep?	2.64			1.75		
	Do you have log details?	2.64			1.50		
	How do you think your bank controls and monitors logs?	1.82			1.25		
	Do you have your bank monitor violations on security systems for analysis and response to events?	3.91			2.00		

Table 4.16 Survey result details (cont.)

Security control objective	Objective	Successful Departure			Failed Departure		
Data Security	Do you have a bank with established data security policy?	4.18	Total	4.02	2.75	Total	2.30
	Do you have a bank that focuses on protection and disposal of storage media?	3.91			2.00		
	Do you think your bank focuses on security of transport and transfers of information between organizations?	3.91			2.00		
	Does your bank focus on classified information, defining the use of data file protection and setting priority of information?	3.91			2.00		
	Does your bank limit employee rights?	4.18			2.75		
Service Provider Oversight	Do you think your bank has analyzed the procurement and selection of service providers?	3.55	Total	3.95	2.00	Total	2.50
	Do you think banks focus on confidentiality and integrity of information by contracts with service providers?	4.18			2.75		
	Does you banks verify by external auditors in order to assess the security of the services?	4.27			3.00		
	Is your bank consistent in terms of response policies with service provider compliance in order to provide service alerts regarding violation events?	4.18			2.75		
	Does your bank gain verification from external audits?	3.55			2.00		

Table 4.16 Survey result details (cont.)

Security control objective	Objective	Successful Departure			Failed Departure		
Business Continuity Management	How important does your bank consider having sufficient computers and printers for use?	3.18	Total	3.36	1.75	Total	1.95
	Does your bank use efficient computers and printers compared to usage?	3.91			2.75		
	Do you think business continuity planning is important to business?	3.55			2.25		
	How often does your bank prepare business continuity planning by department?	2.64			2.00		
	Is your bank aware of business continuity planning?	3.55			1.00		
Insurance	Does your bank's insurance cover system risks?	3.55	Total	3.85	2.00	Total	2.90
	Do you have additional insurance coverage when new system risks occur?	4.55			3.75		
	What risks do you think insurance covers?	3.36			1.75		
	Do you think insurance offers sufficient coverage for reputation risks?	3.55			3.00		
	Do you think insurance offers sufficient coverage for customer confidentiality risks?	4.27			4.00		

The above results can be discussed as follows:

1. Access Control

- Bank access rights and improvements change every 3 months.
- Usernames and passwords are never shown or shared.
- Passwords on systems are changed after more than 1 year.
- Default passwords are changed within 1 month after receipt.
- Bank operation access control restricts authority and logging.

2. Physical Security Control

- The bank's datacenter has a security guard, has visitors exchange cards before entering the building and datacenter and records the times of datacenter building entry-exit.

-The bank's datacenter is never affected by disasters such as fires, floods, earthquakes, explosions, propagation of electromagnetic waves, power interruptions, plane crashes or destruction of chemicals.

- The bank's datacenter has CCTV, gas and fire detection equipment with lighting and auto warning switches when the circuit is cut-off.

- Safes or cabinets feature heat prevention for at least 1 hour, theft prevention or difficulty moving with passwords and locks.

- The distributed computing system has a screen screensaver password, username and password for the PC with the use of an automatic cut-off system.

3. Encryption

- The bank has operation system and application encryption.

- The bank's information system has a strong encryption technique because information is non-disclosed.

- The system is reliable because information is non-disclosed and the system has authentication.

- Encryption management has data handling and key management.

- Encryption techniques are effective when intruders attempt to change information without permission 12 times per year.

4. Malicious Code Security Control

- The bank realizes the great importance of malicious code protection for banks.

- The bank has installed anti-virus programs on computers.

- Anti-virus programs are updated every three months.

- The bank has malicious code surveillance.

- The bank has training, intranet and internet to ensure that employees have information security awareness.

5. System Development, Acquisition and Maintenance

- Information security policy for application development has documented approval for system use; use of auditing trails, logging and international standards for information security.

- Information security of input data has controlled access to input and change data, as well as checking for errors in input data.

- The information security of processing data uses batch control totals.

- Version control is used when programs are changed.

- Program changes require approval.

6. Personal Security Control

- The bank checks the criminal history, educational background and employment history of new employees.

- Significant contract terms and conditions are defined as follows:

    - No disclosure of sensitive information.
    - No violation of customer information and rights.
    - No violation of the organization's rules and regulations.
    - No violation of criminal law.
    - Prohibition of fraudulent work.

- The bank has policy awareness acknowledgements.

- The bank has training on information security policy or laws for employees.

- Information security training details are as follows:

    - Acceptable user policy.
    - Log-on requirements.
    - Password administration guidelines.

7. Electronic and paper-based media handling.

- Sensitive data stored in back-up tapes and optical storage.

- The bank has accessed storage media from intruders as follows:

    - Alteration of data.
    - Disruption of business activities.

- The bank reviews policy and storage media procedures every year.

-The bank protects handling and storage by tracking and logging.

- The bank uses encryption for transit-sensitive data and verifies storage media for security control of transit data.

8. Logging and Data Collection

- The bank secures stored data of benefit as follows:
    - To identify responsible parties.
    - System monitoring.
    - Aid in reconstructing compromised systems.
- The bank keeps operation system logs, access logs and event logs.
- Log details have transaction ID, terminal ID, dates and times.
- The bank controls and monitors logs.
- Logs are stored independently and separately from other computers.
- Good monitoring of violations on security systems for analysis and response to events.

9. Data Security

- Establish data security policy.
- Protect and dispose of storage media.
- Limit employee rights.
- The bank focuses on the security of information transport and transfer between organizations.
- The bank has classified information that is defined by using data file protection and prioritizing information.

10. Service Provider Oversight

- Analyze to find and choose a service provider.
- Focus on the confidentiality and integrity of information by contracting service providers.
- Verify external auditors in order to assess the security of the service.
- The bank looks for consistencies between response policies with service provider compliance so service provision alerts about violation events.

- The bank gains verification from external audits.

11. Business Continuity Management

- The bank has sufficient computers and printers to use at a moderate level.
- Computers and printers crash at an average of every 6 months when compared to usage.
- Business continuity planning is important to the business.
- Business continuity planning is prepared annually.
- The bank is aware of business continuity planning.

12. Insurance

- Insurance covers the following system risks:
    - Denial of service attacks.
    - Violations of customer confidentiality.
    - Destruction or changes in data by intrusion.
    - Counterfeit customer information.
- Additional insurance coverage when new system risks occur.
- Insurance covers reputation risks and customer confidentiality risks.

CHAPTER V
DISCUSSION

Survey result concerned about manager

Survey result can be described manager concern as Access Control**,** Physical Security Control**,** Malicious Code Security Control, Personal Security Control and Logging and Data Collection. Executives commented that should be improving process to secure more information as follow;

Table 5.1 Objective concerned about manager

Objective	Successful departure	Failed departure
1.Access Control	3.15	2.51
2.Physical Security Control	3.05	2.70
3.Logging and Data Collection	2.71	1.65

The discussed above results concerned about manager as follows.

1. Access Control

Table 5.2 Access control of result

No.	Objective	Success project
1	**Access Control**	**3.15**
	1.1. Do you think priority rights to access and improvements access rights should be periodically changed? If so, how often?	3.28
	1.2. How often your friends show or share usernames and passwords?	4.37
	1.3. How often do you change the password on your system?	2.18

Table 5.2 Access control of result (cont.)

No.	Objective	Success project
	1.4. How long did you wait to change your default password after receiving it?	3.55
	1.5. Do you have operation access control to your bank?	2.36

Result

- Right to access and improving access rights of bank change every 3 month.
- Never show or share username and password.
- Change password on system more than 1 year.
- Change default password after receive it within 1 month.
- Operation access control of bank is restricting authority and logging.

Risk

- Unauthorized person access to system who change information
- Access right was not update effect to unauthorized user using information and do not know to use information.

Recommendation

- There should be immediately change default password and password on system.
- Operation access control of bank should increase tracking and monitoring; granting privilege access and security patches

2. Physical Security Control

Table 5.3 Physical security control of result

No.	Objective	Success project
2	**Physical Security Control**	**3.05**
	2.1. What security controls does the bank use at the datacenter?	2.82

Table 5.3 Physical security control of result (cont.)

No.	Objective	Success project
	2.2. To what kinds of disaster has your bank data center been exposed?	4.64
	2.3. What kinds of warnings and information are provided during data center emergencies?	2.82
	2.4. What safety or cabinet features are provided for information security?	2.73
	2.5. How are physical security measures or settings established for the distributed computing system?	2.27

Result

- Datacenter of bank has a security guard, exchange cards before entering the building and data center and record time when entering and exit building datacenter.

-Datacenter of bank never affect disaster such as fire, water floods, earthquake, explosion, propagation of electromagnetic waves, power interruption, struck by a plane and destruction of chemical.

- Datacenter of bank has CCTV, gas fire; detection equipment has lighting and auto warning switch when the circuit is cut off.

- Safe or cabinet feature prevent heat least 1 hour, theft or difficult to move, password and lock

- Distributed computing system has screen screensaver password, username and password for your PC and using cutting automatically system.

Risk

- Intruder access physical such data center etc.

- Intruder may be steal information.

- There was accident happens then it do not have responsible.

Recommendation

- Security controls do the bank increase at the datacenter as follow**;**

- Submit written application forms before entering the data center.
- Place a security guard before entering the data center.
- Exchange cards before entering the data center.
- Kinds of warnings and information are provided during data center emergencies as follow;
    - Moisture prevention
    - Shock absorption
- Distributed computing system increase demarcation of work, PC key locks, UPS protected power outage to prevent data corruption; PC user names and passwords.

3.Logging and Data Collection

Table 5.4 Logging and data collection of result

No.	Objective	Success project
3	**Logging and Data Collection**	**2.71**
	3.1. What benefits do you think bank data storage security will yield?	2.55
	3.2. What logs does your bank keep?	2.64
	3.3. Do you have log details?	2.64
	3.4. How do you think your bank controls and monitors logs?	1.82
	3.5. Do you have your bank monitor violations on security systems for analysis and response to events?	3.91

Result

- Bank secures storing data that it will benefit;
    - Identification of responsible parties
    - System monitoring
    - Assistance in compromised system reconstruction
- Bank keeps operation system log, access log and event log.

- Log detail has transaction ID, terminal ID, date and time

- Log controls and monitors has stored independently and separately from other computers.

- Good monitor violated on security system for analysis and respond event

Risk

- If log were incomplete, it cannot problem cause.

- It cannot track abnormal event because it does not log file management process.

Recommendation

- Bank aware security storing data to employee;

  - Response to security

  - Enforcing employee, customer and partner compliance with information security policies.

  - Review and analysis of unauthorized system access

  - Report support to human resource management

  - Awareness of security violations

- Bank should add transaction log, firewall logs and remote access logs.

- Log detail should more add access system behavior, request service and transaction.

- Bank should increase Log controls and monitors as follow;

  - Log encryption

  - Log integrity

  - Log back-up and disposal

  - Writable log storage media (not once, but multiple times).

  - Centralized logging

  - Parameter configuration that cannot be edited.

- Log cannot edit and change from administrator.

REFERENCES

PCI DSS. (2012). Risk Assessment .Risk Assessment Guidelines November 2012, 1(1), 3

ISACA. (2004). Committee of Sponsoring Organizations, Enterprise Risk Management Integrated Framework ,1, 16

ISACA. (2008). IS Audit guideline, G13 Use of Risk Assessment in Audit Planning,1 ,4

Paras Shah ., David Roche ., Anthony Rodrigues . (2013). IT risk management .IT risk management: Drivers, challenges and enablers for Australian organizations, 1,1-20

Bank of Thailand. (2009). Security Controls Implementation. Security Controls Implementation Using Bank of Thailand Standards,1(1),17-110

Christine Bellino, Jefferson Wells., Steve Hunt, Enterprise Controls Consulting LP (2007). Risk Assessment. Audit Application Controls, Altamonte Springs :The Institute of Internal Auditors (IIA),

National Electronics and Computer Technology Center. (2007).ISO/IEC27001. Information security standard ,Phathumthani: National Electronics and Computer Technology Center

Alan Calder. (2013). Information security & ISO 27001, Retrieved 11 October 2013. www.itgovernance.co.uk

ISACA. (2012). COBIT5 Enabling Processes. Illinois: ISACA.

ISACA. (2012). COBIT 5 Framework. Illinois: ISACA.

Basel Committee on Banking Supervision. (2011). The internal audit function in banks. Retrieved 1 November 2013. www.bis.org

Basel Committee on Banking Supervision. (2012). The internal audit function in banks. Retrieved 1 November 2013. www.bis.org

Basel Committee on Banking Supervision. (2013). Principles for effective risk data aggregation and risk reporting. Retrieved 1 November 2013. www.bis.org

APPENDICES

Questionaire

การศึกษาด้านความปลอดภัยระบบสารสนเทศของธนาคารตามแนวทางธนาคารแห่งประเทศไทย

ส่วนที่ 1 : ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1.1 เพศ ❑ ชาย ❑ หญิง

1.2 อายุ ❑ น้อยกว่าหรือเท่ากับ 25 ปี ❑ 26-35 ปี ❑ 36-45 ปี
❑ 46-55 ปี ❑ 56 ปีขึ้นไป

1.3 การศึกษา ❑ ปริญญาตรี ❑ ปริญญาโท ❑ ปริญญาเอก

1.4 อายุการทำงาน ❑ น้อยกว่าหรือเท่ากับ 5 ปี ❑ 6-10 ปี ❑ 11-15 ปี
❑ 16-20 ปี ❑ 21-25 ปี ❑ 26-30 ปี
❑ 30 ปีขึ้นไป

1.5 ตำแหน่ง

❑ พนักงานปฏิบัติงาน (ระดับปฏิบัติการ)
- ❑ Security Administrator ❑ IT Developer
- ❑ IT Operation Administrator ❑ Network administrator
- ❑เจ้าหน้าที่ ด้านอื่นๆ โปรดระบุ.....

❑ ผู้บริหาร (ระดับหัวหน้าหน่วยขึ้นไป)
- ❑ Security Administrator ❑ IT Developer
- ❑ IT Operation Administrator ❑ Network administrator
- ❑เจ้าหน้าที่ ด้านอื่นๆ โปรดระบุ.....

ส่วนที่ 2 : ข้อมูลการแสดงความคิดเห็นของผู้ใช้งานและดูแลระบบงานสารสนเทศของธนาคาร

กรุณาทำเครื่องหมาย ✓ ในช่องที่ตรงกับความคิดเห็นของท่านมากที่สุด (ถ้าข้อใดที่หน่วยงานท่านไม่มีการควบคุมเรื่องดังกล่าว กรุณาข้ามไป)

1.Access Control

1.1.ท่านคิดว่าธนาคารให้ความสำคัญการดูแลสิทธิ์การเข้าถึงข้อมูล การปรับปรุงสิทธิ์ ทบทวนสิทธิ์ เมื่อมีการเปลี่ยนแปลงของพนักงานและระบบงาน บ่อยเพียงใด

❑ทันที ❑ทุก 1 เดือน ❑ทุก 3 เดือน ❑ทุก 6 เดือน
❑ มากกว่า 1 ปี

1.2.ท่านเคยเห็น User และ Password ของเพื่อนร่วมงานที่วางไว้ตามโต๊ะ หรือเคยเห็นเพื่อนร่วมงานใช้ User และ Password ร่วมกันที่เกี่ยวกับการทำงาน มากน้อยเพียงใด

❑ไม่เคย ❑เคยเห็น 1-5 ครั้ง ต่อเดือน ❑เคยเห็น 5-10 ครั้ง ต่อเดือน
❑เคยเห็น 10-15 ครั้ง ต่อเดือน ❑ทุกวัน

1.3.ท่านมีการเปลี่ยนรหัสผ่านในการใช้งานระบบงานหรือใช้ในการพัฒนาระบบงาน บ่อยเพียงใด

❑ทุก 1 เดือน ❑ทุก 3 เดือน ❑ทุก 6 เดือน ❑ มากกว่า 1 ปี ❑ไ ม่ เ ค ย

1.4.เมื่อท่านให้ความสำคัญในการเปลี่ยนรหัสผ่าน เมื่อได้รับรหัสผ่านใหม่ (Default Password) เพียงใด

❑ทันที ❑ทุก 1 เดือน ❑ทุก 3 เดือน ❑ทุก 6 เดือน
❑ มากกว่า 1 ปี

1.5.ธนาคารมีการควบคุมการเข้าถึงระบบปฏิบัติการ ดังนี้ **(ตอบได้มากกว่า 1 ข้อ)**

❑การจำกัดสิทธิ์ ❑การติดตามเฝ้าดูแล
❑การบันทึกการทำรายการ ❑การให้สิทธิ์ Privilege Access
❑การปรับปรุงระบบรักษาความปลอดภัย (Security Patches)

2.Physical Security Control

2.1.ท่านคิดว่าธนาคารมีควบคุมการเข้า-ออกการเข้าห้อง Datacenter ของภายนอกบุคคลภายนอกและบุคคลภายในธนาคารเพียงใด ดังนี้ **(ตอบได้มากกว่า 1 ข้อ)**

❑มีพนักงานรักษาความปลอดภัยก่อนเข้าอาคาร ❑การแลกบัตรก่อนเข้าอาคาร
❑บันทึกเวลาการเข้า-ออกก่อนเข้าอาคาร ❑มีการเขียนใบคำร้องก่อนเข้าห้อง Datacenter
❑การแลกบัตรก่อนเข้าห้อง Datacenter ❑บันทึกเวลาการเข้า-ออกก่อนเข้าห้อง Datacenter
❑มีพนักงานรักษาความปลอดภัยก่อนเข้าห้อง Datacenter

2.2.ศูนย์ Datacenter หรือศูนย์ปฏิบัติการด้านสารสนเทศ ของธนาคารเคยได้รับผลกระทบจากภัยพิบัติ หรือภัยอื่นๆ ดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑ไฟไหม้ ❑น้ำท่วม
❑แผ่นดินไหว ❑การแผ่กระจายของคลื่นแม่เหล็กไฟฟ้า

❑กระแสไฟฟ้าถูกรบกวน ❑การพุ่งชนของเครื่องบิน
❑การทำลายล้างจากสารเคมี ❑การระเบิด

2.3.ศูนย์ Datacenter หรือศูนย์ปฏิบัติการด้านสารสนเทศ ของธนาคารมีมาตรการแจ้งเตือนภัยและการให้ข้อมูลเพื่อการสืบสวนเพื่อการดำเนินคดี ดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑มีสวิตส์ควบคุมการทำงานแจ้งเตือนภัยอัตโนมัติเมื่อวงจรไฟฟ้าถูกตัดขาด
❑แก๊สดับเพลิง
❑อุปกรณ์ตรวจสอบผู้บุกรุกโดยอาศัยแสงสว่าง
❑เครื่องตรวจจับควันไฟ
❑อุปกรณ์เรดาร์จับภาพเคลื่อนไหวของคนร้าย
❑เครื่องตรวจจับความร้อน
❑การยกระดับพื้นห้องคอมพิวเตอร์
❑ระบบโทรทัศน์วงจรปิด

2.4.ตู้เซฟ หรือตู้เก็บเอกสารของธนาคารมีคุณสมบัติด้านการรักษาความปลอดภัยสารสนเทศ ดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑ป้องกันความร้อนจากไฟไหม้อย่างน้อย 1 ชม.
❑ทนต่อแรงกระแทก ไม่ชำรุด บุบ พังง่ายๆ
❑ป้องกันการขโมย ถูกเคลื่อนย้ายได้ยาก
❑มีรหัสผ่าน กุญแจ
❑ป้องกันความชื้น

2.5.ธนาคารของท่านมีการกำหนดมาตรการรักษาความปลอดภัยทางภาพสำหรับระบบคอมพิวเตอร์แบบ Distributed หรือเครื่อง PC ที่ใช้งาน ดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑มีการกั้นเขตในการทำงาน
❑มีการใช้กุญแจปิดล๊อคเครื่อง PC
❑การใช้หน้าจอ Screensaver password
❑การใช้ระบบตัดการทำงานอัตโนมัติ
❑มีเครื่อง UPS ป้องกันกระแสไฟฟ้าตกที่ทำให้เกิดความเสียหายของข้อมูล
❑มีการใช้ Username และ Password สำหรับการใช้งานเครื่อง PC

❑มีตั้งค่าความปลอดภัยเพื่อการป้องกันเข้าถึงแฟ้มข้อมูลโดยไม่ได้รับอนุญาต เช่น ตั้งรหัสผ่าน จำกัดสิทธิ์ในการใช้งานแฟ้มข้อมูล เป็นต้น

3. Encryption

3.1.ธนาคารมีการเข้ารหัสในสภาวะแวดล้อมด้านเทคโนโลยีสารสนเทศ ดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑ระบบปฏิบัติการ ❑อุปกรณ์คอมพิวเตอร์ หรือ Middleware ❑Application

❑File system ❑Protocal

3.2.ท่านคิดว่า ธนาคารมีเทคนิคในการเข้ารหัสที่มีความเข้มแข็งเพียงพอต่อการป้องกันข้อมูลไม่ให้ถูก**<u>เปิดเผยข้อมูล</u>**ไปสู่หน่วยงานอื่นหรือองค์กรอื่นมากน้อยเพียงใด

❑ไม่เคยถูกเปิดเผยข้อมูล

❑ข้อมูลถูกเปิดเผยข้อมูลรายปี (1 ครั้งต่อปี)

❑ข้อมูลถูกเปิดเผยข้อมูลรายไตรมาส (4 ครั้งต่อปี)

❑ข้อมูลถูกเปิดเผยข้อมูลรายเดือน (12 ครั้งต่อปี)

❑ข้อมูลถูกเปิดเผยข้อมูลรายวัน (มากกว่า 12 ครั้งต่อปี)

3.3.ท่านคิดว่าระบบงานของธนาคารมีความน่าเชื่อถือเพียงใด อาทิ ด้านข้อมูลลูกค้า ข้อมูลทางด้านการเงิน ข้อมูลพนักงาน เป็นต้น **(ตอบได้มากกว่า 1 ข้อ)**

❑ข้อมูลไม่ถูกเปิดเผย ❑ข้อมูลมีความถูกต้องครบถ้วน

❑มีการยืนยันตัวบุคคลเมื่อใช้งานระบบงาน

3.4.ธนาคารมีการบริหารจัดการการเข้ารหัสดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑Data Handing ❑Key Management ❑Actual Encryption3

3.5.ท่านคิดว่าธนาคารมีเทคนิคการเข้ารหัสที่มีประสิทธิภาพเพียงใดเมื่อผู้บุกรุกพยายามจะเปลี่ยนแปลงข้อมูลเมื่อมีการรับ-ส่งข้อมูล

❑<u>ไม่เคย</u>ถูกเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

❑ข้อมูลถูกเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต<u>รายปี</u> (1 ครั้งต่อปี)

❑ข้อมูลถูกเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต<u>รายไตรมาส</u> (4 ครั้งต่อปี)

❑ข้อมูลเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตรายเดือน (12 ครั้งต่อปี)
❑ข้อมูลเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตรายวัน (มากกว่า 12 ครั้งต่อปี)

4.Malicious Code Security Control

4.1.ท่านคิดว่าธนาคารให้ความสำคัญเกี่ยวกับการป้องกันโปรแกรมที่เป็นอันตราย (malicious code) เพียงใด

❑สำคัญมาก ❑สำคัญ ❑เฉยๆ ❑น้อย ❑น้อยที่สุด

4.2.คอมพิวเตอร์ที่ท่านใช้งานมีการติดตั้งโปรแกรม Anti-virus หรือไม่

❑มี ❑ไม่มี

4.3.คอมพิวเตอร์ที่ท่านใช้งานมี**การอัพเดตโปรแกรม Anti-virus** เพียงใด

❑ทุกวัน ❑ทุกสัปดาห์ ❑ทุก 1 เดือน ❑ทุก 3 เดือน
❑ทุก 6 เดือน ❑มากกว่า 1 ปี หรือไม่เคย

4.4.ท่านคิดว่าธนาคารมีการเฝ้าระวังโปรแกรมที่เป็นอันตรายเพียงใด อาทิ ไม่สามารถเข้าถึงบางเว็บไซต์ ไม่สามารถดาวโหลดข้อมูลจากเว็บไซต์ เป็นต้น

❑มี ❑ไม่มี

4.5.ธนาคารของท่านมีให้ความรู้บุคลากร เพื่อให้พนักงานตระหนักถึงรักษาความปลอดภัยสารสนเทศผ่านทางช่องทางใดบ้าง **(ตอบได้มากกว่า 1 ข้อ)**

❑จัดอบรม ❑วารสารของธนาคาร
❑Intranet/Internet ❑จัดกิจกรรมด้านการรักษาความปลอดภัยสารสนเทศ
❑ประชาสัมพันธ์ของธนาคาร ❑E-mail
❑Social Network ❑ไม่มี

5.System development, Acquisition and Maintenance

5.1.ธนาคารของท่านมีการนำมาตรการรักษาความปลอดภัยสารสนเทศมาใช้ในการพัฒนาระบบและโปรแกรมอย่างไรบ้าง **(ตอบได้มากกว่า 1 ข้อ)**

❑กำหนดมาตรการรักษาความปลอดภัยก่อนพัฒนาระบบงานหรือจัดหาระบบงานใหม่

❑จัดทำเอกสารการอนุมัติให้นำระบบงานออกใช้งานจริง
❑จัดเก็บเอกสารหรือข้อกำหนดที่ใช้ในการพัฒนาระบบงานอย่างเป็นลายลักษณ์อักษร
❑นำมาตรฐานสากลมาใช้ในการรักษาความปลอดภัยสารสนเทศ เช่น ISO27001 เป็นต้น
❑จัดทำร่องรอยในการตรวจสอบ
❑มีการจัดเก็บ log
❑เมื่อมีการเปลี่ยนแปลงแก้ไขระบบงานมีการนำ Patch program มาช่วยเสริมสร้างความปลอดภัย

5.2.ธนาคารของท่านมีการนำมาตรการรักษาความปลอดภัยสารสนเทศในการนำเข้าข้อมูลสู่ระบบงานเพียงใด **(ตอบได้มากกว่า 1 ข้อ)**
❑ควบคุมการเข้าถึงป้อนข้อมูลและการเปลี่ยนแปลงข้อมูล
❑ตรวจสอบข้อผิดพลาดในการนำข้อมูลเข้า
❑ตรวจสอบข้อมูลที่ไม่ปกติหรือที่น่าสงสัย
❑ตรวจทานและอนุมัติรายการสำหรับข้อมูลหรือรายการธุรกรรมที่สำคัญ

5.3.ธนาคารของท่านมีการนำมาตรการรักษาความปลอดภัยสารสนเทศในการประมวลผลของระบบงานเพียงใด **(ตอบได้มากกว่า 1 ข้อ)**
❑มีการควบคุมยอดรวมของงานชุดนั้นๆ (Batch control totals)
❑มีการ Hash จำนวนข้อมูลทั้งหมดหลังการประมวลผล
❑เมื่อข้อมูลถูกเปลี่ยนแปลงควรมีการแสดงข้อมูลให้ทราบ
❑มีการตรวจเช็คว่ามีการประมวลผลเป็นไปตามลำดับ

5.4.เมื่อมีการเปลี่ยนแปลงแก้ไขในการพัฒนาระบบงานหรือโปรแกรมต้องมีการขออนุมัติก่อนทำการแก้ไขหรือไม่
❑มี ❑ไม่มี

5.5.เมื่อมีการเปลี่ยนแปลงแก้ไขในการพัฒนาระบบงานหรือโปรแกรมมีการควบคุม Version หรือไม่
❑มี ❑ไม่มี

6. Personal Security Control

6.1.ท่านคิดว่าธนาคารมีการตรวจสอบประวัติพนักงานใหม่ ดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑ประวัติจากองค์กรเดิม ❑ประวัติอาชญากรรม ❑ประวัติด้านการเงิน

❑ประวัติด้านครอบครัว ❑ประวัติการศึกษา

6.2.ท่านคิดว่าในการทำสัญญาว่าจ้างกับธนาคาร มีสาระสำคัญที่ระบุถึงเรื่องดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑ห้ามเปิดเผยข้อมูลสำคัญ ❑ห้ามละเมิดข้อมูลและสิทธิของลูกค้า

❑ห้ามละเมิดข้อกำหนดของหน่วยงาน ❑ห้ามสร้างความเสียหายต่อชื่อเสียงธนาคาร

❑ห้ามละเมิดกฎหมายอาญา ❑ห้ามทุจริตในหน้าที่การงาน

6.3.ธนาคารมีการกำหนดนโยบายที่พนักงานจะต้องรับรู้หรือไม่ (Policy Awareness Acknowledgements) เพื่อให้พนักงานทราบในสิ่งที่พึงจะต้องปฏิบัติและสิ่งที่ไม่พึงปฏิบัติ

❑มี ❑ไม่มี

6.4.ธนาคารมีการอบรมให้ท่านตระหนักถึงภัยคุกคามที่มีต่อระบบสารสนเทศ นโยบายด้านการรักษาความปลอดภัยสารสนเทศ และพรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ 2550 หรือไม่

❑มี ❑ไม่มี

6.5.ในการอบรมด้านการรักษาความปลอดภัยสารสนเทศของธนาคาร ประกอบด้วยรายละเอียดดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑ข้อตกลงในการเข้าใช้บริการด้านคอมพิวเตอร์ (Acceptable Use Policy)

❑การรักษาความปลอดภัยของคอมพิวเตอร์ (Desktop Security)

❑ข้อกำหนดการเข้าถึงระบบ (Log-on Requirements)

❑แนวทางในการบริหาร Password (Password Administration Guidelines)

❑แนวทางในการป้องกันการตีสนิทเพื่อหลอกล่อเอาข้อมูล (Social Engineering)

7.Electronic and paper-based media handing

7.1.ธนาคารมีการจัดเก็บข้อมูลสำคัญไว้ในรูปแบบใดบ้าง **(ตอบได้มากกว่า 1 ข้อ)**

❑Paper Document ❑Back-up Tapes ❑Disk

❑Cassettes ❑Optical Storage

7.2.ธนาคารเคยถูกผู้บุกรุกเข้าถึงสื่อเก็บข้อมูลจนให้เกิดความเสียหายดังนี้หรือไม่ (ตอบได้มากกว่า 1 ข้อ)

❑เปิดเผยข้อมูลลับขององค์กร (Exposure of corporate secret)

❑เปิดเผยข้อมูลความลับของลูกค้า (Breaches in customer confidentiality)

❑การเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Alteration of data)

❑การบุกรุกจากผู้ที่ไม่ได้รับอนุญาตทำให้การดำเนินงานต้องหยุดชะงัก (Disruption of business activities)

❑การบุกรุกโดยสร้างความเสียหายต่อสื่อจัดเก็บข้อมูล

7.3.ธนาคารมีการทบทวนนโยบายและขั้นตอนในการเก็บรักษาสื่อเก็บข้อมูลเพียงใด

❑ทุก 1 เดือน ❑ทุก 3 เดือน ❑ทุก 6 เดือน ❑ทุก 1 ปี ❑ไม่เคย

7.4.ธนาคารมีมาตรการควบคุมและจัดเก็บ Handling and storage ทั้งด้านกายภาพและสภาวะแวดล้อม อย่างไรบ้าง **(ตอบได้มากกว่า 1 ข้อ)**

❑ป้องกันไฟไหม้ ❑ป้องกันน้ำท่วม ❑จำกัดการเข้าถึง

❑การติดป้ายทะเบียน ❑บันทึกการทำรายการธุรกรรม

7.5.ธนาคารมีการควบคุมความปลอดภัยของสื่อเก็บข้อมูลที่อยู่ระหว่างการส่งผ่านข้อมูล (Transit) อย่างไร**(ตอบได้มากกว่า 1 ข้อ)**

❑เข้มงวดในการคัดเลือกบริษัทหรือบุคลากรที่ทำหน้าที่จัดส่งสื่อเก็บข้อมูล

❑มีกระบวนการตรวจสอบความถูกต้องของสื่อเก็บข้อมูลที่ได้รับ

❑กำหนดระบบการจัดเก็บสื่อเพื่อป้องกันความเสียหาย

❑มีการใช้เทคนิคการเข้ารหัสในการส่งข้อมูลที่สำคัญ

❑มีการทำข้อตกลงเรื่องการไม่เปิดเผยข้อมูลกับผู้ที่ทำหน้าส่งผ่านข้อมูลหรือจัดส่งข้อมูล

8. Logging and Data Collection

8.1.ท่านคิดว่าการจัดเก็บข้อมูลในการทำรายการที่ปลอดภัยจะเป็นประโยชน์ด้านใดบ้าง **(ตอบได้มากกว่า 1 ข้อ)**

❑ช่วยระบุผู้รับผิดชอบ (Identify)

❑ตอบโต้สถานการณ์ด้านความปลอดภัยสารสนเทศต่างๆ (Respond to security)

❑เฝ้าระวัง ตรวจตรา ระบบงาน (Monitoring to system)

❑ใช้บังคับพนักงาน ลูกค้า และคู่ค้าให้ปฏิบัติตามนโยบายด้านความปลอดภัยสารสนเทศ

❑สามารถทบทวนและวิเคราะห์ความพยายามเข้าถึงระบบ (Review and Analyze unauthorized access systems)

❑รายงานนำไปสนับสนุนการบริหารงานบุคคลได้ (Report support to human resource management)

❑ทราบถึงการล่วงละเมิดด้านความปลอดภัยสารสนเทศ (To know security violation)

❑สามารถนำข้อมูลจาก Log มาสร้างระบบที่เสียหายขึ้นมาใหม่ได้ (Aid in Reconstruction Compromised Systems)

8.2.ธนาคารมีการจัดเก็บ log ด้านใดบ้าง **(ตอบได้มากกว่า 1 ข้อ)**

❑การทำรายการเคลื่อนไหวของข้อมูลเข้า/ออก โดยผ่านช่องทางอินเตอร์เน็ต

❑บันทึกเหตุการณ์ที่สำคัญของ Firewall

❑บันทึกเหตุการณ์ที่สำคัญที่เข้าสู่ระบบตรวจจับการบุกรุก

❑การปฏิบัติงานของระบบคอมพิวเตอร์กลางและเครือข่าย

❑การเข้าถึงระบบปฏิบัติการและระบบงาน

❑การเข้าถึงระบบจากระยะไกล

8.3.รายละเอียดของ log ที่จัดเก็บมีข้อมูลใดบ้าง **(ตอบได้มากกว่า 1 ข้อ)**

❑หมายเลข ID ของการทำรายการ ❑หมายเลขเครื่อง

❑วันและเวลา ❑พฤติกรรมการพยายามเข้าถึงระบบ

❑การขอใช้บริการ ❑การทำรายการ หรือ การใช้งานบนระบบ

8.4.ท่านคิดว่าธนาคารมีการควบคุมและเฝ้าติดตามการเข้าถึง log ดังนี้หรือไม่ **(ตอบได้มากกว่า 1 ข้อ)**

❑การเข้ารหัสข้อมูลที่ Log

❑Log ที่จัดเก็บสามารถเก็บข้อมูลได้ครบถ้วน

❑มีกระบวนการสำรองข้อมูลและกำจัด log ที่ไม่ใช้งาน

❑จัดเก็บ log ไว้อย่างอิสระและแยกออกจากคอมพิวเตอร์อื่น

❑จัดเก็บ log ลงบนสื่อที่สามารถเขียนได้ครั้งเดียวแต่อาจได้หลายครั้ง

❑ระบบจัดเก็บข้อมูลแบบ Centralized logging
❑ตั้งค่า Parameter เพื่อไม่ให้แก้ไขข้อมูลได้

8.5.ธนาคารมีการติดตามเหตุการณ์ล่วงละเมิดระบบรักษาความปลอดภัยบนระบบงาน เพื่อใช้ในการวิเคราะห์ หรือโต้ตอบในเหตุการณ์ที่ผิดปกติ หรือไม่
❑มี ❑ไม่มี

9. Data Security

9.1.ท่านคิดว่า ธนาคารมีการกำหนดนโยบายและควบคุมการปฏิบัติตามนโยบายในการบริหารและเก็บรักษาข้อมูล หรือไม่
❑มี ❑ไม่มี

9.2.ท่านคิดว่าธนาคารให้ความสำคัญในการป้องกันและรักษาความปลอดภัยในการกำจัดสื่อเก็บข้อมูลที่มีความสำคัญเพียงใด
❑มี ❑ไม่มี

9.3.ท่านคิดว่าธนาคารให้ความสำคัญการรักษาความปลอดภัยของข้อมูลระหว่างการเคลื่อนย้ายและการโอนข้อมูลให้หน่วยงานอื่นทั้งภายในและภายนอกองค์กรเพียงใด
❑มี ❑ไม่มี

9.4.ธนาคารของท่านมีการจัดประเภทข้อมูลและกำหนดมาตรการป้องกันการนำแฟ้มข้อมูลแต่ละไปใช้งาน รวมถึงจัดลำดับความสำคัญของข้อมูล หรือไม่
❑มี ❑ไม่มี

9.5.ธนาคารมีการจำกัดสิทธิพนักงานเข้าถึงข้อมูลน้อยที่สุดหรือเพียงพอต่อการใช้งานตามหน้าที่การงานเท่านั้นหรือไม่
❑มี ❑ไม่มี

10. Service Provider Oversight

10.1.ท่านคิดว่า ธนาคารมีมาตรการในการวิเคราะห์เพื่อค้นหาและเลือกผู้ให้บริการหรือไม่

❑มี ❑ไม่มี

10.2.ท่านคิดว่าธนาคารให้ความสำคัญในการรักษาความลับ ความถูกต้องของข้อมูลระหว่างผู้ให้บริการโดยการทำสัญญารับประกัน เพื่อรับผิดชอบในการรักษาความปลอดภัย ควบคุมการดำเนินงาน และรายงานผล รวมถึงผู้ให้บริการลงนามไม่เปิดเผยข้อมูลของธนาคาร หรือไม่

❑มี ❑ไม่มี

10.3.ท่านคิดว่าธนาคารมีการตรวจสอบจากผู้ตรวจสอบจากภายนอกองค์กร เพื่อเข้าไปประเมินระบบการรักษาความปลอดภัยของผู้ให้บริการหรือไม่

❑มี ❑ไม่มี

10.4.ท่านคิดว่าธนาคารมีความสอดคล้องกันระหว่างนโยบายในการโต้ตอบกับสถานการณ์ของธนาคารและข้อกำหนดที่ธนาคารบังคับให้ผู้ให้บริการจะต้องเตือนภัยในสถานการณ์ที่เกี่ยวกับการล่วงละเมิดระบบรักษาความปลอดภัย หรือไม่

❑มี ❑ไม่มี

10.5.ธนาคารได้รับการตรวจสอบจากหน่วยงานภายนอก เพื่อประเมินการรักษาความปลอดภัยของผู้ให้บริการหรือไม่

❑มี ❑ไม่มี

11. Business Continuity Management

11.1.ท่านคิดว่าอุปกรณ์คอมพิวเตอร์และเครื่องพิมพ์ที่มีอยู่ในปัจจุบัน มีสัดส่วนมากน้อยเพียงใด เมื่อเทียบกับปริมาณความต้องการใช้งาน

❑มากที่สุด ❑มาก ❑ปานกลาง ❑น้อย ❑น้อยที่สุด

11.2.ท่านคิดว่าอุปกรณ์คอมพิวเตอร์และเครื่องพิมพ์ที่มีอยู่ในปัจจุบัน มีประสิทธิภาพมากน้อยเพียงใด เมื่อเทียบกับความต้องการใช้งาน

❑ชำรุดมากกว่า 1 ปี หรือไม่เคยชำรุด ❑ชำรุดทุก 6 เดือน ❑ชำรุดทุก 3 เดือน

❑ชำรุดทุก 1 เดือน ❑ชำรุดรายสัปดาห์

11.3.ท่านคิดว่าระบบสารสนเทศที่ท่านใช้งานมีความจำเป็นเพียงใดที่ต้องมีแผนสร้างความต่อเนื่องทางธุรกิจเมื่อมีเหตุการณ์ที่ทำให้ธุรกิจหยุดชะงัก อาทิ เมื่อเกิดไฟดับจะต้องมีแผนการดำเนินการอย่างไรเพื่อให้ธุรกิจไม่หยุดชะงัก

❑มากที่สุด ❑มาก ❑ปานกลาง ❑น้อย ❑น้อยที่สุด

11.4.หน่วยงานของท่านมีมาตรการเตรียมความพร้อมเมื่อเกิดเหตุการณ์ผิดปกติให้เป็นไปตามแผนการดำเนิน
ธุรกิจแบบต่อเนื่องมากน้อยเพียงใด

❑เตรียมความพร้อมทุก 3 เดือน ❑เตรียมความพร้อมทุก 6 เดือน
❑เตรียมความพร้อมทุก 1 ปี ❑เตรียมความพร้อมทุก 2 ปี ❑ไม่เคย

11.5.ธนาคารมีการฝึกอบรมเพื่อสร้างความเข้าใจเกี่ยวกับแผนการดำเนินธุรกิจแบบต่อเนื่อง และทราบถึงบทบาทหน้าที่ในการรักษาความปลอดภัยหรือไม่

❑มี ❑ไม่มี

12. Insurance

12.1.ท่านคิดว่า ธนาคารมีสัดส่วนการทำประกันป้องกันการละเมิดความปลอดภัยสารสนเทศโดยเพิ่มความคุ้มครองโดยการทำประกันให้ครอบคลุมความเสี่ยงที่มีต่อระบบงาน หรือไม่

❑มี ❑ไม่มี

12.2.ท่านคิดว่า ธนาคารมีเพิ่มความคุ้มครองเมื่อเกิดความเสี่ยงใหม่ๆ ที่เพิ่มขึ้นกับระบบงาน หรือไม่

❑มี ❑ไม่มี

12.3.ท่านคิดว่าการทำกรมธรรม์ประกันภัยต่อระบบงานนั้น ควรระบุความคุ้มครองไปถึงความเสี่ยงในเรื่องใดบ้าง **(ตอบได้มากกว่า 1 ข้อ)**

❑การเข้าไปแก้ไขข้อความบนเว็บไซต์ ❑การถูกโจมตีจนระบบไม่สามารถให้บริการ
❑การสูญเสียรายได้ ❑การถูกโจรกรรมข้อมูล
❑การล่วงละเมิดความลับลูกค้า ❑ข้อมูลถูกทำลาย หรือถูกเปลี่ยนแปลงจากการบุกรุก

❑การปลอมแปลงข้อมูลลูกค้า

12.4.ท่านคิดว่า ธนาคารมีการทำกรมธรรม์ประกันภัยต่อระบบงานนั้น คุ้มครองความเสี่ยงด้านชื่อเสียงเพียงพอหรือไม่

❑เพียงพอ ❑ไม่เพียงพอ

12.5.ท่านคิดว่า ธนาคารมีการทำกรมธรรม์ประกันภัยต่อระบบงานนั้น คุ้มครองความเสี่ยงด้านลูกค้าและการรักษาความลับของลูกค้าเพียงพอหรือไม่

❑เพียงพอ ❑ไม่เพียงพอ

ส่วนที่ 3 ข้อมูลความคิดเห็นของผู้บริหารเกี่ยวกับความสำคัญของการควบคุมด้านความปลอดภัยเทคโนโลยีสารสนเทศของธนาคาร โดยจัดลำดับ 1-5 ตามความสำคัญ (สำคัญมากที่สุด =5, สำคัญน้อยที่สุด =1)

_____ Access Control

_____ Physical Security Control

_____ Encryption

_____ Malicious Code Security Control

_____ System development, Acquisition and Maintenance

_____ Personal Security Control

_____ Electronic and paper-based media handing

_____ Logging and Data Collection

_____ Data Security

_____ Service Provider Oversight

_____ Business Continuity Management

_____ Insurance

BIOGRAPHY

NAME	Miss Sasitorn Silamanothum
DATE OF BIRTH	6 February 1988
PLACE OF BIRTH	Bangkok, Thailand
INSTITUTIONS ATTENDED	Mahidol University, 2006-2009 Bachelor of Management (Management Information System) Mahidol University, 2010-2014 Master of Science (Technology of Information System Management)
HOME ADDRESS	59/207 Phetkasam Rd. Nong Kang Plu, Nong Kheam, Bangkok 10160 Tel: 0896784605 E-mail: zhahi_ink@hotmail.com