2012

Institutionalization of Information Security: Case of the Indonesian Banking Sector

Muhamad Faisal Fariduddin Attar Nasution
Virginia Commonwealth University

INSTITUTIONALIZATION OF INFORMATION SECURITY: CASE OF THE INDONESIAN BANKING SECTOR

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University.

By

Muhamad Faisal Fariduddin Attar Nasution
MBA, University of Missouri at Saint Louis
SKom, Computer Science, Universitas Indonesia

Director: Dr. Gurpreet Dhillon
Department of Information Systems

Virginia Commonwealth University
Richmond, Virginia

08/2012

Acknowledgement

"Read! In the name of your Lord who created - Created the human from something which clings. Read! And your Lord is Most Bountiful - He who taught (the use of) the Pen, Taught the human that which he knew not." (Quran 96:1-5)

"He [Allah] grants wisdom to whom He pleases; and he to whom wisdom is granted indeed receives a benefit overflowing. But none will grasp the Message except men of understanding." (Quran 2:269)

This dissertation is an ultimate dedication to Allah, the Lord of the universe, the Wise and the Benevolent. It is through His will and mercy shall I be able to complete this journey. This dissertation is nothing but a tiny fraction of my tireless pursuit to serve Him. The Lord has commanded us to seek knowledge and to use it for the better of us. And it is an honor and my privilege that He appoints such duty to me, empowering my decision to take my destiny as a scholar.

This effort can be traced back in year 2006 when I decided to attend Virginia Commonwealth University for a doctoral in business program and befriended my then wife, Mayang. It is her unconditional love and indefinite support that help me bear some of my happiest and darkest time during the past 6 years. We experienced the ups and downs of becoming higher-ed students as we were both students. She sacrificed her scholastic duty many times regardless her responsibility as a student herself, allowing me to pursue my own academic duty. Her strong personality and attitude often push me beyond my boundary, particularly during times when I almost surrendered and lost faith in myself. I will always cherish her faith in me, her love, and her support. As I always said to her, she is my everything, she is my world: my wife, my best friend, my confidante, my source of wisdom, the mother of my children, and my sometimes counterpart.

During times when most married doctoral students refrain from having offspring, Mayang and I are blessed with two beautiful children: Nayyara and Rayhan. Their laughter, smile, behavior and act, cries fill my world, put a smile on my face, and sometimes give me a constant headache. While some might believe that it is during the unfortunate time of wealth despair as a graduate student that they arrive to this world, Nayyara and Rayhan become a part of an interesting, stimulating, and intelligent journey of mine. I regret the moments when I gave them a hard time due to my very own distress but I cherish their love and support and am grateful that they are always by my side in my quest for scholarly achievement. May Allah bless you abundantly with love, mercy, and wisdom: Mayang, Nayyara, and Rayhan.

My doctoral journey at Virginia Commonwealth University began with my encounter with my then dissertation chair, my teacher, my supervisor, and my "father" Dr. Gurpreet Dhillon. I remember the day when I first stepped into the old business-school building in the early of 2006 and met with Dr. Dhillon for the first time in which he took me on a tour around the 4th floor where the information systems department was once located. It was a couple of days after his daughter Anjun Dhillon was born. Dr. Dhillon is an intelligent person, a great teacher, a well-known scholar, and a patient individual who can also be firm when needed. He instills in me the pyramid of research and the concept of security control dimension that now becomes a solid grounding in most of my scholarly work. It is an honor for me to pursue this academic journey under his tutelage. Other special thanks go to Dr. Roland Weistroffer who keeps remind me of the importance to emphasize work that has contribution to theory and academic and to Dr. Allen Lee who introduces me to the diversity of research methodology.

This journey would also be impossible to pursue without the support and the love from my parents and parents in law. All four parents instill in me the importance of education and knowledge. My sincere gratitude to my parents for supporting me emotionally and financially and to my parents in law for their moral support and help with taking care of Nayyara and Rayhan when Mayang and I were busy with school. I could not complete this pursuit if not of their blessing, prayers, and support. My uncle Anton and aunt Ifa for their support and invitation to have fun and socialize, keeping my feet on the ground as a social creature. Last but not least, my brother Kiki, sisters in law Dita and Sari, and brother in law Harry. It is my sincere wish that I have made you all proud.

Table of Contents

List of Tables

List of Figures

Abstract

INSTITUTIONALIZATION OF INFORMATION SECURITY: CASE OF THE INDONESIAN BANKING SECTOR

By: Muhamad Faisal Fariduddin Attar Nasution, Ph.D.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University.

Virginia Commonwealth University, 2012

Director: Dr. Gurpreet Dhillon

Department of Information Systems

This study focuses on the institutionalization of information security in the banking sector. This study is important to pursue since it explicates the internalization of information security governance and practices and how such internalization develops an organizational resistance towards security breach. The study argues that information security governance and practices become institutionalized through social integration of routines and system integration of relevant technologies. The objective is to develop an understanding of how information security governance and practices in the Indonesian banking sector become institutionalized. Such objective is built on an argument that information security governance and practices become institutionalized through social integration of routines and system integration of relevant technologies. Pursuing this study is necessary to conceptualize the incorporation of security governance and practices as routines, the impact of security breaches on such routines, and the effects of a central governing body on such routines altogether.

Accordingly, the concept of institutionalization is developed using Barley and Tolbert's (1997) combination of institutional theory and structuration theory to explain the internalization of security governance and practices at an organizational level. Scott's (2008) multilevel institutional processes based on institutional theory is needed to elaborate security governance and practices in an organization-to-organization context. The research design incorporates the interpretive case-study method to capture communicative interactions among respondents. Doing so provides answers to the following research questions: (1) how institutions internalize information security governance and practices, (2) how an external governing body affects the institutionalization of information security governance and practices in institutions, and (3) how security breaches re-institutionalize information security governance and practices in institutions.

Several important findings include the habitualized security routines, information stewardship, and institutional relationship in information-security context. This study provides contributions to the body of literature, such as depicting how information security becomes internalized in an organization and the interaction among organizations engaged in implementing information security.

1 INTRODUCTION

1.1. Prologue

This study focuses on information security institutionalization in the banking sector. Institutionalization is a process of building a social structure that embodies concepts in regulation and change resistance (Burrell and Morgan 1979). Unlike any other concepts, institutionalization depicts the dynamic process of creating structure (Barley and Tolbert 1997). The use of institutionalization is aimed at depicting how information security is governed and practiced as routine and how radical changes or disruptions such as security breach incidents have the possibility of disturbing the routine. The radical changes in general are usually indicative of a problem with managing of information security in organizations. While studies have identified good security policies (Dhillon 1997; Dhillon and Torkzadeh 2006) and frameworks for security governance (Brotby 2009; Da Veiga and Eloff 2007; Von Solms and Von Solms 2009), there is a lack of understanding about how security breach incidents have the potential to impair the implementation of security policies and security governance in the long run.

Individuals, organizations, and businesses use banks to safeguard and secure, lend, or invest money. As the economy of a nation progresses, the banking sector and its activities become one of the country’s fundamental economic indicators. Any nationwide economic turbulence often results in negative impacts (e.g., reputational damage) on commercial banks. However, such adverse impacts can be prevented or lessened by governmental intervention and involvement. This can be demonstrated by clearly determining the banks' permissible activities, corporate structure, ownership, and maximum leverage ratios (Flannery 1998). While advances in information and communication technologies have created opportunities for growth, expansion and myriad other benefits for banks and their customers, such technologies pose potential dangers and pitfalls of tremendous significance and staggering proportions. In fact, currently the most prevalent examples of the potentially negative impact of technology advancement on the banking sector are electronic-banking transaction sniffing and debit card identity theft.

A simple definition of a bank is "an institution for receiving, lending, exchanging, and safeguarding money and, in some cases, issuing notes and transacting other financial business."[1] Keeping this definition in mind, the perception of a bank as an institution refers to an organization with an existing synergy of norms and regulations. Furthermore, these norms and regulations are enforced through various methods such as rewards, punishment, or supervision. The supervisory function of a central bank ensures systematic stability, as it conducts prudential supervision (solvency of banks), monitors transparency, and ensures correct practices (Quaglia 2008). The prudential banking supervision is a powerful tool that the central bank uses to govern and control the functioning of commercial banks and other financial institutions. Any situation arising out of the Central bank's failure to supervise commercial banks or any commercial bank's failure to comply with regulations mandated by the central bank, results in not only harming customers but can also trigger off a countrywide economic crisis. An example of such a scenario is the plight of Japanese banks in the 1990s. This national crisis in the banking sector

[1] http://dictionary.reference.com/browse/bank

and colossal failure was attributed to the inadequate alignment of the Japanese banks' governance structure to the dynamic nature of business environments in the 1980s (Kawaura 2004).

Information security in banking sector is a vibrant and interesting topic that has long been under careful investigation by scholars, researchers, and economists alike and continues to be pursued rigorously. The topic is such that it is a major concern for every practitioner, especially bank personnel, governmental agencies, law enforcement and prevention agencies and the general public alike, which comprise the wide catchment of the banking sector's stakeholders.

Information security in the banking sector demands and necessitates one of the most highly enforced security governances and control mechanisms due to the nature of bank operations. The key factor of information security in banking sector is how central banks govern and enforce sets of regulations and policies to minimize information security breaches, and how central banks enforce the enhancement of information confidentiality, integrity, and availability. In this respect, as the initiators, protectors and supervisors of good information security practices, central banks should define good practices in information security, which allow commercial banks to provide convenient and secured financial transactions and thus maintain the stability of a nation's macroeconomic operations and general welfare. Furthermore, commercial banks need to abide by a set of regulations and policies enforced by the central bank which concern their information security. A commercial bank may have its own set of standards and policies pertaining to information security, reflecting the information security guidelines issued by the central bank. Therefore, issues in information security governance in banking sector coincide with issues of regulations and governance.

1.2. Research Motivation

The motivation for this study is based on three facets of information security: 1) security governance and practices that form routine actions, 2) disturbance of such routines by security breaches, and 3) effects of central governing bodies on such routines. As such, there is a gap in information security studies. Most studies in information security focus on the first or the second facet. Not many studies, however, have attempted to connect security governance routines with the impact of security breaches. The three motivational facets can be linked to the multilevel governance in a complex institutional setting through the concept of institutionalization (Hall 2008). The banking sector provides a perfect empirical scenario, portraying a complex institutional setting. Any activity by a commercial bank is overseen and controlled by the central bank. For example, a commercial bank manages its information risk not only to safeguard its information assets, but also because this action is compulsorily regulated by the central bank. Failure to manage information risks has often caused greater damage than mere privacy violation, mostly involving loss of financial assets (Dhillon and Moores 2001).

Studies in information security have revealed various practices, techniques, and frameworks aimed at preserving security from a technical aspect, a behavioral aspect, or a combination of both. Studies have also investigated various computer crimes. Most studies, however, have not investigated how all these aspects can be intertwined into what would emerge as a routine that is unique to one organization.

This study focuses on conceptualizing the formation of information security in an organization as routine security behavior. Institutionalization concept introduced by Barley and Tolbert (1997) is borrowed to capture how information security can be delineated as a daily, habitual practice (routine) by members of an organization. This study therefore explores three important aspects of information security as proposed by Dhillon and Moores (2001) and by Dhillon (2007): technologies and technical procedures, organization and formal regulations, and informal communication and security awareness. Extant studies rarely emphasize on combining the three aspects.

Studies in information security have not reflected nor incorporated the idea of a central governing body. Governance, control, and supervision by a central governing body draws upon the simplification of prudential supervision. This study adopts the prudential banking supervision by emphasizing the act to enforce policies, standards, and permissible activities in banks. The application of prudential banking supervision can be perceived as a macro-institutional phenomenon by which the central bank governs the practice of information security in commercial banks. The application of prudential banking supervision can also be perceived as a micro-institutional phenomenon wherein such institutionalization can be conceptualized to depict information security governance and practices within each individual bank. Prudential banking supervision is hence a key factor towards defining and formalizing the institution or institutionalizing the phenomena, i.e., enforcing regulations and norms of permissible activities in banks. This supervision effort is one such method to safeguard the unsavory impact of bank failures, which inflict an open wound leading to severe economic losses and reputational damage to a bank (Pennathur 2001).

Finally, studies in information security focusing on computer crimes often depict only types of computer crimes, impacts of such crimes on organizations, and preventive and mitigation measures undertaken by organizations. Studies implicitly acknowledge, if not openly regard, computer crimes and security breaches as an unsubstantial implementation of information security. Studies often regard computer crimes and security breaches as a separate entity that is not integral to security practices. Even when performed by members of an organization (e.g., employees), computer crimes are considered subversive acts rather than a regular instantiation of information security practices (Dhillon and Moores 2001).

This study is therefore built upon the incorporation of security governance and practices as routines, the impact of security breaches on such routines, and the effects of a central governing body on such routines. The fundamental concept of this study lingers between the technology/technical aspect, organizational aspect, and informal-communication aspect. Using institutionalization allows the viewing of security breaches as an instantiation of information security and integration of such a view into routine security governance and practices. Security breaches should be viewed as a radical event that provokes change within the institutionalization (i.e., re-institutionalization) of information security (Powell and DiMaggio 1991).

Therefore, this study is developed to achieve the following objective: to develop an understanding of how information security governance and practices in the Indonesian banking sector become institutionalized. The argument of this study is that information security governance and practices become institutionalized through social integration of routines and system integration of relevant technologies. To accommodate such an objective, this study seeks to answer the following questions:

- How do institutions internalize information security governance and practices?
- How does an external governing body impact the institutionalization of information security governance and practices in institutions?
- How do security breaches re-institutionalize information security governance and practices in institutions?

1.3. Definition

1.3.1. Information Security

Cornell University’s Legal Information Institute defines Information Security as a means of “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability”[2]. Information security breaches in banking sector can be cumbersome and hence are viewed as a crucial issue. Since it deals with financial information, a bank becomes a lucrative target for data and information thefts. Banks manage information risk through liability transfer, indemnification, mitigation, and retention to minimize vulnerabilities, accidents, losses, and countermeasure effectiveness (Blakley et al. 2001). Information security practices in general comprise of activities that deter, prevent, detect information security breaches (Straub and Welke 1998), and recover the damages attributed to lack of emphasis on information confidentiality, integrity, and availability (Dhillon and Backhouse 2000; Page et al. 2007).

Most often, researchers focus on the technical aspects of information security such as network security (Alfaro et al. 2008), firewall (Finne 1996), and cryptography (Rindfleisch 1997). Researchers mostly look at the management aspect of information security, focusing on the information security policy and the management of information risks. The management aspect of information security also deals with issues in upper management’s support, addressing the need to support the campaign for certain standards and codes of conduct which are used to apply controls based on the organizational and formal regulations aspect. Moreover, researchers also agree that establishing and socializing organizational culture and norms is essential for employees’ adaptation to attempts that reinforce controls using informal communication and

[2] Source: http://www.law.cornell.edu/uscode/44/3542.html

security awareness among social agents. Specifically, Straub and Welke (1998) allude to the importance of raising security awareness through education and training programs, in order to progress toward the development of information systems security through risk analysis, countermeasures, and security implementation.

This study adopts the concept of information security that embodies such concepts as the technical aspect, management aspect, and informal communication. Reviewing these concepts in totality provides insights into the interaction between controls based on technology and technical procedures, formal organization, and informal communication among social agents. These interactions provide a fundamental ground for conceptualizing information security governance. The minute details and nitty-gritty's of security governance practices can be explained using institutionalization.

1.3.2. Institutionalization

Institution is defined as "a well-established and structured pattern of behavior or of relationships that is accepted as a fundamental part of a culture"[3]. Examples of an institution include marriage, higher education, and banks. Commercial banks along with the central bank form an entity of financial institutions that engage in financial activities (Lewis et al. 2008; McLaughlin 1999; Shull 2002) and determine the stability of a nation's macroeconomic welfare (Cecchetti and O'Sullivan 2003; Hellier 1999/2000; Quaglia 2008). Bank as an institution consists of individuals who are bound under similar regulations and share similar beliefs (Stern and Barley 1996). Tsoukas and Chia (2002) define an organization as an abstraction of generalizing and institutionalizing human action through cognitive representations and as a

[3] Source: http://dictionary.reference.com/browse/institution

pattern that can be shaped and constituted, and which is evolutionary in nature. Barley and Tolbert (1997) assert that organizations can be viewed as an institution, which leads to the conception of it being an organization consisting of a framework of rules and representations of symbols derived from cumulative history and interaction.

The essential concept that distinguishes institution from organization is regulation, which refers to governance or supervision. In a practical sense, bank regulations, imposed by the central bank, regulate capital requirements, mandatory restrictions on asset choice (e.g., the use of ICT), and deposit insurance (John et al. 2000; Laeven and Levine 2009). From a micro-institutional perspective, the banking corporate governance body has already defined the concept of banks as financial institutions. The board of directors and senior management are responsible for corporate governance in a bank (Singh 2006). Hence, policies and regulations are enforced by the board of directors and senior management of each bank. Hence, from a macro-institutional perspective, the existence of and the supervisory activities of the central bank help refine the concept of banks as a notion of financial institution. The policies and regulations of each bank are based upon the policies and regulations imposed by the central bank according to the demands of a nation's financial situation. The enforcement of policies and regulations reflects the strength of the central bank (Quaglia 2008).

In order for banks to avoid such malfunctions, banks need to formulate strategic use of their information systems and pay attention to their information security. The strategic use of information systems can be exercised by the management of information security, through the enforcement and supervision of information security policies in banks; hence formulating and enforcing the practice of information security governance. There are two views of information security governance practice in banking sector: the micro-level practice or the (inter) micro-institutional perspective, and the macro-level practice or the (intra) macro-institutional perspective. The micro-institutional perspective views the enforcement and supervision of information security policies in each individual bank, while the macro-institutional perspective looks at such enforcement and supervision in a top-down approach (i.e., the enforcement and supervision of such policies by the central bank).

1.4. Structure of Dissertation

This study is organized as follows: chapter 2 looks at the extant literature in the fields of information security, banking regulations, banking business and activities, and prudential banking supervision. Points of interest include managing information risks in banking sector, managing information security in banking sector, permissible bank activities and bank structures, bank regulations, and prudential banking supervision, i.e., the relationship between the central bank and commercial banks.

Chapter 3 covers the philosophical elucidation of institutional theory and structuration theory. The institution theory is elaborated using seminal works by S. Barley (1986), W. R. Scott (1987, 2008), and P. Selznick (1969) while the structuration theory borrows conceptual frameworks offered by A. Giddens (1994), W. J. Orlikowski (1992, 2000), and G. Walsham (1993). These theories together have created the concept of institutionalization using the approach introduced by S. Barley and P. Tolbert (1997), providing a powerful theoretical framework that can be used to explain the practice of information security governance in banking sector. This chapter also serves to establish the theoretical framework for this study using the institutional theory as well as the proposed research methodology.

Chapters 4, 5, and 6 offer the theoretical case studies based on empirical data. Chapter 4 presents a case study of the institutionalization of information security in the central bank (Earl Capita Bank), chapter 5 presents a case study of the same process in a government-owned commercial bank (Centro Metropolitan Bank), and chapter 6 provides such case study in a private commercial bank (Blue Sequoia Bank). Chapter 7 provides a synthesis and presents a thorough discussion of the three case studies.

This study ends at chapter 8, which provides concluding remarks and implications for further research and practice.

2 LITERATURE REVIEW

2.1. Introduction

This study essentially looks at how information security governance and practices are internalized in an organization. In doing so, this chapter presents concepts that reflect the socio-organizational orientation of information security (Dhillon and Backhouse 2001), emphasizing on a behavioral perspective of information security. The socio-organizational orientation of information security looks at the synergy between technical controls that direct technology use and technical procedures, formal controls that focus on formal organizational aspect such as policies and regulations, and informal controls that emphasize the importance of informal communication aimed at raising security awareness. These three controls comprise the security-control dimensions (Dhillon and Moores 2001; Dhillon 2007). Information security governance, which is the most important concept in this study, introduces frameworks that direct the implementation of information security and incorporates the three security-control dimensions.

The frameworks in general suggest managing information risk (Blakley et al. 2001; Brenner 2007) and information security policy (Herath and Rao 2009; Hong et al. 2006). Literatures are selected to cater to information-security studies that focus on behavior and social interaction, including those that explore ethics in information security (e.g., Dhillon and Backhouse 2000; Workman and Gathegi 2007) and security policy compliance (e.g., Bulgurcu et al. 2010; Moulton and Coles 2003).

Most literature, however, regard security breach as a menace and an aberration. Scholars do not consider security breach an integral component of information security and often do not include breach in theoretical frameworks they develop. In addition, many literatures in information security governance confine governance in an internal system and do not recognize external formal body that may have significant influence on internal governance. This study seeks to bridge such gaps by reviewing and finding connections between security literature and other relevant literature. Some literature from banking theories and concepts are revisited to provide better understanding of banking governance.

This chapter aims to revisit literature in information security governance and literatures in behavioral information security. Section 2.2 presents various views of information security governance. These views focus on the fundamental issues and concepts in information security and information risk, information security policy, and information security governance in banking sector. These concepts will be formulated as components of the theoretical framework that builds the thesis for this study, as depicted in section 2.3 and 2.4 that conclude this chapter.

2.2. Information Security Governance

Governance is generally "an inherently social, relational phenomenon" (Hall 2008, p. 4). Scholars have attempted to define (corporate) governance (Brotby 2009; Hall 2008; Von Solms and Von Solms 2009). Brotby (2009, p. 5) defines governance as:

> "The set of responsibilities and practices exercised by the board and executive management with the goal of providing *strategic direction*, ensuring *objectives are achieved*, ascertaining that *risks are managed appropriately*, and verifying that the enterprise's *resources are used responsibly*."

A definition by Von Solms and Von Solms (2009, p. 2) depicts governance as a set of activities that "(1) direct, or plan, or establish responsibilities, and (2) control outcomes, or ensure implementation, or enforce compliance." They also argue that risk management is one of the essential factors to be considered in corporate governance. Schooner and Taylor (2009) denote that the corporate governance standard emphasizes that bank management assumes the sole responsibility to conduct business, and not the supervisory agencies. Flannery (1998) asserts the importance of assessing the institution's condition and implementing any disciplinary action when necessary.

The concept of governance by an external-central body occurs as a result of a system of multilevel governance (Hall 2008). This implies a set of corporate governances within each institution governed by a superior institution that assumes higher power. Hall (2008) has introduced the deontic power and constitutive power of central bank as a denominator of the higher hierarchy in the banking social system. These powers bestow the central bank the capacity for macro-prudential supervision, which is "the monitoring and assessment of risks to the stability of the financial system as a whole" (Krauskopf and Steven 2009, p. 1174).

The conceptualization of prudential supervision is dependent upon the existence of the central bank. The central bank is a higher, regulatory authority as denoted by Hall (2008):

> "Possession of either or both of these forms of independence leaves the central bank in command of enormous authority over, for example, the domestic money supply and the supply and price of short-term credit to the banking sector, as well as the price of money in the short-term money markets. It also permits central banks to delegate authority to other actors, including private sectors in the financial markets."
>
> R. B. Hall (2008, pp. 1-2)

The consensus view of the central bank is that this institution is responsible for maintaining price stability by keeping inflation low and stable (Ising 2009). Hall (2008) denotes that the central bank possesses "deontic powers." Such possession means that "the powers of central banks, in the same fashion, are uniformly deontic powers in the form of rights, duties, obligations, authorizations, permissions, empowerments, requirements, and certifications that endow the central bank with social and economic power as a result of the collective assignment of its status functions" (Hall 2008, p. 57). Hall borrows the concept of deontic power from deontology, which is "the science of duty; that branch of knowledge which deals with moral obligations; ethics" (Hall 2008, p. 49). Hall further implies that the deontic power of central bank is a manifestation of power arising from social relations of a specific form of constitution, which is one that results from collective assignment of status functions. Hence the central bank also possesses constitutive power resulting from status functions of the bank as a government agency, lending it the authority to "(1) socialize risk, (2) determine the level of national wealth held in reserves in the form of foreign exchange, and (3) determine how many of these reserves to expend to uphold the exchange rate when it comes under pressure" (Hall 2008, p. 96). Quaglia (2008) examines the strength of the central bank and measures such strength in terms of tangible and intangible resources (e.g., credibility, expertise, and international ties), and existing policy competences. In addition to Hall's (2008) deontic power and constitutive power, Silva and Backhouse (2003) introduce two types of power that emerge from social conditioning. The first type, dispositional power, resembles Hall's (2008) deontic power, accumulating from social integration. The second type, facilitative power, is a power that endows an entity with the capacity to persuade or force other entities to behave accordingly.

The first type of literature in information-security governance is one that deal with governance frameworks. Wibowo and Batra (2010) introduce an information-security governance framework that incorporates internal and external threats and note the damages caused by any security breach involving such a framework. Dos Santos Moreira et al. (2008) develop an information security governance framework based on the decision-making structure which prevails in information systems, containing operational level (daily activities), tactical level (review/follow-up), and strategic level (annual reviews, establishing policies, and organization view). The framework reflects policy controls, process of implementing controls, people who are responsible for the policy controls, and the technology used for implementing policy controls. Da Veiga and Eloff (2007) provide a more detailed framework for information security governance. This framework highlights the technology, processes, and people aspects, specifically comprising the strategic framework (e.g., sponsorship, strategy, and risk management), managerial and operational framework (e.g., security management and organization, security policies, user security management) and technical framework (e.g., system development, incident management, technical operations, physical and environmental, and business continuity).

Another type of security-governance literature looks at other details of the security governance framework, particularly through the assessment of model and outcomes. Brotby (2009) details six outcomes that information security governance needs to achieve for it to be accepted as desirable. These outcomes are (1) strategic alignment between security activities and business strategy, (2), risk management, (3) business process assurance/convergence, (4) value delivery with a view of optimizing investments in support of business objectives, (5) resource management, and (6) performance measurement. Von Solms and Von Solms (2009) introduce a model for information security governance, consisting of (1) three levels of management (strategic level or board and executive management, tactical level or senior and middle management, and operational level or lower management and administration), (2) direct part of the cycle from the strategic level to the operational level (the top-down cycle), (3) execution part by the operational level, and (4) control part of the cycle going from the operational level to the strategic level (the bottom-up cycle).

Studies have found the executive and top management's involvement to have significant impact on information security governance (Dutta and McCrohan 2002; Khalfan and Alshawaf 2004; Knapp et al. 2006). Ward and Smith (2002) state that access control policies for information systems should follow corporate governance guidelines and risk management strategies. They propose that information security policies should be implemented through information security responsibilities, management accountability policy, and other baseline access control security policies within individual and distributed systems. Von Solms (2001) creates a direct link between corporate governance and information security, emphasizing issues in corporate information security and the necessity to include information security in corporate governance documents. Von Solms (2005) also states that in order to create effective information security governance, implementation should be supported by good practices in IT governance and corporate governance. The implementation should be conducted by not only the IT department, but also the Information Security Compliance Management Department. Von Solms and Von Solms (2006a) develop a framework for information security governance depicting the direction, execution, and control of management levels of information security, including strategic, tactical, and operational. They emphasize the need for the board to control (manage) the organization effectively in order to ensure sound information security governance. Von

Solms and Von Solms (2006 b) also emphasize that boards and executives should pay particular attention to issues in information security even if they pose no immediate danger or imminent risk, as a general practice in information security governance.

Other studies investigate the direct role and impact of executive and top management. Posthumus and Von Solms (2004) underline the importance for executive management, including the board and CEO, to carefully consider issues in information security and encourage the need to integrate information security in corporate governance through a sound information security governance framework. Moreover, Moulton and Coles (2003) define corporate governance as a managerial attempt to efficiently manage a corporation and exploit its resources and an attempt to balance power between managers and investors. In the context of information security governance, they add that corporate governance should consider (1) security responsibilities and practices, (2) strategies/objectives for security, (3) risk assessment and management, (4) resource management for security, (5) compliance with legislation, regulations, security policies and rules, and (6) investor relations and communications' activity (as related to security). McFadzean et al. (2007), unfortunately, contend that management only pays attention to information security if the strategic information systems are considered important for the well being of the organization and there is an imminent risk or threat to information.

Information security governance requires active participation of not only the CISO and his team, but also the board and the CEO of the organization. For instance, information security governance requires participation, and even intervention, by higher authorities. Information security governance depicts the synergy between people, organization, technology, and strategy. Scholars agree with the concept that information security governance is the control of information security policies and regulations, reflecting the good corporate practices of an organization (Mishra 2009). The governance, however, involves controls of managers (management) by boards, boards by stakeholders, and stakeholders by management (Von Solms and Von Solms 2006). Information security governance is therefore an effective and efficient mechanism to ensure the interaction between social actors and their wider social systems. Most studies, however, do not consider how security governance is driven by external factors other than security breaches. These studies often focus on internal factors such as the role of executive and top management, risk management, security rules and policies, and framework. Identifying such gap, this study seeks to explore a level that involves an interaction between social actors in an internal institution and an external governance body in the wider social system.

2.2.1. Information Security: Fundamental Issues and Applications in Banking Studies

Studies often focus only on the technical perspective of information security. These studies look at the design and application tools for information security and hence define security as a tangible and concrete concept (Baskerville 1993; Dhillon and Backhouse 2001). Nowadays, scholars have begun to consider the non-technical perspectives of information security, i.e., the socio-organizational perspective (Dhillon and Backhouse 2001). The scholars studying these aspects advocate that while technology is important, organizational and human factors also significantly contribute to the success of information security (Dutta and Roy 2008). Some of these scholars often refer to risks when discussing information security (Blakley et al. 2001; Jones 2007). Some scholars have linked information security to the values of confidentiality, integrity and availability of information (Anderson 2003; Dhillon and Backhouse 2000). Dhillon and Backhouse (2000) extend the notions of confidentiality, integrity, and availability of information security to responsibility and knowledge of roles, integrity (as a requirement of membership), trust (which is distinct from control), and ethicality (as opposed to rules). Anderson (2003) presents information security as an assurance of a balanced information risks and controls. Kulczycki (1997) defines information security as all activities undertaken to safeguard assets, which includes financial and accounting responsibility as well as intangible valuables (e.g., proprietary product information, intellectual property, and basic computer system integrity). Kulczycki further contends that advances in information and communication technologies have caused data and information to become more powerful and easier to manipulate and hence there is a need for more potent, advanced technology to protect the data and information.

Dutta and Roy (2008) express that information security involves an intertwining of technical, organizational, and behavioral factors. Hazari et al. (2008) believe that in information-security, organizational and behavioral factors are contrived upon the employees' integrity and commitment to safeguarding their organizational assets and interest. Moreover, Hazari et al. (2008) notice that the integrity of these individuals is influenced by attitude, subjective norm, and perceived behavioral control. In his paper, Dhillon (2001) denotes the use of formalized rules in the form of security policies, normative controls such as culture, value or belief system, and monitoring of employee behavior. Dhillon argues that the act of breaching information is performed as a result of the combination of an individual's behavioral and normative beliefs. Rhee et al. (2005) take a different direction while investigating information-security related behavioral factors by demonstrating that the users' optimistic bias in their risk perceptions about information security has a relation to the perception of controllability. Rhee et al. argue that individuals tend to believe that negative events are less likely to happen to them than to others. With respect to information security breach in banking sector, several scholars have attributed such breaches to insider threat (Dhillon 2001; Dhillon and Moores 2001). Albrechtsen (2007) denote that employees' security awareness and cautious behavior play an important role in information security performance of organizations, particularly banks. The security awareness and causes behavior can be improved by using the user-involving approach, whereby employees are engaged in various awareness activities such as participation in information security workshops. In a similar argument, Stinchcombe (2006) states that 70% of security breach cases occur from within organizations. Stinchcombe also brings to the managers' attention several factors that contribute to information security breaches. These issues are password leakages and misuse , identity theft, phishing, spamming, etc.

In terms of the attack method, Botha and Solms (2001, 2002) note various ways in which hackers attempt to breach security of information in corporations, government and banks. They contend that insiders often perform non-malicious attack attempts while outsiders may conduct both non-malicious and malicious attack attempts (2001). They also introduce the proactive identification model (PAIM), a fuzzy methodology to combat hacking proactively (2002).

Kaleem and Ahmad (2008) conduct a survey of bankers' perception of electronic banking and find that bankers in Pakistan perceive electronic banking as a tool that minimizes inconvenience, reduces transaction costs, and saves time. However, Kaleem and Ahmad also opine that bankers have a perception that electronic banking opens a security hole, allowing government access to public data, increasing the chances for fraud and reducing the level of security. Castiglione (2002) argues that despite the fact that banks successfully protect their information assets in the Internet realm using passwords, firewalls, encryption, etc., they, overlook the non-technical information security aspects such as trashcans, photocopiers or employee desks. Miller and Engemann (1996) introduce the Information Security Management

Planning (ISMP) program to proactively identify and analyze resources that are vulnerable to risks. They emphasize on the importance of proactive involvement of the management. Tsaih et al. (2008) support this notion by extending the importance to even non-information technology managers. They use a study of a bank's loan process, which involves non-information technology managers dealing with safeguarding gaps of physical information assets and their digital formats, as well as the information-processing infrastructure to arrive at this conclusion.

Accordingly, this study takes the view that information security is a socio-organizational instance that requires intensive and complex interaction between technology, organizational, and individual behavior. IT security has been mistakenly styled as information security, with the former being a mere technological artifact that secures the information asset of an organization. The view of technological aspect, however, is not sufficient to describe information-security concept since the technological aspect restricts the dynamic of social interaction, which is constructed by human interactions, whether in a non-formal, non-hierarchical setting or in an organizational setting (Dhillon and Backhouse 2001). Moreover, the organizational setting demands more attention since human interactions in organizational setting are defined and formalized within well recognized norms and goals. In addition, the organizational setting distinguishes the roles of its individual members.

2.2.2. Information Risk

Information risk is an essential component of information security governance. In relation to the banking concept, information risk is a subset of operational risk. Studies in banking concept and theory do not directly point out information risk. Governance and control studies in information security and in banking sector have stated that risk management is an essential component of corporate governance. This subsection aims to create a connection between information risk that has been extensively investigated in information security studies and operational risk that is one of risk factors in banking concept and theory. By first looking at how operational risk is defined in banking concept and theory, one can see how information risk can be positioned in banking concept and theory.

Banks are exposed to various types of risks, which are mainly categorized into four areas: financial, credit, market, liquidity, operational, business, and event risks (Van Greuning and Brajovic Bratanovic 2000; Gupta 2009; Jarrow 2008). The impediment of technology is usually related to the obstruction of operational risk management (Schooner and Taylor 2009). Schooner and Taylor (2009, p. 174) details operational risk as following:

> "It thus includes situations involving fraud, e.g., when traders deliberately falsify information, management failure, and inadequate procedures and controls. Technical errors may be due to breakdowns in information, transaction processing, settlement systems, or more generally, problems in operations that deal with the record-keeping of transactions and the reconciliation of individual trades with the firm's aggregate position (typically refered to as the *back office* functions)."

Issues in information systems are a major concern in operational risk. Studies that investigate information security in banking sector often refer to the problematic concept of information risk and various applications of such an issue. Flores et al. (2006) explain the socialization and enforcement of Basel II norms on the measurement and control of operational risk and the bank's effort to comply with these new requirements within their existing information systems. They propose to use a socio-technical approach that involves the personnel, IT systems (including information risk), organizational structures, and internal controls in order to diminish such a gap. Scholars have linked information risk to information security breaches and procedures to prevent these breaches. Brenner (2007) states that ISO 27001 is an international standard that aids information risk management by implementing and monitoring strong security controls. Von Solms and Von Solms (2009) introduce a variety of frameworks that can be used as a basis for information security policies (e.g., COBIT, ISO 27001, ISO 27002). Ryan and Bordoloi (1997) identify main causes of information security breaches, often including viruses/bombs/worms, inadequate or non-existent logon security, access to data/system by outsiders, loss due to inadequate backups or log files, uncontrolled read and/or update access, uncontrolled user privilege levels, accidental data destruction by employees, and inadequate audit trails. Maguire (2002) states that there are many areas of potential risk during the system development process, and hence this process needs to be carefully analyzed and managed. He identifies potential behaviors and circumstances that result in vulnerability of information to security breaches, including:

1. Use of previously unused platform (failure to deal with known or unknown bugs).
2. Multitasking capabilities (inability to handle user numbers and response times).
3. Changes in the development team (several project managers).
4. Lack of rigorous testing (inability to test in a “live” environment).
5. System development methodology (inappropriate application leading to divergent approaches).
6. Number of stakeholders (failure to satisfy the system requirements of the disparate groups).
7. Immovable end date.
8. Limited access to users (lack of analysis in business areas).

9. Consultancy support (several suppliers of consultancy with separate aims and objectives).
10. Local business requirements (failure to reconcile separate design needs).
11. System changeover (lack of contingency planning).
12. Lack of availability of qualified staff.

Straub and Welke (1998) suggest the importance of raising security awareness through education and training, and progress towards the development of information systems security through risk analysis, countermeasures, and security implementation.

The effectiveness of information security risk is strongly dependent upon the efficient management of information security. McFadzean et al. (2007) contend to this notion by stating that the effective management of information security is accomplished by acknowledging the strategic importance of information systems within the organization and is enhanced by how risk is perceived. Adding to this concept, Bodin et al. (2008) argue that the Chief of Information Security Officer (CISO) needs to recognize and understand the nature of risk. They present three measures to determine and capture various aspects of information security risk. They further denote that risk involves multiple dimensions and meanings within the context of information security. Moreover, according to Blakley et al. (2001), risks of information security breaches can be technically managed through liability transfer, indemnification, mitigation, and retention, and information security risk control can be measured through vulnerabilities, incidents, losses, and the effectiveness of countermeasures. They also suggest that management of information risk emphasizes on reporting, the analysis of information risk, and the evaluation of information security technology. In addition, Jones (2007) recommends the development of a framework for information security risk assessments within an organization. Risk framework should therefore consist of phases that include risks identification (e.g., compliance with standards and regulations, and risk ownership), risks assessment (e.g., risk modeling and testing), risks treatment (e.g., prioritization of risk mitigation), and risks monitoring and reporting.

Information security breaches can also be caused by employees. Scholars have acknowledged security breaches resulting from insider threat. For instance, Dhillon and Moores (2001) assert that computer crimes are often conducted by employees or insiders, and should therefore be prevented and controlled at the very least. They discuss two case studies of computer-crime scandals involving employees of respectively the Kidder Peabody & Co and the Daiwa Bank. Aldhizer III (2008) seconds this finding by presenting facts presented by PriceWaterhouseCoopers (PWC) Global State of Information Security Study in 2007 which finds that 69% of database breaches are caused by people inside the organizations. He propogates another measure to safeguard the insider risk by implementing centralized and automated identity and access management (IAM) controls. Several studies have provided solutions and frameworks to predict and deter insider threat as well as to safeguard information assets. Schultz (2002) presents framework and models dealing with insider attack-related behaviors. Workman and Gathegi (2007) find that punishment and ethics training can be effective in mitigating threats to information and communication technologies by employees. However, the effectiveness of these efforts relies heavily on the underlying motivations of the employees.

Information risk as part of operational risk needs to undergo ongoing evaluation by key players in order to avoid losses, particularly catastrophic losses. This effort requires internal controls, as well as risk monitoring and mitigation, inscribed in the bank policies and procedures; all of which are an essential component of information security governance. Overall, the role of regulatory or supervisory authorities is important in order to govern and monitor the practice of risk management (Adeleye et al. 2004). Therefore, risks of security breach (i.e., information risk) are inherent in the use of technology, and hence can be considered issues in operational risk. As with the management of operational risk, the management of information risk requires participation and involvement of key players in a bank (Van Greuning and Brajovic Bratanovic 2000; Fragniere et al. 2010; McFadzean et al. 2007; Dutta and McCrohan 2002; Khalfan and Alshawaf 2004; Knapp et al. 2006). Information risk can be viewed mostly as a risk that may harm or lead to the misuse of information by relying on inappropriate access to information and communication technologies belonging to a certain organization (Blakley et al. 2001). The most threatening risks, are those posed by insiders, who are employees of the organization or are closely connected to these employees. Various standards and frameworks (e.g., ISO 27001 and COBIT) have been prescribed to safeguard information from these threats. Therefore, the management of information risk resembles the management of operational risk whereas the role of the executive management and regulatory or supervisory authorities is necessary for success. Scholars agree that information risk can be effectively decreased only through management support. Top management or executive support therefore sustains the development of sound information systems security, enhances the adherence of organizational culture to good security practices, and increases the level of enforcement of existing security policies (Dutta and McCrohan 2002; Khalfan and Alshawaf 2004; Knapp et al. 2006).

Studies in information security in banking sector have asserted the importance of managing and mitigating information risk and highlighted how failure to do so can cause a calamity in the victim organization. Studies in banking concept and theory however do not recognize information risk and do not associate information risk with operational risk. Furthermore, studies in information security in banking sector do not directly state that information risk is a component of operational risk. This subsection aims to position information risk in studies in banking concept and theory. By doing so, this subsection has discovered regulatory frameworks (e.g., Basel II and ISO 27001) to manage and mitigate information risks in banking sector.

2.2.3. Information Security Policy

One of the essential concepts in corporate governance is the formulation and implementation of policies and regulations. Bank regulators govern and control the formal responsibility of banks to protect the interests of legal stakeholders (Singh 2006). Quaglia (2008) contends that policy competences affect the central bank's ability to influence the change of supervisory arrangements. Central banks have mostly governed the monetary policy as an attempt to stabilize the nation's economic welfare but tend to overlook the supervision and governance of particular policies related to operational risk (Aguiar and Martins 2008; Batini 2007; Christiano et al. 2008; Ising 2009; Lees 2007). Nevertheless, the actions taken concerning the monetary policy are similar to those taken for other regulatory measures (Ising 2009). Lamy and Moyer (1995) state that the assessment and development of banking regulation needs to take into consideration the perspective of various parties involved: the banking industry, the banking regulators, and the banking consumer. Yang and Zhang (2007) contend that the new anti-money laundering regulations in China impose more severe punishment than do the old regulations. They also state that the new regulations help reduce the likelihood of breaches by imposing stringent requirements of client identity recognition, retention of client identity documents and trading records, and reporting of large-sum transactions and suspicious transactions.

Issues pertaining to top management support of information security necesitate the need to include issues in information security policy (Hong et al. 2006; Fulford and Doherty 2003).

Information security as part of the information technology plans needs to be directed and formulated. Smith and Jamieson (2006) define information security policies as policies that ensure the confidentiality, integrity, and availability of information and assets through protection from theft, tampering, manipulation, or corruption. Chandra (2008) states that the initiation of information security policies denotes management's commitment to advance and safeguard information as an asset. Ross (2008) seconds this notion as he states that information security policies and standards depict management's objective. Knapp et al. (2009) conduct an exploratory study to develop a practice-based organizational model for a comprehensive information security policy for organizations. Knapp et al. also categorize information security policy based on policy management and organizational environment.

Doherty and Fulford (2006) argue that carefully and explicitly aligning information security policy and strategic information system plans enhance the security of the information systems. They find that there is a strong impact of a carefully designed information security policy on the planning of strategic information systems. Knapp et al. (2006) find that top management support has a significant impact on the enforcement of information security policy as well as on the organization's security culture. Whitman (2003) quotes findings by scholars which indicate that only half of the surveyed organizations had effectively designed and enforced information security policy and 90% of those organizations ironically detected computer security breaches within the past 12 months. He implies that IT executives identified information security as a necessary component but not as a critical issue and that information security has been constantly ignored by top management. However, Doherty and Fulford (2005) find no significant relationship between the formulation and implementation of information security policies and the incidence of information security breaches. They attribute this anamoly to factors such as difficulties of raising awareness, difficulties of policies enforcement, policy standards being too complex, inadequate resources, and failure to tailor policies. In relation to information security policy, Vroom and Von Solms (2004) state that auditing the employee behavior with regard to policy compliance is difficult and suggest a less structured and more informal approach by looking at the organizational culture. Bulgurcu et al. (2010) examine the antecedents of employee compliance with information security policy in an organization and discover that the effects of attitude, normative beliefs, and self-efficacy in an employee's intention to comply are significant.

Baskerville and Siponen (2002) enunciate the importance of security policy formulation, particularly in an emergent organization, to the implementation and development of information systems security. Baskerville and Siponen argue that the use of meta-policy is important for the implementation and development of information security, particularly the use of information security policy in an emergent organization. Cuppens and Cuppens-Boulahia (2008) connote that requirements and context are extra conditions that demand specific treatment, whereby information security policy can be applied. Herath and Rao (2009) develop a framework for information security compliance in organizations. An important finding of this study is that there is a strong connection between social influence and organizational commitment, and policy compliance intention. Hong et al. (2006) develop a summary of procedures for building information security policies, which include security policy development and security awareness and policy education.

Information security policy is a necessary determinant of how information security should be formulated and adopted to prevent and deter security breaches. Information security needs to reflect the strategic formulation and implementation of the holistic information systems of the organization. Therefore, the existence of top management and executive support contributes to a clear and precise formulation and adoption of information security policies. Information security policies may exist as rules, permissions, prohibition, obligation, or dispensation to ensure good practices of organizational information security and should hence be defined and formulated by information security meta-policies to maintain consistency and stability (Cuppens and Cuppens-Boulahia 2008; Baskerville and Siponen 2002). In addition, information security policies need to be precise and concise, and should be introduced and socialized in order to be effectively adopted and implemented in organizations. This is because employees' policy compliance attitudes are often influenced by threat perception, organizational commitment and self-efficacy.

2.3. Summary and Discussion

> "Information Security Governance (ISG) consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technology and compliance enforcement mechanisms, all working together to ensure that the confidentiality, integrity, and availability (CIA) of the company's electronic assets (data, information, software, hardware, people, etc.) are maintained at all times."
>
> S. H. Von Solms and R. Von Solms (2009, p. 24)

Based on the literature review, this section aims to conceptualize and synthesize distributed concepts of governance elicited from banking studies and security governance studies. The ultimate aim is to discover the intersection between such concepts in a wider social system such as banking sector. The literature unfolds the concept of two-level governance that is extensively present in the banking sector. Of the two types of governance, studies in banking concepts and theories introduce the macro-institutional perspective of corporate governance, termed as macro-prudential supervision. This type of governance is controlled by the central bank, resulting from the central bank's possession of deontic power, constitutive power (Hall 2008; Krauskopf and Steven 2009), and facilitative power (Silva and Backhouse 2003).

The concept of information security governance is essentially similar to the concept of conventional corporate governance. Da Veiga and Eloff (2007), Knapp et al. (2006), and Dos Santos Moreira et al. (2008), have emphasized the importance to exercise control and regulative authorities to achieve strategic objectives. Schooner and Taylor (2009), and Von Solms and Von Solms (2006a) second this notion by stressing the importance of management in exercising direct internal control to achieve strategic objectives. Schooner and Taylor (2009, pp. 105-106) state that:

> "Corporate governance involves a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring. The presence of an effective corporate governance system, within an individual company and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper functioning of a market economy."

Schooner and Taylor (2009) have indentified key players in banking corporate governance. These key players are the bank's board of directors, senior management, shareholders, customers and other relevant stakeholders. In light of the information security governance, many of the key players for the banking corporate governance are the same personnel accompanied by additional stakeholders. Indeed, key players do play an important role as well in ensuring sound information security governance. Information security scholars have emphasized the importance of executives or top management as participants and involved members in the management of information security. Von Solms and Von Solms (2009) specify these key members as the board of directors, senior executives, steering committee, and the CISO. Each of these key players has an important role in accomplishing sound information security governance. Furthermore, these key players constitute the upper-stratum in the inter-level view of information security governance.

Risk is an important aspect that needs to be considered and handled in corporate governance, as well as in information security governance. Strategic actions and controls need to be performed by key players in order to achieve desirable outcomes. Both banking corporate governance concept and information security governance concept entail the damaging impact of risk as a result of ineffective governance. Scholars have identified the results of such issue, leading to other harmful effects on the nation's economic stability (Malkawi and Malkawi 2007; Penn 2005; Yang and Zhang 2007). Banking corporate governance concept has identified risk caused by the use of technology as part of operational risk. Regulatory authorities have created the Basel II as a guideline for managing operational risk in banks. Such a guideline, however, is geared toward the management of general activities in operational risk. However, aspects of both operational and information risk management emphasize the following: measurement and identification of risk, strategic actions and direct control by key players, and ongoing risk evaluation (McFadzean et al. 2007; Blakley et al. 2001; Jones 2007; Stone and Marotta 2003; Van Greuning and Brajovic Bratanovic 2000; Fragniere et al. 2010). Ongoing evaluation includes raising awareness through education and training (Straub and Welke 1998; Workman and Gathegi 2007).

The use of technology, particularly IT, is an important aspect of information security governance. Improper use of technology and lack of risk socialization by insiders may harm the institution (Flores et al. 2006; Hall 2008; Van Greuning and Brajovic Bratanovic 2000; Schooner and Taylor 2009). Despite the fact that IT plays an important role in effective and efficient banking operations, the improper and unethical use of IT by insiders may prove counterproductive (Dhillon 2001; Castiglione 2002; Dhillon and Moores 2001; Kaleem and Ahmad 2008). Scholars conclude that IT and security need to be regulated and should therefore conform to the standard notion of security: confidentiality, integrity, and availability (Dhillon and Backhouse 2000; Anderson 2003; Brotby 2009).

Another important aspect of corporate governance is the effect of regulations and policies (Singh 2006). Regulations and policies are key components of an institution, and the creation and the enforcement of these produce the effect of institutionalization. The central bank, acting as a regulatory and supervisory authority, is responsible for creating and enforcing regulations and policies for banks and other financial institutions to adhere to. Despite the implementation of Basel II, the central bank seems to take for granted the implementation of regulations and policies for the prevention of operational risk, particularly information risk. Scholars, however, have underlined the importance of regulations and policies for governing information security (Hong et al. 2006; Fulford and Doherty 2003). As such, the existence of the implementation of such regulations and policies is contingent among banks on the micro surface.

The highlight of this study is, however, the aspect of multilevel governance, or the existence of the central bank as the upper-stratum institution among banks as individual institutions. This social instance has conjured a different type of governance, the macro-prudential supervision, conducted only by the central bank (Hall 2008; Krauskopf and Steven 2009). This study looks at the two levels of information security governance. The within-the-bank governance, called the inter-level governance, is implemented by top management within any individual bank. Governance that involves a central governance body is the intra level, which is governed by the central bank in relation to other banks. The macro-prudential supervision lies within the concept of deontic power and constitutive power (Hall 2008). The central bank itself has its own micro-level information security governance implemented by its own key players.

Table 2.1 is developed to highlight the key themes inferred from prior literature. Based on concepts from the literature review, information security governance can be categorized according to the security-control dimensions. Von Solms and Von Solms (2009) introduce a model of information security governance that consists of two major parts: the core part and the expanded part. The core part details the direct and control execution by management actions at the strategic level, tactical level, and operational level. The expanded part provides concepts on directives, control, risk management, organization, and awareness. The technical aspect is inherent in the direct and control aspects but is latent within the core part. The technical aspect is implemented particularly in the operational level of both direct and control aspects in the core part. Scholars have linked operational risk to risk of using information technology (Evans et al. 2008; Flores et al. 2006; Schooner and Taylor 2009; Van Greuning and Brajovic Bratanovic 2000). As for the other control dimensions (i.e., formal and informal), Von Solms and Von Solms (2009) state that the expanded part is to be developed using best practices in information security. Except for the information risk strategic action and control, all managerial themes are categorized under both formal control and informal control. This is because the directive and control of information risk require underlying frameworks (e.g., ISO 27001) (Brenner 2007; Von Solms and Von Solms 2009) and strategic procedures (Blakley et al. 2001; Jones 2007), and are supervised and directed by top management (Bodin et al. 2008; McFadzean et al. 2007). According to Dhillon (2007), security awareness and education fall under the informal control dimension. Security awareness and education are an essential component of sound information-security governance.

Key Themes	Research Methodology	Relevant Literature	Security Control Dimension
Institutional Authority:	Grounded Theory (McFadzean et al. 2007),	McFadzean et al. (2007); Hong et al. (2006); Bodin et al. (2008); Schooner and Taylor (2009); Adeleye et al. (2004)	Formal control and informal control
Board of Directors	Survey Method (Fulford and Doherty 2003;	Fulford and Doherty (2003);	
Senior Executives	Khalfan and Alshawaf 2004;	Dutta and McCrohan (2002);	
Steering Committee	Adeleye et al. 2004),	Khalfan and Alshawaf (2004); Knapp et al. (2006);	
CISO	Mix Method (Knapp et al. 2006)	Von Solms and Von Solms (2006; 2009)	
External Authority	Explanatory Case Study (Quaglia 2008)	Hall (2008); Krauskopf and Steven (2009); Quaglia (2008); Schooner and Taylor (2009); Adeleye et al. (2004)	
Information Risk Strategic Action and Control	Grounded Theory (McFadzean et al. 2007), Analytic Hierarchy Process (Bodin et al. 2008), Multistage Stochastic Program (Fragniere et al. 2010), Survey Method (Adeleye et al. 2004; Gupta 2009), Cox Counting Processes (Jarrow 2008)	Bodin et al. (2008); McFadzean et al. (2007); Brotby (2009); Von Solms and Von Solms (2006; 2009); Da Veiga and Eloff (2007); Blakley et al. (2001); Jones (2007); Workman and Gathegi (2007); Schooner and Taylor (2009); Fragniere et al. (2010); Stone and Marotta (2003); Van Greuning and Brajovic Bratanovic (2000); Gupta (2009); Jarrow (2008); Adeleye et al. (2004)	Formal control

Ongoing Use of IT	Case Study (Dhillon 2001; Flores et al. 2006; Dhillon and Moores 2001), Survey Method (Kaleem and Ahmad 2008)	Dhillon (2001); Castiglione (2002); Dhillon and Moores (2001); Kaleem and Ahmad (2008); Flores et al. (2006); Van Greuning and Brajovic Bratanovic (2000); Schooner and Taylor (2009)	Technical control
Risk Policies and Regulations	Case Study (Doherty and Fulford 2006; Smith and Jamieson 2006), Logistic Regression Analysis (Batini 2007), Survey Method (Doherty and Fulford 2005; Herath and Rao 2009; Hong et al. 2006), Grounded Theory (Knapp et al. 2009), AS-AD Macroeconomic Structure (Aguiar and Martins 2008), Taylor-Rule Formulation of Monetary Policy (Christiano et al. 2008), Linear-Quadratic Framework (Lees 2007)	Smith and Jamieson (2006); Hong et al. (2006); Chandra (2008); Ross (2008); Knapp et al. (2009); Doherty and Fulford (2005; 2006); Herath and Rao (2009); Aguiar and Martins (2008); Batini (2007); Christiano et al. (2008); Ising (2009); Lees (2007); Singh (2006)	Formal control and informal control
Lower-Stratum Institution: Corporate Governance	Design Science (Dos Santos Moreira et al. 2008)	Dos Santos Moreira et al. (2008); Da Veiga and Eloff (2007); Brotby (2009); Ward and Smith (2002); Von Solms and Von Solms (2006; 2009); Flannery (1998); Hall (2008)	Technical control, formal control, and informal control
Upper-Stratum Institution: Macro-Prudential Supervision		Flannery (1998); Hall (2008); Krauskopf and Steven (2009)	Technical control, formal control, and informal control

Table 2.1 – Conceptual Elements of Two-Level Information Security Governance in Banking Sector

2.4. Conclusion

This chapter analyses the various bodies of literature pertaining to banking management and governance, and information security governance. Extant literature reveals widely accepted conceptualizations of information security governance, including key players in governance, risk management, IT in banks and information security, regulations and policies, and macro-prudential supervision. It is believed that the intra-level governance of information security, hence termed as information security macro-prudential supervision, delineates similar information security governance at the micro level, barring the only difference in terms of the key players and institutional strata. Hence the information security governance in banking sector reveals two-level governance: one within each institution (inter-institutional perspective) and the other by an institution to other institutions (intra-institutional perspective).

The institutionalization of information security as an impact of the two-level security governance enhances the view of information security as a socio-organizational instance. As the building block for a socio-organizational study of information security, the three security-control dimensions are applied to each component of the information-security governance ontology. With the use of IT exclusively linked to the technical control, the other dimensions are applied to the managerial and informal aspects of information security governance.

3 THEORY AND RESEARCH FRAMEWORK

3.1. Introduction

The essence of institutional theory comprises of issues in society, broadly categorized into order and conflict, stability and change, or consensus and coercion. This chapter seeks to explore two theoretical frameworks that portray institutionalization of information security in the inter level (i.e., within an organization) and the intra level (i.e., between organizations). Both frameworks denote institutionalization as a process, originating from institution. Another objective of this chapter is to present a research design for this study, using the interpretive case study. This study borrows the view of institution from Scott (2008), who points towards the infinity of institutions, and Powell and DiMaggio (1991), who contend that there are different faces of institutionalization.

The first theoretical framework looks at the combination and conjunction between institutional theory and structuration theory as introduced by Barley and Tolbert (1997). Applying such a combination can demonstrate the dynamic interactions among social elements in banks, as well as the formulation of policies and regulations, dictating the formation of banks as collective institutions. Institutional theory is concerned with the maintenance of societal cohesiveness, the elemental unity of society, which creates a harmonic entity, and the explanation of the role of regulation in society (Burrell and Morgan 1979). On the other hand, structuration theory presents an explanation of dynamic social structuring of agency's interaction with resources (Barley and Tolbert 1997). Structuration theory provides an understanding of how the use of resources or artifacts can become a habit (Berger and Luckmann 1966). The two theories complement each other. Institutional theory depicts the internalization process of an interaction between agency and modalities while structuration theory shows the dynamics of such an interaction. Whatever approach one undertakes, institutional theory and structuration theory as social-science theories attempt to discover knowledge that guides everyday life, i.e., to portray the reality of everyday life (Berger and Luckmann 1966). The contention of this chapter is that the inter-level institutionalization is an important combined concept of institutional theory and structuration theory.

Another theoretical framework that is used in this study is derived from Scott's (2008) view of multilevel institutional processes. This view alludes to the interaction and relationship between two entities and their larger social environment. While each entity affects one another, each entity manages its affair respectively. This view also pinpoints the influence of social environment on the activity of each entity. This framework serves as a roadmap for the intra-level institutionalization.

The organization of this chapter is as follows: section 3.2 reviews various concepts of institutions. Section 3.3 provides a thorough view of institutionalization that is built from institutional theory. These two sections contain various conservative perspectives of institutional theory as covered in this section, including the background of institution, the notion of institutionalization as a social phenomenon, and the variety of institution-related seminal works by researchers who have developed or often used institutional theory in their work. These include works by W. Richard Scott, Walter W. Powell and Paul J. DiMaggio, Philip Selznick, and Stephen Barley. Section 3.4 covers the development of the two theoretical frameworks using Barley and Tolbert's combination of institutional theory and structuration theory, largely based on the structuration usage and legitimacy usage (Björck 2004), and Scott's multilevel institutional processes. This section explains the theoretical frameworks based on inter-level perspective of institutionalization and intra-level perspective of institutionalization. Section 3.5 discusses and proposes the research methodology designed for this study. Section 3.6 concludes this chapter.

3.2. A Review of "Institution"

An abstract view of an institution is that it is a result of ongoing "typification of habitualized" actions by social actors (Berger and Luckmann 1966, p. 54). Such typification, or actions that become a habit, is shared among all members of a social system and typifies individual actors as well as individual actions in return (Berger and Luckmann 1966). This typification is an ongoing process that over time begins to be viewed as rational, and is taken for granted, by the members (Scott 2008). The rational view of institutional theory is taken from its economic roots (i.e., the rational actor model of organizations) whereby actors seek to achieve objectives and perform collective tasks or functions in a certain, regulated manner in a formal organization (Powell and DiMaggio 1991; Lawrence 2003; Scott 2008). Furthermore, Selznick (1969, p. 77) refers to "the emergence of rationality as an attribute of a system." Another conceptual view of institution is that it embodies structural principles as a reproduction of societal totalities in a time-space extension (Giddens 1984). Powell and DiMaggio (1991, p. 145) describe institution as "a social order or pattern that has attained a certain state or property." Several examples of institution are marriage, academic tenure, the contract, wage labor, insurance, the motel, the academic discipline, voting, the corporation, the handshake, the army, and formal organization. One of the originators of institutional theory terms an institution as:

> “Multifaceted, durable social structures made up of symbolic elements, social activities, and material resources. Institutions exhibit distinctive properties: They are relatively resistant to change. They tend to be transmitted across generations, to be maintained and reproduced… Institutions exhibit these properties because of the processes set in motion by regulative, normative, and cultural-cognitive elements. These elements are the central building blocks of institutional structures, providing the elastic fibers that guide behavior and resist change.”
>
> W. R. Scott (2008, pp. 48-49)

Such a view of institutions recognizes an important concept: the notion of change resilience. Burrell and Morgan (1979) introduce the concepts of “sociology of regulation” and “sociology of radical change.” Through conceptualization, institutional theory resents the notion of change, and thus enquires into the epistemic and the ontology of maintaining and reproducing social order and stability. Such an enquiry characterizes institutional theory as one belonging to the sociology of regulation. Despite its nature of resenting change, institutional theory also concerns itself with destructuration of an institution, i.e., deinstitutionalization, in which an institution begins to lose credibility and experiences change (Scott 2008). Furthermore, the foundation of institutional theory rests on the investigation of the impact of social control on human activity (Berger and Luckmann 1966). According to Selznick (1969, p. 8), law is required to enforce control, and order, and is therefore necessary to encourage “peace, settle disputes, suppress deviance.”

Scott (2008) has developed exhaustive concepts for institutional theory. He contends that an institution is created when repetitive, rational actions become internalized by individual social actors. He also states that institutions “do not emerge in a vacuum; they always challenge, borrow from, and, to varying degrees, replace prior institutions” (Scott 2008, p. 94). He forwards two approaches to studying social facts using institutional theory: one that concerns institutional creation and another that deals with institutional change. The study of institutional creation, as stated earlier, does not lend itself to the belief of an empty initial state. It rather examines how an institution morphs into a new institution as a consequence of ascension from its initial state and its contamination with reproduced interactions of beliefs, norms, and organizations within time-space extension (Giddens 1994; Scott 2008). The study of institutional change, on the other hand, looks at "how an existing set of beliefs, norms, and practices comes under attack, undergoes de-legitimization, or falls into disuse, to be replaced by new rules, forms, and scripts" (Scott 2008, p. 94). There are four types of institutional change (Powell and DiMaggio 1991, p. 152):

- Institutional formation: this concept is similar to the one about institutional creation as introduced by Scott (1987, 2008). Powell and DiMaggio (1991, p. 152) moreover provide their own definition for institutional formation as "an exit from social entropy, or from non-reproductive behavioral patterns, or from reproductive patterns based on 'action'."
- Institutional development (or elaboration): this institutional change represents "a change within an institutional form" where the institutional form advances and continues to become complex and meaningful. This form is always evolving and nowhere near its extinction.
- Deinstitutionalization: this concept represents the destruction of institutional form, or "an exit from institutionalization."
- Re-institutionalization: this concept is almost similar to deinstitutionalization, which represents an exit from institutionalization. Re-institutionalization, however, depicts an

entry into a completely different institutional form, “organized around different principles or rules.”

Formal structures are structured social forms that act like a blueprint, for examples offices, departments, positions, and programs. These formal structures are similar to those elucidated by proponents of structuration, in which formal, or social, structures are shaped by habitualized interactions between agency (or actors), rules, and resources (Giddens 1984). Powell and DiMaggio (1991) introduce the function of formal structures as myths, which serve to rationalize and impersonalize the existence of technical functions of social object and can later be taken for granted as functions become regular, everyday guidelines. The notion of “taken-for-granted” refers to the fact that formalized, i.e., institutionalized, actions are superficially embedded in any social actor’s behavior in organizational contexts, thus becoming embedded in regular behavior (Berger and Luckmann 1966; Powell and DiMaggio 1991; Scott 2008). Furthermore, the notion of “taken-for-granted” is viewed as rational by other social actors in a similar organizational context and is a requirement for conformity. In other words, with acceptance emerging as a regular feature in any institution, legitimacy becomes invisible and imperceptible since social actors behave according to prescribed institutionalized procedures. Hence, this concept of “taken-for-granted” legitimate procedures, programs, technologies, techniques, or professions comes to be perceived as a myth.

3.3. Institutionalization as Social Structuration

Institutionalization is a social process of creating an institutionalized social structure (Berger and Luckmann 1966; Giddens 1984; Powell and DiMaggio 1991; Scott 2008). Powell and DiMaggio (1991) state that formal organizations become institutions through institutionalization, hence institutionalization is best represented as a particular state or property of a social pattern. Powell and DiMaggio specifically define institutionalization as "a constraining process that forces units in a population to resemble other units that face the same constraints" (Powell and DiMaggio 1991, p. 194). Scott (1987) refers to institutionalization as a process to instill values beyond the technical requirements of a task over time, and as a process of creating social reality, which is independent of any actor's view and actions but is taken for granted. Berger and Luckmann (1966) contend that institutionalization is typification of habitualized actions, implying the impact of history and control on activities within an institution. History is needed for any institution to be able to reflect on its past records, i.e., to reproduce itself in a modified format. Control is required as a method to ensure that an institution functions according to its legitimacy. These elements infer the importance of reproduction in any institution and that institutionalization reproduces an institution. Powell and DiMaggio (1991) introduce four avenues of institutional reproduction: (1) the exercise of power, (2) complex interdependencies, (3) "taken-for-granted" assumptions, and (4) path-dependent development process. Barley and Tolbert (1997) argue, however, that institutionalization does not depict a comprehensive process of institutionalizing formal structure since institutional scholars do not empirically denote the creation, alteration, and reproduction of institutions. Essentially, institutionalization is not only an institutional process, but also contains property variables (Scott 2008).

A key element to institutionalization is the exercise of control. As such, this key element bears resemblance to the essence of governance systems, as defined by Scott (2008):

> “…those arrangements which support the regularized control – whether by regimes created by mutual agreement, by legitimized hierarchical authority or by non-legitimate coercive means – of the actions of one set of actors by another.”
>
> W. R. Scott (2008, p. 186)

Borrowing the conceptual view of corporate or information security governance from chapter 2, institutionalization indeed requires regulations and authorities which control and enforce such regulations. Selznick (1969, p. 254) denotes that “the legitimacy of authority should be assured,” meaning that authorities should be clearly defined and are required to act in accordance with their scope and “principles of legitimacy.” He also contends that act of governance needs to be constrained to the extent of protecting all legal interests. Furthermore, he introduces the concept of bureaucratization, which is a result of governance on formal organization. Bureaucratization embodies the following characteristics: (1) performance of tasks or functions under an explicit purpose, (2) requirement of a determinate organizational hierarchy as a chain of command, (3) appointment of and control by officialdom as the designated authorities, and (4) governance and administration according to policies and regulations.

An additional element highlighted in chapter 2 is multilevel governance. Scott (2008) introduces multiple levels of institutional processes in formal organizations. Scott (2008) enunciates that organizational field pinpoints a locus between individual actors and organizations at inter-levels, and between systems of societal and trans-societal actors at intra-levels. The use of inter-levels of institutional processes provides “a wider institutional environment within which more specific institutional fields and forms exist and operate” (Scott 2008, p. 191). Furthermore, this allows for the bidirectional influences among social actors in institutions. Top-down processes, e.g., “constitutive activities, diffusion, translation, socialization, imposition, authorization, inducement, and imprinting," describe the governance, administration, or control of authorities (higher stratum) to their subordinates (lower stratum) (Scott 2008, p. 191). On the other hand, the bottom-up processes, e.g., "selective attention, interpretation and sense-making, identity construction, error, invention, conformity and reproduction of patterns, compromise, avoidance, defiance, or manipulation," depict the opposite effect, i.e., the influence of the lower stratum on the higher stratum (Scott 2008, p. 191). As such, the bidirectional influence that can be depicted in a recursive fashion shows an ongoing, cyclical institutional creation, diffusion, and reproduction. The recursive manner represents a situation through which institutionalization may emerge at multiple levels, with the inner processes denoting the inter-levels and vice versa.

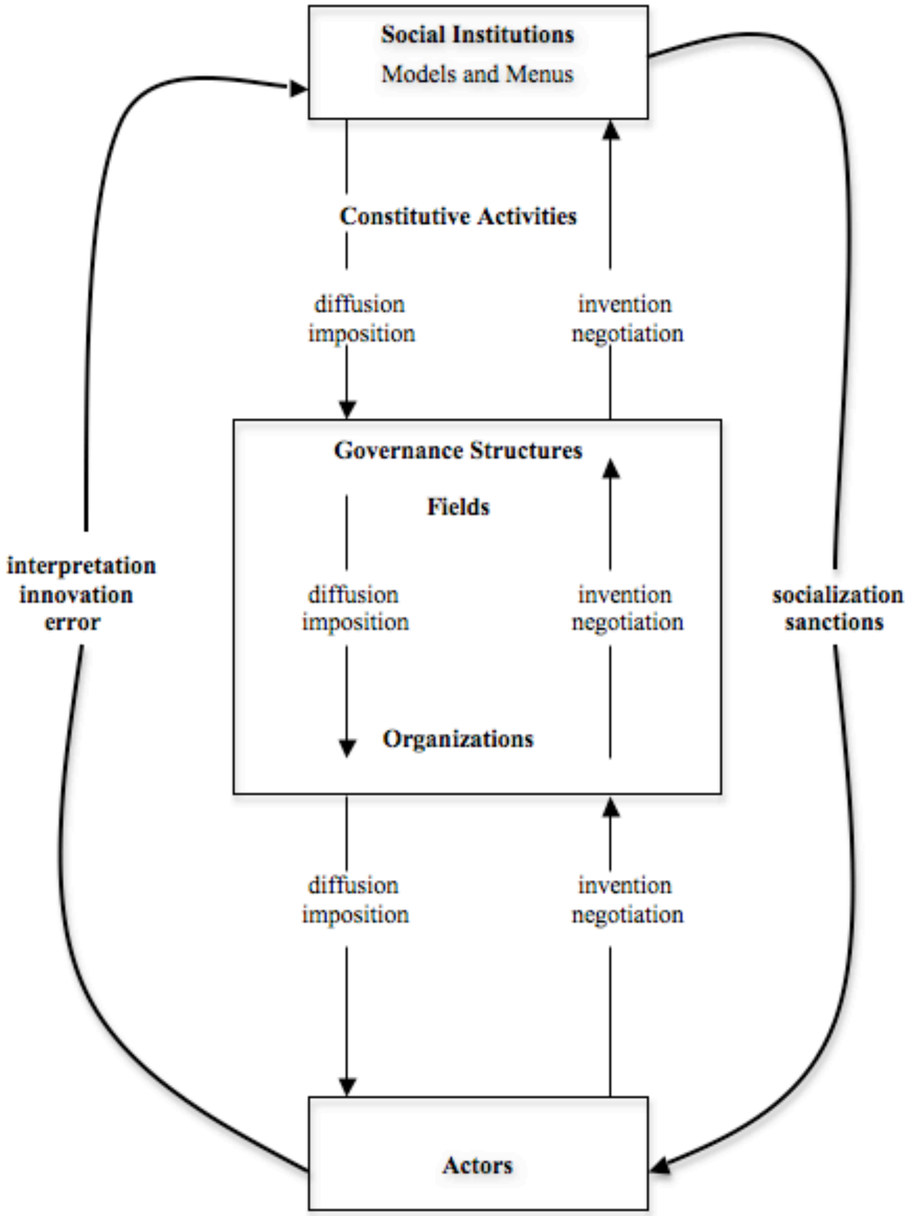


Figure 3.1 – Multilevel Institutional Processes: Top-Down and Bottom-Up Processes in Institutional Creation and Diffusion (Scott 2008, p. 192)

A distinguishing feature of intra-level institutionalization is the authoritative powers possessed by higher-stratum societal institutions. Hall (2008) introduces the relationship between institutions and deontic powers and constitutive powers. Hall contends that:

> “Deontic powers, deriving from the collective assignment of status functions, thereby constitute social structures of power relations by generating institutional facts that function as structures that generate desire-independent reasons for action.”
>
> (Hall 2008, p. 50)

Specifically, he denotes that “deontic powers, in the social realm, create social relations of power, such as rights, duties, and obligations” (Hall 2008, p. 49). Hall further states that deontic power provides trans-societal actors with the ability to exercise authority and certify “states of affairs” and assigns them status functions (Smith and Searle 2003; Hall 2008). In other words, the authority status functions of certain trans-societal actors having deontic powers provide such trans-societal actors with higher authority over their subordinates. In relation to the notion of deontic powers and institutions, Smith and Searle (2003, pp. 285-286) highlight the two-level ontology of social reality. The lower level refers to the ‘brute’ facts, by which facts can exist independently of human beings and their institutions (i.e., observer-independent phenomena), while the upper level refers to institutional facts, whereby facts are crafted intentionally by human institutions (i.e., observer-dependent phenomena) (Smith and Searle 2003; Hall 2008). Institutional facts are composed of two elements: (1) “they are constituted first through collective intentionality” (Hall 2008, p. 47), and (2) they emphasize on “assignment of function to an object, person, or group which does not intrinsically have that function but acquires it only by virtue of the assignment of function” (Hall 2008, p. 48).

Another aspect of intra-level institutionalization involves the exercise of constitutive powers. Larner and Le Heron (2005) imply that constitutive power of institutions is one such factor that affects the governance of practices within institutions. Hall (2008) states that while deontic power emerges from the collective assignment of status functions, constitutive power is derived from the social relations of constitution. One such example is the institutional power of money, arising from financial and economic constitutions, or constitutive rules (Hall 2008). Another example by Ansolabehere and Snyder (1999) depicts money as an institution that has an impact on how politicians behave in order to achieve their subjective goals. Furthermore, constitutive power relations describe how “particular social relations are responsible for producing particular kinds of actors” (Hall 2008, p. 84). Therefore, such actors are bestowed with the constitutive powers to determine social relations.

Using their argument of the lack of dynamism in institutional theory, Barley and Tolbert (1997) offer a combination of institutional theory and structuration theory to delineate a more dynamic approach to institutionalization. The fundamental concept is the habitualized interactions between agency and modalities (e.g., rules and resources). Such habitualized interactions become rational and taken for granted (Giddens 1984; Orlikowski 1992; Orlikowski 2000; Orlikowski et al. 1995; Walsham 1993; Walsham and Han 1991). These habitualized interactions are then institutionalized as actors become familiar with their routine activities in a formal organization, characterized by the creation of orderly interactions called a *script* (Barley 1986; Barley and Tolbert 1997). The script serves as a link between action (represented by realm of action) and institution (represented by institutional realm).

3.3.1. Institutional Realm

Central to this concept is the resentment of change that is a fundamental characteristic of an institution (Scott 2008). Institutional scholars (e.g., Barley 1986; Barley and Tolbert 1997) have sought to add the concept of resistance to change to the duality of structure. Thus has developed a concept of a dynamic structure that seeks to maintain social order and stability, creating an institutional realm. Institutional realm, or the "realized structure" (Barley 1986), is an abstract framework of typifications of habitualized actions (Berger and Luckmann 1966) which actors use to make sense of their actions based on their cumulative past experience with their actions (Barley 1986; Barley and Tolbert 1997). The three social structures – signification, domination, and legitimation – are abstracted within the institutional realm and are continuously produced, maintained, and altered.

There are various interpretations of the institutional realm in relation to social structures. Orlikowski (1992) states that institutional properties such as organizational culture and business strategy promote the interactions between agency and artifacts (e.g., technology). She denotes that institutional properties embody social structures. Furthermore, Barley (1986) and Orlikowski (2000) support the notion of continuous production of institutional realm as a result of situated action (Barley 1986) and knowledge of an actor's experience with the use of artifacts (Orlikowski 2000).

As indicated earlier, the institutional realm appears in different aspects. Barley (1986) introduces the concept of evolution of structure, taking into account sociologists' observations of organizational differences as a result of structuring processes and the production and reproduction of structures as a result of situated action. In her more recent work, Orlikowski (2000) presents a recursive structurational use of technology in which an agency draws on the knowledge of their past experience with the use of technology and the current situation, the resources available to him/her, and the rules that dictate his/her interaction with technology, and apply all such modalities to produce the structurational usage. As such, this explanation provides positive evidence that structuration theory demonstrates that social processes are continuous processes recurring across time and space (Giddens 1984).

3.3.2. Realm of Action

The realm of action is defined as the “actual arrangements of people, objects, and events in the minute-by-minute flow of the setting’s history” (Barley 1986) or the “social life’s unfolding” (Barley and Tolbert 1997). This realm, also called the “interaction order,” represents the continuous interaction between an agency and all three modalities (Barley 1986) in an ordered manner (Orlikowski 2000). Modalities, particularly artifacts and regulations, are the agency’s creation and become meaningful only through their interaction with the agency (Orlikowski 1992; Orlikowski 2000). The social construction of reality (Berger and Luckmann 1966) denotes an instance of meaningful use of modalities when these modalities are used by the agency in an ordered manner (Orlikowski 1992). The ongoing use of artifacts (e.g., technology) may create different patterns of structured use of artifacts as the agency interacts with different artifacts (Orlikowski 2000).

3.4. Theoretical Framework

This section seeks to encapsulate and synthesize concepts presented in previous chapters. The objective is to construct frameworks that will guide observations and organize findings. There are four assumptions as to how social scientists approach their subjects: ontology, epistemology, human nature, and methodology (Burrell and Morgan 1979; Lee 2004). As stated in the previous sections, the theoretical framework borrows the nomalism view of ontological stance. This is due to the nature of social construction of reality which social scientists need to internalize, meaning that a social scientist is expected to understand his subjects by diving into the mind of his subjects (Schutz 1962-66; Berger and Luckmann 1966; Burrell and Morgan 1979). By doing so, the social scientist is able to conclude that no behavior is irrational and that certain circumstances lead to certain behavior. A major distinction between positivism and interpretivism is that the former ignores the fact that human subjects have the ability to communicate.

The institutional theory, including one that is combined with elements borrowed from structuration theory, embodies all such assumptions of interpretive social science. It is the combination that appropriates the use of interpretive scheme, since structuration theory involves the communicative interaction among subjects; a property captured only by using the interpretive scheme (Berger and Luckmann 1966; Giddens 1984). The combination introduced by Barley and Tolbert (1997) is primarily used to model the inter-level institutionalization. The multilevel-institutional-processes framework by Scott (2008) used for the intra-level institutionalization is appropriate to delineate relationships between institutions and a central governing body in governing and implementing information security.

The use of institutional theory also best represents the situational illustration of information security practices in organizations. The information security practices in organizations involve maintaining the integrity of three dimensions of information security: technical controls (i.e., technological aspects such as hardware and software as well as technical aspects such as encryption), formal controls (i.e., management, governance, and control of information security practices), and informal controls (i.e., socializing security practices and increasing security awareness such as training and education programs) (Dhillon 2007). Technical-controls dimension alone does not suffice to maintain effective and efficient information security practices (Blakley et al. 2001; Dhillon 2007). Furthermore, maintaining the integrity of these three dimensions involves the use of various social actors; hence depicting the institutionalization of information security in organizations (Dhillon 2007).

3.4.1. The Inter Level: A Structuration View of Institutionalization

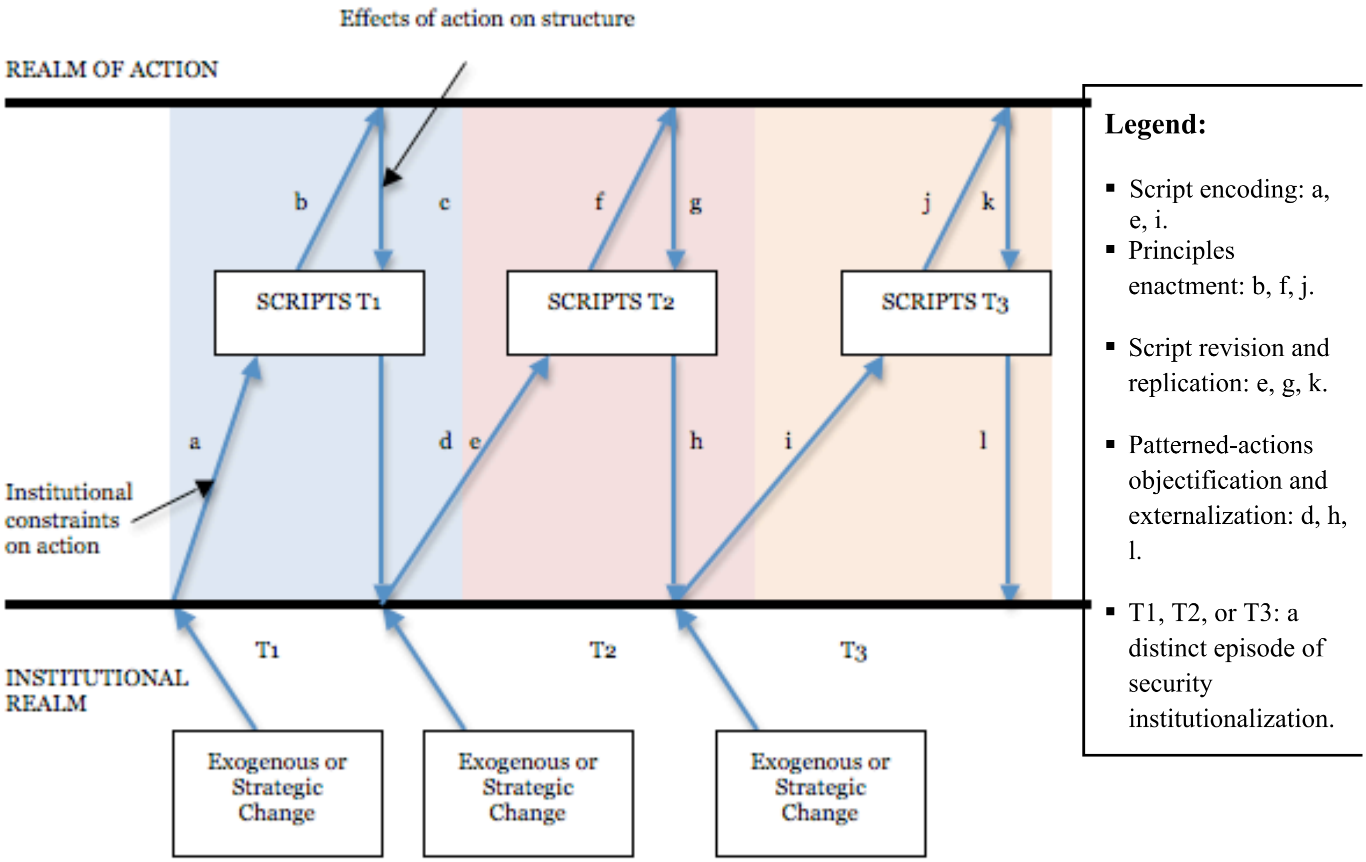
The lower-stratum institutionalization, henceforth termed as inter-level institutionalization, is constructed using elements of structuration theory, particularly the "duality of structure" (Giddens 1984, p. 25). Researchers explain the duality of structure as a manifestation of synergic relationship between agency and structures, whereby social structures are produced and continuously reproduced by human actions and interactions, and as such become a routine that is taken for granted (Giddens 1984; Orlikowski 1992; Orlikowski et al. 1995; Orlikowski 2000; Walsham and Han 1991; Walsham 1993). The use of institutional theory in conjunction with structuration theory provides social scientists with dynamic, recursive and iterative production and reproduction of institutions (Barley and Tolbert 1997). Structuration theorists and researchers have also lent the concept of "institutional realm" to the social structure, with the addition of the concept of resistance to change (Barley and Tolbert 1997, p. 97; Giddens 1984; Orlikowski 1992; Orlikowski et al. 1995; Scott 2008). These researchers contend that human interaction with technology creates institutional properties of structured technological practices (Barley and Tolbert 1997; Orlikowski 1992; Orlikowski et al. 1995; Orlikowski 2000).

The general picture of structuration begins with the duality of structure. Giddens (1984), Walsham and Han (1991), and Walsham (1993) state the importance of power when illustrating structuration. Studies have demonstrated that deontic power, constitutive power, and facilitative power are an appropriate concept to explain status functions and social relations of constitution, for instance in banking-sector context (Smith and Searle 2003; Larner and Le Heron 2005; Hall

2008). Constitutive power has been shown to be an exclusive property of central bank due to its governance functionality and its impact on constitution (Larner and Le Heron 2005; Hall 2008). Moreover, the notion of resources or artifacts has widely been espoused by structuration scholars. Such notion is essentially in context of IT artifacts, represented by the view that IT, e.g., hardware and software, is an object that is manufactured, used, or modified by humans (Orlikowski and Iacono 2001). In this sense, the technical-control dimension of organizational information security can be considered as being that of the information security artifacts. This view is enhanced using the notion of exploring beyond the “technical means of protecting information resources” (Dhillon and Torkzadeh 2006). In support of this artifact notion, Orlikowski (1992) has maintained that technology is created by an agency, but is dynamic since the structure of technology is repeatedly created through the routine use of technology.

Social structures, associated with the property of change resistance, create an institutional realm. Enmeshing information security artifacts, deontic and constitutive powers, and risk policies and regulations in the structuration context creates an institutional realm of structured information security practices in institutions. The structuring of information security practices in each institution therefore experiences continuous production and reproduction. The institutional process that includes exercising control, i.e., institutionalization, in the inter level is conducted by the agency that directly structures information security practices in a particular institution. Moreover, in a lower stratum institution, agency’s actions and interactions may be affected (i.e., governed and controlled) by higher-stratum agency’s sanctioning. This level borrows the structuration view of institutional theory (Björck 2004) and is constructed by combining institutional theory and structuration theory.

The theoretical framework for the inter-level institutionalization is largely built upon the concept of duality of structure. Taking into account the approach introduced by Barley and Tolbert (1997), however, causes some modifications to the traditional concept of duality of structure. Barley and Tolbert (1997) develop a combination of structuration theory and institutional theory to model an institutionalization of habitualized actions. This model embraces the institutional realm and the realm of action, and proposes recursive instances of an institutionalized structure. The recursive instances depicting the social structure reflect an attempt to maintain stability or social order (Berger and Luckmann 1966). Each episode of institutionalization depicts a unique structure affected by certain phenomena or a particular incident (e.g., security breach). Barley (1986) terms the episodic institutionalization as the evolution of structure. The model hence produces a series of information security institutionalizations involving a script for each episode, serving to support the recursive institutionalization. The script is characterized as the "observable, recurrent activities and patterns of interaction characteristics of a particular setting" (Barley and Tolbert 1997, p. 98). The script, however, should not be regarded as one of the three modalities as in the original structuration theory. This is because a modality is a tool that is used by the agency or is used to support the interaction between an agency and other modalities.


Effects of action on structure
REALM OF ACTION
b
c
f
g
j
k
SCRIPTS T1
SCRIPTS T2
SCRIPTS T3
a
d
e
h
i
l
Institutional constraints on action
T1
T2
T3
INSTITUTIONAL REALM
Exogenous or Strategic Change
Exogenous or Strategic Change
Exogenous or Strategic Change

Legend:

- Script encoding: a, e, i.
- Principles enactment: b, f, j.
- Script revision and replication: e, g, k.
- Patterned-actions objectification and externalization: d, h, l.
- T1, T2, or T3: a distinct episode of security institutionalization.

Figure 3.2 - Inter-level Institutional of Information Security Governance Using Barley's Model of Institutionalization (1986)

Figure 3.2 depicts the institutionalization episodes as described by Barley and Tolbert. The model introduces two general streams of institutionalization: the effects of action on structure and the effect of institutional constraints upon action. Each stream constitutes two processes that shape either action or structure. The processes corresponding to the institutional constraints on action involve the process of encoding principles in the script in a specific episode (see arrows a, e, and i) and the process of enactment of the principles in the script by actors (see arrows b, f, and j). Script encoding refers to the moment when policies and regulations are successfully formulated and begin to be adopted in a formal organization, while principles enactment entails social actors beginning to realize and accept such policies and regulations that guide actors' behavior. The other processes (i.e., those that correspond to the effects of action on structure) include the process of script revision or script replication (see arrows c, g, and k) and the process of “objectification”[1] and externalization of patterned actions (see arrows d, h, and l). Script revision and script replication explain the moment when scripted behavior is replicated in the institutional abstraction. However, this process can also be used to explain the moment when policies and regulations that have been successfully adopted are revised after a negative incident. Patterned-behavior objectification and externalization denote the moment when both the regulatory aspect and behavioral aspect in a formal organization becomes successfully implemented and habitualized. As shown in figure 3.2, each box depicts an episode of institutionalization. Arrow a and arrow b in the left box (episode T1) is similar to arrow e and arrow f in the middle box (episode T2) and arrow i and arrow j in the right box (episode T3). These arrows are diagonal arrows that describe how the institutionalized structure directs and controls the agency's action (represented by the realm of action). The vertical arrows (arrow c and arrow d in episode T1, arrow g and arrow h in episode T2, or arrow k and arrow l in episode T3) describe the agency's actions that institutionalize social structure (represented by the institutional realm). The episodes may be infinite since institutions are always evolving after they come into existence, are always being challenged, and hence keep on changing their facets. Each transition between two episodes (e.g., a transition between T1 and T2) signifies an institutional change (e.g., institutional development or re-institutionalization). Such institutional change can

[1] Barley (1986) and Barley and Tolbert (1997) introduce the notion of objectification to demonstrate how patterned actions become an abstract entity (i.e., principles) that occupies the institutional realm.

be triggered by an exogenous event (e.g., technological change or security breach), an endogenous event (e.g., implementation of new rules and standards), or a combination of both exogenous and endogenous events (e.g., security breach that prompts the central bank to create new guidelines for new security policies).

3.4.2. The Intra Level: Macro-Prudential Supervision of Information Security Practices

Figure 3.3 shows the holistic information security governance in banking sector, henceforth termed as the information security macro-prudential supervision. This framework depicts the practices of information security governance in separate institutions, centrally governed by one institution as the higher authority (i.e., the central bank). The framework in figure 3.1 can be seen to represent a component of this holistic theoretical framework. Such a framework shows that each institution structures its own information security practices. The central bank, however, possesses powers (deontic, constitutive, and facilitative powers), which enable the central bank to govern and control commercial banks. This action represents the top-down process of institutional creation and diffusion (i.e., institutional process (Scott 2008)). Hence, the central bank possesses the authority to govern and control security practices of commercial banks.

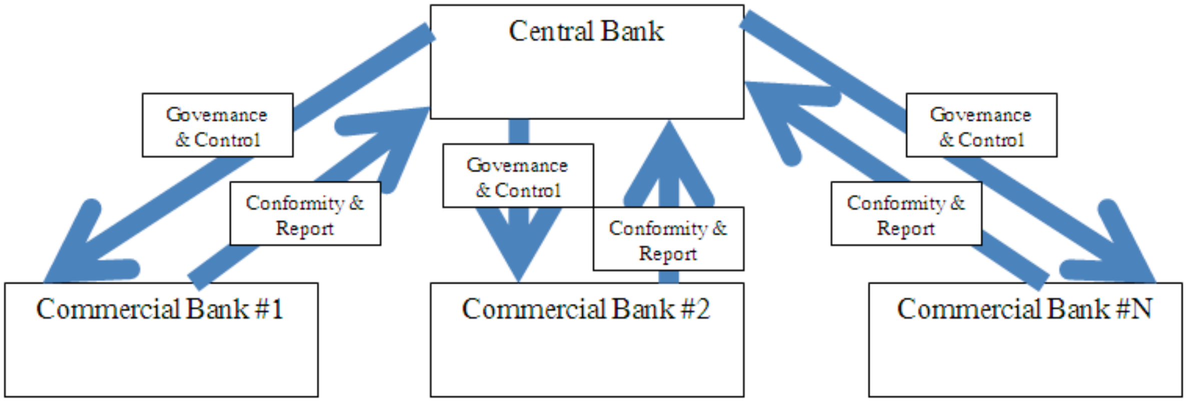


Figure 3.3 – The Macro-Prudential Supervision of Information Security Governance in Banking Sector (Reproduction of Scott's Model of Multilevel Institutional Processes (2008))

Commercial banks reciprocate the conformity governed by the central bank through policies and regulations. Commercial banks are also required to report information security governance and practices, directed internally by each commercial bank's institutional management (e.g., board of directors, senior executives, steering committee, and CISO). This action represents the bottom-up process of institutional process (Scott 2008). As such, in this context, institutions affect one another via their agency. In other words, the intra level of institutional process involves interactions among agencies of institutions. This level assumes the legitimacy view of institutional theory (Björck 2004).

Therefore, both processes affect the structuration of information security practices in each institution, whereby each institution sanctions and informs security practices in two directions (i.e., between higher-stratum institution and a lower-stratum institution). The institutionalization of two-level information security governance presented in this framework mimics the multilevel institutional processes.

3.5. Research Design

Research activity is socially constructed and is approved and conducted by scientists and scientists are instruments of their research activity, i.e., observation (Berger and Luckmann 1966; Lee 1999). The methodology is designed to influence research activity by providing guidance using theoretical framework. This study uses the interpretive case-study research since the use of structuration theory that supports the institutional theory involves communicative interactions among respondents (i.e., subjects). Such interactions can only be captured using the interpretive scheme (Berger and Luckmann 1966; Giddens 1984). The interpretive scheme of research methodology requires that such methodology begin "from the position that our knowledge of reality, including the domain of human action, is a social construction by human actors" (Walsham 2006, p. 320). To preserve the interpretive nature, this study therefore incorporates a case-study research in the tradition of Walsham (1993; 1995) and Eisenhardt (1989).

The unit of analysis for this study is the banking sector in Indonesia. Three institutions have been observed for this study. The first institution is the nation's central bank. The other two institutions are large commercial banks. These banks are selected due to their great influence on the nation's economic welfare. The first bank, Centro Metropolitan Bank, is a large government-owned commercial bank that is known for its substantial assets, loans, and deposits. The second bank, Blue Sequoia Bank, is the nation's largest private commercial bank that owns a large number of ATM machines distributed in almost every geographical region in Indonesia. Data collection is performed in the respondents' natural setting. While there are various data collection methods for case study research, this study uses interviews as its main data source. The interviews involved approximately 30 respondents, ranging from an entry-level analyst to a senior executive. There are 18 respondents from the Earl Capita Bank, 8 respondents from Centro Metropolitan Bank, and 4 respondents from Blue Sequoia Bank.

In a case study research, building theories from case studies involves a “frequent overlap of data analysis with data collection” (Eisenhardt 1989, p. 538). Such an overlap provides flexible data collection and allows for a head start in analysis. While the primary source of data is interviews, other sources include secondary materials such as pamphlets as in the case of Blue Sequoia Bank and magazines, which are supporting materials to analyze the Centro-Metropolitan-Bank case. Interviews are tape recorded and transcribed to provide easier analysis of patterns and categories (e.g., reputational risk, security policies, institutional relationship). Since interviews are tape recorded, interviews are semi structured and open ended to allow for casualty and flexibility in probing respondents. Translations are derived from the transcription. Analysis of patterns and recognitions as well as theory building is developed from the translations.

Data analysis in interpretive scheme, however, is not expected to attend to issues of generalizability. This is due to the ideographical nature of its methodological stance, as opposed to the nomothetical view of positivist scheme. Nomothetical view dictates the necessity of controlling formal procedures and provides evidence of “formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon from a representative sample to a stated population” (Klein and Myers 1999, p. 69; Orlikowski and Baroudi 1991). Furthermore, positivism has dictated the use of “certain criteria of validity, rigor, and replicability in the conduct of scientific research” (Orlikowski and Baroudi 1991, p. 12). Such positivist features are clearly distinct from those of an interpretive scheme as adopted for this study. According to Lee and Baskerville (2003), a theory conducted as an interpretive based study in a single setting is valid by the nature of interpretive scheme and can be applied to other settings. Therefore, generalizability in interpretive scheme can be achieved by applying the theory that has been confirmed in one setting to descriptions of other settings (Lee and Baskerville 2003, p. 233).

3.6. Conclusion

This chapter seeks to explore and build theoretical frameworks and to develop a research design for this study. The social phenomena under investigation are essential for achieving social order, and instrumental in determining the consequences of not doing so. Drawing on the elements of information security governance, institutional theory has been found suitable for use in modeling the conceptual framework of this study. Björck (2004) denotes that institutionalization can be used to "explain why formal security structures and actual security behavior differs" (Björck 2004, p. 5). Several similarly important elements between institutional theory and information security governance include the intentness of authorities, governance, and regulations.

Since this study uses theoretical frameworks that mandate communicative interactions among respondents, the interpretive case-study research is selected to capture such interactions. Research in information systems and security has demonstrated the wide use of institutional theory for capturing structuration and legitimacy issues. The next three chapters cover case studies of the three banking institutions, beginning with the central bank case study.

4 THE CASE OF EARL CAPITA BANK

4.1. Overview

The objective of this chapter is to present a thorough analysis of the nature of information security governance in Earl Capita Bank. Earl Capita Bank., the highest authority in banking sector, alludes to the fact that no other institution in the sector directs and controls the institutionalization of information security in Earl Capita Bank. The initiative comes within the purview of the institution's community itself, which in this case are the Earl Capita Bank's personnel. The institutional instances of information security governance are examined from the internal perspective and also in terms of the institutional relationship that exists between the central bank and commercial banks in general. The case study concerning the internal practice is organized according to the model introduced by Barley and Tolbert (1997) to delineate the institutionalization of information security. Four processes are identified as the themes for the case study: the script encoding, the principles enactment, the script revision and replication, and the patterned actions objectification and externalization.

Section 4.2 describes the nature and characteristics of Earl Capita Bank as the nation's central bank. This section details the institution in terms of its position as a central bank, its historical background, and its organizational structure. Section 4.3 presents the empirical analysis for the Earl Capita Bank case. This section contains the following subsections: the internal security practices that define the micro-level institutionalization of information security governance within Earl Capita Bank, and the

Earl Capita Bank's relationship with commercial banks by employing the macro-prudential supervision of information security governance. This section also provides a discussion at the end of each subsection. Section 4.4 concludes this chapter.

4.2. Organizational Background

4.2.1. Earl Capita Bank as the Central Bank

As the Central Bank of Indonesia, Earl Capita Bank's primary objective is to achieve and maintain the stability of the nation's currency. In 2004, Earl Capita Bank became an independent state institution and consequently free from influences and interferences by all external parties, including the government. In support of such a statement, Schooner and Taylor (2009) and Ullrich (2007) denote that a Central Bank needs to be independent of political control so that it can be free to determine interest rates. As such, Earl Capita Bank possesses the autonomy to fully formulate and implement its authority as a deontic monetary institution. This is because as an institution, it manifests power that arises from a specific form of constitution, distinct from other financial institutions (Hall 2008). Furthermore, Earl Capita Bank has the authority to issue policy rules and regulations as a public legal entity, meaning that it possesses constitutive power because of its deontic status (Hall 2008). Consequently, as a civil legal entity, the bank also has the right to represent itself in and outside a court of law.

In order to achieve the above mentioned objectives, while maintaining its right and authority as a legal institution, Earl Capita Bank is obligated to upholding the principles of accountability and transparency in implementing its duties, authorities, and budget.[1] Given such obligations, Earl Capita Bank has to maintain information symmetry between public, government, and commercial banks. The dilemma lies in the provision of information, which in the Earl Capita Bank is expected to be handled and disseminated as is done in all financial institutions. Information security breach, however, may negatively impact institutional reputation and even harm the nation's economic stability. In addition, Earl Capita Bank, as a premier authoritative institution, realizes the need to protect and preserve its own information. In doing so, Earl Capita Bank maintains judicious internal information security and supervises the governance of information security in other commercial banks.

4.2.2. History of Earl Capita Bank

The history of Earl Capita Bank can be divided into two eras: the colonial and post independence era and the reformation era. The colonial era of Earl Capita Bank can be traced back to the founding of *De Javasche Bank* by the Dutch East Indies government in 1828.[2] The bank was developed for circulating and issuing currency. Despite this seemingly crucial function, the bank was merely operating as a commercial bank. It continued to operate until the colonial Dutch government transferred sovereignty to Indonesia in 1949. In 1953, it was nationalized (post independence era) as the Republic of Indonesia's circulation bank[3]. In 1953, the government of Indonesia passed the Act of Earl Capita Bank and declared the establishment of Earl Capita Bank and endowed it

[1] Source: http://www.bi.go.id/web/en/Tentang+BI/Fungsi+Bank+Indonesia/Akuntabilitas/
[2] Source: http://www.bi.go.id/NR/rdonlyres/FC7439FE-0C50-44F1-A042-2CFB6FE5CA43/18316/07_sejarah_rev1.pdf
[3] Source: http://www.papermoney-indonesia.com/de-javasche-bank-1828-1953-still-under-construction/

with the additional central bank status held previously by the De Javasche Bank. In addition to being a commercial bank, the newly founded Central Bank performed the following functions: monetary, banking, and the payment system. The bank also held supplementary duties in relation to the government. In 1968, the government passed the Act of Central Bank, detailing the status and functions of Earl Capita Bank as a Central Bank and hence abolishing the bank's previously commercial bank status. In addition to the aforementioned three core tasks of a central bank, Earl Capita Bank provided assistance to the government, functioning as a development agency supporting real sector productivity and developing and creating employment opportunities aimed at public welfare.

After the downfall of the new era regime and the rise of the reformation era, Act No. 23/1999, which concerns Earl Capita Bank, restated the objective of Earl Capita Bank yet again as one aimed at achieving and maintaining the stability of the nation's currency. In 2004, the government issued act concerning Earl Capita Bank was amended to place more emphasis on critical aspects of the bank's mandated tasks and authorities, including the strengthening of its governance. In 2008, the government issued another regulation in lieu of law No. 2 of 2008 concerning the second amendment of Act No.23 of 1999, which identified Earl Capita Bank as a part of the efforts to maintain financial system stability. The amendment was designed to strengthen the resilience of Indonesian national banks in facing the global financial crisis by improving any bank's access to the Short-Term Funding Facility provided by Earl Capita Bank.

4.2.3. Organization Structure

Earl Capita Bank is managed by a Board of Governors; led by a Governor who is assisted by a Senior Deputy Governor (Vice Governor) and several Deputy Governors. The Board of Governors oversees the directors of the main sectors: Monetary, Banking, Payment System, and Internal Management.

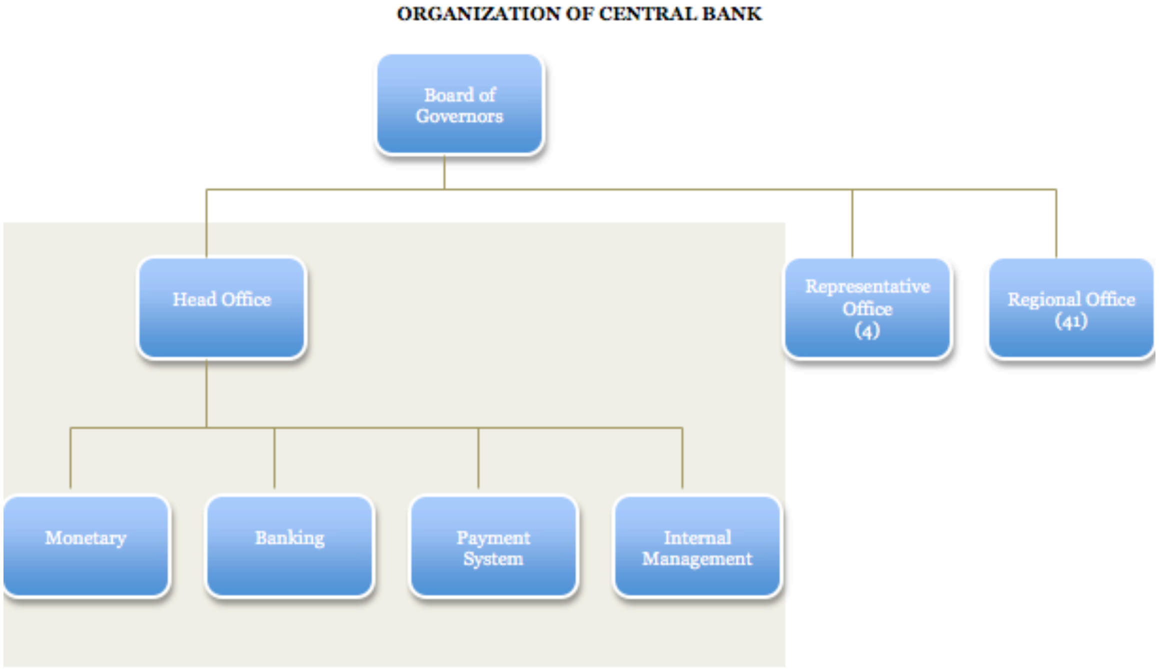


Figure 4.1 – The Higher-Level Organization Chart of Earl Capita Bank

Each main sector consists of several departments and each department is managed by a director. Departments under the monetary sector mostly deal with tasks of controlling money supply and interest rates. Hence these departments do not deal directly with commercial banks and financial institutions. The departments under the Banking sector and Payment System sector deal mostly with commercial banks and financial institutions. The Internal Management sector includes departments that manage the operability of Earl Capita Bank. The respondents for this dissertation are personnel of departments other than the monetary sector.

The internal security practices of Earl Capita Bank include the provision of the information-security governance practice which is overseen by departments that handle information processing and technology within the institution. These departments, namely the Information Technology Department and the Information Management Division, are divisions of the Internal Management Sector.

Internally, each department of Earl Capita Bank attempts to safeguard access to its information according to unique regulations and cultures prevalent within that particular department. Each department maintains and regulates its own information systems where as the Information Technology Department manages the technical maintenance for these information systems. In the past, each department possessed absolute authority over the control and use of information extracted from its own information systems, including the electronic data warehouses installed in each department. In 2002, Earl Capita Bank established the Information Management Division to oversee the manipulation and distribution of information within Earl Capita Bank and from Earl Capita Bank to external parties. However, internal departments still reserve the right and authority for information access and manipulation of such information within their own departments. In other words, each department is the sole administrator of its applications, whereas the Information Technology Department is the administrator of systems databases and networks. The Senior Analyst at the information management division states that:

> “Our campaign is to raise awareness across the bank that any particular department doesn’t own information. Information belongs to the bank. And raising this awareness is

very hard work for us since this practice has been established for a long time and has become an institutional norm. It's very difficult to change."

Security Policies and Supervision

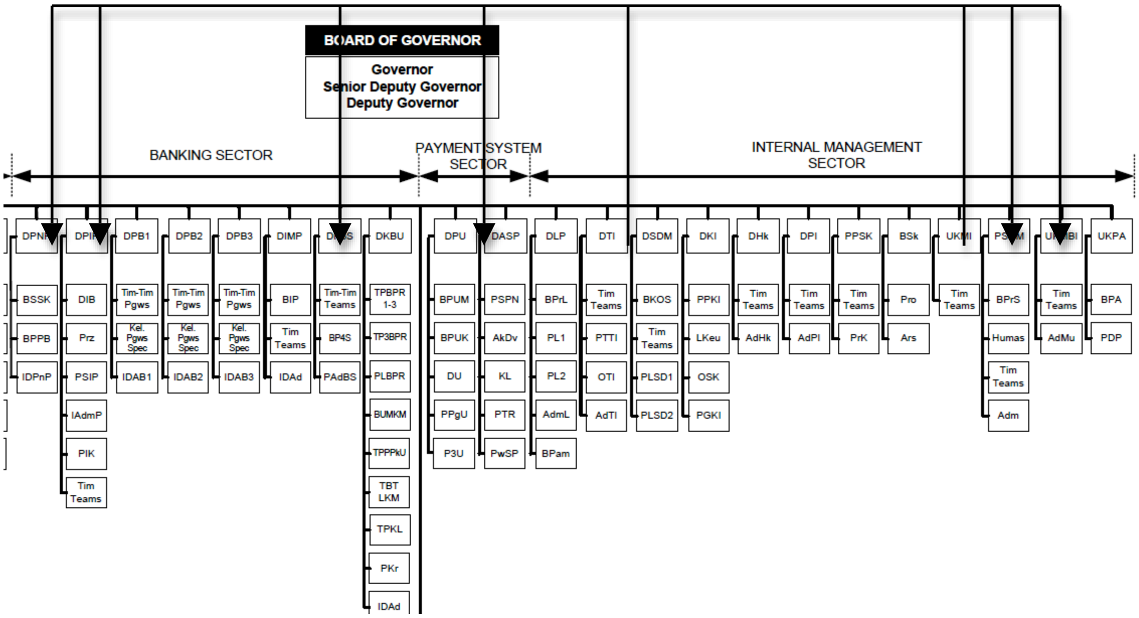


Figure 4.2 – A Partial View of the Internal Governance of Information Use and Security

The roots of internal governance of information, its use and security within Earl Capita Bank are embedded in the Information Technology Department and the Information Management Division. The internal governance includes the formulation of regulations and policies as well as the supervision and enforcement of regulations and policy. The Information Technology Department oversees the technical control of information security while the Information Management Division supervises the formal control of information security. Both departments, however, create and supervise the informal control of information security by educating employees and raising their awareness levels about the importance of information security[4]. For instance, the Information Technology Department does so by distributing flyers which describe the dangers of password cracking while the information management division reminds personnel of the importance of information security by holding seminars on newly developed software packages. Correspondingly, the Information Technology Department manages the password control while the Information Division Management determines which information is considered confidential and unsuitable for sharing with the public. Despite the demarked responsibilities of formal control and technical control between these two departments, Earl Capita Bank also maintains the three information-security controls: technical, formal, and informal (Dhillon and Moores 2001; Dhillon 2007). The implementation detail of governance practice varies within each department and is dependent on each department's culture and functionalities.

4.3. Empirical Analysis

This section contains a case study that is organized according to two objectives: Inter- Institutionalization and Intra-Institutionalization. The Inter Institutionalization adopts the Barley and Tolbert's Model Of Institutionalization. Institutionalization comprises of four processes: the process of encoding principles in the script in a specific episode (or script encoding), the process of enactment of the principles in the script by agency (or principles enactment), the process of script revision or replication (or script revision and script replication), and the process of objectification and externalization of

[4] Both departments share the same responsibility for enforcing the informal control of information security in addition to their primary roles within the institution. This statement is based on the author's deduction.

patterned actions (or patterned-actions objectification and externalization). The Intra Institutionalization borrows Scott's Model of Institutional Creation and Diffusion.

4.3.1. Inter-Level Institutional of Information Security Governance

4.3.1.1. Script Encoding: As the premier authoritative institution, Earl Capita Bank's main concern is its reputation. Even a minor information-security breach can destroy the institution's credibility, leading to financial chaos and even political instability. The Head of Risk Management Team says:

> "As a public institution, we are expected to be transparent. However, there are some rules of the game, specifically the rules regarding information disclosure. Whether or not it is confidential, information, especially about policies, if disclosed before formal approval or leaked out can lead to information asymmetry in the financial market. Some market players who feel they have never received the 'disclosed' information may think that we have favorites as regards providing information. This can disrupt the market and damage our reputation by leading to our being perceived as unfair and unprofessional. This is one of the major downsides of information leak."

To preserve confidentiality of its information, Earl Capita Bank formulates regulations and supervises compliance concerning the production and dissemination of information within itself and to external parties. Security issues in an organization are often recognized when a security breach occurs (Bodin et al. 2008; Gordon et al. 2003) or when security risks are acknowledged. The Risk Management Team assists other departments in identifying risks. The Head of Risk Management Team explains such assistance as follows:

> “Departments know exactly what they need. Every three months, departments submit a report of risks profile through an integrated system. They indicate the types, events, incidents, and measurement, indicating whether a risk is low, moderate, or high. If a risk is indicated to be high, or red, then the department needs to devise a mitigation plan. Especially for prospective risks, the mitigation plan is absolutely required. For example, the Information Management Division would want to submit to us a risk profile regarding information risk and create a mitigation plan.”

Once the risk profile and the mitigation plan have been created and submitted, the department in charge manages and oversees the risks mitigation. It has been indicated that information risk is the responsibility of the Information Technology Department and the Information Management Division. The existence of the Information Management Division, however, is disrupted by authority issues, despite its relatively strong and equitable position vis` a vis` other departments. This division is regarded as the stepchild in the institution. One of the Information Management Division’s major tasks is the creation of an information-confidentiality category, with the highest rating (top confidential) to be accessed only by the Board of Governors and executive directors. The lowest category is for public consumption such as information posted on the institution’s homepage. The Information Management Division hence views information security as a users’ issue. Such categorization is regulated and communicated to users of all other departments within Earl Capita Bank. Other departments identify the category and apply it to the hardcopy and electronic documents they are producing. Any violation of the security of these documents is considered a felony and the penalties, regulated and enforced by the Human Resource Department, may include work termination and incarceration.

The division, however, has little power to convince departments to integrate their data; hence centralizing information is a difficult task. Despite the uniform security policies, the implementation and the enforcement of the policies varies amongst departments, partially attributable to the data ownership issue. The success achieved by the division is apparent in the formulation of the Board of Governors Regulation of Information Management in Earl Capita Bank. Senior Analyst at the Information Management Division elucidates:

> "According to the Board of Governors Regulation of Information Management in Earl Capita Bank, information is stated not to belong solely to a department or to a division. This was because during the 1999 transformation program, many still considered information to be his or her power domain. During the financial crisis, the governor would announce the currency rate early in the morning and suddenly the senior governor deputy would announce a different rate at mid morning due to their sources being from different departments. We then stated that information belongs to Earl Capita Bank only. Basically, we aim to change each department's perception regarding data ownership."

As described earlier, a departmental request to another department for sharing its data and information is relatively difficult to accommodate due to the issue of data ownership. Each department behaves like a kingdom and assumes full authority to determine what part of the information under its control can be distributed to other departments, to personnel of other departments, and even to the public[5]. Surprisingly, there is a distinct possibility that there could be an instance or occasion when a document may be pronounced top confidential by a department but is treated as belonging to a

[5] This statement is based on the author's deduction after several interviews with the respondents from the information management division.

lower confidentiality bracket by another department, depending on its usage purpose. The Information Management Division merely watches over how the confidentiality category is implemented but does not have the power to determine the detail and implementation of any category. Although this information management division has seen limited success, Earl Capita Bank is beginning to witness centralized information usage and centralized information confidentiality management directed by the Information Management Division.

Current practice denotes that the Information Management Division manages how information should be used, whereas the Information Technology Department maintains devices by which information is processed and used. The other departments reserve the right to use and distribute this information. The Information Technology Department has full authority over the implementation and maintenance of technology in Earl Capita Bank. The department regards information security as an issue that is strongly related to those in hardware and software. The department enforces office-hour access to websites, for instance, by not allowing employees to access social-network websites during office hours. It conducts password maintenance, upgrades antivirus software and firewall applications, etc. The department also initiates disaster recovery and business continuity plans. In essence, both departments also educate personnel of the other departments of the importance of information security and attempt to raise their awareness. The Head of Information Technology Department expresses that:

> “The business continuity plan (BCP) that we designed is probably one of the exemplary BCPs in the nation. We take pride in our BCP despite the fact that our disaster recovery center is located in the same geographical area as our headquarters.”

The formulation of policies and regulations directing the secured use of information asset signifies the dual centralized authority, equally divided between the Information Management Division and the Information Technology Department. The difference, however, is that the sole authority to formulate policies and regulations regarding the use of software and hardware is with the Information Technology Department while the authority to use that information is with the Information Management Division.

4.3.1.2. Principles Enactment: Information usage is interpreted and implemented according to their own discretion by departments and varies according to each department's goal and functionalities within Earl Capita Bank. Departments also interpret and apply various confidentiality categories to their information assets. The interpretation process creates an institutional structure by which departments within Earl Capita Bank recognize the need to attach different levels of confidentiality of their information asset, hence safeguarding their top confidential information which is to be consumed only by the Board of Governors and executive directors. Despite such variations, the goal of the information management division is ultimately achieved: which is to have each department classify, mark, and safeguard its electronic and hardcopy information.

Designating departments to manage their own data and information creates a notion of information stewardship. Information stewardship allows departments to own and manage their own data warehouses with a sense of departmental ownership. While Earl Capita Bank in a larger context owns an Electronic Data Warehouse (EDW) managed by the Information Management Division, other smaller data warehouses are distributed to departments to house information systems that may serve as links to external parties (e.g., commercial banks and financial institutions). According to an Analyst of the Information Management Division:

> "About information stewardship, this functionality is given to each department that owns and operates information systems in Earl Capita Bank. Each department selects a person responsible as the information steward. This person manages data and chooses which data to share with selected people outside the department."

In addition to managing their own data and information, departments own the right to operate their information systems as part of their information-stewardship functionality. Some of these information systems, which are the institution's most critical systems, include:

- The LHBU ("*Laporan Harian Bank Umum*" or "Commercial Bank Daily Report") system, which is owned by several departments. The ownership depends on the usage context; for example: the Accounting and Payment System Department oversees the electronic-payment report of the LHBU system.
- The RTGS ("Real-Time Gross Settlement") system, which are co-owned by the Accounting and Payment System Department and the Information Management Division.
- The SID ("*Sistem Informasi Debitur*" or "Debitor Information System") system, which is exclusively owned by the Directorate of Bank Licensing and Banking Information.

- The SIMWAS ("*Sistem Informasi Manajemen Pengawasan*" or "Supervision Information Management System"), which is exclusively owned by the Directorate Of Bank Licensing and Banking Information.
- The SOSA ("*Sentralisasi Otomasi Sistem Akunting*" or "Centralized Automated Accounting System") system, which is exclusively owned by the Accounting And Payment System Department.
- The SKN ("*Sistem Kliring Nasional*" or "National Clearance System") system, which is co-owned by the Accounting and Payment System Department and the Directorate of Banking Research and Regulation.

Information stewardship can be used to grant partial access to data and information to external users of the departments. These external users are Earl Capita Bank's personnel, commercial banks, and financial institutions. The procedure for external users to obtain data and information is, as stated by an Analyst of the Directorate of Bank Licensing and Banking Information as follows:

> "If there are external users wishing to access data and information from systems that we administer, they simply need to come to us. The procedure they need to follow is a formal one regardless of whether they are Earl Capita Bank's staff. They need to create a memo and send us this memo, informing us of their intention to use our information systems, stating their affiliation, which data or information they need to use, and the purpose of using our systems, data, or information. We will decide whether to grant them access to our systems, data, and information. And if granted, we will request user names and passwords to be created for them. The role and privilege are limited according to their needs and we monitor how they use our systems."

This seemingly intricate procedure to obtain access to a department's information systems as well as their content boosts the security of these systems. The implementation of data ownership seems to create a sense of power on one hand and security on the other hand. This concept affects not only selected individuals that can interact with the systems, but also imposes a restriction on the interactions and how these interactions are practiced. The Analyst of the Directorate of Bank Licensing and Banking Information further confirms the security effect of such a procedure:

> "As far as I'm concerned, there has never been any record of a breach of our systems and those of the other departments. There has also been no record indicating the misuse of our data and information, or even of those across Earl Capita Bank."

Despite such selectivity and monitoring practices, departments do not hold the capacity to create usernames and passwords. The creation of usernames and passwords belongs to the Information Technology Department. The Information Technology Department possesses the sole authority to formulate policies and regulations regarding the use of usernames and passwords and to supervise such usage. The Senior IT Researcher reaffirms such authority:

> "Based on the legislation by the Board of Governors, the IT department holds the full authority to govern the internal IT systems of Earl Capita Bank. This also includes sole authority to govern the security of IT systems and the disaster recovery plan of Earl Capita Bank."

The seemingly rigorous selectivity and monitoring practices, however, do not seem to cause the same restrictive effect on internal personnel of the owner department. However, the procedure and regulation tightly restrict external users' access to systems, data, and information of each department. With regard to the procedure and regulation, the Analyst of the Directorate of Bank Licensing and Banking Information states that:

> “We have to make a formal request to access permission if we want to use a system that belongs to any other department. The same procedure is followed by other departments if they want to get access to our systems. We also need to request permission to use and analyze data and information processed by other departments. Let’s say, we request a permission to view the electronic-payment report of the LHBU system. For that, we need to create and send a memo to the accounting and payment system department before they can order the IT department to grant us the permission to view the report.”

Any data and information transmission or use of information systems other than those regulated or proposed through the information steward is considered a felony, the impact of which can jeopardize the personnel’s career and can even lead to fine and incarceration. Once there is a violation of the use of the institution’s asset or properties by personnel, the matter is handed over to the Human Resource Department and the penalty is imposed according to the severity of the impact caused by the misconduct. The Senior IT Researcher states that:

> “We regard our information technologies, data, and information as our asset and property. We regulate the conduct and the use of our systems. For example, we create a firewall that also controls which websites our personnel can access during office hours. We block websites such as porn sites and even Facebook and Twitter. So basically we hope that they access only websites relevant to their work and don’t waste their productive hours by browsing around cyberspace. Any staff member who manages to get away with this and gets caught later on will be handed over to the Human Resource Department and will be charged accordingly. Thank goodness there hasn’t been any such incident in recent years.”

The issue that now arises is whether the same procedures and regulations apply to external users that are not personnel of Earl Capita Bank. The procedure and regulations are enforced for access to Earl Capita Bank's information systems as well as its data and information content if their confidentiality category is not categorized as public data and information (example of public data is the information content on the Earl Capita Bank's official website). Individuals, commercial banks, or financial institutions wishing to get access to Earl Capita Bank's information systems need to request a formal permission from Earl Capita Bank. The Analyst of the Directorate of Bank Licensing and Banking Information states such a procedure and regulation to be as follows:

> "If someone wants information about a person's credit score or record, he needs to come to us and make a formal request for that information. He needs to provide valid documents such as his own existing credit validation, ID, and whatever he has as proof that validates his need. We will consider the request to be a fraud if he manages to obtain the data but fails to provide any evidence or valid document. The penalty is a Rp.-50-million fine per one piece of information."

The penalty for misconduct and misuse of Earl Capita Bank's information systems is managed by the general court according to the severity of impact caused by the misconduct. . The fine is regulated for ID Rp. 50 million (approximately US $5,807.20) per one piece of data or information.

4.3.1.3. Script Revision and Script Replication: The script replication in Earl Capita Bank occurs when an individual's behavior becomes entrenched and minor deviations of behavior occur which are not worthy of causing a stir in the institutionalization process (Barley and Tolbert 1997). Script revision, on the other hand, emerges only when major incidents such as a security breach or policy change cause a radical change. As stated earlier, Earl Capita Bank does not have any record of security breach in the past few years. Since there has been no major exogenous incident (e.g., security breach), then personnel are likely to reinforce their actions in order to conduct habitualized actions. This is the core concept of script replication.

The practice of script replication and revision becomes visible when there is a growing need to accommodate technology change. Whenever information technologies need to be upgraded or replaced, policies and regulations that direct the use of such technologies are revised as well. The artifact and regulatory revision is an authority that belongs to the Information Technology Department. An elaboration of such authority by a Senior Analyst at the Information Management Division is as follows:

> "The authority to upgrade and replace IT hardware, software, applications, and suchlike belongs to the Information Technology Department. The procedure requires that a department requesting for a technology upgrade forward a formal request to the Information Technology Department. When the Board of Governor agrees and a budget has been allocated, the upgrade takes place. The Information Technology Department usually sends expert staff members to deal with the upgrade. They also formulate and socialize new policies and regulations for using the new technology. Of course, they will also assign access privilege and security to the new technology."

Earl Capita Bank has not undergone radical institutional change of its information security. The focus of this subsection shifts to script replication instead. The script replication emerges when agencies become familiar with what is expected of them and begin to internalize such expectations. The difference between the script replication and revision phase and the earlier one is within the consciousness of action. Whereas the previous phase denotes the personnel's willingness to accept the regulation that shall dictate their behavior, this phase depicts the threshold of behavior according to such acceptance and deviations from approved behavior that might occur during the acceptance. Regarding the issue of data ownership, for instance, the Senior Analyst at the Information Management Division describes such an issue:

> "Data ownership is part of the culture in Earl Capita Bank. It's an ugly truth, yes. People here do it anyway and it's very difficult for us to change. This is mainly because they think of us as the baby in Earl Capita Bank, or the stepchild that the Board of Governors would get rid of sometime soon. It took us several years to finally convince them to change their mindset that data and information belong to Earl Capita Bank, and not to a particular department. They gradually accept this concept but yes, it does take time. But I'm very confident that information systems in Earl Capita Bank will be completely centralized in the future. Everything related to information systems, whether it's about data, software, hardware, and even security. We at the Information Management Division are working hard to make this happen."

The issue with unconscious script replication seems to relate to corporate culture and maintenance of *status quo*, which is closely linked to social stability. The data-ownership issue reflects a slow deviation from the *status quo*. Regardless of the attempt to deviate data ownership towards centralized information systems, the security of Earl Capita Bank's information systems is well maintained. Many of the institution's personnel confirm that there has never been a case of security breach in Earl Capita Bank.

Information security has been widely accepted as mandatory in Earl Capita Bank and personnel have acknowledged its importance and identified procedures to implement it. Despite the issue with data ownership, departments have enforced security practice and have controlled access to their information systems according to the prescribed policies and regulations. The prescribed policies and regulations are a privilege assumed only by the Information Management Division and the Information Technology Department. The unconscious implementation of information security, signifying institutionalized information security, marks the final phase of information security institutionalization. This phase delineates the objectification and externalization of patterned information-security actions and behavior amongst the community of Earl Capita Bank.

4.3.1.4. Patterned-Actions Objectification and Externalization: The issue with objectification and externalization of patterned actions emerges as an agency begins to accept the revised script and behave accordingly (Barley and Tolbert 1997). The focus is therefore on how actions and behavior become habitualized and rational, and how they replicate the script prior to objectification and externalization. In the case of Earl Capita Bank, personnel have begun to accept security policies and regulations, and interact with technologies and security artifacts according to laid down policies and regulations.

The acceptance of and interaction with technologies and security artifacts denote the typification of habitualized actions by Earl Capita Bank's personnel. When the actions and behavior become habitualized, the personnel unconsciously strive to maintain information security in Earl Capita Bank. The Senior IT Researcher states that:

> "Again, we have the best BCP in the country. So what I can tell you is that our staff and management take the regulation and penalty for the same under serious consideration.

> We put every effort into becoming an example of dedication and conformity. If you ask me, I personally believe in our integrity and commitment as a community of Earl Capita Bank."

Earl Capita Bank maintains a high standard of integrity and commitment as regards its personnel. Earl Capita Bank regards information security as a socio-organizational issue and is particularly confident of the integrity and commitment of its personnel. The institution relies exceedingly on its policies and regulations that even restrict internal behavior. This is in line with the position of the institution as a premier governing body that formulates and enforces law, policies, and regulations. The Head of Risk Management Team describes Earl Capita Bank and its personnel as:

> "… a governing public institution that takes care of commercial banks and monetary issues in Indonesia. We understand the risk regarding personnel's misconduct that can severely damage our reputation as an institution. That's why we try to keep the risk as minimum as possible, even zero. If we fail to manage our own integrity, the public's trust is at stake."

According to the concept of patterned-actions objectification and externalization, the integrity and commitment of Earl Capita Bank's personnel creates high resilience towards minor changes (e.g., technology upgrade) to the institutionalization of information security in Earl Capita Bank. In addition to the integrity and commitment of its personnel, the fact that Earl Capita Bank enjoys the highest authority in banking sector in Indonesia contributes to the high resilience.

The objective of patterned-actions objectification and externalization is therefore to highlight the interaction between social actors (i.e., agency) and artifacts, which in this case are technologies and security artifacts. Information and technology are the media, i.e. artifacts, for structuring information security in organizations, including Earl Capita Bank. As one of the modalities that that an agency socially constructs, the technologies are used to routinely produce and reproduce social structures (Orlikowski 1992; Orlikowski et al. 1995; Orlikowski 2000). Through agency's interaction with these media, behavioral and cognitive, (e.g., power, communication, sanction, etc.) properties in the structuration of information-security institution emerge. Technology is regarded as a tool to assist personnel in processing information and completing their day-to-day tasks whereas technological use leads to information, which is the processed object. Earl Capita Bank relates the use of technology to operational risk. Any information security breach is one of the greatest lurking threats that can harm Earl Capita Bank's reputation. Despite there being no record of such a security breach, the central bank realizes the potential for such incidents. Therefore governance of the use of technology is highly enforced by the Information Technology Department and by the department that owns the technology. The Head of Risk Management Team states that:

> "As a public institution, the government and the people demand us to be transparent. However, there are certain parts that need to be kept confidential. Potential leak is what we call an operational risk and such a leak may create information asymmetry that can harm the market. We have rules that regulate information which is for public consumption and specific times when this information can be made available."

The Information Technology Department manages the technical controls of information security, conducting one of the department's functionalities within Earl Capita Bank. In addition to maintaining the operability of Earl Capita Bank's Information

Technologies System, the department maintains the security of the technologies and asserts the necessity to safeguard the use of these technologies. The department is also responsible for raising the awareness about the importance of safeguarding the use of the Earl Capita Bank's information technologies amongst its personnel. The result of this is the usage and implementation of secure information technologies by personnel and the regulatory act to safeguard their use of these technologies. This implementation and act has become a habitualized routine whereby personnel realize the importance of keeping their username and password to themselves[6]. From the technological perspective, the habitualized routine practices of technical controls and informal controls of information security therefore socially structure the institution of information security in Earl Capita Bank.

4.3.1.5. Discussion: The high emphasis on legality and regulation placed at Earl Capita Bank identifies it as an information-systems focused institution. The issue with data ownership, however, seems to be the most prominent stumbling block in efforts to centralize information systems. Regardless of the seemingly disparate control and ownership of information systems, data and also information within Earl Capita Bank, the governance of information security is in reality under the authority of the Information Technology Department and Information Management Division. The information-security governance of the logical content belongs to the Information Management Division, while the Information Technology Department assumes full authority on the governance of the security of the institution's technology and infrastructure.

[6] The security culture of making use of a username and password in Indonesia is so low that an employee may share their office username and password with any "trusted" colleagues, hence allowing them access to their personal professional information.

The governance of information security within Earl Capita Bank is not centralized; i.e., the governance practice is not directed by a single department. Rather, the concrete responsibility is dichotomized and empowered to two departments (i.e., the Information Technology Department and the Information Management Division)[7]. While the Information Technology Department directs the technical controls of information security, the Information Management Division manages the formal controls of information security. The two departments share the responsibility to oversee the informal controls of information security (e.g., raising personnel's awareness of the importance to secure the distribution and dissemination of information and providing and promoting education of the personnel concerning the importance of safeguarding their username and password). These three dimensions of information security are continuously enforced so that they become grounded as a regular practice of safeguarding the Earl Capita Bank's information asset. Hence the practice of governing and implementing these three dimensions forms social structures that have become routine and are highly resilient, creating an institution (Björck 2004; Scott 2008). Other departments simply determine which information systems, data, and information to share, and select which users can gain access to their systems and access and utilize the departments' data and information. The other departments have the freedom to determine the implementation of information-security practices and are required to contribute to the security culture which is in turn governed by the two departments.

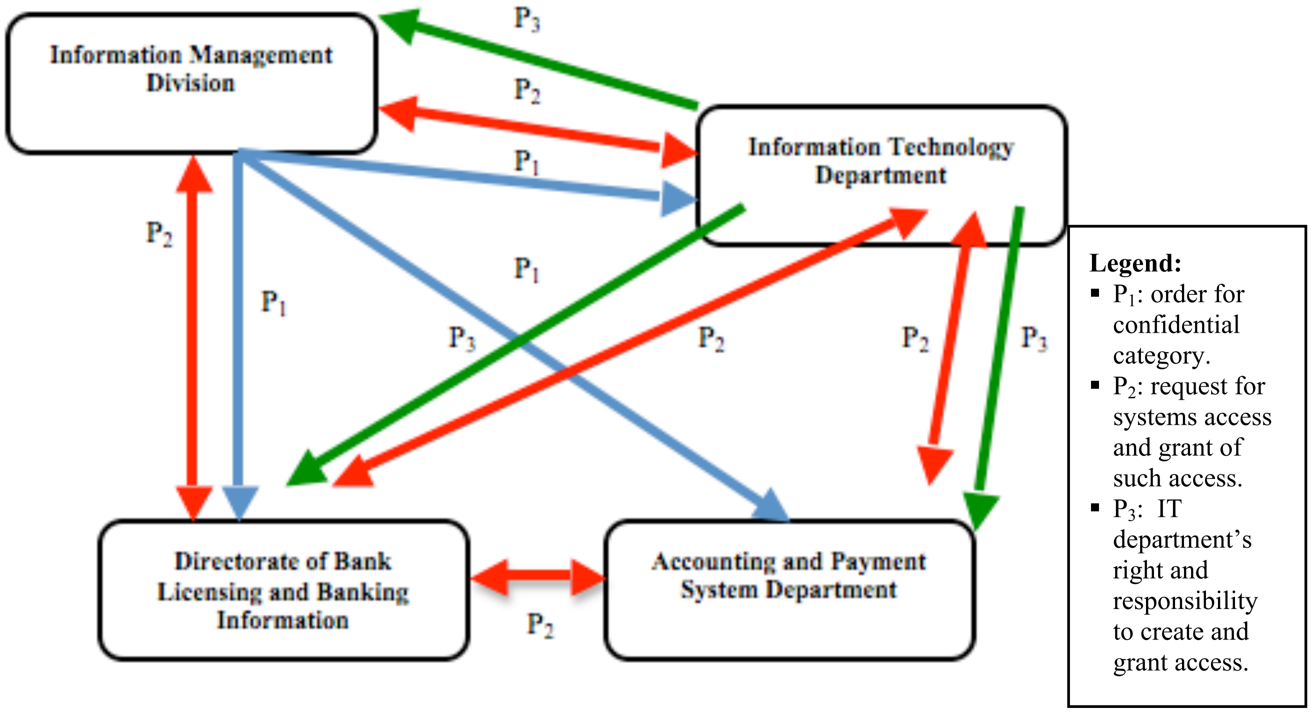
The data ownership issue, however, may hinder the effectiveness of information security governance within Earl Capita Bank, interrupting the continuous reproduction of

[7] The dichotomized concrete responsibility is one that embodies the technical controls and the formal controls. These are two of the three dimensions of information security as envisioned by Dhillon (2007).

institutionalized information security. Each department within Earl Capita Bank possesses power over the use of and access to information processed from its own information systems. Personnel of each department are very knowledgeable about managing and processing the information of their department's information systems. However, they can only access processed information from other department's information systems under permission of the department concerned. These personnel can only procure a read-only access to information from someone else's department and use the end-result for analysis only. Each department has its own regulations concerning the use of and access to its information systems and sanctions only such use and access. This depicts the strong data ownership system that has its own merits and drawbacks. The advantage is the guaranteed security of the access to Earl Capita Bank's information systems. The drawback is the uncoordinated and dispersed information that is supposedly derived from the same data, but mostly leads to the creation of "the lack of architecture interoperability, incompatible data standards, lack of relevant integration expertise, and the existence of legacy processes" (Lam 2005). Figure 4.3 depicts the flow of authority and responsibility among departments in Earl Capita Bank.

Figure 4.3 depicts the dual governance of information security, which is shared between the Information Technology Department and the Information Management Division. Process P_1, denoted by the blue arrows, delineates the implementation of information-confidentiality category by the Information Management Division and information stewardship. Other departments such as the Information Technology Department, the Directorate of Bank Licensing and Banking Information, and the

Accounting and Payment System Department, implement the categorization and the stewardship according to their function and need.


Information Management Division
Information Technology Department
Directorate of Bank Licensing and Banking Information
Accounting and Payment System Department
P3
P2
P1
P2
P1
P1
P3
P2
P2
P3
P2

Legend:
- P_1: order for confidential category.
- P_2: request for systems access and grant of such access.
- P_3: IT department's right and responsibility to create and grant access.

Figure 4.3 – The Flow of Information-Security Authority and Responsibility in Earl Capita Bank

The bidirectional red arrows of process P_2 demonstrate the requests for systems access and the granting of such access among departments. The green arrows of process P_3 highlight the right and responsibility of Information Technology Department to create and grant technical access (e.g., username and password) upon request or when any technological change takes place.

Despite the data-ownership issue that constrains the authority of the Information Management Division, the consistent effort to safeguard the Earl Capita Bank's information asset creates the continuous structure of an institutionalized information security. In an attempt to resolve the data-ownership issue, the Information Management

Division created an information-stewardship concept, which highlights “trust and competency; adoption of technology” (Rosenbaum 2010). This concept allows departments to decide which of the data and information under their management can be shared with users outside their departments. The practice is to ask departments to assign different levels of confidentiality category to their data and information. Despite the rigid procedure for external users and even internal personnel to gain access to data, information, and information systems, Earl Capita Bank possesses one of the most reliable and secure information-security systems in the nation. The effort is partially due to the institution’s pledge as a public institution and a central governing body.

The summary of the institutionalization of information security in Earl Capita Bank can be elucidated using the institutionalization model by Barley and Tolbert (1997). The institutional realm signifies the structure of information security in Earl Capita Bank while the realm of action signifies the agency and the behavior that shapes the structure. Furthermore, since Earl Capita Bank is the highest authority in the nation’s banking sector, external forces of information security institutionalization are due to technology change or environmental change that initiates strategic change. The first process, namely the script encoding, signifies the moment when, for example, the Information Management Division introduces the information stewardship concept or the Information Technology Department puts a new policy regarding the use of social network websites during office hours in place. When personnel begin to acknowledge the new regulations and departments begin to socialize these regulations, the principles of this script become enacted as evidence imbedded in the agency’s behavior. Several stumbling blocks such as the data-ownership issue might lead to similarities among several minor deviated behaviors. They are, however, resolved through behavior revision and are replicated back in the script as principles that emerge from personnel's interaction with artifacts (Orlikowski 2000). The behavior revision is progressing slowly as the data-ownership issue has not been completely resolved in Earl Capita Bank. Finally, the replicated script is permanently recorded in the institutional realm when personnel's behavior becomes a rationale amongst one another and is recognized as having become habitualized and accepted as the norm in Earl Capita Bank.

4.3.2. Relationship with Commercial Banks

4.3.2.1. The Macro-Prudential Supervision of Information Security Governance: Earl Capita Bank is the regulator and supervisor of commercial banks and other financial institutions in Indonesia. As a means to achieving financial system stability, Earl Capita Bank also undertakes crisis management among commercial banks and conducts banking intermediation. Earl Capita Bank attempts to maintain the nation's financial stability as depicted in its function to formulate financial regulations and policies that are to be adhered to by commercial banks and financial institutions. It also supervises banks and institutions in ensuring their adherence to such regulations. Such a function elevates Earl Capita Bank's status as an authorized auditor and supervisor of commercial banks and renders it the deontic power. Evidence in support of this statement is the historical fact of Earl Capita Bank being a governmental institution whereby its Governor was a member of the Cabinet.

Today, Earl Capita Bank possesses the freedom to maintain financial stability. It monitors and ascertains current domestic and international economical stance and determines financial regulations in support of this stance. In doing so, Earl Capita Bank regards information as a crucial aspect and recognizes that any failure to safeguard it may harm the nation's financial stability. Earl Capita Bank supports and protects information confidentiality belonging to each commercial bank and encourages commercial banks to safeguard its information from unauthorized and inappropriate access. Three departments within Earl Capita Bank, the Accounting and Payment System Department, the Banking Research and Regulatory Department, and the Bank Supervisory Department, are in charge of regulating and governing the information access of commercial banks.

Various matters related to credit card payment, debit card payment, electronic banking, or SMS (text-messaging) banking are handled by the Accounting and Payment System Department. This department issues regulations concerning processing and accessing of payment information. It also grants permission to commercial banks for launching new electronic related banking products. The department is therefore responsible for the security of this information. It owns several information systems which are used to process information for electronic related banking products and card payment products. Users from other departments wishing to have access to these information systems can only do so with permission granted by the Accounting and Payment System Department. The department also has the right to independently audit and supervise commercial banks on their electronic-banking activities and card payment functionalities. In fact, the accounting and payment system department is the only department that oversees electronic related banking products and card payment products. As evidence of this fact, the Head Payment Information Systems Supervisor denotes that:

> "If we want to further investigate their security system report, we can summon them for verification or we can pay them a visit in order to audit their system."

Furthermore, the department possesses sole authority to impose penalties on commercial banks that fail to follow electronic banking or card payment regulations. Failure to adhere to these regulations may result in several implications for commercial banks, ranging from payment of fine to losing the permit to run their electronic related banking products or card payment products. According to the Head of Payment Information Systems Licensing:

> "After the first and the second reminder, we always coach them. We don't just leave them to figure out what to do themselves. However, if they still fail to follow the rules after the third reminder, then we have to decide that they are not suitable for owning such a banking product."

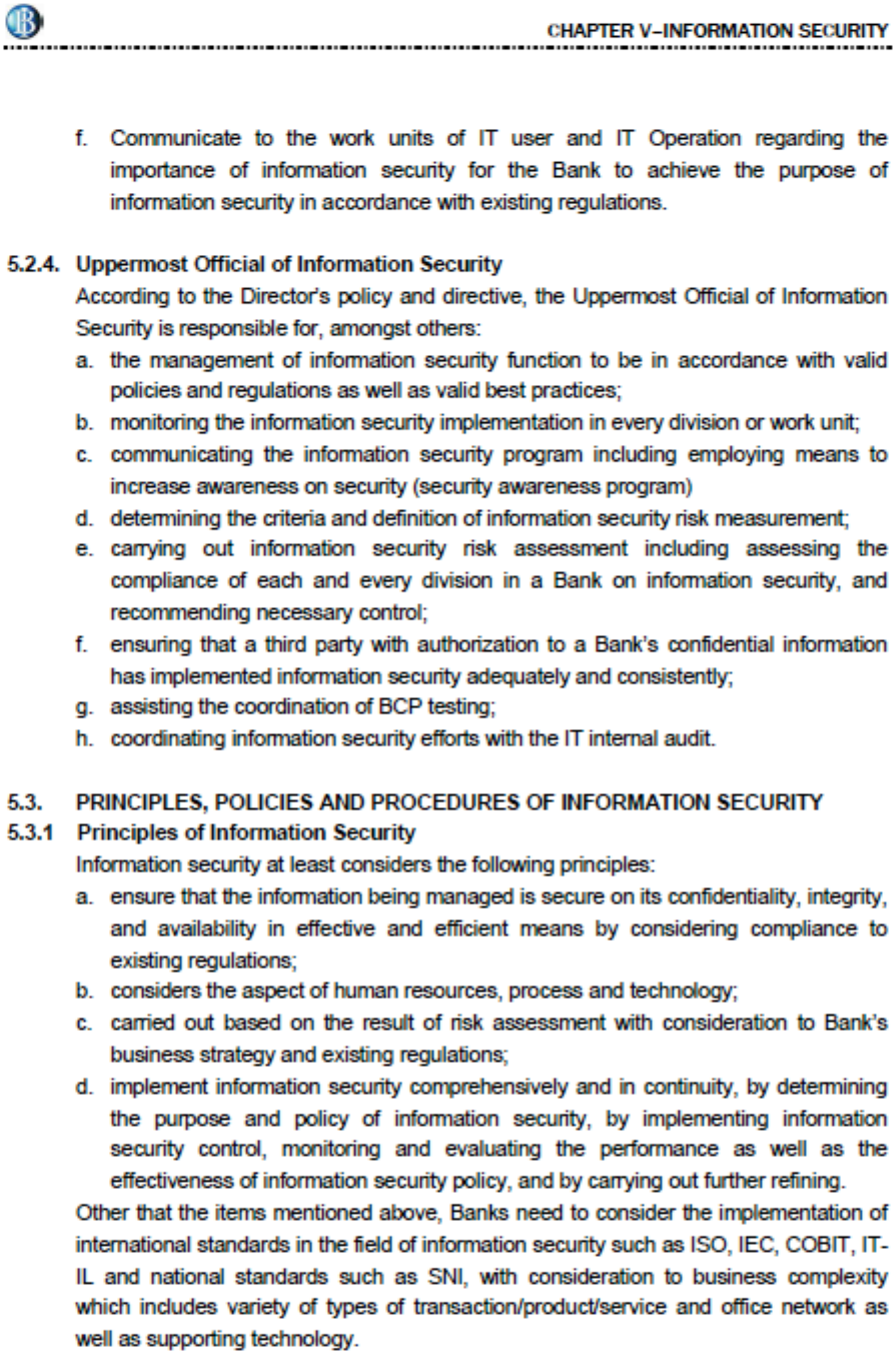
Other auditory and supervisory tasks are handled by the bank's supervisory department. In general, this department is divided into three subdivisions: the State Banks Supervisors (Bank Supervisory Subdivision 1), the Foreign Banks Supervisors (Bank Supervisory Subdivision 2), and the Private National Banks Supervisors (Bank Supervisory Subdivision 3). The department assumes similar responsibilities as those of the Accounting and Payment System Department in more general areas. It performs annual regular audit and random audit. Annually, the department dispatches a group of auditors responsible for visiting a bank according to the legal status of a bank. The auditory team may consist of up to 10 personnel. For instance, subdivision 1 dispatches auditors for a state bank. The Senior Private Bank Supervisor explains that:

> "We make annual auditory visits to each bank. Prior to these visits, we create the annual Audit Booking Plan, which is based on the bank's current performance and future potential risks. Specifically for Blue Sequoia Bank, we focus on three risks: credit risk, operational risk, and strategic risk."

Such a visit involves auditing a commercial bank's information systems, including the security of such systems. For instance, the auditors determine the appropriateness of network and server location, installed firewalls, regular updates of antivirus software, etc. Random auditory visits, however, usually involve incidents (e.g. security breach) that potentially threaten the reputation and operability of the bank.

Unlike the Accounting and Payment System Department, however, the Bank Supervisory Department does not possess legal authority to formulate regulations. This right is owned exclusively by the Banking Research and Regulatory Department. This department formulates and develops policies and regulations concerning currency rate, financial stability, and commercial banks. The Senior Researcher of the Directorate of the Banking Research and Regulation explains the formulation of regulations as following:

> "These are not the regulations or policies that dictate the practice of information security in commercial banks. These are just guidelines that we have created that banks can follow and modify according to their own conditions. I call them guidelines since these contain basic information security principles that commercial banks need to meet, along with the privilege of modifying them to meet their conditions. When we created this guideline document back in 2006, I personally had less than five hours of sleep almost every night. And it took us a year to complete the formulation process. We hosted several sharing sessions where we invited large commercial banks and consultants to share their ideas and experiences with information security. Although the guidelines are exclusively reserved for use by commercial banks, we also incorporate some of the very essential ideas for our internal use. This is exemplified by the use of ISO 27001 as the basic framework for our internal security policies and regulations."



CHAPTER V–INFORMATION SECURITY

f. Communicate to the work units of IT user and IT Operation regarding the importance of information security for the Bank to achieve the purpose of information security in accordance with existing regulations.

5.2.4. Uppermost Official of Information Security

According to the Director's policy and directive, the Uppermost Official of Information Security is responsible for, amongst others:

a. the management of information security function to be in accordance with valid policies and regulations as well as valid best practices;
b. monitoring the information security implementation in every division or work unit;
c. communicating the information security program including employing means to increase awareness on security (security awareness program)
d. determining the criteria and definition of information security risk measurement;
e. carrying out information security risk assessment including assessing the compliance of each and every division in a Bank on information security, and recommending necessary control;
f. ensuring that a third party with authorization to a Bank's confidential information has implemented information security adequately and consistently;
g. assisting the coordination of BCP testing;
h. coordinating information security efforts with the IT internal audit.

5.3. PRINCIPLES, POLICIES AND PROCEDURES OF INFORMATION SECURITY

5.3.1 Principles of Information Security

Information security at least considers the following principles:

a. ensure that the information being managed is secure on its confidentiality, integrity, and availability in effective and efficient means by considering compliance to existing regulations;
b. considers the aspect of human resources, process and technology;
c. carried out based on the result of risk assessment with consideration to Bank's business strategy and existing regulations;
d. implement information security comprehensively and in continuity, by determining the purpose and policy of information security, by implementing information security control, monitoring and evaluating the performance as well as the effectiveness of information security policy, and by carrying out further refining.

Other that the items mentioned above, Banks need to consider the implementation of international standards in the field of information security such as ISO, IEC, COBIT, IT-IL and national standards such as SNI, with consideration to business complexity which includes variety of types of transaction/product/service and office network as well as supporting technology.

Figure 4.4 – A partial view of the Information-Security Chapter codified in the Earl Capita Bank's Guidelines

Due to the diverse conditions prevailing in commercial banks, the department is obliged to formulate abstract and general regulations applicable to any condition and technological advancement. Hence, these policies and regulations need to be further enhanced by each bank to satisfy its personal circumstances. As a result, these policies and regulations can even accommodate the needs of manual information-processing banks (i.e. those with no automated/electronic information systems). Figure 4.4 depicts a partial view of the guidelines, suggesting the required basics that commercial banks need in order to satisfy the implementation of information security. The Senior Researcher of the Directorate of the Banking Research and Regulation elucidates this notion as follows:

> "Banks are a complicated entity. Some of them would actually come to us, asking us to reconsider enforcing our guidelines. They would be whining about their legacy networks and servers, their security system that is not up to date, and they would even beg us to consider their manual information systems. I told them that the guidelines are meant to be guidelines for every bank for creating policies and regulations according to their own situations. You could probably hire more security officers if you have a manual information system, heighten your existing security policies and regulations, or improve your employee satisfaction for better commitment. Just because your system doesn't have a sophisticated security feature or is not automated, doesn't mean we have to bend the rules just for you. A rule is a rule- you have to deal with it."

4.3.2.2. Discussion: The macro-prudential supervision framework highlights the relationship between Earl Capita Bank as the governing body and commercial banks. The relationship consists of two reflexive processes: the governance and control process by Earl Capita Bank and the conformity and report by commercial banks.

The macro-prudential supervision of information security governance uses the legitimacy view of institutional theory (Björck 2004). The top-down lines labeled as the governance and control lines as depicted in the macro-prudential supervision framework (see figure 3.3) represent the supervisory acts by the Earl Capita Bank. These supervisory acts include formulating and enforcing security policies and regulations, regular auditory visits, and random auditory visits. The reciprocity acts (i.e., the bottom-up lines in figure 3.3) include the conformity actions taken with respect to the security policies and regulations governed by Earl Capita Bank and the reporting acts of routing practices of information security as well as security incidental cases.

Another department that owns independent information systems and possesses liberty to formulate policies and regulations for using in such information systems is the Bank Licensing and Banking Information Department. This department exclusively owns the debiture information systems, which connect commercial banks and financial institutions to a customer's credit score, and serves as the administrator for the use of this system. The system connects commercial banks to financial institutions and the department provides policies and regulations for using the system. The department also owns the right to penalize banks that fail to follow the regulations and grants (and deny them) access to the system. In a response to a statement by the Analyst of the Bank Licensing and Banking Information Department about access permission, the Senior Analyst of this department states that:

> "We issue regulations for use of the debiture information systems and we also determine who can have access to this system. For instance, if a bank wants to assign some of its employees to become admin for its application that connects to our system, the manager

> needs to register his employees with us and they need to complete and sign a request form and send it back to us.”

4.4. Conclusion

Earl Capita Bank is a premier institution that acts as the central bank of Indonesia. The bank originated in the Dutch colonial government as a commercial bank that functioned to manage inflation rate and currency. When Indonesia gained its independence in 1945 and matured as an independent nation, the bank was renamed as Earl Capita Bank and achieved a central bank status. Such a status empowers Earl Capita Bank with a deontic power and constitutive power enabling the institution to audit and supervise commercial banks and financial institutions operating in Indonesia. Such auditory and supervisory privileges allow Earl Capita Bank to audit and supervise the practices of information security in commercial banks and other financial institutions. As an independent institution, however, Earl Capita Bank also implements the practices of information security internally.

The objective of this chapter is to present and discuss the empirical analysis of the practices of information security of Earl Capita Bank. The practices of information security are therefore divided into internal practices and auditory and supervisory practices. The empirical analysis delineates the implementation of the three dimensions of information security: technical controls, formal controls, and informal controls. The implementation of these dimensions is not centralized, however- meaning that it is not directed by a single department. Rather, two departments initiate the first two dimensions and together, these departments manage the other dimension with respect to their main obligations. All units in the institution reciprocate thereby socially constructing the structure of information security practices and continuously reproducing this structure, creating an institution of information security.

Externally, Earl Capita Bank possesses the deontic power and the constitutive power to audit and supervise the information security practices in commercial banks. Empirical analysis has shown that the power property endows the authority and government status to Earl Capita Bank. Commercial banks and financial institutions respond to such status through conformity and adherence. The institutional theory used to reflect such a relationship depicts two lines with opposite arrows: one line describes the governance and control of information security regulations and practices by Earl Capita Bank and the other line denotes conformity with the information security regulations and reporting of the information security practices by commercial banks.

The issue of data ownership has long been shrouded in ambiguity at Earl Capita Bank. The data ownership issue creates inconsistency of data and information in Earl Capita Bank. Such an inconsistency may interfere with the practices of information security, particularly in terms of the formal controls of information security. Reasons for such interruption (e.g., lack of architecture operability, incompatible data standards, lack of integration expertise and use of legacy processes) are evidence of the practice of inconsistent information in Earl Capita Bank. Personnel need to be vigilant against information risk as security threat has the potential to become a distinct possibility.

5 THE CASE OF CENTRO METROPOLITAN BANK

5.1. Overview

This chapter presents a case study of an instance of the implementation of information security governance at a commercial bank amidst considerable government participation. The case study is also an example of a commercial bank's conformity with the central bank's security regulations and policies as well as its compliance with reporting norms concerning information security practices s laid down by the central bank. As an independent commercial bank, Centro Metropolitan Bank has the authority to put into place a routine practice of information security, thus creating an institutionalized information security in Centro Metropolitan Bank. In addition, this chapter presents a security specific case whereby the bank attempts to resolve such an issue with the involvement and interference of the central bank. Such involvement and interference are elaborated upon in more detail at a subsequent section, using the institutional theory to depict the top-down process (i.e., governance and control) and the bottom-up process (i.e., conformity and reporting) between Earl Capita Bank as the central bank and Centro Metropolitan Bank as the commercial bank.

This chapter therefore aims to present a comprehensive description and depiction of information security practices and governance in Centro Metropolitan Bank. The practices and governance have been theoretically prescribed to involve external parties such as the central bank and external threats. In this chapter, institutionalization of information security reflects both the internal and external information security governance that is strongly influenced by the central bank. The organization of this chapter is as follows: section 5.2 presents the history of Centro Metropolitan Bank as well as its characteristics. Section 5.3 provides the empirical analysis for the Centro Metropolitan Bank case. Various aspects such as the internal security practices elucidated by a combination of institutional theory and structuration theory, the relationship between the bank and the central bank as depicted by the institutional theory, and the descriptive security incident or case study of electronic data-capture fraud. Section 5.4 summarizes and closes this chapter.

5.2. Organizational Background

5.2.1. A Government-Owned Commercial Bank

Centro Metropolitan Bank is a large government-owned bank and is considered to be the nation's financial backbone. The bank is the largest bank in the nation in terms of assets, loans, and deposits. As a government-owned bank, Centro Metropolitan Bank receives full attention from the government and from the central bank in particular. By December 2006, the bank had grown into one of the nation's essential and key economic and financial players and had even established three principal subsidiaries: *Bank Syariah CMetro, CMetro Sekuritas*, and *AXA CMetro*. As a commercial bank, Centro Metropolitan Bank is obliged to fulfill the following duties: (1) act as a financial intermediary, (2) create and process information about firms, and (3) participate in the nation's payment systems (Scott et al. 1992). The financial service that Centro

Metropolitan Bank provides is one of the best examples of its kind in the nation, reflecting its efficiency and effectiveness in transactions involving financial instruments (e.g. auto loans, mortgage notes, bonds, demand deposit currency, etc.) (Fixler 1993). Like other large banks in the nation, the bank is headquartered in Jakarta.

In support of its commitment as a financial entity with an unimpeachable reputation, the bank "maintains independent Offices of Compliances, Audit and the Corporate Secretary, and is under regular scrutiny from external auditors representing Earl Capita Bank and the Supreme Audit Agency (BPK), as well as international auditing firms" [1]. Centro Metropolitan Bank has enjoyed a solid reputation in internal audit practice, which audits every aspect of the bank including the information security practices. In fact, the bank's internal Information Technology Audit Services are one of the major management tools for directing its information security (Da Veiga and Eloff 2007; Knapp et al 2009). Centro Metropolitan Bank has envisioned the abiding commitment to prudential banking practices and displayed the willingness to comply with regulations and laws. The objective is to maintain good relationships among the bank's various elements, including management, stakeholders, and the Board of Commissioners, on the basis of ethics, corporate culture, and corporate value. As a result, the bank prides itself on its strong commitment to corporate governance and has proven this by receiving many awards for best corporate governance practice and banking service excellence.

[1] Source: http://www.bankmandiri.co.id/english/corporate01/about_profile.asp

5.2.2. History of Centro Metropolitan Bank

Historically, the bank has emerged as a result of the merger of four government-owned banks and has undergone a series of major reorganizations. The bank was officially founded on October 1998. The merger was accomplished in 1999 as part of the government's bank-restructuring program, which was one of its attempts to remedy the economic crisis which befell the nation in 1998. The history of the bank can be traced back to the existence of the four government-owned banks that no longer exist but that served as the bank's foundation. These banks are:

1. *World Heritage Bank*: This bank originated as a result of an exhaustive process to nationalize *De Nationale Handelsbank NV*, a Dutch-owned bank, which became *Bank Umum Negara* in 1959. In 1964, *Chartered Bank*, a British-owned bank, was also nationalized and its operational right was given to *Bank Umum Negara*. In 1965, *Bank Umum Negara* was merged into *Bank Negara Indonesia*, becoming *Bank Negara Indonesia Unit IV*. Three years later, the Unit IV separated and became an independent bank named as *World Heritage Bank*[2].
2. *National Commerce Bank*: This was one of the oldest banks in the nation. It was initially founded as *Nederlandsch Indische Escompto Maatschappij* in Batavia (now Jakarta) in 1857. The bank was renamed as *Escompto Bank NV* in 1949 and was then nationalized and renamed as *National Commerce Bank* in 1960[3]. The bank served to finance the industrial and mining sectors before it was merged with the other three banks.

[2] Source: http://id.wikipedia.org/wiki/Bank_Bumi_Daya (translated)
[3] Source: http://id.wikipedia.org/wiki/Bank_Dagang_Negara (translated)

3. *Exima Bank*: The bank's name stands for *Bank Ekspor Impor Indonesia*. It was a government-owned bank that financed import and export. The history of this bank is traceable back to *NV Nederlansche Handels Maatschappij*, a Dutch-owned firm, which was founded in 1842. The operational activities included banking activities in 1870. The bank was nationalized in 1960 and was merged into *Bank Negara Indonesia* to become *Bank Negara Indonesia Unit II*. In 1968, the Unit II was divided into two separate units, of which one served specifically to handle exportation and importation. This subunit was then renamed as *Exima Bank*[4].
4. *Bapindo*: Bapindo stands for *Bank Pembangunan Indonesia*, which originated in 1951 as *Bank Industri Negara*. Unlike the other three banks, Bank Industri Negara was founded by the government of Indonesia and immediately served as a government-owned commercial bank. The bank was intended to support the nation's economic sector, particularly in areas such as farming, industry, and mining. The bank was renamed as *Bapindo* in 1960. In 1970, *Bapindo* served to help direct the nation's development process, specifically serving to finance the manufacturing, transportation, and tourism industries.

All these banks have had significant impacts on the nation's economical welfare and have immensely contributed to it also. Hence the economic and financial turmoil that tremendously impacted the nation in 1998 also hit the banks severely. The government decided to merge these four banks, restructuring and reorganizing the new bank thus formed. As of today, the bank has about 956 branch offices, 6 overseas branches and

[4] Source: http://id.wikipedia.org/wiki/Bank_Ekspor_Impor_Indonesia (translated)

representatives, 2500 ATM machines, and three principal subsidiaries (CMetro Syariah Bank, CMetro Sekuritas, and AXA CMetro)[5].

5.2.3. Organization Structure

Centro Metropolitan Bank is directed by an executive management team of Board of Directors, headed by a President Director. The management and governance are supervised by the Board of Commissioners appointed directly by the nation’s Ministry of State-Owned Enterprise.

[5] Source: http://www.bankmandiri.co.id/english/corporate01/about_profile.asp

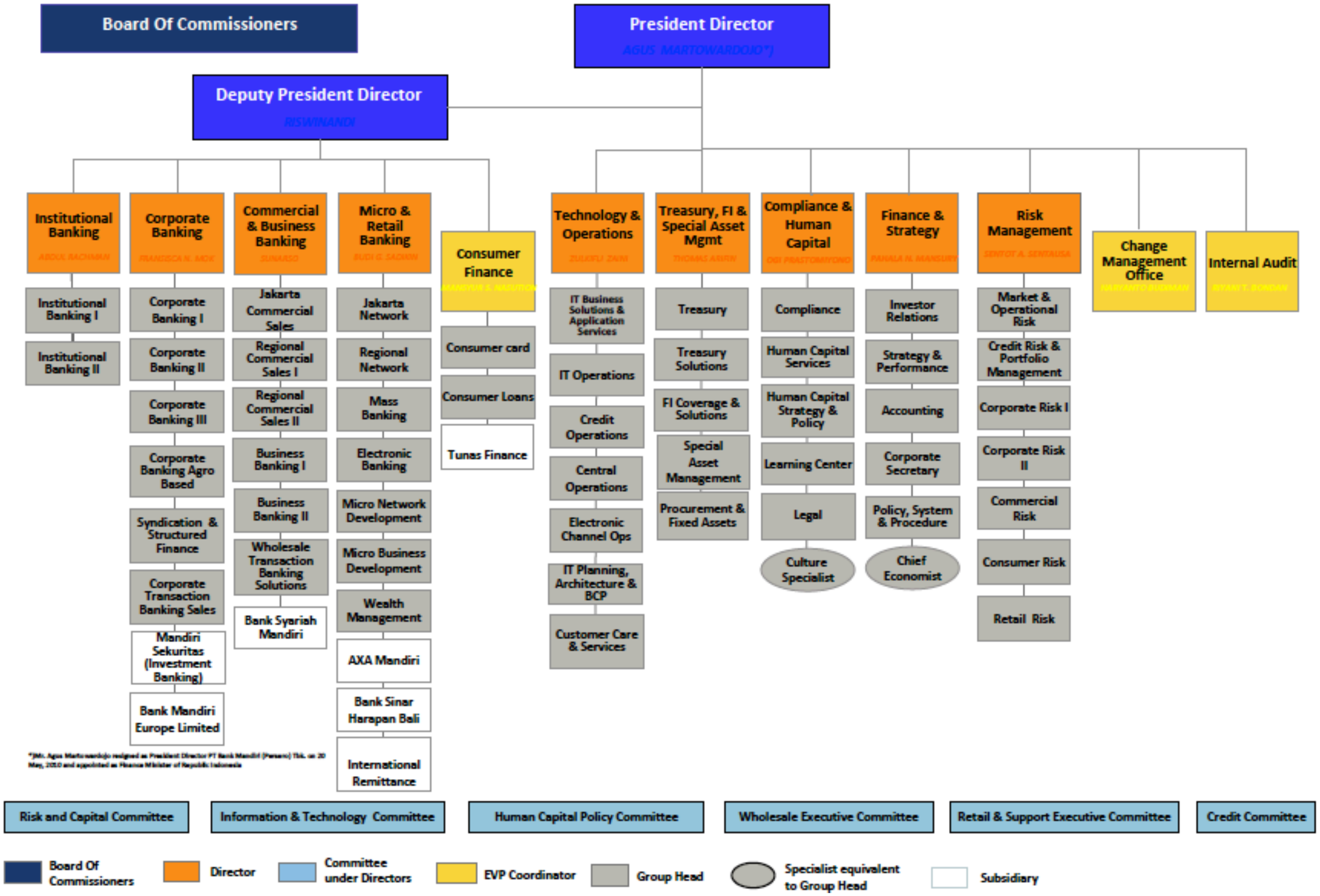


Figure 5.1 – Organization Chart of Centro Metropolitan Bank

As a large institution, Centro Metropolitan Bank contains divisions each of which is managed by a director. Each division oversees a subdivision (i.e., group), which plays a significant role in conducting the bank's operational activities. The governance and practices of information security are managed by the IT security department, which is a part of the IT Planning, Architecture, and BCP (Business Continuity Plan) group. This group is structured under the Technology and Operations Division, which is responsible for overseeing all issues regarding the implementation of Information Technology System in the bank and by the bank's customers.

Unlike those of Earl Capita Bank, the internal information-security practices in Centro Metropolitan Bank are initiated solely by the IT Security Department. The Vice President of the IT Security Department states the following:

> "The vision and mission of the IT security department is based on the idea of safeguarding our information assets. The formal statement is prescribed in the functionality statement of our department, which states that it is our responsibility to conduct the analysis, formulation, synthesis, development, implementation, and evaluation of an IT security instrument to ensure the security of information technology as an asset, whether physical or logical (i.e., data and information) of the bank in the short term and in the long term."

Hence the governance of information security within the bank is centralized around the IT security department, involving controls of the technical aspects, formal aspects, and informal aspects of security (Dhillon and Moores 2001; Dhillon 2007). The department's main responsibilities include:

1. To coordinate the implementation of IT security solutions including infrastructure, application, and operating system in which all functions aiming at safeguarding the bank-wide information and data security.
2. To evaluate the internal IT security system and the best practices to create, develop, and implement the bank-wide IT security blueprint and infrastructure.
3. To coordinate the review process for business strategy, operation and business process and application development, aiming to develop, synchronize, and implement the IT security blueprint and strategy.

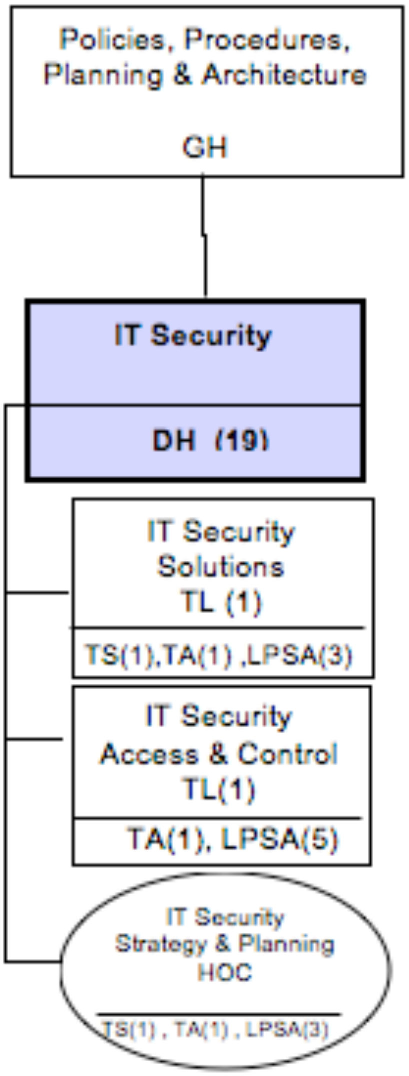


Figure 5.2 – Organizational Structure of the IT Security Department

4. To ensure that user ID assignment and access right is in accordance with policies, and to direct the custodian user ID and password using security administrator, key management, as well as the public key infrastructure certificate to ensure confidentiality and security of the Information Technology System.

5. To monitor and direct the implementation of the IT strategic plan and architecture so as to safeguard the integration of the IT security infrastructure as well as its synchronization even through changes in IT as a whole.
6. To manage the administrative process, human resource, and budget in the IT Security Department in order to ensure the implementation of regulations at the departmental level, optimize resources (e.g., personnel and budget) allocation, and develop personnel's capability by providing training and structured assignments.

As shown in figure 5.2, the IT Security Department consists of three subunits: (1) the IT security solutions unit that conducts the IT security systems development, (2) the IT security access and control unit that oversees the user access and privilege, and (3) the IT security strategy and planning unit that formulates the IT security strategic plan and blueprint as well as the IT security policy and procedures. These units respectively provide effective information security governance and practices which are synchronous with information security best practices, the bank's culture and identity and the technologies owned by the bank.

5.3. Empirical Analysis

This section delivers a theoretical review of the Centro Metropolitan Bank case study. Drawing upon institutional theory and structuration theory, the case study elucidates the institutionalization of information security from a sociological stance.

Unlike the Earl Capita Bank case study, this case study includes a presentation of a security breach incident, which is essential to delineate an instantiation of re-institutionalization. Similar to the previous case study, the organization of this case study is structured on the basis of the internal security practices as an inter-level institutionalization and the relationship with the central bank regarding practices of information security.

5.3.1. Inter-Level Institutional of Information Security Governance

5.3.1.1. Script Encoding: Just as Earl Capita Bank considers reputational risk as its consequential threat, so does Centro Metropolitan Bank. Centro Metropolitan Bank regards reputational risk, which is closely linked to operational risk, as a leading cause of crowding out customers, potentially creating financial losses. With regard to information security and technological security Centro Metropolitan Bank identifies access to information and use of technology as potentially damaging risks if they are not properly handled. The bank characterizes such risks as an operational risk and abides to the handling of such risk using Basel II framework as a guideline. The Operational Risk Management Team Leader defines risks within the bank as follows:

> “We use the common definition for risk as a potential loss that may harm the bank. We define operational risk using Basel II’s definition of operational risk, which we believe all banks should refer to. This definition states that this risk is a harmful risk that is caused by dysfunctionality, or inadequacy, or failure, and it damages the bank through its people, procedures, systems, and events.”

Risk related to systems, or the use of technology, is closely linked to reputational risk as it may harm the bank's customers. For instance, if the bank's information systems are down, the resultant impact is manifested in the form of customers' dissatisfaction whereby such dissatisfaction can lead to negative publicity that harms the bank's reputation. As such, the bank regards operational risk as more damaging than financial risk.

Hence the bank rigorously maintains its information systems and their security. Consequently, it possesses some of the most solid corporate information systems in the nation. The bank prides itself on the fact that its most precious information (i.e., its customers' data) has never been found susceptible to any leakage. The information technology security is maintained and preserved by the IT Security Department. One of the department's goals is to ensure the security of information technology assets, either the physical or logical components (i.e., data and information), both in the short and long run. This department also formulates policies and regulations on how information technology and electronic applications are to be used to preserve information security. Electronic applications include the bank's intranet system, electronic banking, ATMs, electronic data capture (EDC) machines, etc. In addition to ensuring the proper use of information technology, the department also educates stakeholders and raises their awareness about the importance of information security. The Head of IT Audit Unit maintains that:

> "All tasks that include regulating, enforcing, controlling, and revising standard operating procedures or policies regarding risk of using IT are performed by the Information Technology Department. They assume full responsibility for these tasks."

Policies and regulations in Centro Metropolitan Bank are recognized as the Operational Guidance Standard (OGS). This guidance standard is specifically developed for operational activities and is used to manage operational risk, including information technology and its security. Information security as part of the operational activities is given special consideration. As a policy and regulation, the information security SPO is formulated by the IT security department. The Vice President of IT Security Department says about the information security SPO:

> "When I create policies to secure information, or security policies, before they are enacted, they have to be tried by the ORC (operation risk committee). And then, we give presentations about these policies, and the ORC reviews and challenges the policies. When the policies get through, the Board of Directors, particularly the Risk Director and the Technology and Operation Director, sign the policies."

In general, information-security policies and regulations are formulated based on international framework and references in order to ensure rigor and functionality. These framework and references include COBIT, ISO 17799, and ISO 27001 from which the Centro Metropolitan Bank has received a certificate of excellence. However, the drive to formulate and enforce policies and regulations is based on Earl Capita Bank's guidelines concerning information security governance and practice. Centro Metropolitan Bank creates information-security policies and regulations according to its needs and culture, blending all framework and guidelines given by the central bank. The Vice President of IT Security Department states that:

> “Earl Capita Bank does provide regulations and guidelines for use of information technology and for securing their use. However, we want to modify such guidelines to suit our culture so that we can use technology according to what we need and become what we want to be in a cultural context.”

Hence, the IT security department owns the quasi-exclusive governance of information security in Centro Metropolitan Bank. The department oversees matters of technical controls, formal controls, and informal controls of information security, although some matters may be shared with other departments within the bank. Despite the privilege of formulating policies and regulations, the IT security department does not assume the responsibility of regulating e-information usage. Consequently, other departments control the access to information, what information can be accessed, and permits for such an access.

To quote an example, the Electronic Banking Group, which falls under the micro and retail banking division, initiates and maintains procedures and regulations related to the use of electronic banking products, including SMS (text messaging) banking, phone banking, EDC machines, debit or credit card payment etc. Such a responsibility enjoins the group to invent electronic-banking products, whereby the technology creation and maintenance aspects are handled by the IT Planning, Architecture, and BCP group. The Electronic Banking group also has to formulate and enforce the formats and the use of personal identification number (PIN) for electronic-banking products among others. As such, the group enforces how these products are to be properly used to maintain information security. According to the Assistant to the Mass-Banking Vice President, the framework to maintain the information security of an electronic-banking product is:

> “First of all, staff members that are involved in developing the card are sworn by employment contract to protect the information about such a product. We regard the development of a banking product as a program or project. Hence the staff members also understand their duties and know what information is confidential or which of it can be put up for public consumption who again vary according to the categories they have been assigned. For instance, news reporters will be asked to identify themselves, the organization to which they are affiliated, why they need to access our information, etc. Another example is our newly launched program by which a customer shops at a local market and receives a local brand of juice for free. We cooperate with the local market that sells the juice and the juice distributor. We agree by law and contract that we won’t disclose each other’s data. For instance, if we would like to disclose to our customers that they can receive similar benefit at other local market, we need to ask permission of the local market that is bound to us via our legal cooperation.”

The formulation of information-security policies and regulations, particularly the SPO, marks the script encoding in the Centro Metropolitan Bank case. As a large financial institution and a formal organization, Centro Metropolitan Bank initiates such formulation based on risk management.

In the later section that describes an actual case, the formulation of policies and regulations came to be initiated after an incident of fraud. The policies and regulations serve as guidelines for governing and practicing information security in Centro Metropolitan Bank.

5.3.1.2. Principles Enactment: The regulatory body of information security in Centro Metropolitan Bank is assumed to be the Information Security Department. In fact, all actions concerning information security from the level of branches to even the headquarters is centralized from the information security department. The department assumes full authority and responsibility for overseeing information security in the bank. Using a technical illustration based on the network and infrastructure, the Vice President of IT Security Department states about the centralization as follows:

> "The technology infrastructure and network of the bank is star-shaped. Probably it can also be likened to the star network topology. It goes up from branches to headquarters. Right here at the IT security department is where security is enforced and controlled. We are the center for ensuring information security for the bank. All areas of IT operational are protected using relevant tools."

The branches are equipped with workstations, but do not maintain databases and function merely as clients. Servers (i.e., the core-banking) are installed on the 4th floor in the bank's headquarters and make use of IBM AS/400 machines. Servers installed at branches therefore only connect branches to headquarters. From a non-technical perspective, any action occurring at the branch level should be reported to headquarters. The report could be an initiative report, particularly reports for incidental cases such as any security breach. These reports are intended to report new products, organizational reformation or incidents. Branches have an autonomous right exclusively to maintain their lower-level operations (e.g., hiring and delegating branch staff). As indicated, however, maintenance of information systems and their security is a function which belongs to headquarters, with the information-security governance and control being delegated to the IT security department.

Other departments determine what information can be accessed, how it can be accessed, and who can access it through the aid of the IT Security Department. As for information security, the other departments provide conceptual plans for information-security implementation and delegate the technical implementation to the IT Security Department. The Electronic Banking Group also determines the logical implementation of security identification for electronic-banking products. For instance, to access the bank's electronic banking feature by using text messaging (i.e., the SMS banking feature), the bank regulates and enforces two modes of phone banking using PIN:

- Plain text: consumers may simply type in transactions using keypads.
- Real-time menu: consumers experience interactive banking transactions. All data is encrypted during transmission from server to customer's cell phone).

Whatever be the nature and type of the products it develops and maintains, the group consults and requests assistance from the IT Planning, Architecture and BCP group, particularly the IT Security Department, for the development of the products' security. Hence, the technological aspect of these products is developed and maintained by the Information Technology Department. In addition, any issue regarding these products, including security breach, is handled by a special investigation team comprising of the IT Security Department, the Mass Banking Group, the IT Audit Unit, and Board of Directors.

The implementation and practice of SMS banking, which is the bank's signature electronic-banking product, provides one such example. Similar to the case of Earl Capita Bank, data ownership seems to be the major parameter that determines how information and data can be shared among personnel of different departments within the bank. As such, other departments requesting access to data and information from a particular department need to provide a formal request to that particular department. Furthermore, the department that receives such a request needs to request access to the IT Planning, Architecture, and BCP group since data and information belong to the IT Planning, Architecture, and BCP group, which is physically housed at the 4th floor of the headquarters building. The group finalizes the request and provides the access permission. For example, personnel from other departments are required to provide formal request to the Electronic Banking Group should they intend to access e-banking data. The E-Banking Product Manager verifies this notion:

> “If a department wants our data, they have to make the request to me. For instance, it could be a request by the Customer Care Department for the purpose of producing a report on the total new customers for this month. That request should be addressed to me, the owner of that product. But in order for me to get that data, I have to request the data from the IT Planning, Architecture, and BCP group. But again, we act as the final doorkeepers to the data because they’re not supposed to make such a request to the group directly. All requests to access e-banking data and information should be made through us."

Therefore, the difference between data ownership in Centro Metropolitan Bank and Earl Capita Bank is in the power and authority of the division/department that oversees information security. The data ownership issue displays a strong sense of power over the use of and protection of data. Information stewardship as in Centro Metropolitan Bank on the other hand merely emphasizes on data protection and recovery (Baldwin et al. 2011). In Centro Metropolitan Bank, while departments address a formal request to an information-steward department, that department is required to submit another request for grant of access to the main IT department, which is considered the owner of the data and information. Centro Metropolitan Bank also has developed a dual-approval procedure, which is a manifestation of exercising control as is directed by the central bank. This essentially refers to a procedure of applying for approval to two bodies of authority before a request can be granted. The data access request is an example of a dual approval, whereby the teller has to request an approval from the head teller when the head teller faces the decision to act beyond her authority.

The principles of the enactment of information security institutionalization in Centro Metropolitan Bank can be summarized as a framework aimed at preventing and managing fraud. The components of such framework include details such as:

- Multiplicity of personnel performing duties: each task is performed by several personnel, departments, or a taskforce consisting of personnel from different departments.
- Individualized access levels: this concept is similar to the access privilege whereas each personnel involved in a specific task is given an access right according to his or her unique role in the task.
- Dual control and approval.
- Supervision.
- Transaction and post transaction control.
- Exception reports: reports generated to detect unusual transactions.
- Workflow.

- One-way passwords: each transaction request needs to pass the system supervisor. The system supervisor determines the access eligibility of the individual presenting such a request.

5.3.1.3. Script Replication: As a commercial bank with nationwide operations, Centro Metropolitan Bank owns branches, ATM machines, and EDC machines distributed throughout the geographical expanse of the nation. The operational aspects of these entities are managed by regulations issued by headquarters and these regulations reflect the unique culture of Centro Metropolitan Bank as a corporation. The Operational Risk Management Team Leader says:

> “All policies and procedures are determined at management levels. There is no way anyone can create and implement procedures if there is no referring policy. These procedures are not just for people at headquarters, but also for every stakeholder of the bank. These procedures reflect our culture.”

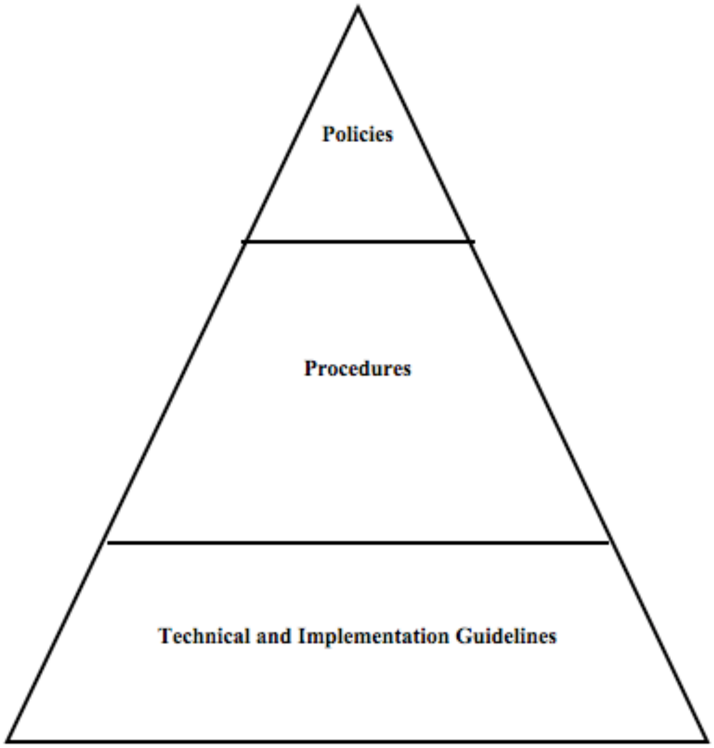


Figure 5.3 – The Triangle of Regulations of Centro Metropolitan Bank

The procedures, regulations, policies, and culture of Centro Metropolitan Bank are depicted as a triangle. The top of the triangle, which comprises the policies, is depicted as the highest level of regulations and functions across the bank. Policies are translated into procedures, which are strategic and end-to-end[6]. Each procedure pertains to a certain business unit within the bank and needs to be acknowledged and agreed upon by the board of directors. An example of procedures is the procedure to handle payment cards. These procedures belong to the mass-banking group. The procedures include:

a. Procedures to create payment cards.

b. Procedures to issue payment cards.

[6] This means that procedures need to be explicit and clear, and depict operational procedures from beginning to the end.

c. Procedures for use of payment cards by customers.

The lowest level, which is very unique to each branch or each merchant that uses the EDC machines, represents the technical and implementation guidelines. These guidelines are to be acknowledged and agreed upon by the head of business unit. Illustrating this point is the requirement that the use of EDC machines needs to be acknowledged and agreed to by a store manager before the machines can be adopted. Another example is the implementation of dual-approval procedure at local branches. The Operational Risk Management Team Leader talks about these risks:

> "We have to maintain and heighten controls at our branches and at stores that use our EDC machines. They are physically away from us here at the headquarters. We can't bear any consequences due to our failure to identify risks relating to people and procedure."

At these levels, all regulations are adopted and implemented according to the orders issued from the headquarters. Personnel and stakeholders (e.g., customers) at the lowest level reciprocate this sensitivity to security to support the bank's identity and culture. The replication of such regulations (i.e., scripted behavior) is present across the bank: from top level to bottom level and from headquarters at the nation's capital to regional and local branches. The paths of translating policies to technical and implementation guidelines signify the script replication whereby principles contained in policies are transferred and further developed from business units at the headquarter to guidelines at local branch offices.

5.3.1.4. Patterned-Actions Objectification and Externalization: Due to the great diversity and the number of people involved in the bank's operational activities, control is rigorously implemented at branch level and merchant level (for EDC transactions). This is because the likelihood of people- risk and procedure -risk becomes much more apparent at these levels. The degree of control required for handling such risks is higher to prevent manipulation by personnel. The E-Banking Product Manager says:

> "Once we had a case of deception by our branch staff. They were found to be playing around with our dual-approval procedure. That one time, a customer registered for our product and did not fill out his phone number. But a customer relation staff used her own number and asked her supervisor to approve the form. That could happen and it did happen. And then, when this form was verified, we found out that the phone number was the phone number of the staff's cousin. This incident was reported to us, and we immediately started thinking of steps needed to be taken to make our dual-approval procedure more effective. So my team and I sat down with IT, market operational risk, compliance, and audit, and discussed how to improve the procedure."

The biggest issue which arises with diversity is the protection and perpetual strengthening of the organizational culture. Due to the eclectic and diverse ethnic groups in Indonesia, diversity in culture causes Centro Metropolitan Bank to emphasize utmost on assigning authority to the headquarters. Local branches adhere to such authority. In information security, such authority in general determines how production, distribution, and storage of data is implemented. The biggest issue is, however, lack of security awareness. The Vice President of the Head Corporate Center Audit specifies this concern:

> "The biggest problem that we have is the lack of security awareness, especially at our lowest level. We put the onus to increase awareness responsibility upon our branch managers. They are then made responsible to raise awareness of local branch staff and customers alike. This responsibility allows managers to enforce the disciplinary act on staff failing to comply with security guidelines. The penalty is hierarchical and is categorized as follows: mild, medium, and severe. If there is a security breach at a local branch, the penalty is considered medium. The staff involved will receive warning and their misconduct will be recorded. They will also receive a salary cut for 6 months and a poor annual performance appraisal."

As such, branches are technologically linked with workstations connected to headquarters to enforce control. Every activity at branch level has to adhere to the policies and procedures enforced and are supervised by the Board of Directors and the Board of Commissioners. The dual-approval procedure is strictly enforced to ensure that personnel at the branch level comply with the policies and procedures. This procedure consists of verification steps that a supervisor needs to implement in order to verify the validity of a transaction.

As for EDC machines, merchants need to comply with rules about the use of EDC machines which are prescribed by the acquiring bank and the central bank. Centro Metropolitan Bank admits to the difficulty of controlling the EDC implementation, particularly when the bank is the issuing party[7]. This is because it is impossible for Centro Metropolitan Bank to supervise and control the use of its card products on EDC machines that have offline feature. The only opportunity that the Centro Metropolitan Bank has is to control its own EDC machines through regulatory mechanism and

[7] This means that Centro Metropolitan Bank is the issuing bank whose card product is used on an EDC machine that belongs to another commercial bank (i.e., the acquiring bank).

technology control. Centro Metropolitan Bank employs some of the strictest and most rigorous procedures for merchants who wish to obtain the bank's EDC machines (see part B of subsection 5.3.1.3). In addition, the bank maintains the security of its EDC machines by employing the following features:

- Content security: this feature uses various cryptography schemes.
    - Terminal line encryption (TLE): an encryption method that encrypts data before it is transmitted from the EDC machine to the host.
    - Pretty good privacy (PGP): this encryption method involves a third party (e.g., Visa or Mastercard). Data is encrypted before it is transmitted from Centro Metropolitan Bank to the third party.
    - Triple data encryption system (3DES): this is a feature to encrypt PIN numbers.
- End point security: this is a feature to secure entities such as laptop computers, servers, hosts, etc.
    - Host-based intrusion prevention system (IPS): a system that detects unusual activities at computer hosts end.
- Security management:
    - To consolidate monitoring of security tools.
    - To adhere to international and local standards and frameworks.

The drive to conduct such practices is a part of the bank's effort to maintain its vision and mission and to better serve its customers. These practices demonstrate how doing so or using the given tools becomes a rational habit and a routine among not only bank personnel, but also its customers and third-party card issuers.

5.3.1.5. Case: Electronic Data Capture (EDC) Fraud: This subsection presents the security breach incident that occurred at Centro Metropolitan Bank in late December 2009. The case has never been publicized and is still undergoing investigation. This subsection is divided into two parts: the incident and the aftermath.

A. The Incident: In general, the EDC fraud case is an information security breach case in which a fictitious merchant, a fictitious customer, and subsequently a fictitious transaction resulted in financial loss to a commercial bank. Parties other than the fictitious merchant and customer directly involved in this case, which occurred in late December 2009, include Centro Metropolitan Bank and another commercial bank, Silver Blue Bank, which suffered from financial loss. This case also drew attention and intervention from Earl Capita Bank, which acted as an intermediary between the two banks and also as a consultant. This case indirectly involved a credit card issuer, which in this case was Visa. The case has never been made public as it is capable of causing significant damage to the reputations of both commercial banks involved.

The case became a subject of serious attention when Silver Blue Bank, as the acquiring bank, sent a chargeback on February 2010 after settlement (Base 2 transaction) occurred. However, the Base 1 transaction, which was the requesting transaction, had never occurred. This is due to the fact that Silver Blue Bank had allowed the use of offline transactions involving debit card, a feature that should not be permitted for non-credit transactions in Indonesia. Debit card is less secured compared to credit card since debit card relies only on magnetic strip as an identification mechanism. Furthermore, magnetic strip is not embedded with fraud detection aids. Since the Base 1 transaction never existed, the credit card issuer could not debit the issuing bank (i.e., Centro Metropolitan Bank); hence payment could not be made in favor of Silver Blue Bank. If the transaction had been made online, Centro Metropolitan Bank would be able to immediately reject the transaction during the Base 1 transaction. However, the offline transaction allowed only for card number verification but was not able to verify the magnetic strip.

The perpetrator of this fraud was very familiar with Centro Metropolitan Bank's Bank Identity Number (BIN), which comprise of the first five digits of a debit card number. The perpetrator also had knowledge of transaction procedures using debit card and the offline transaction feature that Silver Blue Bank offers. The perpetrator was able to withdraw more than US $ 1 million and committed the crime from various spots in Jakarta. To commit the crime, the perpetrator created and used a fake debit card that used Centro Metropolitan Bank's debit card characteristics and obtained an EDC machine from Silver Blue Bank using a fictitious identification and false requests. The ease with which he was granted a product shows the leniency of the procedures in Silver Blue Bank. Centro Metropolitan Bank's procedures require prospective customer to provide proof of merchant permit, location permit, and applicant validity. Centro Metropolitan Bank also demands proof of administrative legality and business continuity (i.e., product shall not be granted if business is on the verge of bankruptcy).

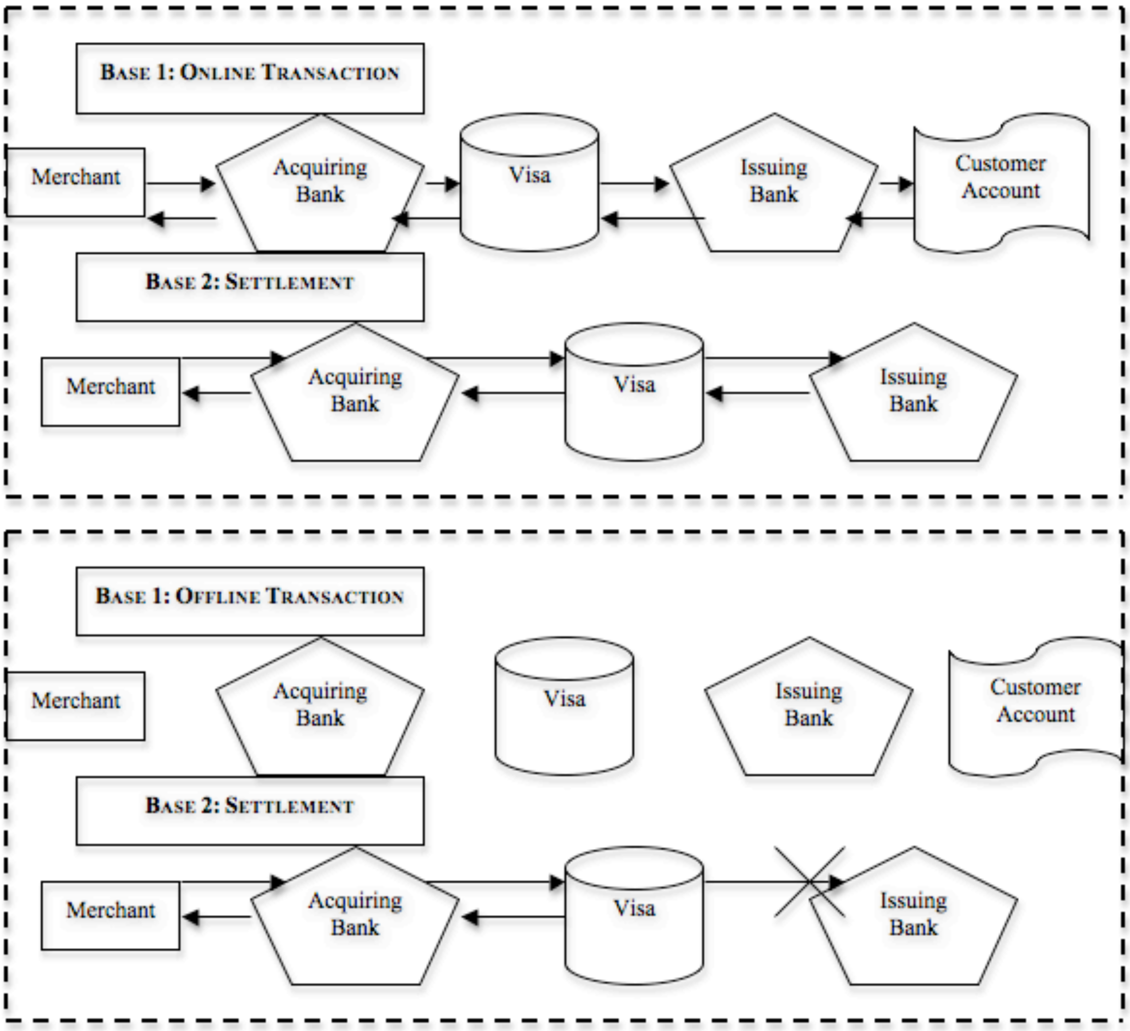


Figure 5.4 – Two Modes of Credit Card Transaction

Figure 5.4 describes the transaction processes using a credit card. The top box depicts a credit-card transaction process using an online mode EDC. An online-mode EDC transaction allows for direct customer verification as depicted by the base-1 procedure. When a customer enters his credit-credit identifiers (e.g., credit-card number and expiration date) or swipes his credit card, the merchant's EDC machine forwards the identifiers to the acquiring bank that owns the EDC machine, requesting for customer verification. The acquiring bank acknowledges the request and forwards the request to the credit-card issuer (e.g., Visa or American Express). The credit card issuer acknowledges this request and forwards it to the issuing bank, which is the bank to which the customer belongs, for verification and validation. The issuing bank then verifies the validity of the customer and sends back the verification. The objective of the settlement process, which is depicted in the base-2 transaction, is to make the payment request to the issuing bank by the merchant through his acquiring bank. In an online electronic credit-card transaction, the merchant requests for the payment by sending a request to the acquiring bank. The acquiring bank sends the request to the credit-card issuer, which forwards the request to the customer's issuing bank. The issuing back acknowledges the request and deducts the payment from the customer's account.

The lower box, however, depicts the offline electronic credit-card transaction. This type of transaction is one that was implemented by the Silver Blue Bank and the perpetrator for the EDC fraud case. The base-1 transaction demonstrates the merchant's assumption that the customer is valid during the initial transaction. In the offline-mode base-1 transaction, the merchant accepts the payment that will be credited during the settlement at a later time. In other words, the merchant does not immediately validate and verify his customer. The merchant does so when he sends a payment request to the customer's issuing bank. The problem emerges when the customer or the credit card is fictitious. When the acquiring bank sends a request for a payment that is based on either a fictitious customer or a fictitious credit card, the issuing bank rejects the request as shown in the base-2 settlement transaction. Unable to retrieve the payment, the credit-card issuer requests the payment from the acquiring bank instead causing the acquiring bank to pay up and lose money.

In this instance, after Centro Metropolitan Bank rejected the chargeback, Silver Blue Bank and Centro Metropolitan Bank both contacted their respective bank supervisors at Earl Capita Bank. They also consulted about the case with their respective accounting and payment system supervisors at Earl Capita Bank. Both banks realized that if the case became public, they would suffer damage to their reputations and credibility in the eyes of the public. In addition, Silver Blue Bank suffered a financial loss of more than US $ 1 million. The accounting and payment system supervisors of Silver Blue Bank examined Centro Metropolitan Bank systems and demanded progress reports on resolution, action plan, and mitigation progress from Centro Metropolitan Bank through the Audit Department. Progress was monitored and reports were requested and delivered from January 2010 to March 2010. In addition, Earl Capita Bank also conducted random inspections of all EDC machines as an attempt to ensure that EDC machines were being used for online transaction only. One of the members of the perpetrator syndicate was apprehended. The case is still under investigation as of now.

B. The Aftermath: When an exogenous event such as an incidental case occurs, a formal organization strives to return to social stability. In the case of Centro Metropolitan Bank, such an effort entails attempts to diminish any damaging impact caused by the EDC fraud incident. Internally, Centro Metropolitan Bank formed a taskforce to handle this case. The objective of the taskforce formation is to investigate any serious incident such as the EDC fraud incident and to coordinate the implementation of preventive measures and actions. The taskforce consisted of personnel from the IT audit unit as well as the team coordinator, IT Security Department (a subsidiary group of

IT Planning, Architecture, and BCP subdivision), Customer Care Group, and Electronic Channel Operation Unit. The duties of the taskforce are as following:

- Assessment of the losses suffered by Centro Metropolitan Bank.
- Indicating latent risks that potentially threaten Centro Metropolitan Bank in the long run.
- Remedying the acquiring process of Centro Metropolitan Bank's EDC machines.
- Planning actions to remedy any loss and to prevent similar incidents in the future.
- Reporting the action plans to the Board of Directors.

In addition, Centro Metropolitan Bank also launched the following projects of:

- Enhancing the security of Centro Metropolitan Bank's EDC machines.
- Reformatting the merchant acquisition policies to ensure the existence of no fictitious merchant.
- Forming a new unit whose task is to monitor transactions involving debit card and guarding against any misuse or fraud concerning the card. This was done because earlier this unit was a part of the credit card unit.
- Modifying/reformatting the back office that handles electronic transactions so that it is able to immediately detect a transaction that is marked or indicated as a possible fraud.

These efforts can best be described as controlled maintenance. Controlled maintenance can be perceived as a period in time when structure becomes stabilized and hence rules and habits become typified and grounded. Controlled maintenance is ultimately stated as a post condition to the institutionalization and *a priori* condition to an incidental or exogenous event. As such, when institutionalization occurs, controlled maintenance emerges over time through habitualization of resource use. Controlled maintenance, however, also signifies an activity that is initiated as a result of a security breach incident after which the enforcement becomes heightened due to the strong involvement of the central bank. Therefore, the objective of controlled maintenance is to promote social order and stability in the organization. In terms of electronic banking transactions, the E-Banking Product Manager describes this controlled maintenance as follows:

> “We provide policies for customers who wish to use our SMS (i.e., text-messaging) banking system and educate our customers on how to use this system. For example, they are required to create a PIN during feature activation and we show them how to do this through pamphlets. This breakthrough program is not a required electronic banking product decreed by the central bank.”

The objective of the Bank’s controlled maintenance and task-force formation is therefore to maintain social order and preserve social stability. The patterned-actions objectification and externalization is a final process preceding a re-institutionalization, creating a new episode of institutionalization. Centro Metropolitan Bank, suffering from a serious incident that threatened its reputation, has put every effort into retaining the already formed patterned-actions. The result of implementing controlled maintenance and taskforce formation is an implementation of preventive measures, which the Head of IT Audit Unit concurs with:

> "We continue to take serious steps to prevent any case similar to this EDC fraud case from happening in the future. For example, we created a new unit that specifically monitors and controls electronic debit-card transactions and enforces the policies of such transactions. We also reformatted our back office that handles electronic transactions to enable early detection of suspicious transactions. This case also attracted several preventive actions by the central bank. The central bank has ordered that all EDC machines are to be used for online transactions only. So no more offline EDC machines! There is a six-month grace period to allow all commercial banks to change their EDC machines."

The newly reformatted back office emphasizes on the importance of reporting unusual transactions (e.g., a base-2 transaction that is not preceded by a base-1 transaction for debit-card transactions). The initial focus was on the use of technology. However, the mere utilization of technology has proved to be less reliable due to human creativity and the general customer's lack of security understanding. The Vice President of IT Security Department confirms this statement:

> "Most security cases are not caused because of technology failure. People can be very creative. They can simply put a stick of cigarette matches inside the ATM's card reader so that any card inserted gets stuck. When the gullible customer gets confused, and obviously starts panicking, the criminal steps in, disguised as our technical support. When he succeeds in getting the card back, he gives a false instruction to our customer, telling her to hand over the card and her identification to him for further investigation."

The reporting mechanism is therefore a combination of human effort and technology operation. In addition to reformatting its back office, Centro Metropolitan Bank also enhanced its EDC machine features, mainly to prevent offline transactions. Such efforts depict Centro Metropolitan Bank's intention to reorganize its operational activities by addressing the major obstacle (e.g., security breach incident). Such efforts have redirected the operational activities into becoming a habit and an action that is taken for granted.

5.3.1.6. Discussion: Centro Metropolitan Bank views technology as an artifact that is created by humans and used by them to aid them in their daily activities. The interaction between humans, who act as the agency, and technology, provides meaningful attributes to the technology as it becomes useful to humans. Technology alone does not commit any crime, the combination of humans and technology, however, has a potential to cause damage to an institution, including Centro Metropolitan Bank. In addition to technology, the bank therefore, carries a strong belief that threat to information security may be due to human factor. The practice of securing its information is in compliance with the definition of operational risk by Basel II. When auditing the bank's information systems, the auditory team of the audit unit investigates factors that contribute to operational risk: people (e.g. faults due to human error or lack of responsibility), process (e.g. false procedures), external factors (e.g. hackers or outsiders), and system (i.e., technology) (Scandizzo 2005; Flores et al 2006: p. 384). Many procedures and standards are formulated in a way that belongs to and is comprehended only by bank's personnel and customers. These procedures and standards are developed using ISO 27001 framework, particularly for specific scope such as one that regulates data center. To audit the bank's information systems and their security, the auditory team uses a combination of ISO 27001 and COBIT (i.e., for high level maintenance use such as governing risks related to the use of information technology). In addition to these frameworks, procedures and standards are formulated to conform to and reflect regulations as issued by Earl Capita Bank. These procedures and standards become a habit and are communicated among personnel, forming and reflecting the culture of Centro Metropolitan Bank.

The view that humans and technology together may cause harmful impact is adopted by Centro Metropolitan Bank. This view is a fundamental notion of the socio-organizational view of information security. Similarly, this interaction enables the emergence of behavioral and cognitive (e.g., power, communication, sanction, etc.) properties in the information security institutionalization. As such, the central notion to this is that of technology as an artifact. The procedures to access technology in Centro Metropolitan Bank are centralized as they are maintained by the IT Security Department. As such, the interaction between personnel and technology is regulated by the bank whereby such interaction shapes the bank's structure and needs to be secured in order to maintain the bank's existence.

The practices and implementation of information security in Centro Metropolitan Bank are almost exclusively directed by the IT Security Department. The IT Security Department enjoys the privilege to direct the three information-security controls (i.e., technical, formal, and informal). The formal control, however, is shared with other groups or departments that own and manage the manual format of the automated banking feature or product. The technical control and the informal control are therefore the exclusive privilege of the IT Security Department. Unlike that of the Earl Capita Bank, the governance of information security in Centro Metropolitan Bank is centralized.

Centro Metropolitan Bank relies on Basel II's definition of operational risk. This definition highly emphasizes on people, process, external factors, and system and believes that the functions of any system depend on people and process. Centro Metropolitan Bank mandates one department- the Information Technology Department, to maintain and regulate information systems and security, through its IT security unit, within the bank. The IT audit unit functions to ensure that the operations of Centro Metropolitan Bank's information systems support the operations of Centro Metropolitan Bank in general. Security breach cases in Centro Metropolitan Bank are generally individual cases of security fraud at branch level and hence the appropriate actions are usually taken by the branch management. Each branch has autonomy (i.e., independent power). Each branch usually delivers regular reports regarding any activity as well as any newly launched product, reorganization, or incidental case to headquarters. However any action involving the use of information systems and security needs to involve the bank's headquarters. The Head of IT Audit Unit explains:

> "Autonomy here means that branch may formulate its own policies within its scope. If it involves system, management needs to report to the ones 'above'. For instance, if a branch says they want an IT operational staff, they will have to make a request to the headquarters. If branch were given autonomy for the entire system, that would be very difficult since our systems are very diverse."

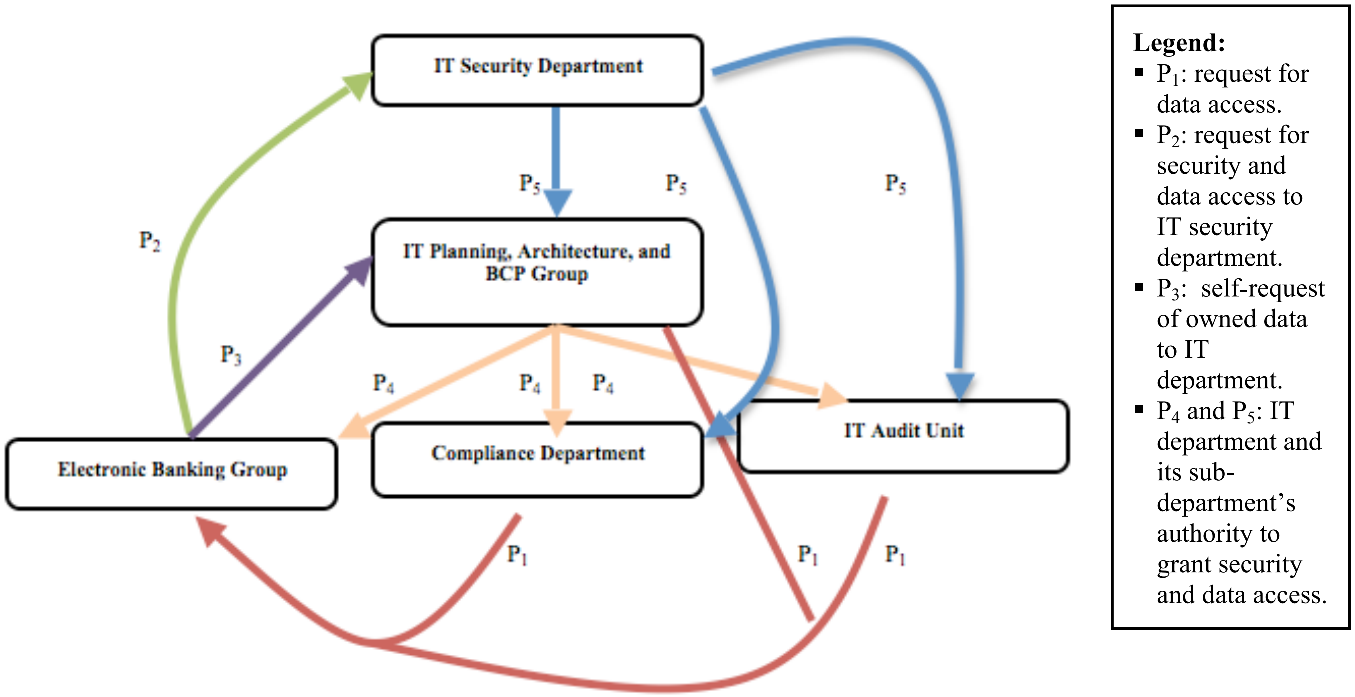

IT Security Department
IT Planning, Architecture, and BCP Group
Electronic Banking Group
Compliance Department
IT Audit Unit
P_5
P_5
P_5
P_2
P_3
P_4
P_4
P_4
P_1
P_1
P_1
Legend:
P_1: request for data access.
P_2: request for security and data access to IT security department.
P_3: self-request of owned data to IT department.
P_4 and P_5: IT department and its sub-department's authority to grant security and data access.

Figure 5.5 – The Flow of Information Security Authority and Responsibility in Centro Metropolitan Bank

Unlike Earl Capita Bank, each department in Centro Metropolitan Bank needs to send a request to the Information Technology Department in order to access data, as IT Department is supposedly the information steward. Hence, access to data is regulated by the IT security department, while other departments own the privilege to process data according to their own need. For instance, if the electronic banking group needs to request for access to the Internet banking data, the group sends the request to the IT Security Department. According to its needs, the electronic banking group is given the access and modification privileges to process and analyze the Internet banking data to recreate other electronic-banking products and regulations. Figure 5.5 above shows the implementation and practices of information security among divisions in Centro Metropolitan Bank. P_1 denotes divisions requesting for electronic-banking data and access to such data to the electronic banking group. P_2 entails the electronic banking group making security and access requests on behalf of the divisions to the IT security department. Interestingly, P_3 entails the electronic banking group making data request for itself as well as other divisions to the IT planning, architecture, and BCP group. P_4 and P_5 denote the divisions' authority to grant data access and security access, with P_4 specifically denoting permission to use data by the IT planning, architecture, and BCP group while P_5 denotes access privilege by the IT security department.

The institutionalization of information security in Centro Metropolitan Bank can be simplified according to episodes T1, T2, and T3. Each episode denotes all the four institutionalization processes: script encoding, principles enactment, script replication and or revision, and patterned-actions objectification and externalization. Episode T1 denotes a condition prior to the EDC fraud incident. Episode T2 depicts a situation when the incident took place in which each process demonstrates the efforts undertaken by Centro Metropolitan Bank to cope with the impact. Episode T3 emerges as an effect of such efforts in episode T2, in which social order and stability have successfully been maintained. Script encoding in episode T1 describes a situation when Centro Metropolitan Bank adopted the guidelines given by Earl Capita Bank, taking into account Centro Metropolitan Bank's unique culture and additional regulative frameworks (e.g., Basel II, ISO 27001). When principles are enacted in this episode, Centro Metropolitan Bank's personnel began to adopt the recently formulated regulations into their everyday operational activities. Moreover, personnel manage to habitualize their action as script is further replicated. This is because there is no incident or event that affects a change in Centro Metropolitan Bank as an institution. An example of this situation is the regular practice of information security and governance, which pervades every place from headquarters to local branches. Finally, the moment when personnel's action becomes successfully habitualized and hence institutionalized denotes the patterned-actions objectification and externalization. In episode T2, script encoding is preceded by the EDC fraud incident, resulting in much of the encoding effort initiated by the strong influence of the central bank. The subsequent institutionalization processes denote the bank's struggle to overcome the impact of the incident by implementing the orders issued by the central bank. Script revision applies in lieu of script replication since the incident caused a dramatic change in the institution and personnel are aware of such change and crave for improvement. Script encoding in episode T3 depicts a situation when regulatory efforts take into consideration previous efforts in episode T2. The subsequent processes in this episode repeat the processes of principles enactment, script replication, and patterned-actions objectification and externalization in episode T1 with the difference being that these processes signify successful maintenance of social order and stability.

5.3.2. Relationship with the Central Bank

5.3.2.1. The Macro-Prudential Supervision of Information Security Governance: A risk that becomes an actual threat with the potential to cause a devastating impact on the bank and public in general is regarded as a reputational risk. Any imminent threat related to reputational risk will often invite the central bank - Earl Capita Bank to interfere and help in finding solutions to combat such a threat. As a regular practice in adherence with Earl Capita Bank's policies and regulations, Centro Metropolitan Bank, as a commercial bank, delivers regular (e.g. weekly, monthly, or annual) reports to Earl Capita Bank and welcomes auditory visits by a team dispatched by Earl Capita Bank. Owing to its own diligent reporting practice, Centro Metropolitan Bank attempts not to involve Earl Capita Bank in issues that it is confronting; rather the commercial bank strives to conform and abide with Earl Capita Bank's policies and regulations and to consult with Earl Capita Bank when necessary. The interference by Earl Capita Bank often results in bad publicity for a commercial bank since it may be perceived as being unreliable and unable to resolve its own problems.

Despite the effort to avoid interference by Earl Capita Bank whenever issues or emergencies arise, regular activities (i.e., regular reports by Centro Metropolitan Bank and regular auditory visits by Earl Capita Bank) are administered through "one single door", which is the Compliance Department. This department assumes a major responsibility to deliver reports and written progresses to Earl Capita Bank. It also assists departments in composing reports so that the requirements and format of deliverables conform to those enforced by Earl Capita Bank. The Compliance Department is the backbone for the bank's institutional relationship with Earl Capita Bank. The Vice President of Compliance Group confirms this in terms of the bank's institutional relationship with the central bank in the following words:

> "The objective of our group is to represent our bank in maintaining institutional relationship with the central bank. This relationship hinges on our obligation to provide any activity report to the central bank. In return, they are watching over us too. An important impact of this relationship is that we are required to adopt and implement statutes and guidelines enacted by the central bank. All commercial banks are required to abide by the laws enacted by the central bank and penalties are enforced on banks that fail to abide. Of course, we select and evaluate only those that are relevant to our culture.

> Keep in mind that not all the statutes and guidelines can have significant impacts on our operations."

The practice of regular reporting begins with creating lists, which depict the recognized and inventoried bank's responsibilities. These lists are passed to the corresponding departments in charge of maintaining practices of certain items in the lists and the person in charge within such department is to elaborate upon the report. In essence, this department strives to maintain good institutional relationship between Centro Metropolitan Bank and Earl Capita Bank. Penalties are, however, imposed whenever there is an error in reporting or late delivery. The Vice President of the Compliance Department remarks on penalties, whereby:

> In general, penalties are awarded when report delivery passes its due date. Another reason for penalty is due to typing error in the report. For instance, there was an incident by which a branch was trying to submit a report online, instead of typing of 3 million, the person in charge typed 3 thousand. But this incident was immediately red-flagged and handled so that penalty could be avoided."

As the central bank, Earl Capita Bank, equipped with its deontic power, controls all operational activities of commercial banks, including Centro Metropolitan Bank. The implementation of such a control is based on the principles and guidelines that Earl Capita Bank issues and enforces. Such control is also applied to operational routines (e.g., e-banking products monitoring) in addition to control practices for incidental cases. This control lays much less emphasis on punishment unless extraordinary impact takes its toll on operational routines. In addition to the statement on electronic banking products, the E-Banking Product Manager makes another statement regarding the central bank's control on electronic banking products:

> "…This breakthrough program is not a required electronic banking product decreed by the central bank. The central bank, however, pays close attention to this service to ensure that it's working properly and it does not harm confidential data and information."

Not only does Earl Capita Bank oversee the governance and implementation of information security in Centro Metropolitan Bank, but Earl Capita Bank also exercises its deontic power to interfere into Centro Metropolitan Bank's incidental cases, including security breach incidents. Earl Capita Bank plays its role as an external governing body by summoning Centro Metropolitan Bank's representatives for risk education, demanding intensive reports on mitigation progress, and dispatching auditory teams. With regard to the EDC fraud incident, the Head of IT Audit Unit says:

> "…The central bank also dispatches a team to randomly inspect merchants whether their EDC machines have been changed by their host bank to conduct offline transactions only."

In terms of information security case, the reporting practice is similar to the reporting practices of other cases and itemized reports. The reporting practice of information security case may be delivered by the Compliance Department, or not. . This decision depends on the nature of complexity of the report. If the case to be reported is delicate, the report is then composed with the assistance of the Compliance Department and is also delivered by the Compliance Department. If the case involves inputs from various departments in addition to the IT Security Department, the Compliance

Department shall act as a coordinator for these departments. Before the report is delivered to Earl Capita Bank, it is reviewed once more by the IT Security Department and passed on to the Board of Directors to be challenged and debated. The final draft is then signed by the Board of Directors and delivered to Earl Capita Bank.

5.3.2.2. Discussion: This section can be summarized using Scott's multilevel institutional processes, similar to the discussion of the same section in the previous chapter. The focus of this section is trained on Centro Metropolitan Bank's institutional relationship with the central bank.

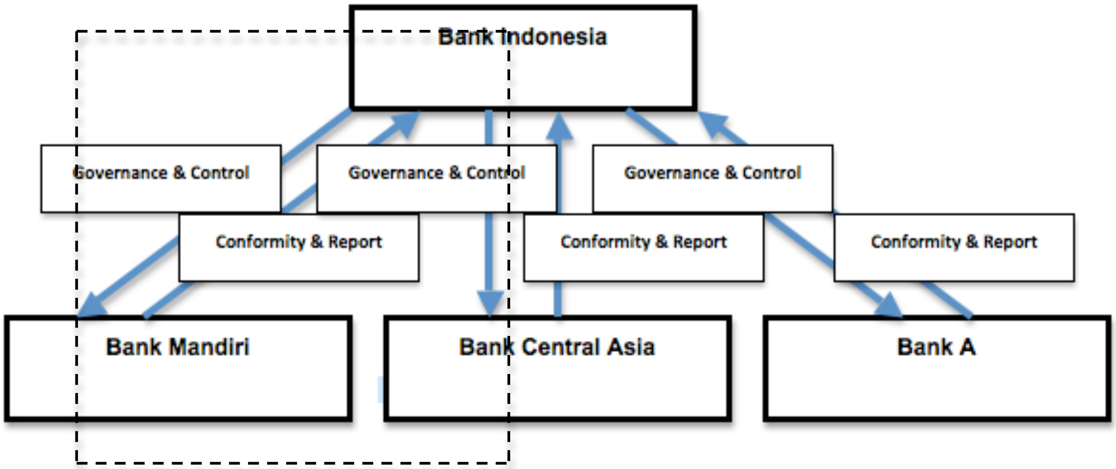


Figure 5.6 - The Institutional View of Information Security Governance Focusing on the Governance Relationship between Earl Capita Bank and Centro Metropolitan Bank

Figure 5.6 depicts the institutional view of the information security governance of Centro Metropolitan Bank which is governed and controlled by Earl Capita Bank. Similar to the theory covered in the same section of the previous chapter, the line with the arrow facing towards Centro Metropolitan Bank depicts the governance and control of information security practices by Earl Capita Bank. The governance and control practices include controls on operational routines such as overseeing of the correct implementation of electronic banking products according to prescribed regulations (Van Greuning and Bratanovic 2000), demanding reports on information security implementation, raising information security awareness, and auditing information security implementation. The line with the opposite direction depicts the conformity and report of information security practices by Centro Metropolitan Bank to Earl Capita Bank. This one-to-one governance and supervisory relationship, which focuses on individual institutions, signifies the micro-prudential supervision relationship (Khoury 2009; Krauskopf and Steven 2009). As indicated earlier, the micro-prudential supervision of information security in Centro Metropolitan Bank is administered by the Compliance Department in a manner called "single door." The representative tasks include providing regular or requested reports to Earl Capita Bank and assisting Earl Capita Bank's audit team during auditory visits. The formal relationship between Earl Capita Bank and Centro Metropolitan Bank, particularly in terms of information security governance and practices, stems from uncertainty avoidance and power distance between the two institutions (Shankarmahesh et al. 2003).

5.4. Conclusion

Centro Metropolitan Bank is a large government-owned commercial bank which has come into being as a result of the merger of four large government-owned commercial banks. Three of the four government-owned commercial banks originated from Dutch commercial banks and underwent the nationalization process after Indonesia gained its independence in 1945. The economic crisis that hit almost all nations in Asia, including Indonesia, in 1998 plunged the country into financial difficulty. Troubled commercial banks were either abolished or merged and restructured. The four large government-owned commercial banks were merged and restructured to become what is now known as Centro Metropolitan Bank.

The objective of this chapter is to discuss and analyze the case study of information security in Centro Metropolitan Bank. Centro Metropolitan Bank is deemed to become an example for other commercial banks in terms of IT and security governance practice. Unlike Earl Capita Bank whose information security governance is shared by two departments, Centro Metropolitan Bank empowers its IT security department to oversee the governance of information security. The governance, however, is not exclusively enjoyed by the department. The department is required to share the implementation of the logical security regulations. An example of this being the regulations that require the use of username and password to gain access to the Internet Banking, formulated and governed by the Electronic Banking Group.

An incidental case, such as the EDC fraud, demonstrates government's intervention through the deontic power and constitutive power possessed by Earl Capita Bank. The case depicts a fictitious transaction using credit card made possible by an offline-mode EDC. In addition to the delineation of deontic power and consecutive power, the case also demonstrates that implementing information security is a responsibility shared among all subjects within an institution. This evidence is obvious as Centro Metropolitan Bank formed a taskforce that consists of not only personnel of the IT security department, but representatives of other departments to investigate the case of fraud.

6 THE CASE OF BLUE SEQUOIA BANK

6.1. Overview

Similar to the case presented in the previous chapter, the case of Blue Sequoia Bank also provides insightful depiction of the governance and practices concerning information security in a large commercial bank. Blue Sequoia Bank is one of the large banks in Indonesia and is a private commercial bank that has the capacity to leave substantial systemic impacts on the nation's financial well being. As a commercial bank, the bank provides a wide array of services to its customers, including electronic banking, deposit accounts, export-import facilities, and foreign exchange facilities. This chapter focuses on the implementation of governance and practices of information security in a private commercial bank.

In Blue Sequoia Bank, the information security implementation invites lesser intervention from the government compared to Centro Metropolitan Bank as outlined in the previous case study. Therefore, it can be safely assumed that the difference between a government-owned commercial bank and a private commercial bank may lie in the extent of government involvement. As in the previous case study, the case of Blue Sequoia Bank also begins with the background description. It proceeds with details about the governance and practices of information security within the bank and the impact of the Central Bank's governance on the internal practices of this bank.

The objective of this chapter is similar to the objective of the previous chapters: to provide a theoretical depiction of information security practices and governance in Blue

Sequoia Bank. The organization of this chapter is as follows: Section 6.2 provides the historical background and characteristics of Blue Sequoia Bank. Section 6.3 provides the empirical analysis for the Blue Sequoia Bank case, consisting of the following: the bank's internal security governance and practices modeled using the structuration view of the institutional theory, the relationship between the bank and the Central Bank depicted by the institutional theory, the descriptive security incidental case of the skimming of automated teller machines, the interconnection between the structured security practices and the institution of information security, and the impact of technology on structured information security practices and vice versa. Section 6.4 provides the closing remarks and summarizes this chapter.

6.2. Organizational Background

6.2.1. A Private Commercial Bank

Blue Sequoia Bank (BSB) is one of the largest private banks in Indonesia. It is probably one of the few banks in Indonesia that own a large number of ATM machines distributed in almost every geographical region across Indonesia. It is also the bank that has the largest number of EDC machines used by merchants everywhere in Indonesia and provides sponsorships for many social and entertainment events. The bank provides a wide range of useful, efficient, and convenient services, which can be attributed to[1]:

1. A highly professional management team that is always on top of national and international banking policies and regulations.
2. Highly trained, customer-oriented human resources.
3. A bouquet of innovative products and services that meet real needs.

[1] Source: http://www.klikBSB.com/individual/silver/company.html?s=2

4. Appropriate use of the most advanced technology.
5. Relentless efforts to maintain the highest level of banking security.
6. A large network of branches and sub-branches throughout Indonesia.
7. A broad choice of distribution channels to ensure maximum banking convenience.
8. As on March 31, 2010 BSB has around 6710 cash ATM, non-cash ATM, and Cash Deposit Machines installed at strategic places throughout the country.

Blue Sequoia Bank's underlying objective is to always focus on the evolving customer requirements. The bank strives to achieve this objective by continually enhancing their products and services, i.e., adding more features to increase customer-banking convenience. For example, the bank rigorously adds more facilities such as ATMs, features and services for Internet banking, features and services for mobile banking, etc. In addition, the bank further tailors its services for its commercial and business customers. The following is a list of services provided by Blue Sequoia Bank:

Types	Name of Products or Services
Deposit Accounts	TAHAPAN savings, TAPRES savings, Demand Deposit, Time Deposit, CD
Credit Cards	BSB Card, BSB Master Card, BSB Visa, BSB JCB
Electronic Facilities	ATM BSB, DebitBSB, TunaiBSB, KlikBSB Internet Banking, m-BSB mobile banking, BSB Link,Call Center
Banking Services	Safe Deposit Box (SDB), fund transfer, travelers cheques, clearing, foreign currency
Loans	KPR (mortgage), KKB (vehicle loan), capital loan, syndicated loan, export credit, trust receipt
Bank Guarantee	Bid bond, payment bond, advance payment bond, performance bond, and Import Duty Exemption and Refund Center

Export-Import Facilities	LC, negotiation, bill discounting, documentary collections, bankers acceptance
Foreign Exchange Facilities	Spot, forward, swap and other derivative products

Table 6.1 – Products and Services Provided by Blue Sequoia Bank

6.2.2. History of Blue Sequoia Bank

The bank was founded on August 10, 1955 as the "*NV Perseroan Dagang Dan Industrie Semarang Knitting Factory*" and commenced operations as the Blue Sequoia Bank on February 21, 1957. In the 1970s, the bank provided additional channels, as it became the Foreign Exchange Bank in 1977. During the 1980s, the bank expanded its branch network and enhanced its information-technology services by establishing an online system for its branch office network. It also added new products such as saving accounts.

In the 1990s, the bank developed an ATM network as an alternative delivery channel and installed 50 ATMs in Jakarta and its vicinity. To enhance the ATM delivery-channel service, the bank cooperated with the nation's premier telecommunication provider and Citibank. This cooperation allowed customers to pay their phone bill or their Citibank credit-card bill through the bank's ATM. Throughout its long history, this bank too has undergone a lot of ups and downs. It most notably survived the severe 1997 economic crisis that hit Indonesia. However, the panic rush forced BSB to seek assistance from the government. As a result, BSB was one of the banks that were restructured and reorganized by the Indonesian Banking Restructuring Agency (IBRA). Eventually, the bank overcame the crisis in the following year due to its exceptional management and decision-making savvy.

The recovery was clearly evident: assets increased from US $5.9 million in December 1997 to US $7.5 million in December 1998[2]. Public confidence was fully restored and IBRA released BSB to Earl Capita Bank in 2000. BSB became a public company the same year and hence its shares were slowly diverted from IBRA until the agency had finally released 51% of its shares by 2002. A Mauritius-based financial institution, Farindo Investment Ltd., won the tender. Today, BSB holds the distinction of being one of the banks that exhibit good corporate governance, sound risk management, and strong commitment to the needs of customers. It also boasts of being the bank in Indonesia with the largest number of ATMs; by virtue of having 6000 ATMs distributed across Indonesia.

6.2.3. Organization Structure

The management structure and organization of Blue Sequoia Bank is similar to that of Centro Metropolitan Bank. The executive management team is the Board of Directors, led by a President Director. Similarly, Board of Commissioners, headed by a President Commissioner, supervises the management and governance practices in Blue Sequoia Bank. The only difference is that the Board of Commissioners is not appointed by the nation's government. For instance, the bank's main shareholder, Farindo Investment, appointed an American citizen to become the Chairman and President Commissioner of the bank in 2002[3].

[2] Source: http://www.klikBSB.com/individual/silver/company.html

[3] Source: http://www.institutionalinvestor.com/article.aspx?articleID=1026439

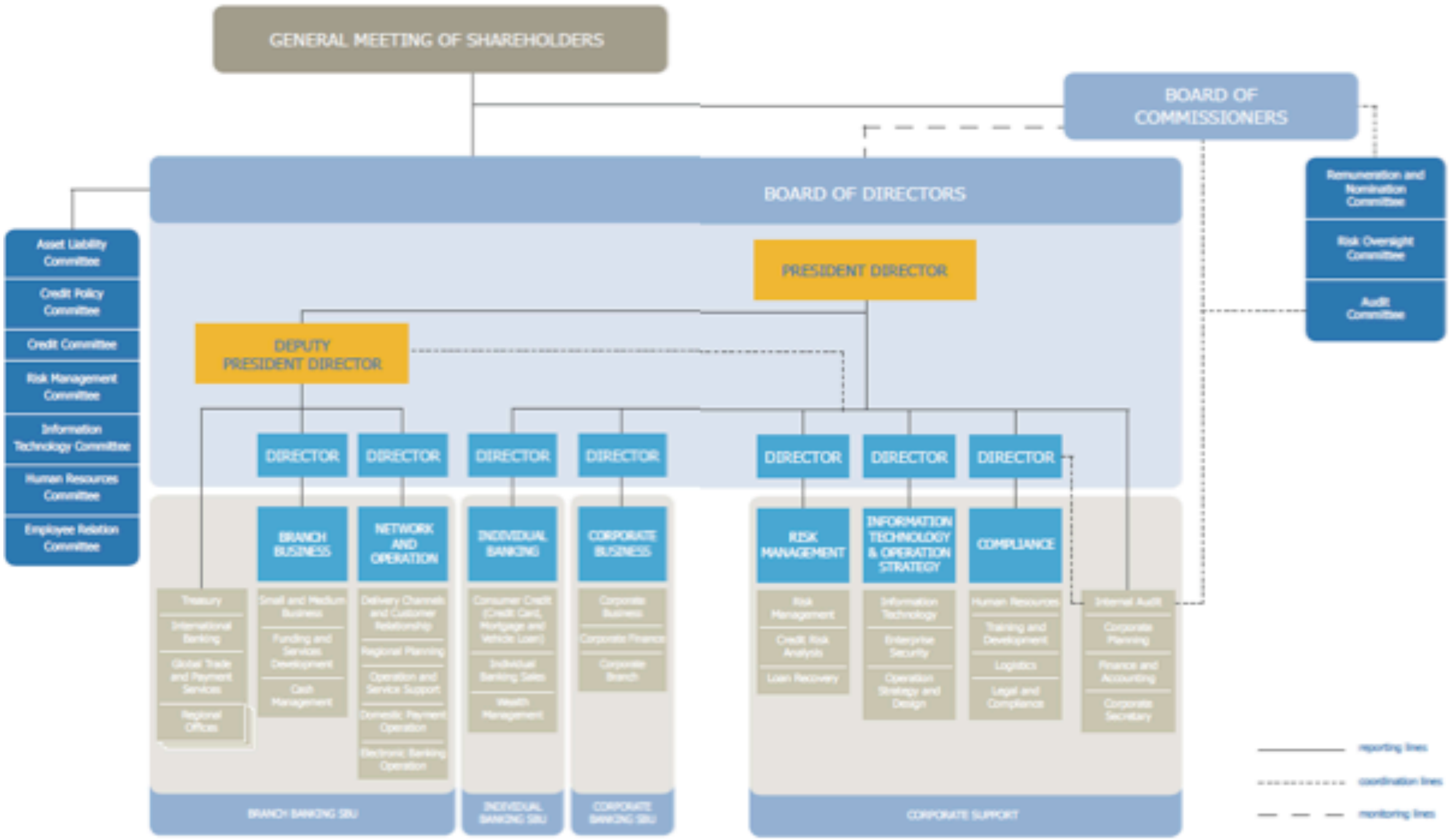


Figure 6.1 – Organizational Chart of Blue Sequoia Bank

Similar to the structure of Centro Metropolitan Bank, each division within Blue Sequoia Bank is managed by a Director and each division manages groups that perform certain functionalities and roles that support the bank's operational activities. The practices and implementation of information security in Blue Sequoia Bank are governed by the Enterprise Security Group. This group is listed under the Information Technology and Operation Strategy Division. This division is part of the Corporate Support Business Unit, which is one of the bank's four business units (i.e., Branch Banking Business Unit, Individual Banking Business Unit, Corporate Banking Business Unit, and Corporate Support Business Unit). Similar to the case of Centro Metropolitan Bank, the governance and practices of Blue Sequoia Bank are the sole responsibility and privilege of the Enterprise Security Group. In general, the Enterprise Security Group is responsible for not only the IT security system of the bank, but also the business continuity plan (BCP) for the bank. The Head of the Enterprise Security Group asserts this in the following words:

> "Our group manages the following: information security, physical security, and business continuity. Yes, this means that we also deal with business continuity. We have a unit that specifically handles business continuity and crisis as well as incident management. This special unit manages our disaster recovery plan and actions. The Business Continuity Management ensures that our operation is always continuous and crisis management takes care of incidents that could lead to a possible crisis such as dealing with power outrages."

With respect to this assertion, the Enterprise Security Group deals largely with the infrastructure and technical aspect of information security. The bank prides itself on having one of the most reliable Disaster Recovery Centers amongst all the institutions in the nation. Unlike those of the other institutions covered in this dissertation, the Disaster Recovery Center of the bank is located in a different geographical location from headquarters. The credit for these measures can be attributed to the group's belief that disaster recovery and business continuity represent the 'availability' element of information security's core elements: confidentiality, integrity, and availability.

6.3. Empirical Analysis

6.3.1. Internal Security Practices (Inter-Level Institutional of Information Security Governance)

6.3.1.1. Script Encoding: Similar to that of Centro Metropolitan Bank, information security implementation and practices at BSB too are handled by one department: the Enterprise Security Group. This department oversees issues in physical or architectural security and business continuity. Any policy regarding information security is initiated and conceptualized at the level of the Enterprise Security Group. Hence this department assumes the responsibility and privilege of formulating and enforcing policies and procedures regarding information security and business continuity. The initiation of these rules is based on corporate needs. For example, a security policy is initiated due to a need which has been analyzed and initiated by the Enterprise Security Group or in response to a need for a tighter application procedure for new customers' at a branch due to the localized culture and higher crime rate in the area where the branch is located. The Head of the Enterprise Security Group says:

> "The initiation is often made by us, especially if we feel there is an urgent need to make a new security policy and regulation. But sometimes, a branch feels the new policy restricts

> their freedom to conduct business and may request the modification of a policy in order to make it fit their needs better. Anyway, it doesn't have to be so rigid. We are very flexible."

As with policy frameworks for Centro Metropolitan Bank, the BSB uses ISO 27001 and ISO 27002 as its base frameworks for security policies and procedures. The main framework reference the BSB uses is ISO 27001 so that the bank can fully comply with regulations governed by Earl Capita Bank. Hence, the implementation of information security in Blue Sequoia Bank shows a similarity to security implementation in Earl Capita Bank. In Blue Sequoia Bank, divisions possess the authority and ownership to own and process information assets. The implementation in Blue Sequoia Bank however differs from that in Earl Capita Bank in terms of physical data ownership. This practice in BSB is rather similar to security implementation practice in Centro Metropolitan Bank. The Head of the Enterprise Security Group states this differentiation as follows:

> "Divisions own the right to own and manage their own data and information. If there is a request received to access data belonging to some division, the permission needs to be requested from that division. But we're the one that give the final access to the data. Take this case for example: a user from division A wants access to information which is owned by division B. Then, division A needs to make a request to division B. After which, we, the Enterprise Security Group, provide access to the information."

Similar to Centro Metropolitan Bank, even if a group or division is the Information Steward, the Information Steward still needs to make a request to access its data to the

Information Technology and Operational Strategy Division. The Head of the Electronic Banking Operation Group states the following:

> "That's right, we own the data. But we still need to make sure that they, the IT people, provide us access to our own data, this is because they have the server."

In practice, new information security policies and procedures are formulated by a task force which is coordinated by the Enterprise Security Group. This task force analyzes the gap between the bank's needs and the requirements by Earl Capita Bank. These rules are then finalized and approved by the Board of Directors. In terms of business continuity, the formulation procedures include studying the impact analysis, formulating strategies and procedures, and educating stakeholders. Through the Enterprise Security Group, the bank seeks helps from consultants or higher institutions to formulate business continuity procedures.

While the social and behavioral (i.e., human related) aspects of information security of certain banking products are mostly handled by departments that own such products, the Enterprise Security Group owns the privilege to deal with the physical and technical aspects of the information security of such products. The department manages installations and upgrades of IT systems security tools (e.g., anti virus software or firewalls) and maintains the use of security management applications (e.g., identity management application or user ID management application). The department reviews these applications annually to assess the needs for further enhancement. Security tools enhancement depends on availability of new patches or versions of such tools. These maintenance and enhancements depend upon:

- User (i.e., the bank's personnel) request.

- Policies made by the Enterprise Security Group or by the Information Technology Department (usually for development of new hardware).
- Demand by a business unit or a department (e.g., the need to develop a new banking product).

Regarding the maintenance and enhancements issue, the Head of the Enterprise Security Group states that:

> "Yes, the process is that way. So, if you ask me about any changes of technology and security, there are three sources for such changes. These are the user, the policies issued by IS or the IT and Operation Strategy Division, and a demand made by a business unit. If a request comes from a business unit, it's usually because of a new product or a new service. So if a business unit makes a proposal request, we will assess the need based on the IT requirement, security requirement, and service requirement, before it's implemented. All these could dramatically change the existing information security. But you can also say that a user request represents a request by a business unit because a user is the bank's staff and a member of a certain business unit."

In addition to the above mentioned security policies, the Enterprise Security Group, has the authority to formulate and enforce policies regarding the bank's Business Continuity Plan. Policies and procedures regarding Business Continuity Plan are considered complex policies and procedures.

6.3.1.2. Principles Enactment: In general, the bank classifies security risk as internal risk or external risk. The bank believes that security risk often generates outside of the bank and therefore feels the need to ensure transaction security and convenience for its customers. However, the bank also realizes that risk can be an internal issue, which is likely to be caused due to unethical conduct by the bank's personnel. An example of this is data leaked by an employee for monetary exchange. Given this premise, the bank feels the need to develop and implement integrated information security governance. Despite the fact that breach incidents are often caused by human conduct, the focus of security governance in Blue Sequoia Bank is largely on procedures to secure technology.

Just like any other institution, the bank also believes and does realize that security risk is closely related to people- failure (i.e. socio-engineering issue) as stated by the Head of the Enterprise Security Group:

> "Security is not simply a matter of technology. Therefore, security is linked to the process and people aspects. So we're trying to make sure that the policies and procedures that we have formulated meet the current technology development as exists out there."

A shift towards more "human and organization oriented" security governance has actually been initiated. Blue Sequoia Bank considers reputational risk to have a more destructive impact than financial risk. As an attempt to implement a more human and organization oriented security governance, the bank's focuses on raising security awareness, using standards prescribed by the International Standards Operation (ISO). Some of these efforts include:

- Annual security campaign by issuing encouraging statements to personnel.
- Security education, for example displaying videos on security best practices for personnel.
- Customers' awareness: efforts have been made as a part of the security campaigns. These campaigns are short advertisements on national television

or statements on how to securely type in a PIN number in an ATM, which are published in newspapers and magazines.

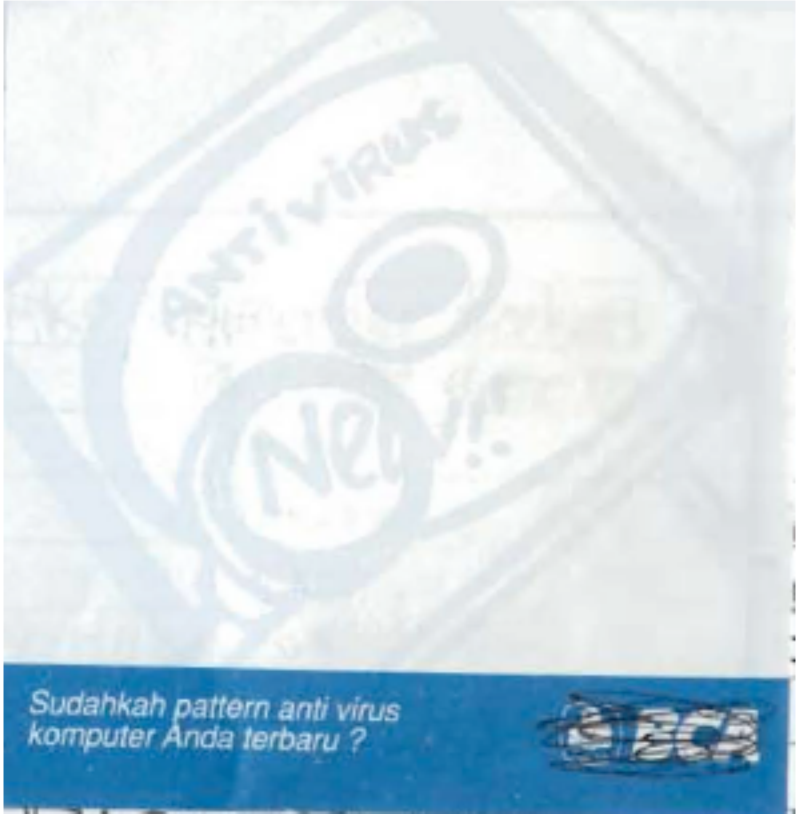


Figure 6.2 – An Example of Security Campaign Using Sticky Note Aimed at Bank Personnel

Figure 6.2 depicts an example of the Annual Security Campaign which shows statements aimed at the bank's personnel. This statement is printed on a sticky note that is distributed to the personnel. It is seen, and then is implemented internally by personnel. The statement is loosely translated as "*Is your computer anti-virus application in its latest version?*"

The practice of addressing a business unit or any specific demand by a department starts by the Board of Director's evaluating procedures and services for implementation of the new product. The implementation is then supervised by the Enterprise Security Group. When such a demand is addressed, new policies are circulated and distributed throughout the Headquarters and to branches. Branches receive the new policies and procedures through electronic copies or via Local Area Network (LAN). Complex policies and procedures (e.g., policies and procedures for Business Continuity Plan) require socialization of the entire hierarchy from the branch manager to the lowest functionary or clerks. As an effort to socialize staff to the new policies and procedures, Enterprise Security Department personnel visit the bank branches to provide solutions for the implementation of these new policies and procedures. Such solutions are the conduction of workshops, developing information kits, providing instructional videos, etc.

While the Enterprise Security Group deals with the physical and technical aspects of security, the Electronic Banking Operation Group, for example, handles electronic banking products such as ATMs, Internet banking, mobile banking, phone banking, debit and cash electronic payments, and the Flazz® card. This department proposes and develops new electronic banking products and maintains such existing products. Despite the security requirements and applications being maintained and managed by the Enterprise Security Group, new product proposals are handled by the Operation and Service Support Group. Hence all policies related to electronic banking products are formulated by the Operation and Service Support Group. Together with the Electronic Banking Operation Group, the Operation and Service Support Group evaluates user requirements for any new electronic banking product. This department also formulates the policies and procedures related to the use of any new product. Security policies and procedures for a new electronic banking product, however, are still formulated and enforced by the Enterprise Security Group. For example, when the Enterprise Security Group formulates security policies for the purpose of electronic payment using a debit card, the department reflects the policies already enshrined in the debit-card payment policies which are distributed and enforced by Earl Capita Bank. However, as the Earl Capita Bank requires a standardized format for debit cards, this mandatory compliance requirement delays BSB's attempt to enhance its security feature for its debit-card payment.

6.3.1.3. Script Replication: Among commercial banks in Indonesia, Blue Sequoia Bank is known for its large number of ATM machines and branches distributed throughout the nation. Such a large number of ATMs and branches gives rise to various challenges as far as promoting secure electronic and banking transactions in a nation with a large population is concerned. The obvious challenge that the bank faces is in the form of the various interpretations of security culture which are prevalent among Indonesians. Owing to low Internet penetration, most security breach cases occur at branch level and involve unaware or even gullible, customers. The Head of the Electronic Banking Operation Group states:

> "Security breach… Cases in security breach usually are caused by customers not knowing the importance of keeping their information and transaction data to themselves. It's simply a question of customers being unaware of security. Indonesian customers are different from western customers. Security breach cases in Indonesia often occur not because of sophisticated attacks, for example hacking cases such as in the west. Here in Indonesia, customers are not avid Internet users. In fact, not many people know about the Internet and ICT, except those in major metropolitan cities such as Jakarta. Customers

> are so gullible that criminals take advantage of the lack of security awareness and prey on these customers. Customers are tricked into handing over their private and sensitive information to undercover criminals. That is what’s happening here.”

While state-of-the-art technologies and security applications have been the bank’s primary concern, Blue Sequoia Bank does realize the importance of the people aspect in information security. The bank understands that a strong security culture begins with security-savvy and well-educated personnel. In general, the practice of information security governance in Blue Sequoia Bank is closely related to and is embedded in the bank’s business process. Any newly employed staff member is educated about information security awareness, particularly on security rules. These rules are initiated and formulated by the Enterprise Security Group. The rules are particularly enforced at the bank’s touch points, which are points where personnel directly relate to and communicate with the bank’s customers (e.g., local branches). Any violation of these security rules is considered a fraud. An example is a staff member’s failure to follow procedures for money transfer.

As a private, non government-owned institution, Blue Sequoia Bank has a more straightforward culture and a less vertical chain of command. Already formulated rules are studied by a task force. The objective of doing so is to analyze and ascertain if the rules have satisfied both the requirements of the Central Bank and also the needs of Blue Sequoia Bank. If not, then a revision is rendered necessary. All rules, including those for information security, once formulated and revised are proposed to the Board of Directors for approval. Once they are approved, a new policy is expanded to include the details of the newly formulated rules in standard procedures. The procedures are implemented for the benefit of all personnel in all strata at various branches (see figure 6.3 for rules and behavioral transfer).

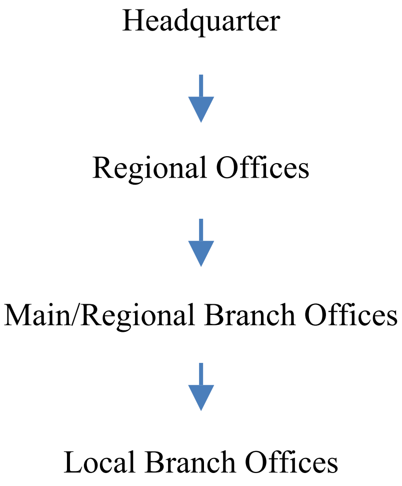


Figure 6.3 – Rules and Behavioral Transfer at Blue Sequoia Bank

As such, the new policies and procedures require thorough and rigorous socialization at each branch, from the branch manager to the lowest level personnel. In order to do so, the Enterprise Security Group at headquarters sends a delegate to each branch. The delegate provides education and solutions of issues arising from the implementation of these policies and procedures. Examples of policies and procedures education and solutions include conducting workshops, distributing pamphlets, and showing videos. Moreover, local branch managers have a right to connect directly with headquarters through the operational development and service division to report and register request for revision. The Head of the Electronic Banking Operation Group expands on the issue of educating and socializing staff about the security rules for electronic banking in the following words:

“Education and raising awareness of e-banking products and their uses are done by us, the Electronic Banking Operation Group. Our efforts include the education and raising of awareness about secure electronic banking. The message is conveyed to customers and our staff using various communication channels, such as emails and newspaper ads. We also put up flyers and banners at local branches.”

6.3.1.4. Patterned-Actions Objectification and Externalization: Blue Sequoia Bank has the most sophisticated technology and information-security technology among its peers in Indonesian banking sector. As the bank realizes that security is also largely connected with people and organizational issues, the bank enhances its technical security features so that people cannot trespass easily. In addition, the bank promotes concentrated campaigns to increase security awareness among its stakeholders and educate its most precious stakeholders- the customers.

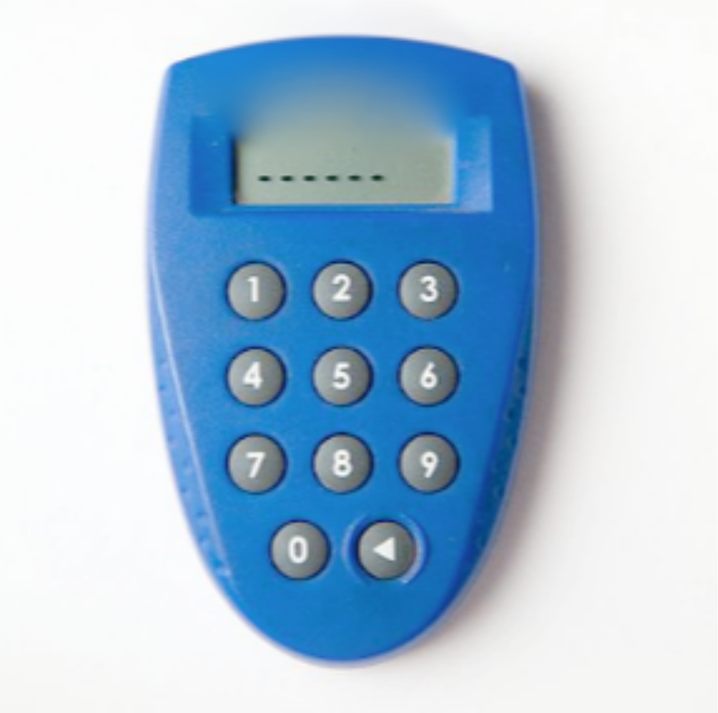


Figure 6.4 – Electronic Token Device

The bank has put comprehensive and sophisticated IT security systems in place. The bank prides itself on its security coverage. The BSB was the first public institution to issue electronic token for online-transaction authentication. The bank prides itself on being the pioneer in the use of token for authenticating electronic transactions. In addition to username and account, certain systems that are prompted for payment using BSB card require a dynamic password that is generated by the token. The token, provided by VASCO Data Security International Inc., is available free to bank customers provided they are able to verify their account validity. The Head of Enterprise Security Group reasons that:

> “Authentication is important as it allows us to differentiate between those who own the right to gain access and those who don’t. In the past, authenticating internal users was easy since these are employees. However, development of technology and Internet has provided the external users, our customers, with the capacity to access our systems. Hence we figure that we need to create usernames and dynamic passwords.”

Other authentication technology includes biometric authentication. The bank has incorporated biometric authentication since 1996, which is a system that works by authenticating user’s fingerprint. Biometric authentication is used merely for internal users, i.e. bank personnel. The bank is very serious about its information systems security and pays particular attention to security technology. The followings are some of the bank’s security technologies:

- Technologies to preserve authenticity: these technologies are intended to authenticate users. Common applications are ones that use user ID and password.

    - Electronic token device (see figure 6.4): This device generates dynamic password (i.e., single-use password).
    - Biometric (e.g., fingerprint scanning): This technology has been around since 1996 and is for branch supervisors to approve any teller transaction that is over the limit (e.g., a deposit of over US $2500 and a withdrawal of over US $5850).
    - External applications: These applications are used by customers such as ones using web banking, requiring PIN or dynamic passwords generated by the electronic token device.

- Security infrastructure: Technologies and applications which are for network use.
    - Firewall.
    - Host intrusion prevention system: Works in a similar way to a firewall operation but is used on a personal desktop or a personnel's terminal. The goal is to limit online access to the desktop.
    - Network segmentation: The concept of dividing network security based on priority and critical impacts on the bank.
    - Tripwire: An integrity checker tool that continuously monitors a server to prevent unauthorized changes in the server's content.
    - Fraud monitoring system: A system that alerts staff about any unusual transaction.
    - Antivirus application.

Tools are also used to monitor the bank's ATMs. In addition, the bank uses surveillance cameras in ATM vestibules and is attempting to migrate its debit card from a magnetic strip to a chip card; a feature found in credit cards. Of BSB's 6000 ATMs, only 200 ATMs do not have the capability to read chip cards. Another tool used, Hewlett Packard® Open View, does not relate to security functionality, however, and is used to monitor and detect the life of the bank's servers and applications.

6.3.1.5. Case: Automated-Teller Machine (ATM) Skimming: This subsection provides a similar overview as the same subsection in the previous chapter, pertaining to the Centro Metropolitan Bank. Since the emphasis is on security breach incident, this section draws upon an incident of script revision resulting from an exogenous event rather than script replication. An automated-teller-machine (ATM) skimming incident is presented in this section.

A. The Incident: The ATM skimming case can be used to describe the information-security institutionalization at Blue Sequoia Bank. The case involved installing equipment on an ATM to steal card's identity. Similar to the incidental case of Centro Metropolitan Bank, the perpetrator of this ATM skimming at BSB case is a syndicate or an organized group of criminals. Episodes of this case were detected in January 2009 when there were instances of unauthorized debit from Bulgaria and Canada. More than ten customers complained that their accounts were debited without their knowledge.

Once these unauthorized debits were identified, the bank discovered skimming equipments (the skimmer and disguised surveillance cameras) mounted in ATM vestibules in 13 locations in Bali. The bank immediately blocked international transactions for debit cards that had been used in ATMs in Bali during the period from August to September 2008.

In January 2010, a huge increase in complaints by customers was addressed to Blue Sequoia Bank. The complaints came from customers whose debit cards were not debarred from initiating international transactions. The incidents showed unauthorized debits from Bali and Australia. The bank then immediately terminated all debit cards that had been used in ATMs in Bali during the period of August to September 2008 and replaced these cards with new debit cards for the customers whose debit cards were terminated.

The bank immediately performed an investigation and discovered the following patterns:

- The victims had transactions in Bali.
- Unauthorized transactions (i.e., debits) always occurred abroad, specifically in Bulgaria and Canada. The authentic customers were able to provide evidence that they had never been abroad when the transactions occurred.

Based on these facts, the bank inferred that there was a syndicate that installed ATM skimming equipments in several ATM vestibules active in Bali in 2008. The syndicate was a team of Indonesians who are capable of using skimming technology from Eastern Europe. The bank initiated preventive action, which concerned mainly securing the PIN pad of ATMs. The ATMs were then equipped with a PIN pad cover so that the disguised camera installed by the perpetrator would not be able to capture the PIN numbers which were fed in by the genuine card holder. Another measure taken by the bank to combat skimming was to install anti-skimming equipment such as jitter technology.

Figure 6.5 – An ATM Equipped with Jitter Technology

In addition to the technical prevention, the bank issued new procedures for use of ATMs: improving ATM installation standards and procedures especially in remote areas, the use of PIN pad cover for all ATMs, and installing surveillance cameras in ATM vestibules and ensuring that these cameras functioned properly.

When the case first came to light in 2009, Blue Sequoia Bank immediately reported the incidents to Earl Capita Bank and sought advice and assistance. The case was reported as an ATM-transaction fraud. The bank initiated meetings with the Central Bank personnel to discuss reports and complaints from the bank's customers. Meetings were conducted mainly with the Central Bank's Accounting and Payment System Department. This resulted in a complaint from the Central Bank's supervisor, which is the subdivision of the Private National Banks Supervisors (i.e., the Earl Capita Bank's bank supervisory department subdivision 3), citing that the report should have been addressed to the Central Bank's Supervisory Department. This complaint, however, showed up the lack of communication among departments within the Central Bank. In March 2010, when the incidents became more prevalent, Earl Capita Bank dispatched an auditory team to study and investigate the ATM skimming incidents in Blue Sequoia Bank.

B. The Aftermath: Contrary to what Centro Metropolitan Bank experienced, Blue Sequoia Bank suffered from reputational damage due to ATM skimming incident. While there was no sizeable financial damage, the bank experienced significant loss of customers' trust in terms of using ATM machines for card transactions. The Head of the Enterprise Security Group mentions about the reputational damage as follows:

> "To be honest, there wasn't that much financial damage caused by this skimming incident. The biggest impact is on our reputation though. This is why we actually wanted to use control. By this I don't mean controlling our reputation, but we want to better manage our reputation so there won't be any negative impact on our reputation. For a bank like us, the financial loss caused by this kind of incident is absolutely nothing compared to the larger impact that could haunt us every year to come. So if you pay attention to the larger impact, which could lead to reputational risk, it's like we are getting huge attacks. Why?..Because in the long run people will never trust our ATM transactions. They are scared of using their debit cards on our ATM machines. This is by far our biggest fear when it comes to security breach incidents such as this one. Not just us, but I believe also all other banks in Indonesia."

The extent to which the ATM-skimming incident impaired Blue Sequoia Bank is delineated by its effort to undo damages caused by the incident. Similar to Centro Metropolitan Bank, Blue Sequoia Bank has been forced to form a task force to handle the

ATM-skimming incident. This task force consists of the bank's personnel representing divisions involved in the otherwise normal operational conduct of debit card transactions as well as ATM support and maintenance. The main objective of this task force is to investigate these incidents. The task force consists of personnel from the following business units:

- The Enterprise Security Group, which acted as the task-force coordinator.
- The Technology Division of the Operation Strategy and Design Group.
- The Operation and Service Support Group, whose primary task was to inform customers who were victims of the incidents of disputed transactions.
- The Public Relation Division.
- The Information Technology Group, whose task was to investigate transaction pattern.
- The Legal and Compliance Group, who communicated the incidents and any recovery-act progress to Earl Capita Bank.
- The Risk Management Committee, which ensured that all recovery acts had minimum risk impacts.
- Division management and the Board of Directors.

Several steps that the bank undertook to prevent similar incidents from occurring in the future are:

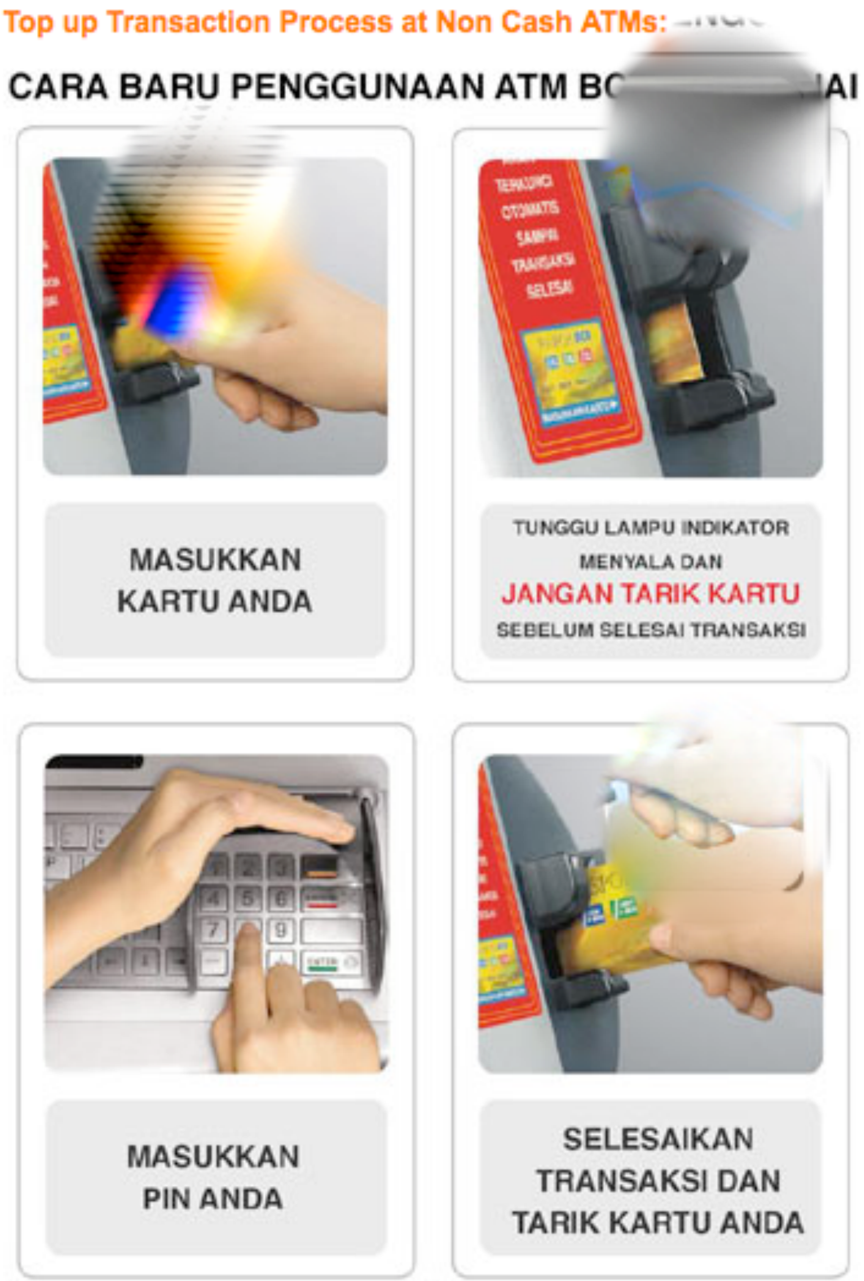
- Improving standards for ATM installation.
- Implementing the use of PIN pad cover.
- Distributing and installing surveillance cameras in every ATM vestibule.

- Most importantly, migrating debit cards from magnetic strip to chip card.

In addition to such steps, the bank conducted a massive campaign to educate its customers on the importance of secured ATM transactions. The objective is to raise security awareness in general and to educate customers on how to securely use ATM cards and make transactions on ATM machines or EDC machines. For doing so, the bank distributed educative brochures and pamphlets, announced messages of information security and debit card transactions on television commercials, and even conveyed the same messages via the bank's biweekly television program called "Gebyar BSB[4]." Figure 6.6 depicts a sample of an online brochure that educates customers on how to securely use their debit cards in ATMs. The Head of the Electronic Banking Operation Group says:

> "We are making every effort to raise our customers' awareness about secured electronic transactions, especially in the aftermath of the ATM skimming incident. This is one of our efforts to gain back our customers' trust and to show them that we are very serious about this. We distributed pamphlets and brochures that tell customers how to use their debit cards in ATM machines and EDC machines when they visit one of our branches or when they do grocery shopping at one of our partnered local stores. Oh, did you watch 'Gebyar BSB'? We educated our customers using our show. The audience nationwide can benefit from this free entertainment show as well."

[4] "Gebyrar BSB" is a national television program run by Blue Sequoia Bank to communicate with its primary stakeholders (i.e., customers). The program is run every other week and is intended to be entertaining and educative.



Top up Transaction Process at Non Cash ATMs: [redacted]

CARA BARU PENGGUNAAN ATM B[redacted]AI

MASUKKAN KARTU ANDA

TUNGGU LAMPU INDIKATOR MENYALA DAN **JANGAN TARIK KARTU** SEBELUM SELESAI TRANSAKSI

MASUKKAN PIN ANDA

SELESAIKAN TRANSAKSI DAN TARIK KARTU ANDA

Figure 6.6 – Online Customer Education about Debit Card Transaction

Blue Sequoia Bank has set a long-term objective to prevent a similar incident from occurring in the future. The bank has developed a chip-card enabled debit card for ATM and EDC transactions. As the bank adds more ATMs throughout the country, the ATMs are enabled with the capacity to read chip cards. As already mentioned, out of 6000

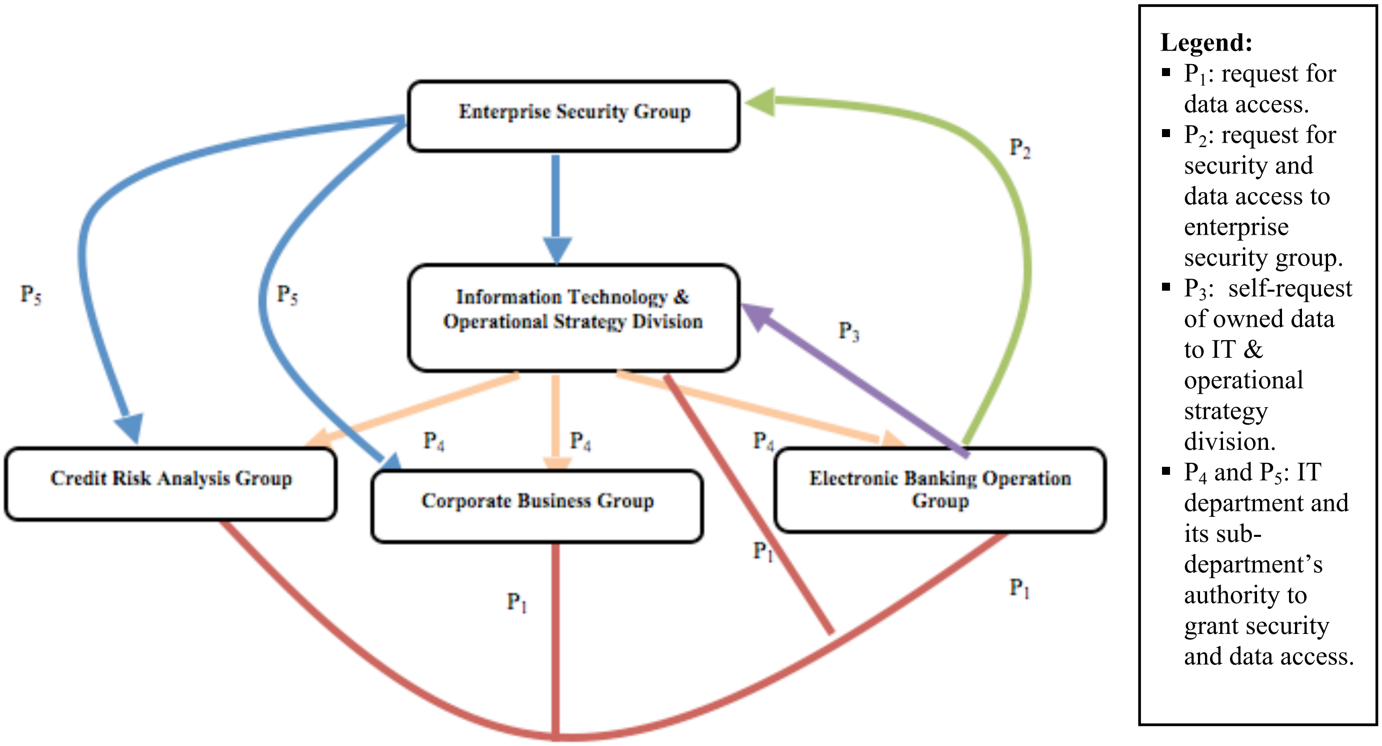
ATMs, only 200 ATMs of the bank do not have the capacity to process chip-based debit cards. EDC machines on the other hand are able to read chip cards since these machines were originally designed to accommodate credit cards, which are chip cards.

6.3.1.6. Discussion: Blue Sequoia Bank is of the view that technology can only be harmful if it is misused by the human actor (i.e., the agent). Technology is regarded as an artifact that aids personnel in their works but it is understood that it can also be harmful for the bank and may even tarnish the bank's reputation. Information security risk is often attributed to the ignorance of the bank's customers about the usage of the technology provided by the bank. This unfamiliarity is often used by criminals to swindle money from the customers. Hence securing technology at the customer's end is the bank's priority in order to maintain its security. The Head of the Electronic Banking Operation Group states:

> "From the customers' point of view, security is a must. What I meant was the security feature for customers' transactions. Once we fail to secure their transactions, our reputation is damaged. This is because customers will never want to use our products due to the mistrust issue."

The bank therefore regulates the use of technology and the dissemination of data and information as an important asset. The belief is that the regulated interaction between bank personnel as the agent and technology creates a structured implementation and practice of information security which is an attempt to safeguard the bank's data and information. As stated earlier, the bank mandates the Enterprise Security Group, which is a subdivision of the Information Technology and Operation Strategy Division. The structured implementation and practices of information security in Blue Sequoia Bank leads to the creation of the institution of information security in the bank, which is governed centrally by the Enterprise Security Group.

Despite the seemingly technology-centric orientation of the bank, Blue Sequoia Bank believes that information security is an organizational issue, involving people, organization, and technology. The Enterprise Security Group therefore handles information security issues from the technological, people, and organizational perspective as well. Similar to the practices and implementation of information security in Centro Metropolitan Bank, the practices and implementation of information security in Blue Sequoia Bank are a quasi privilege assumed by the Enterprise Security Group. The Enterprise Security Group, however, is given exclusive responsibility to govern the technical control of information security in Blue Sequoia Bank. As such, some forms of information-security governance acts are shared between the Enterprise Security Group and other groups (e.g., the Operation and Service Support Group). The Enterprise Security Group therefore has the privilege to direct the three information-security controls- which are the Technical control, Formal control, and Informal control. The formal and informal controls are shared with other groups within the bank while the Enterprise Security Group retains the right to direct the technical controls. Specifically, the formal control and the informal control are shared with other groups or departments that own and direct the non-automated format of a banking product. An example of such responsibility sharing is the customers' security education and awareness which is shared between the Enterprise Security Group and another division depending on the product (e.g., Electronic Banking Operation Group for ATM transaction).


Enterprise Security Group
Information Technology & Operational Strategy Division
Credit Risk Analysis Group
Corporate Business Group
Electronic Banking Operation Group
P_5
P_5
P_2
P_3
P_4
P_4
P_4
P_1
P_1
P_1

Legend:

- P_1: request for data access.
- P_2: request for security and data access to enterprise security group.
- P_3: self-request of owned data to IT & operational strategy division.
- P_4 and P_5: IT department and its sub-department's authority to grant security and data access.

Figure 6.7 – The Flow of Information Security Authority and Responsibility in Blue Sequoia Bank

Only the technical form is governed solely by the Enterprise Security Group. Similar to Centro Metropolitan Bank, the governance of information security in Blue Sequoia Bank is therefore centralized. Figure 6.7 depicts the practice of information security in Blue Sequoia Bank. The BSB's implementation of information security bears a total resemblance to security implementation in Centro Metropolitan Bank, with one division requesting access to information being required to send such a request to the information-steward division before the actual access is granted by the Enterprise Security Group. If a group wants to request an access to electronic banking data and obtain such data, as depicted by process P_1, then the group has to make a formal request to the Electronic Banking Operation Group. If the group permits such a request, the Electronic Banking Operation Group creates a request to the Enterprise Security Group to unlock access to the requested data, depicted by process P_2. Similar to the situation in Centro Metropolitan Bank, all access requests for the data[5] need to be addressed to the Information Technology and Operational Strategy Division, as depicted by process P_3. Finally, P_4 and P_5 denote access to data by the Information Technology and Operational Strategy Division and access privilege by the Enterprise Security Group respectively.

The institutionalization of information security in Blue Sequoia Bank consists of the following three situations: T1 depicts the condition before the ATM skimming incident took place, T2 depicts the situation when the ATM skimming incident occurs, and T3 refers to an episode after the incident occurs and the social order has been reinstalled. In episode T1, Blue Sequoia Bank adopts and implements the security guidelines formulated and issued by the central bank by creating a set of regulations marking the script encoding, the bank's personnel begin to internalize such regulations which denote the principles enactment, and implement them. This implementation finally becomes a habit which demonstrates the patterned-actions objectification and externalization. Similar to the case of Centro Metropolitan Bank, the implementation of regulations and principles in episode T1 denotes the script replication, signifying a normal practice when social order is in place. Episode T2 depicts the situation during the occurrence of the skimming incident: the latter processes (processes principles enactment, script revision, and patterned-actions objectification and externalization) are preceded by the ATM skimming incident and draw the bank's attention towards reprimanding the perpetrators and reinstating order after the incident. Since episode T2 depicts security practice during a breach incident, script revision takes into effect instead as personnel seek to improve

[5] The data is stored in the server owned and operated by the Information Technology and Operational Strategy Division.

security governance and practices. Finally, episode T3 depicts processes that are similar to processes episode T1. This is because episode T3 aims to recreate a momentum of maintaining social order and stability. The difference is that episode T3 depicts processes of maintaining social order and stability post a security breach incident.

Most cases in security breach are caused by external factors (e.g., the ATM skimming case in 2010). Internal security-breach cases are rare, and are usually attributable to improper conduct of employees, and are not directly related to technology misuse. As such, these cases always involve human actors in addition to technology artifacts. In general, the bank regards that incidental cases arise due to the ability of agent (i.e., stakeholders) to exploit weaknesses in the technology. The bank believes that the well being of its information security depends on the harmony between its people, process, external factors, and system. The BSB appoints the Enterprise Security Group to secure the interaction between the vital elements of the people, process, external factors, and system. Similarly, as incidental cases are attributable to actions of the agent, only the group is exclusively responsible for the technical control of information security. It has to share, however, the formal control and informal control with other groups or divisions. Unlike Earl Capita Bank and Centro Metropolitan Bank, user privilege and data access are exclusive responsibilities of Blue Sequoia Bank's Enterprise Security Group. Issues of user privilege and data access are considered technical aspects of information security and hence are some of the main tasks of the Enterprise Security Group.

6.3.2. Relationship with the Central Bank

6.3.2.1. The Macro-Prudential Supervision of Information Security Governance: Earl Capita Bank regards BSB as the most cooperative commercial bank under its purview. BSB views Earl Capita Bank as a partner and consultant rather than a supervisor. The BSB consults and reports any progress without Earl Capita Bank having to request such a report or progress. As a commercial bank, the bank has to abide by the regulations of regularly reporting activities and progresses, immediately reporting incidents and offering solutions to such incidents, and proposals to launch any new banking product to Earl Capita Bank.

Similar to that of Centro Metropolitan Bank, the reporting activity at BSB is a responsibility of the Legal and Compliance Group. Hence, during reporting cycle, each of the other departments develops reports that are submitted to the Legal and Compliance Group. These reports are delivered by the Legal and Compliance Group to Earl Capita Bank. The Head of the Enterprise Security Group expounds on the responsibility of the Legal and Compliance Group as follows:

> "Our door to the central bank is the Legal and Compliance Group. They take care of any matters regarding the central bank. If there is any problem that we want to address to the Central Bank, we go to the Legal and Compliance Group. This includes problems in information security and technology. We formally create a report and give it to the Legal and Compliance People. And then they forward the report to the Central Bank. If the Central Bank people come to visit us for any purpose, the Legal and Compliance People will have to assist them. So no, our institutional relationship in information security is not initiated by my division. We're involved though, but not directly."

When Earl Capita Bank issues new regulations, each department within BSB will study the new regulations that correspond to the department's functionality. The Legal and Compliance Group helps in reviewing the new regulations if a department faces any ambiguity with the new regulations. On the 15th of every month, BSB, as well as other commercial banks, deliver monthly reports online to Earl Capita Bank. These reports include issues with and maintenance of IT security systems. Through its Bank Supervisory Department, Earl Capita Bank conducts an auditory visit to BSB and sends its findings to the bank for further confirmation. Auditory visit also includes auditing the bank's firewall, server location, password reliability, etc. The Compliance Advisor states that:

> "You know what- we are actually being audited by Earl Capita Bank, right here, right now. Their auditory team is just a couple of floors above where we are now. In addition to card-payment products which is an area belonging to the accounting and payment systems, they're auditing just about everything. Yesterday, they audited our IT systems, including our IT security systems such as our server location, antivirus software, server location, and all other such IT security related stuff. But I'm not sure exactly what they did since it's not my area."

Since auditing IT security systems is a separate task, the responsible host is the Enterprise Security Group. This is in accordance with Earl Capita Bank's regulation that it may determine a specific department to provide reports to Earl Capita Bank. Therefore, such department will be the host during Central Bank's auditory visit or be it's primary reporter. The Legal and Compliance Group will only supervise the institutional relationship between Earl Capita Bank and the hosting department that essentially represents the BSB. The Legal and Compliance Group, however, may assist the hosting department if materials requested by Central Bank are deemed ambiguous or complicated. The institutional relationship of auditing security systems of card payment, however, is managed by the Legal and Compliance Group since card-payment auditing and reporting are handled by the Legal and Compliance Group.

As stated earlier, electronic banking and accounting payment systems are audited by an auditory team consisting of personnel of both the Bank Supervisory Department and the Accounting and Payment Systems Department of Earl Capita Bank. Audit is committed via two forms: a random, special audit and a regular audit. Regular audit is an annual routine audit that is holistic in nature and may be performed randomly at any branch. IT audit is, however, a case of random audit, and so is the IT security systems audit.

6.3.2.2. Discussion: Similar to that of the case of Centro Metropolitan Bank, the institutionalization of information security in Blue Sequoia Bank cannot be sufficiently illustrated without elucidating the institutional relationship between Earl Capita Bank and Blue Sequoia Bank. This relationship describes the institutional view of the information security governance of Blue Sequoia Bank as governed and controlled by Earl Capita Bank. Similarly, the relationship is described using the multi institutional process[6] (Scott 2008). While the top-down process denotes the governance and control act by Earl Capita Bank to Blue Sequoia Bank, as well as to other commercial banks, the reciprocity action by Blue Sequoia Bank signifies the information security conformity and reporting by Blue Sequoia Bank, which is mediated by its Legal and Compliance Group. Similar to that of Centro Metropolitan Bank, the institutional relationship of information security

[6] See figure 3.3 and figure 5.6 for illustration.

between Blue Sequoia Bank and Earl Capita Bank is a form of a micro-prudential supervision of information security, which connotes a one-to-one institutional relationship between the central bank and a commercial bank focusing on the implementation of information security.

6.4. Conclusion

Blue Sequoia Bank is a large private commercial bank in Indonesia. The bank boasts of the most branch offices and ATMs distributed across the nation. The BSB originated as a commercial bank specializing in financing textile and garment industry in the nation. The 1997 economic crisis that hit the nation severely damaged the bank whereby a panic rush caused significant financial damage to the bank. The loss prompted it to seek government assistance for restructuring and reorganizing. Today, the bank is one of the strongest and most financially influential commercial banks in the nation.

The objective of this chapter is to provide comprehensive empirical description of practices and governance of information security in Blue Sequoia Bank. Blue Sequoia Bank is the financial institution in the nation with the most advanced technology and well diffused and adopted technology. Similar to the governance of information security in Centro Metropolitan Bank, the governance in Blue Sequoia Bank is undertaken by a department that functions only to direct the security practices and its implementation in the bank.

The difference, however, is that the three security dimensional controls at BSB are almost exclusively maintained by the Enterprise Security Group. The security of the debit card provides an example of how the three dimensional controls are maintained by the group with the formal and informal controls being shared with the Operation and Service Support Group. The highlighted difference is that, rather than completely surrendering the formal and informal controls to other groups or divisions like the responsibility-sharing which is common in Centro Metropolitan Bank, Blue Sequoia Bank opines that the Enterprise Security Group maintain the formal control and the informal control altogether with another group or division.

The incidental case of ATM-skimming of information security breach provides an example that lead to immediate investigations and actions. The case demonstrates the bank's effort to resolve the incidents while preserving customers' trust and convenience. Similar to the incidental case in Centro Metropolitan Bank, the ATM skimming case demonstrates that safeguarding information and implementing information security are important responsibilities shared by all stakeholders, including the bank's customers. Not only did the bank form a task force comprising of various business units which were involved in the crisis to deal with the incidents, but the bank also reestablished its trust with its customers.

7 SYNTHESIS

7.1. Introduction

The previous three chapters have covered the implementation aspects of information security governance in the central bank and in two commercial banks. These three chapters, each of which acts as an intensive study of a single information security practice and governance case, observe “the entire configuration of individuals, groups, and social structure in the setting of an organization” (Lee 1989, pp. 119-120). By pondering on the inferences of the last three chapters, the objective of this chapter is to synthesize important concepts which have emerged from the three chapters and to apply these concepts to reformulate the proposed theory. The emerging concepts are divided into two broad categories: the inter level of security institutionalization and the intra level of security institutionalization. The intra level aims to demonstrate the focal theme of information stewardship, which is a concept that embodies and encompasses the three security controls. Another emerging theme within the intra level is the habitualized security routine. For the purpose of this study, all these topics are visited from the security-control-dimension angle: technical controls, formal controls, and informal controls.

The only theme that emerges based on the intra-level empirical observation is the institutional relationship. Each Bank’s institutional relationship with the central bank is a notion of the micro-prudential supervision of information security (Khoury 2009;

Krauskopf and Steven 2009). Therefore, the notion of the macro-prudential supervision superficially comprises a collection of micro-prudential supervisions.

To recapitulate, this chapter undertakes a comprehensive discussion on emerging themes, which are institutional authority, habitualized security routines, information stewardship, and institutional relationship. The discussion begins by revisiting concepts and theories, wherein particular focus is on the theoretical framework. This chapter is organized as follows: section 7.2 discusses the inter-level institutionalization, provides details on script encoding (section 7.2.2), principles enactment (section 7.2.3), script revision and script replication (section 7.2.4), and patterned-actions objectification and externalization (section 7.2.5). Section 7.3 looks at the macro-prudential supervision of information security practices, covering governance and control (7.3.2) and conformity and report (7.3.3). Section 7.4 focuses on elaborating upon the emerging themes: Habitualized security routines (7.4.1), information stewardship (7.4.2), and institutional relationship (7.4.3). Section 7.5 discusses important concepts which have come to the fore in the earlier section. It also closes this chapter, and provides a summary of the earlier sections.

7.2. The Synthesis: Inter-Level Institutionalization

7.2.1. Overview

Institutionalization is a process of instilling values and creating a social structure (Scott 1987). As a process, an institutionalization depicts sequential and logical steps, and delineates a scenario in each step. In the context of this study, the underlying institutional theory borrows the regulative pillar as institutionalization depicts situations of rule setting, monitoring, and sanctioning (Scott 2008). This study is built upon the regulative pillar based on Scott's institutional pillars and carriers. Scott (2008, p. 52) cited the work of Douglas North to depict a regulatory institution in the following words:

> "[Institutions] are perfectly analogous to the rules of the game in a competitive team sport. That is, they consist of formal written rules as well as typically unwritten codes of conduct that underlie and supplement formal rules… the rules and informal codes are sometimes violated and punishment is enacted. Therefore, an essential part of the function of institutions is the practice of ascertaining violations and the severity of punishment."

The four avenues of institutional reproduction, the exercise of power, complex interdependencies, taken-for-granted assumptions, and path-dependent development process (Powell and DiMaggio 1991), are implicit to the four steps of institutionalization in this study. The framework for institutionalization used in this dissertation borrows the one introduced by Barley and Tolbert (1997), depicting the following processes: script encoding, principles enactment, script revision and script replication, and patterned-actions objectification and externalization. In this study, these processes are used to demonstrate information security governance and implementation in banking sector. In general, the institutionalization of information security is intended to build formal security structures and to depict actual security behavior (Björck 2004).

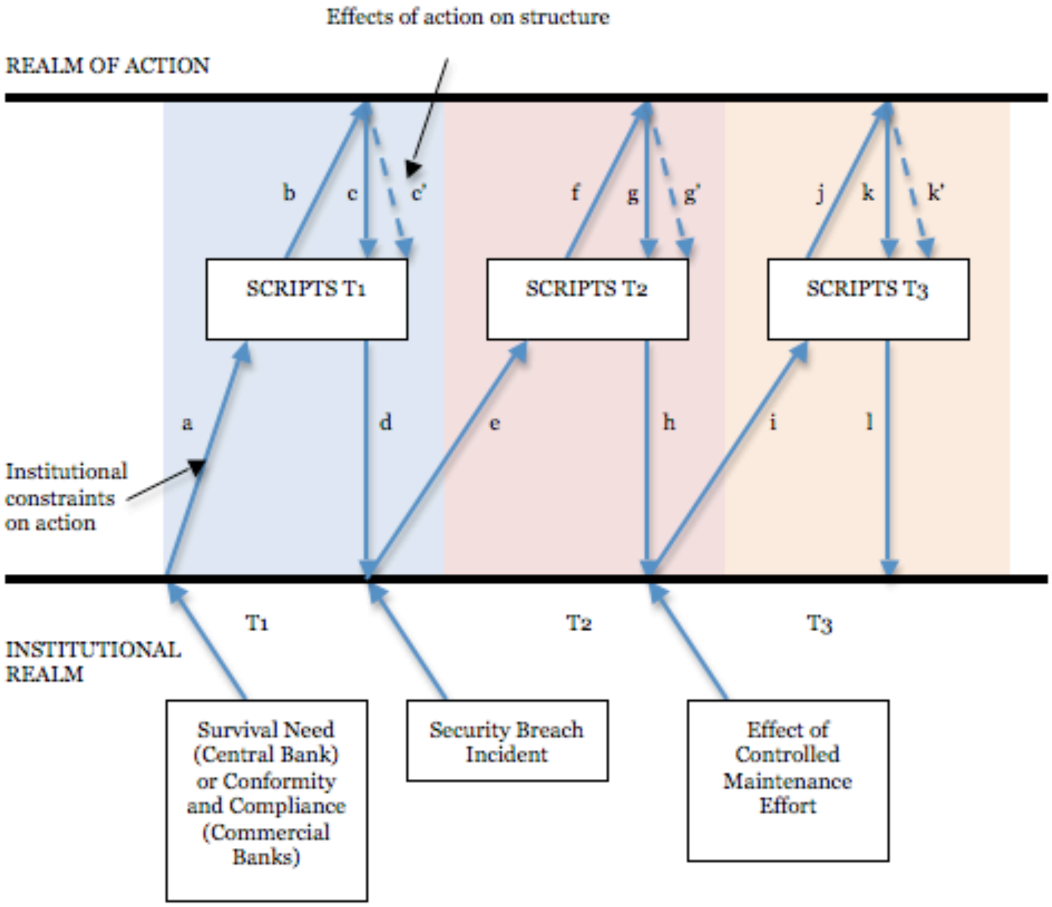

Effects of action on structure
REALM OF ACTION
b
c
c'
f
g
g'
j
k
k'
SCRIPTS T1
SCRIPTS T2
SCRIPTS T3
a
d
e
h
i
l
Institutional constraints on action
T1
T2
T3
INSTITUTIONAL REALM
Survival Need (Central Bank) or Conformity and Compliance (Commercial Banks)
Security Breach Incident
Effect of Controlled Maintenance Effort

Figure 7.1 – The Information Security Institutionalization in Banking Sector – Theoretical Framework

Moreover, the Central Bank lessens the rigid nature of regulatory compliance to allow a certain degree of freedom to commercial banks to apply the information security guidelines according to their specific organizational culture. The Central Bank very well understands that regulations and policies need to correspond with organizational culture to allow for effective acceptance (Hone and Eloff 2002). While the drives for security rules adoption and implementation among commercial banks are compliance and conformity, such adoption and implementation in the Central Bank are driven by narcissism or survival need. As a strategic-change drive, narcissism places an entity as a confident rival to its counterparts (Nana et al. 2010). , In this case, narcissism stems from the Central Bank's desire to become a leading and exemplary institution in the banking sector, including in the arena of information security. An empirical example of this drive is the implementation of Earl Capita Bank's disaster recovery plans and its desire to possess and demonstrate exemplary Business Continuity Plans. The need for survival, which is an exogenous drive, emerges in the form of efforts to remedy security management inefficiency in the central bank. This exogenous drive is similar to the drive to re-institutionalize information security among commercial banks when they are hit by any security breach. An empirical example of this drive is the move to improve employee productivity by using firewalls to prevent access to social network sites (e.g., Facebook.com and Twitter.com) during office hours.

7.2.2. Revisiting Script Encoding: The Creation of Security Culture

The first process that partially portrays the institutionalization of information security is the script encoding. As the first process to occur in an institutionalization episode, script encoding entails socialization and "involves an individual internalizing rules and interpretations of behavior appropriate for particular settings" (Barley and Tolbert 1997, p. 100). Barley (1986, pp. 83 – 84) explains that a script can be used as a primer for action and behavior and formal organization serves as "the grammar of a set of scripts." Scripts, however, are not necessarily rules and regulations. Rather scripts are a set of guidelines for patterned behavior which have been formulated according to recently adopted rules.

The security policies and rules formulation is initiated by the management commitment to advance and safeguard information asset (Chandra 2008). As with any other set of rules and regulations, security policies and rules are formulated to institutionalize "a *kind* of order and a *kind* of social order" (Selznick 1969, pp. 8 – 9) that maintains information security. This study has demonstrated that each institution assigns an IT security subdivision to oversee and control the implementation of security policies and rules. Except for the Blue Sequoia Bank case, the other cases show that rules enforcement affects the organizational culture of the other two institutions. The data ownership issue in the central bank leads to a deviation towards a more centralized and integrated information security management. While ensuring the technical security remains the privilege and responsibility of the IT division, such a deviation towards integration leads to the creation of information stewardship amongst divisions owning data and information. The Centro Metropolitan Bank case shows that implementing security rules needs to be implimented with reference to the innate organizational culture, which allows leverage for implementation and security maintenance on banking products that are unique to Centro Metropolitan Bank (e.g., the SMS/text-messaging banking).

Any conduct that causes the script to be revised has its origins in incidents (e.g., security breach, economic downturn, technology change, etc.) that deviate from routines (Barley and Tolbert 1997). Script encoding starts the moment social actors begin to accept socialized institutional principles such as hiring personnel, evaluating performance, or offering goods or services to customers (Barley and Tolbert 1997). In the context of this study, the script encoding[1] may also begin during the moment when the Central Bank decrees information security rules and commercial banks adopt the rules. Commercial banks readily accept such guidelines that are formulated along with adopted frameworks and strategic information systems plan. Commercial banks understand that the effectiveness of their information security culture depends upon how well aligned the formulated security rules are with their own strategic information systems plan (Doherty and Fulford 2006).

To enforce the adoption and implementation of security rules, the Central Bank utilizes its powers: both deontic and constitutive. The information security guidelines formulated by the Central Bank are to be adopted and implemented by commercial banks. This process therefore serves to underline the importance of power and institutional relationship as well as regulations and compliance, which comprise the regulative pillar of the underlying institutional theory (Scott 2008). The regulative pillar emphasizes the use of rules and laws as symbolic systems of governance and control. As an attempt to adhere to rules and laws enacted by the Central Bank, managements of commercial banks are aware of the fact that if they do not support information security, then this lack of support can inhibit information security practices (Khalfan and Alshawaf 2004). On the other hand, management support has proven to be crucial for the enforcement of security policies and for enhancing the organizational culture's tolerance with good security practices in commercial banks (Knapp et al. 2006).

According to scholars, policies and regulations as sanctioning modalities are one of the three modalities that social actors (e.g., bank personnel and customers) use to produce institution (i.e., structure) (Giddens 1984; Walsham and Han 1991; Walsham 1993).

[1] As shown by processes a, e, and i in figure 7.1

Policies and regulations are created by social actors to preserve social order (Selznick 1969) and are, as such, an artifact used in structuration/institutionalization. Scripts that contain institutional principles of information security emerge as a result of meaningful and continuous interactions between social actors and security artifacts and rules. These institutional principles are a set of patterned actions that have been previously objectified and externalized in a previous episode (TN-1) of an institutional realm. As such, these institutional principles are more than mere policies and regulations, which are only a notion of formal controls. The institutional principles of information security constitute the experiences of the social actors' which arise out of their use of (security) artifacts and from their knowledge of using such artifacts (Orlikowski 2000). Examples include a set of principles to secure the use of ATM machines and a set of principles to secure the use of SMS (text- messaging-service) banking.

How do these institutional principles of information security emerge? A necessary factor for their emergence is that technical security systems should be augmented by adequate organizational support (formal controls) as well as by good information-security governance and security culture (informal controls). Only by maintaining the integrity of the three security-control dimensions shall information security prevail and become institutionalized (Dhillon 2007). Once it becomes institutionalized, all information security practices, originating from patterned-actions objectification and externalization from a previous episode, manifest as a habit that may serve as principles that continuously guide social actors' security behavior. Drawing on institutional principles of information security, bank personnel and customers will always encode these scripts as a behavioral script prior to performing their action. In order to do so, bank personnel and customers own a set of institutional principles of information security that are embedded in the institutional realm, built upon (habitualized) courses of actions drawn from previous episodes.

The habitualized security actions that result compose a corporate security culture which is unique to formal organization. A corporate information security culture supports security rules, procedures, methods, and responsibilities, and becomes a natural habit or a routine that is performed by personnel (Von Solms 2000; Chang and Lin 2007). The objective of information security culture is to assist and guide stakeholders to think about, act upon, and experiment with information security in their organization (Chang and Lin 2007). The major obstacle that hinders the creation of information security culture is often the clash between security rules and the customary ways in which the social actors have conducted their tasks over time (Chang and Lin 2007). Social actors are therefore questioned in terms of their ethical conducts (Dhillon and Backhouse 2000) which form the norm, to adjust to security rules and culture.

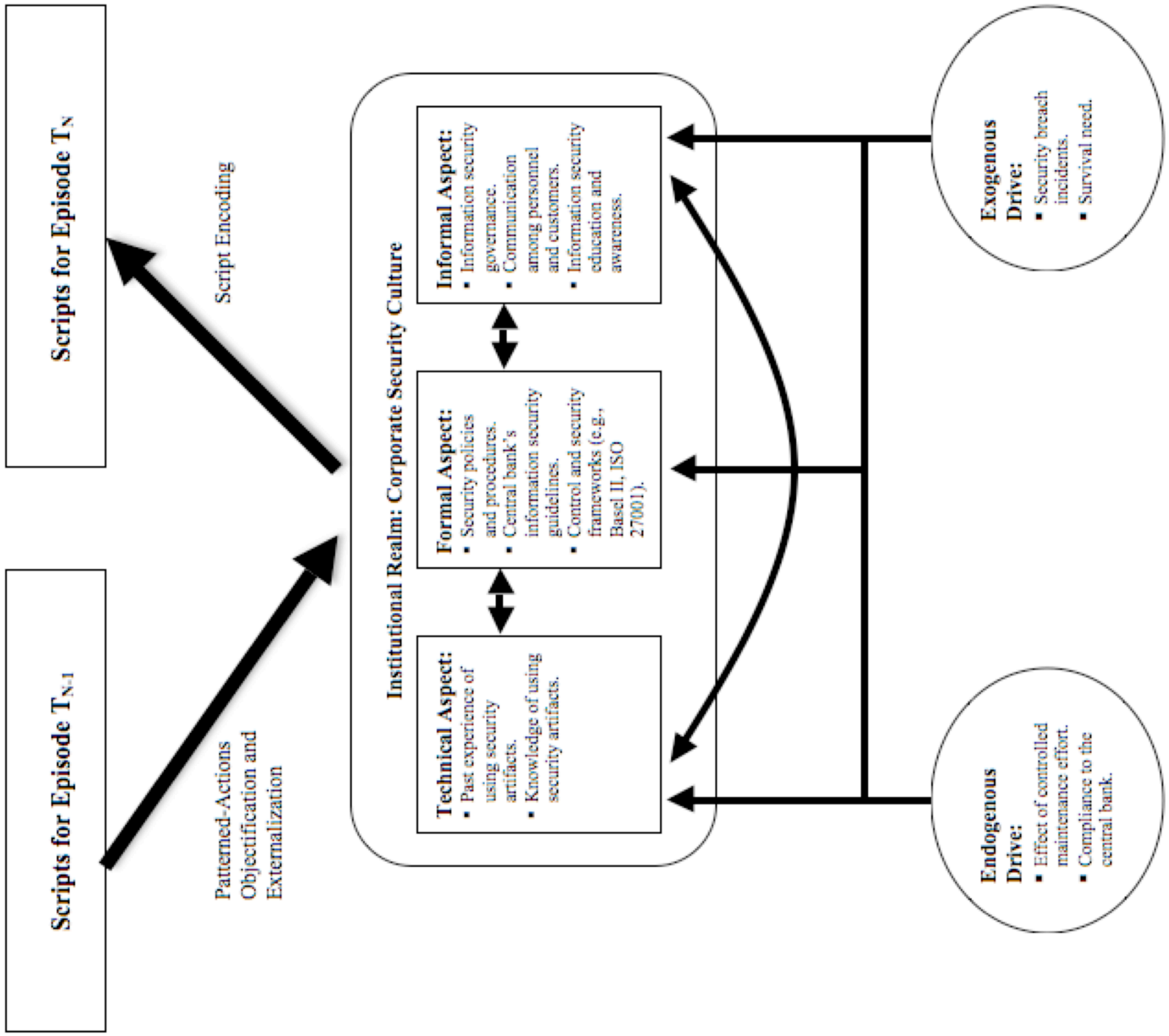

Scripts for Episode T_{N-1}
Patterned-Actions Objectification and Externalization
Scripts for Episode T_N
Script Encoding
Institutional Realm: Corporate Security Culture
Technical Aspect:
▪ Past experience of using security artifacts.
▪ Knowledge of using security artifacts.
Formal Aspect:
▪ Security policies and procedures.
▪ Central bank's information security guidelines.
▪ Control and security frameworks (e.g., Basel II, ISO 27001).
Informal Aspect:
▪ Information security governance.
▪ Communication among personnel and customers.
▪ Information security education and awareness.
Endogenous Drive:
▪ Effect of controlled maintenance effort.
▪ Compliance to the central bank.
Exogenous Drive:
▪ Security breach incidents.
▪ Survival need.

Figure 7.2 – A Framework for Script Encoding at any Given Episode

All institutions in the three case studies agree that effective and efficient information security can only be achieved when controls are implemented simultaneously on technical, organizational, and behavioral aspects (Dutta and Roy 2008). Based on figure 7.2, three security-control dimensions form the corporate security culture and are interchangeable. For example, experience (i.e., cumulative history of actions) of using security artifacts is determined by patterned security behavior according to the already prescribed security policies and procedures. Each dimension is triggered by a combination of endogenous drive, exogenous drive, or both.

The 2008 ATM skimming incident at Blue Sequoia Bank, for example, has afflicted the way customers use ATM machines and their debit cards, changed security policies and procedures at ATM machines and the use of debit cards, and motivated the bank to educate its customers through mass media campaigns. Therefore, bank personnel and customers as the social actors readily accept the institutional principles that already linger and encode these into scripts that guide their security behavior. The act of encoding creates a boundary for social actors to behave according to the scripts, thus constraining their actions.

7.2.3. Revisiting Principles Enactment: Intentional Versus Unintentional Actions

The principles enactment[2] starts from successful adoption of rules and encoded scripts among social actors. At this stage, social actors readily accept regulations and begin to socialize these regulations into their activities in the organization, attempting to make these newly regulated activities a routine or a habit. The acceptance and adoption

[2] As shown by processes b, f, and j in figure 7.1

of these regulations and institutional principles, or script enactment by social actors, ideally does not involve awareness (Barley and Tolbert 1997). The prescribed behavior is viewed as rational by social actors and is the only acceptable way to conform to the social structure. When formalized actions become embedded in a collective organizational behavior, social actors voluntarily behave according to prescribed institutional principles and rules as a routine rationale (Berger and Luckmann 1966; Powell and DiMaggio 1991; Scott 2008). Social actors adjust their behavior, whether or not they are aware of behaving in such a way, when interacting with artifacts and facilities (Barley 1986; Barley and Tolbert 1997; Giddens 1984).

This stage sees the implementation of rules set by the Central Bank, which are formed as institutional principles after repeated institutionalizations. The implementations of the institutional principles in different organizations depend upon the individualized modes of action and organizational culture. Centro Metropolitan Bank, for example, develops a framework for managing fraud, which is an implementation of Information Security Guidelines. On the other hand, Blue Sequoia Bank focuses more on technology. This bank implements the information security guidelines by deploying state-of-the-art security technologies system and investing in technology, most evidently by its use of electronic token device as a complimentary security authentication for electronic banking and transactions. This in turn forces Blue Sequoia Bank to develop standards of procedure for personnel using its security technologies and also adopt measures to raise its customers' awareness about the importance of security.

While there are scripts that serve as a prescription for behavior, social actors often do not consciously follow the scripts (Barley and Tolbert 1997). Social actors behave unintentionally, simply according to the scripts. When they realize that their behavior is according to the scripts, social actors reinstate their rationale in doing so. Bank personnel (e.g., management and staff members) and customers maintain their Organizational Information Security when they are restricted in their organization's institutional realm (Hazari et al. 2008). Managing security behavior can be achieved through the enforcement of security rules, culture, and value system (Dhillon 2001). Security behavior is determined by information security awareness and hence drives actors' compliance with security rules (Bulgurcu et al. 2010).

The prescribed behavior comes with a set of penalties for compliance failure. Penalty as an attribute of law is fundamental for the preservation of social order (Selznick 1969). This study believes that security behavior is a result of compliance with security rules and information security awareness (Bulgurcu et al. 2010). For example, as a governmental public institution, Earl Capita Bank has announced that personnel misusing data or using data for a purpose other than that originally proposed will commit a felony. To avoid misconduct, Centro Metropolitan Bank creates and implements a dual control and approval procedure for its data access request whereby a staff member from one division needs to create a formal request to the data-owning department. The data-owner department in turn forwards the request to the IT department for the actual data. These implementations demonstrate security management control, or institutional authority, of all the three dimensions: technical, formal, and informal. While Blue Sequoia Bank seems to pay more attention to technical control, the other two institutions have imbibed a more balanced focus on the issue of security-control dimensions.

The success of institutional principles of information security enactment is generally based on sanctioning, awareness, and habitualized routine. Studies have pinpointed the importance of sanctioning employees to perpetuate security rules in order to enforce information security (Bulgurcu et al. 2010; Herath and Rao 2009; Hong et al. 2006; Moulton and Coles 2003; Straub and Welke 1998; Von Solms and Von Solms 2009). Such principles enactment can therefore be classified into two general categories:

1. **Intentional/aware:** In this category, social actors safeguard their information asset with the awareness that they are under authority supervision and they feel responsible to the social system (i.e., institution) they belong to. While institutional and structuration scholars argue that institutionalization/structuration emerges from habitualized actions, this study is based upon formal institutions where regulations and bureaucracy are rigid and apparent. The rigidity of regulations and bureaucracy among these institutions is a result of the multilevel governance initiated by the Central Bank at the highest level. Not only do bank personnel feel responsible and obligated to support information security in their institution, bank personnel are threatened by the sanctioning of security rules.

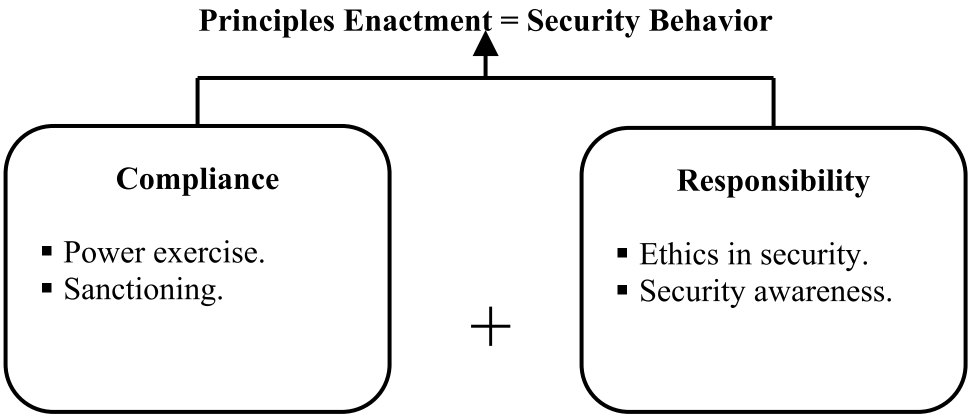


Figure 7.3 – Intentional Principles Enactment

Compliance emerges as an effect of power exercised by institutional authority (see previous section and chapters on deontic power and constitutive power) and sanctioning. Responsibility is an effect of social actors' awareness about their obligation towards information security and the need for engaging in ethical conduct to safeguard information asset (Dhillon and Backhouse 2000).

2. **Unintentional/unaware:** In this category, social actors safeguard their information asset simply because this action has become their daily, natural habit/routine. They are no longer consciously aware of their obligation to secure the information asset of their social system. As the scripts (or corporate security culture) linger in the institutional realm, social actors perform their routine tasks which include actions by which they are also preserving the security of their institution's information asset. Only when information security has become the norm and a culture, should social actors voluntarily preserve it (Vroom and Von Solms 2004). Institutional scholars such as Scott (1987; 2008) and Barley (1986) are strong proponents of this principles-enactment mode, as they believe that social actors unintentionally perform routines that are considered as rational by the members of the social system.

As they interact with information systems, depicted in the realm of action, social actors incorporate the two modes of principles enactment. Guided by scripts containing corporate security culture, social actors manage and maintain information security in their institution according to their conscience, the sense of responsibility that they feel towards the security of their information asset, and the fear of penalties and reprimand by their fellows and/or institutional authority. Due to the formal nature of the institution, the Central Bank and Commercial Banks demonstrate institutionalization as a regulative pillar as proposed by Scott (2008). Despite these actions becoming a natural habit amongst bank personnel during the phase of information security institutionalization, these actions which are done for the management and maintenance of information security are strongly governed and controlled by institutional authority which has the overall objective of preserving social order and stability.

7.2.4. Revisiting Script Revision and Script Replication

In this study, script revision and script replication[3] are used to depict certain moments during the occurrence of security breach incident. This process is actually intended to highlight institutional change due to extraordinary drives (e.g., technological change, economic downturns, or security breach) that cause social actors to purposely alter the institution. Script replication, however, is a connotation of a replication of patterned behavior that has become a habit. In Earl Capita Bank, the relatively non-existent case of security breach places the emphasis on script replication instead. This phase depicts an instance of regulatory adoption and acceptance of regulated behavior. The two cases pertaining to commercial banks which have been analyzed and discussed in the previous chapters depict how security breach incidents force personnel to alter the institutionalized information security and hence delineate script revision. The intricacy and danger of unidentified breach cases, which have the potential to seriously damage the

[3] Figure 7.1 shows two processes for each script revision and script replication. Processes c, g, and k denote script revision while processes c', g', and k' denote script replication.

reputation of both banks, are the drive and the objective for the banks to improve their information security.

In a formal organization, particularly one that exhibits a strong vertical hierarchy, script revision and replication proceed from the highest level to the lowest level in the hierarchy. The three case studies outlined in the previous chapters depict how social actors enforce the scripts, act according to the scripts, or modify the scripts. This process is common to all stakeholders, beginning from institutional authority to bank tellers and customers at a local branch. Bureaucratization creates the chain of command illusion, which relies particularly on rules and is in turn, is highly utilized for formal governance and control by institutional authority (Selznick 1969).

Script revision and replication are therefore a result of information security governance and control, with the objective to accomplish strategic objective, manage and prevent risks, and control and direct actions (see chapter 2). The two modes of script sustainability represent how rules and institutional principles are replicated and further sustained in a normal condition or altered and improved in the aftermath of a security breach incident. Despite these two modes being considered a collective action, script revision and replication occur under the watchful eyes of institutional authority. The institutional authority ensures security control and governance, and it oversees behavior that revises and deviates from security rules and institutional principles or behavior that naturally and voluntarily adheres to these rules and principles.

Now, we arrive at another facet of the issue. Had the breach incidents not occurred, the banks would have been under a wrong impression that their information security was adequate and rigorous (Rhee et al. 2005). One might argue that a security breach should be considered a ramification and a parasite that needs to be terminated. As a drive towards institutional change, however, security breach represents an exogenous environmental shock that thwarts "the successful completion of reproductive procedures" of information security governance and implementation in these two banks (Powell and DiMaggio 1991, p. 153). As such, security breach incidents are considered a focal starting point of re-institutionalization. Re-institutionalization signifies an "exit from one institutionalization, and entry into another institutional form, organized around different principles or rules" (Powell and DiMaggio 1991, p. 152).

A study by Ryan and Bordoloi (1997) identify the most prevalent security threats in medium to large organizations, including access to data/system by outsiders, natural disaster, loss due to inadequate backups, and inadequate or nonexistent logon processes. The breach case at Centro Metropolitan Bank demonstrates a weak physical control by another commercial bank. The Electronic Data Capture (EDC) fraud case of Centro Metropolitan Bank is a hard hit for the bank. However, the incident did not hurt the bank's financial performance. Knowing that the incident may damage its reputation for issuing a debit card that is easily manipulated, Centro Metropolitan Bank immediately pronounced the case to be a serious one that could tarnish the bank's reputation in the long run and the bank paid serious attention to the case.

The ATM skimming case at Blue Sequoia Bank had caused the bank to lose customers' trust. This case is an example of access of data/system by outsiders and the lapse forced the bank to figure out ways to improve their debit card transactions and ATM transactions. All mitigating and preventive measures involving technical upgrades and formal-control modification are a form of security policies improvement. As the two commercial banks alter and improve the security of their electronic-banking transactions, scripts containing security rules and institutional principles for the electronic-banking transactions change and hence are revised. Script revision requires conscious actions, through which social actors aim to improve certain procedures or to survive from a mishap. As an institutional change, re-institutionalization is a result of such modification.

The institutional change in Earl Capita Bank is however slightly different from that in the two commercial banks. Earl Capita Bank is progressing toward centralizing its information security into two information systems divisions: In addition to the two departments sharing responsibility for technical controls, the Information Technology Department is responsible for technical controls and the Information Management Division is responsible for formal controls. The institutional force was an endogenous drive that could have forced rapid changes within Earl Capita Bank's internal security rules. These instances instead have caused a gradual change in Earl Capita Bank. Such institutional change represents the institutional development of information security in Earl Capita Bank as the Central Bank, progressing towards centralization and elimination of data ownership while encouraging information stewardship. This is an instance of script replication.

While re-institutionalization of information security causes script modification, script replication represents institutional development. As introduced by Powell and DiMaggio (1991), institutions during institutional development are nowhere close to abolishment (i.e., de-institutionalization) but instead they become more complex. During institutional development, corporate security culture becomes more complex and more embedded in institutional realm as social actors become more familiar with and more accustomed to such a culture. As a subset of organizational culture, corporate security culture contains some of the attributes of organizational culture. Not only does it need to be shared among members of a social system, corporate security culture needs to have sufficiently functioned in order to become valid and capable of being taught to new members of the social system. The scripts replicate as social actors become more familiar with the culture and principles.

While script revision requires conscious actions, script revision is a natural occurrence as social actors continue to pursue their routines. Barley and Tolbert (1997) have signified that only contextual and exogenous changes contribute to script revision since social actors tend to resist changes and maintain status quo. Social actors "simply behave according to their perception of the way things are" (Barley and Tolbert 1997, p. 102). In this study, as more and more bank personnel voluntarily perform their routines, scripts that contain security rules and principles become more apparent and are replicated among bank personnel. Scripts based on secure procedures to use ATM, for example, are enforced and implemented by everyone, right from the top-level management at the central headquarters down to customers at a local ATM vestibule.

7.2.5. Revisiting Patterned-Actions Objectification and Externalization

As they become a habit, actions achieve patterns and start dwelling in the institutional realm over time. All collective security institutional principles and rules become a distinct culture in a formal organization. As part of the effects of action on structure, patterned-actions objectification and externalization exhibit how patterned actions accumulate into such a culture that is ready to be used as scripts in a subsequent institutionalization episode. The objectification and externalization of actions into the institutional realm require abstraction of habitualized actions and behavior until the new actions and behavior are considered rational and natural.

Only when patterned actions become a habit can they be habitualized and institutionalized. Social actors need to be acquainted with and socialized to these actions before such actions can be institutionalized (Berger and Luckmann 1966). The abstraction of patterned actions into the institutional realm is also termed as objectivated sedimentation (Berger and Luckmann 1966, p. 69). After a while, the habitualized activities become taken for granted. Social actors become unaware and unconscious and accept the rationality of behaving according to the prescribed script. The concept of rationale conduct serves as a foundation for agreement and acceptance among social actors, or an attribute of a social system (Selznick 1969). This study focuses on how bank personnel's interaction with security artifacts settles intoa habit and a rationale among amongst personnel belonging to the same institution. Prior to having their interactions institutionalized, bank personnel need to understand the information and security risk as well as the importance of information security.

This study demonstrates how personnel of the Central Bank are introduced to information risk and how such a risk can be harmful for the institution's reputation. Such introduction and socialization entails the imparting of information security education in order to raise personnel's awareness of information security. As institutional authority develops and enforces security rules, social actors are forced to adhere to these security rules and behave accordingly. This process requires extensive policy awareness and training, which can be used to reinforce security culture in the institution (Knapp et al.

2009). Security awareness and policy education are also important procedures to build up strong information security policies, which create a security culture when these are integrated into a strategic information systems plan (Doherty and Fulford 2006).

The objective of organizing and directing actions into natural and voluntary patterned actions of safeguarding information assets is to prevent similar incidents from occurring and to minimize any risk that has been previously overlooked. In the two commercial-bank case studies, this study divides the patterned-actions objectification and externalization into two schemes: Institutionalized patterned actions in a normal condition and Institutionalized patterned actions in the aftermath of a security breach incident.

In the aftermath of the EDC fraud, Centro Metropolitan Bank immediately formed a task force that heightened all three security-control dimensions. The ATM skimming case at Blue Sequoia Bank forced the bank to upgrade its online debit-card transaction process and the corresponding technologies. In addition to doing so, the bank also started to educate its customers on the importance of secure debit-card transactions and raised their awareness about information security.

The two cases of commercial banks cover an extensive array of security technologies, which portray the routine interactions between bank personnel and such technologies. Both commercial banks realize the necessity of increasing information security awareness among bank personnel in order to have successful interactions between bank personnel and security technologies. While they draw on their knowledge and experience to interact with technologies, bank personnel as social actors require more than awareness to initiate such interactions. Successful interactions require all resources and rules to dictate such interactions (Orlikowski 2000) and "sediment" these interactions into the social structure (Berger and Luckmann 1966; Barley 1986; Barley and Tolbert 1997).

According to Orlikowski (2000), the following are requirements which form the prerequisites to enact social structure based on sustaining social actors' interactions with technology artifacts:

- Knowledge of using technology artifacts.
- Experience with using technology artifacts.
- Formal rules and regulations about the use of technology artifacts.
- Power to enforce such rules and regulations.
- Communication between social actors on the use of technology artifacts.
- Organizational structure as a basis to reflect changes in social structure due to the use of technology artifacts.

These requirements in time accumulate into scripts for social actors to draw upon when interacting with security artifacts in subsequent institutionalization episodes. Built on the concept of actions upon the institutional properties of an organization as introduced by Orlikowski (1992), these requirements become scripts containing institutional principles of information security that are reinforced through interactions with security artifacts and are less likely to be altered. Using this view, information security is therefore an "enacted environment" that is built and strengthened upon by the conditioning of the three social structures: signification, domination, and legitimation (Orlikowski 1992, p. 411).

When institutional principles are altered due to institutional changes, behavior deviates and social actors become conscious of any such deviation and alteration. The different way social actors interact with security artifacts accumulates and slowly integrates with the existing security culture, creating new scripts to be used in the next security institutionalization episode. The subsequent episode depicts new, and expectedly improved, information security practices and governance. In the two commercial-bank cases, the commercial banks form a special task force that acts as a temporary institutional authority, overseeing improvement in security behavior and technology artifacts. The two commercial banks improve their respective technical controls by upgrading their security technologies, formal controls (e.g., Centro Metropolitan Bank creates a special unit that oversees debit-card transaction), and informal controls by educating their personnel (particularly customers) about changes in security technologies and new procedures for the use of such technologies.

Patterned-actions objectification and externalization serves as the basis for accumulating security culture in the institutional realm of information security practices and governance. Institutional changes such as a security breach incident (e.g., the ATM skimming incident or the EDC machine fraud incident) force script revision that in turn causes a deviation in actions. These new ways of interacting with security artifacts are conscious actions that require changes in technical controls, formal controls, and informal controls of information security. These new changes integrate with the existing security culture, creating new scripts. Routine actions, on the other hand, are natural occurrences that slowly accumulate into a security culture unique to the institution. Social actors unconsciously externalize and naturally objectify their security behavior. Regardless of such unconscious actions, social actors are still constrained by institutional authority, particularly by formal controls and informal controls. As such, while they naturally and voluntarily interact with security artifacts, social actors' security behavior is watched over by institutional authority through security rules and efforts to raise security awareness.

7.3. The Synthesis: Intra-Level Institutionalization

7.3.1. Overview

Unlike the previous framework, the framework for intra-level institutionalization focuses on formal interactions between two entities. This framework borrows the one introduced by Scott (2008), drawing on multilevel institutional processes. The foundation is built upon two types of institutionalization:

- Top-down institutionalization whereby an entity enjoying a higher authority has the capacity to sanction its actions to the other entity which has a lower authority. This process is recognized as the governance and control process in this study.
- Bottom-up institutionalization whereby an entity with a lower authority negotiates its actions with the other entity which possesses a higher authority. This process is termed as the conformity and report process in this study.

7.3.2. Governance and Control

An outstanding feature of this framework is the apparent use of power particularly by an entity possessing a higher authority, and acting as the central governance body. This entity, due to its high status in the social system, instantly assumes deontic power that it uses to sanction its actions (Hall 2008). While this power is prescribed to the governing entity, the deontic power's creation and ascription are artificially crafted by actors of a social system (Smith and Searle 2003). This study shows that, due to its deontic power, Earl Capita Bank, which is the Central Bank, assumes the authority to govern all banking operations in Centro Metropolitan Bank and Blue Sequoia Bank (as well as other commercial banks), including information security practices. This concept reinforces the fact that Earl Capita Bank behaves as such simply because of its authoritative status in the banking sector.

According to Hall (2008), deontic power directly renders the entity (i.e., the Central Bank) with constitutive power, which this entity uses to formulate and enforce rules for itself to adhere to. Hall (2008) states that social relations based on constitutive power can produce particular kinds of actors who behave accordingly in a social system. The central governing body such as the Central Bank that assumes this power has the privilege and authority to direct social relations and thus control behaviors of social actors. Constitutive power is one such powerful tool in the hands of the Central Bank to affect governance of practices in commercial banks and financial institutions alike (Larner and Le Heron 2005).

Equipped with these two types of power, can Earl Capita Bank play its significant role in banking sector (Quaglia 2008), including its role in information security governance and practices? These powers empower Earl Capita Bank to be the authority of investigation if the information assurance of each commercial bank is according to the prescribed information security guidelines. These powers enable Earl Capita Bank to summon a representative of a commercial bank should a security breach incident be caused by the commercial bank's own failure to safeguard its information asset or failure to comply with the prescribed guidelines. This allows Earl Capita Bank to penalize a commercial bank for such failures.

Moreover, Earl Capita Bank also owns the authority to prevent the massive impact that a security breach incident might have (i.e., systemic impact) by formulating and enforcing new, abstract/general rules[4]. The Bank-Indonesia case study has depicted the Central Bank to have developed an information-security guideline for commercial banks and financial institutions operating in Indonesia. The formulation and enforcement of this guideline demonstrates that Earl Capita Bank, acting as the authority, indicates information risks, particularly the levels of each risk and the mitigation plan. This participation is an essential part of information security governance (Brotby 2009; Von Solms and Von Solms 2009). Earl Capita Bank can also dispatch a team to undertake random inspections and conduct audit of information systems (including their security features) of a commercial bank. The EDC fraud case shows how Earl Capita Bank exercised its powers to ensure that all EDC machines were being used for online transactions only so as to prevent similar EDC fraud cases from reoccurring.

The impact of power in institutionalization is significant. Silva and Backhouse (2003) have addressed how power helps routinize (i.e., habitualize) actions so as to

[4] A respondent from the Central Bank opts for the use of guideline in lieu of rule. The reason is to provide liberty and creativity to commercial banks in accordance with each bank's organizational culture.

become institutionalized. Lapke (2008) demonstrates how management utilizes power to force subordinates to comply with security policy to the point where security actions become institutionalized. According to Silva and Backhouse (2003), two types of power, namely dispositional power and facilitative power, are utilized by a social actor or an organizational actor to cause another social actor to do what he/she would not do otherwise. The dispositional power is similar to the concept of deontic power described in this study in that it equips a social actor with the power to enforce behavior due to his capacity in the social system. This type of power emerges due to social conditioning. The facilitative power is concerned with the systemic approach to control. This type of power equips a social actor with various techniques to discipline other social actors. As such, the use of these powers to repetitively, as well as routinely, enforce a desirable behavior causes such behavior to be institutionalized. Unlike that proposed by Lapke (2008), however, social actors that are subordinates are not able to resist the enforcement due to the strong sense of deontic power of Earl Capita Bank that forces commercial banks, including Centro Metropolitan Bank and Blue Sequoia Bank, to comply. In this study, Earl Capita Bank uses the deontic power (or facilitative power) and has the power to use various techniques (e.g., penalty, auditory visit, etc.) to force Centro Metropolitan Bank and Blue Sequoia Bank to implement information security practices and governance. Figure 7.4 shows the use of these power types on the intra-level institutionalization of information security whereas social actor A denotes Earl Capita Bank and social actor B denotes commercial banks, including Centro Metropolitan Bank and Blue Sequoia Bank.

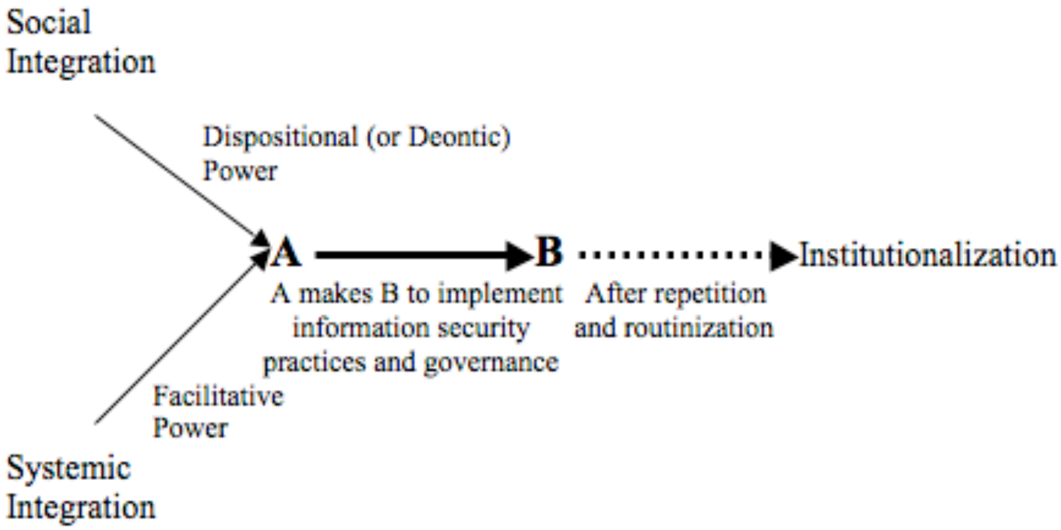

Social Integration
Dispositional (or Deontic) Power
A
B
Institutionalization
A makes B to implement information security practices and governance
After repetition and routinization
Facilitative Power
Systemic Integration

Figure 7.4 – A Reproduced Model of Circuit of Power and Institutionalization by Silva and Backhouse (2003)

In general, the objective of governance and control that the Central Bank practices is to maintain price stability by keeping the inflation rate low and stable (Ising 2009; Ullrich 2007). The macro-prudential supervision is a distinct feature and privilege owned by the Central Bank due to its status (i.e., deontic) in banking sector. The macro-prudential supervision is the governance and control tool that is used to direct and oversee commercial banks and financial institutions, to ensure that risks are minimized in order to sustain financial stability (Krauskopf and Steven 2009). The information security governance and control by Earl Capita Bank is simply a smaller, minor part of the larger macro-prudential supervision that Earl Capita Bank implements to help commercial banks mitigate their operational risk, which comprises information risk. Earl Capita Bank is as such an essential key player whose participation and involvement are significant for the successful management of operational risk (Van Greuning and Brajovic Bratanovic 2000; Fragniere et al. 2010).

7.3.3. Conformity and Report

Due to the strong deontic power as well as other types of power (e.g., constitutive and facilitative), commercial banks and financial institutions are required to adhere and conform to rules enforced by Earl Capita Bank. Herein, the top-down institutionalization and the bottom-up institutionalization in intra-level institutionalization are established due to the strong implication of institutional relationship. The Centro Metropolitan Bank case study and the Blue Sequoia Bank case study have shown the significance of institutional relationship by creating a Compliance Division. As a special business unit in a commercial bank, the Compliance Division is assigned with the responsibility to communicate with the Central Bank on behalf of its institution, to monitor compliance with the Central Bank's regulations, and to assist other business units and divisions to achieve objectives that are regulated by the Central Bank.

There are two types of implementations of prudential bank supervision: off-site surveillance and on-site examinations (Van Greuning and Bratanovic 2000). The on-site examinations require the central bank to dispatch auditory teams to examine the appropriateness of banking operations. These inspections may also be triggered by problems identified by the off-site surveillance reports (Van Greuning and Bratanovic 2000). The case studies have witnessed Earl Capita Bank as sending its auditory teams regularly to commercial banks in normal circumstances. The case studies show that Earl Capita Bank investigated a commercial bank's security policies and regulations, server location and physical IT infrastructure, the security of a commercial bank's Electronic

Banking Services, Business Continuity plans, etc. Earl Capita Bank may also send its auditory teams for unannounced auditory visits after a security breach incident occurs.

The reciprocity actions by commercial banks aim to induce the Central Bank to perform further actions which are necessary to maintain stability in banking sector (Hall 2008). The reporting practice is an extended obligation of commercial banks, as commercial banks are required to conform to a set of guidelines. This practice is an example of off-site surveillance as the Central Bank collects data from reports issued by a commercial bank (Van Greuning and Bratanovic 2000). The policy competencies of the Central Bank affect the supervisory arrangements as these are monitored by the Central Bank (Quaglia 2008).

The Central Bank requires such reporting to be able to monitor individual commercial banks, compare an individual commercial bank's performance among its peer group, and detect any significant deviation from its peer group (Van Greuning and Bratanovic 2000). In the context of this study, commercial banks submit their reports through their Compliance Divisions, depicting institutional development needs, financial sector and regulation, risk management culture, corporate governance, and various risk management practices that include managing operational and information risks. The Central Bank also uses collective reports from commercial banks to determine a benchmark and best practices. The Centro Metropolitan Bank case study delineates Earl Capita Bank conducting unannounced inspections of EDC machines to ascertain that there was no offline feature on EDC machines in use and allowing only the use of online transaction for EDC machines. A commercial bank requires a license not only to operate, but also to provide services such as Electronic-Banking Services. This license, issued by the Central Bank, protects a commercial bank's financial safety net and consumers, and provides a barrier to entry of institutions that do not meet the stringent criteria to operate as a bank (Schooner and Taylor 2009). Figure 7.5 depicts the details of prudential banking supervision context.

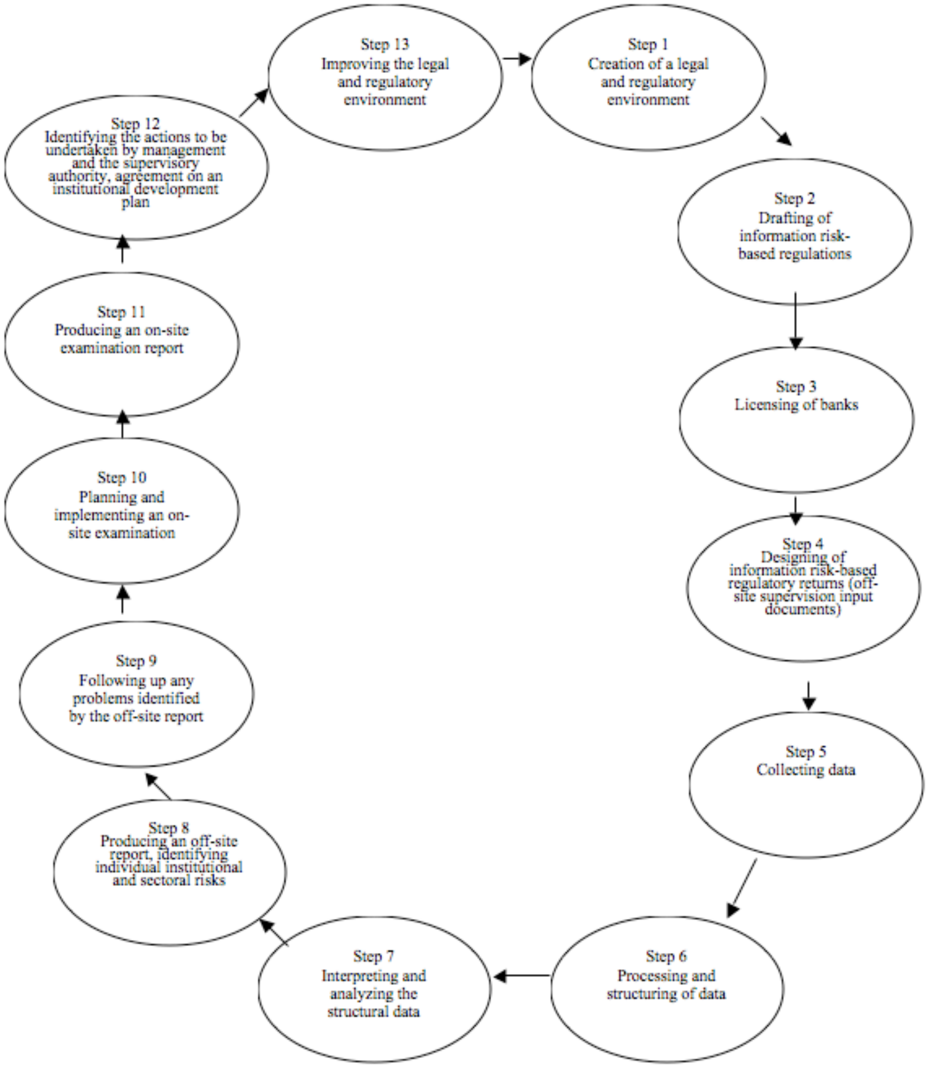

Step 13
Improving the legal and regulatory environment
Step 1
Creation of a legal and regulatory environment
Step 2
Drafting of information risk-based regulations
Step 3
Licensing of banks
Step 4
Designing of information risk-based regulatory returns (off-site supervision input documents)
Step 5
Collecting data
Step 6
Processing and structuring of data
Step 7
Interpreting and analyzing the structural data
Step 8
Producing an off-site report, identifying individual institutional and sectoral risks
Step 9
Following up any problems identified by the off-site report
Step 10
Planning and implementing an on-site examination
Step 11
Producing an on-site examination report
Step 12
Identifying the actions to be undertaken by management and the supervisory authority, agreement on an institutional development plan

Figure 7.5 – A Reproduced Prudential Banking Supervision Context by Van Greuning and Bratanovic (2000)

7.4. Emergent Themes

This study has discovered three important themes that explain the unique context of institutionalizing information security in the banking sector. The themes emerge due to the strong nuance of an institution. The three themes are habitualized security routines, information stewardship, and institutional relationship.

7.4.1. Habitualized Security Routines

Central to the structuration of an information system is the interaction between a social actor and technologies (i.e., the artifact), that allows technologies to manifest as a meaningful variable in the organization (Orlikowski 1992). In the context of information security, the aim of institutionalization is to create a secure social structure in an information system through interactions between social actors and security technologies. Each of the three cases delineates the regulated and structured interactions between stakeholders and security technologies. In addition to the security technologies, additional modalities include the social actor's experience and knowledge of using technologies as well as procedures and regulations of information security. As such, social actors use their knowledge and interpreting ability to interact with security technologies and sanction such interactions vis-à-vis` security policies or regulations. These modalities lay a foundation that links structure and social actions committed by social actors (Walsham 1993). This study has conceptualized an information security culture that embodies security rules, procedures, methods, and responsibilities, and becomes a natural habit or a routine that is performed by personnel (Von Solms 2000; Chang and Lin 2007). As one of such abstractions, habitualized security routines are a manifestation of the principles enactment which social actors readily and unconsciously use to act. Therefore, while script encoding entails encoding security culture from institutional realm to create the script, principles enactment transforms the script into habitualized security routines that linger in any social actors' conscience.

Researchers have denoted that a social structure contains a signification structure, a domination structure, and a legitimation structure (Giddens 1994; Walsham and Han 1991; Walsham 1993). The institutional realm that embodies these three structures also contains institutional properties of social actions in a technology usage context (Barley and Tolbert 1991; Orlikowski 1992; Orlikowski et al. 1995; Orlikowski 2000). In the context of this study, the institutional properties are prescribed in the corporate information security culture, offering detailed elucidations of the practice of security technical controls, formal controls, and informal controls. Institutionalization of information security is best approached using these three dimensions (Dhillon 2007). These security-control dimensions provide a foundation for other aspects that serve the enactment of the three social structures and include security responsibility and modalities (e.g., technologies or regulations). Furthermore, once these security-control dimensions have become a routine within an organization, they produce and shall continuously reproduce the habitualized security routines. The habitualized security routines help resist any attempt to dissolve the information-security institution[5].

The three security-control dimensions do not simply appear as an abstraction of routines. Once they are adopted through principles enactment, these dimensions become visible and tangible in the form of actions. Technical controls are implemented as social

[5] The notion of habitualized routines is conceptualized under the notion of 'taken-for-grantedness' proposed by sociologists (Berger and Luckmann 1966; Powell and DiMaggio 1991; Scott 2008).

actors start to use security artifacts such as PIN number as in the case of Centro Metropolitan Bank's SMS banking, Electronic Token Device to use Internet banking features as in the case of Blue Sequoia Bank. Technical controls are also about procedures or formal methods to protect data and software. For example, encryption, hash totals, reuse prevention, and check bits are all formal methods and procedures that are commonly used in addition to the use of security technologies (Dhillon 2007, pp. 20-21). The three case studies have noted the significant and necessary use of formal controls. Not only formal controls need to be enforced in the intra organizational level, but formal controls are also implemented directly by the Central Bank on a intra level. Lastly, the two commercial-bank case studies have depicted the importance of informal controls for the purpose of communicating security rules and procedures to customers and branch offices. For example, Centro Metropolitan Bank communicates the mechanisms of its dual-approval procedure to all branch offices while Blue Sequoia Bank releases its branch offices from adhering to a strict predefined conduct so as to provide freedom to implement information security according to each branch's culture.

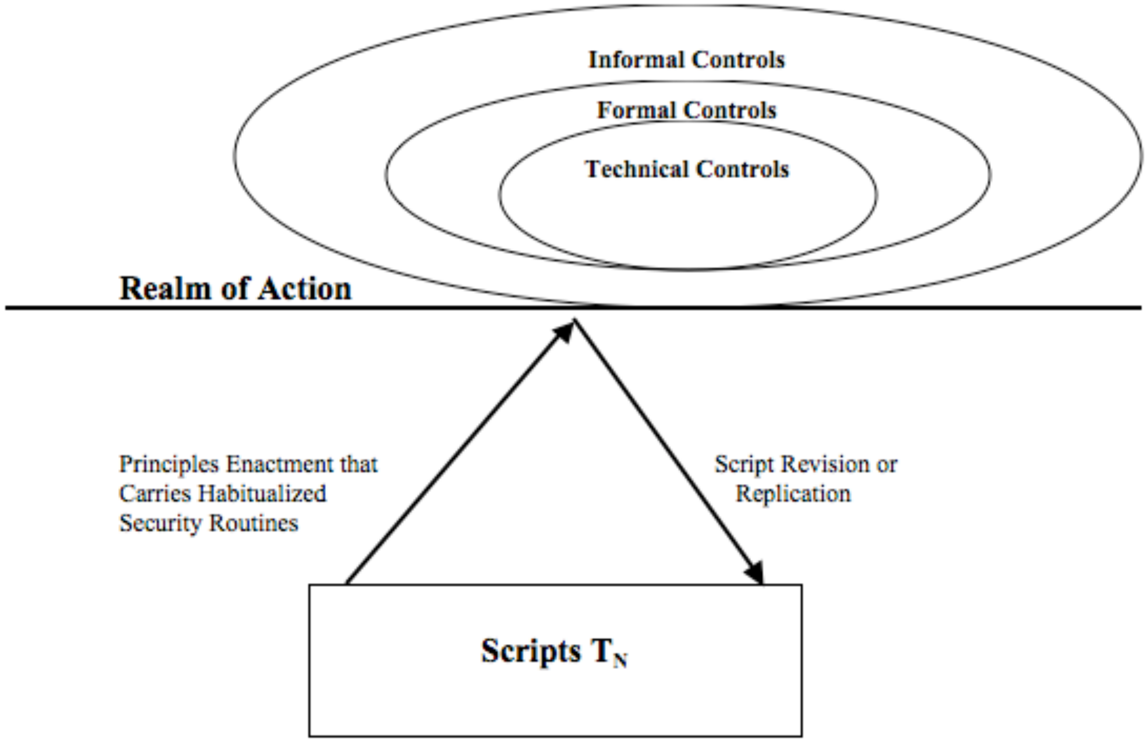

Informal Controls
Formal Controls
Technical Controls
Realm of Action
Principles Enactment that Carries Habitualized Security Routines
Script Revision or Replication
Scripts T_N

Figure 7.6 – A Close-Up View of Realm of Action

Such visible and tangible appearances of the three security-control dimensions manifest as behavior and actions represented at the realm of action. Such conceptualization is in line with that by Barley (1986) and Orlikowski (2000) whereas the realm of action is a continuous interaction between social actors and modalities (interpretive scheme, artifacts, and norm) in an ordered manner. Empirical analysis of the three case studies confirms the order of the interrelation of security-control dimensions as proposed by Dhillon (2007). While the three are said to be intertwined and interrelated, conceptually and evidently, the technical controls are directed by formal controls, which are communicated through informal controls (see figure 7.6).

The fundamental conceptualization of habitualized security routines is devised by the unintentional/unaware principles enactment. Institutional and structuration scholars have acknowledged key concepts such as habit, routine, unintentional, natural, rational, unaware, or unconscious as directing behavior in the long term. The objective of building such conceptualization is to understand the transformation of such complex script into an abstraction of daily chores of information security practices and governance. When a social actor is informed of the script that contains the corporate information security culture, she is naturally translating the script using her experience in and knowledge about information security. Such a natural or unconscious translation cannot occur unless her experience and knowledge of information security has previously "sedimented" (Berger and Luckmann 1966) in the institutional realm as part of the security culture. Therefore, a social actor that is a member of the institution is said to have habitualized all security routines to direct her security behavior. These routines in turn transform into an abstraction (Berger and Luckmann 1966) that originates from a habit of using artifacts (Orlikowski 1992; 2000) and remains as such in the institutional realm (Barley 1986; Barley and Tolbert 1997).

On the other hand, intentional/aware principles enactment cannot contribute to the creation of habitualized security routines. This is because social actors are aware of their routines and may be inclined to object to the performance of such routines. In this sense, power and regulations become a required tool for enforcing 'habitualizing' security routines. The three case studies demonstrate a rigorous enforcement of information security technical controls. The case of Earl Capita Bank depicts the dual technical controls of information security by its IT division and it's Information Management

Division. The two departments oversee the implementation of the physical and logical aspects of security technical controls. The IT Division manages and maintains the institution's IT systems and security systems (i.e., the physical aspect) while the Information Management Division focuses on protecting the information resource of the institution (i.e., the logical aspect). While the IT Division enjoys exclusive privilege to govern the physical aspect of technical controls (e.g., enforcing the use of username and password), the Information Management Division has to share the logical aspect with other departments within the institution. The two divisions also formulate regulations on securely using information systems and communicate such controls (i.e., formal controls and informal controls). As a consequence, personnel of Earl Capita Bank are forced to comply with these controls in order to subsequently form the habitualized security routines in the long run.

7.4.2. Information Stewardship

Dhillon and Moores (2001) suggest that technical controls are not sufficient to provide sound secured information systems. They state that:

> "Merely establishing a password is not enough. What is really needed is an understanding of the organizational structures and business processes and identifying a range of checks and balances that could be established. These could then be incorporated into the systems development processes."

Their argument is based on the assumption that security is an organizational problem. Central to the study of organizations is the stakeholder. Post et al. (2002, p. 19) formally define stakeholders of any organization as "the individuals and constituencies that contribute, either voluntarily or involuntarily, to its wealth-creating capacity and activities, and that are therefore its potential beneficiaries and/or risk bearers." While not all of them have direct obligations to the institution, such individuals and constituencies bear the impact of information risk. This study identifies and portrays the assigning of each division or each business unit as an information steward, which generally functions to protect the institution's information assets. An information steward "develops a sound architecture, motivates and develops IT staff, aligns IT plans with business plans, and protects the organization's information assets" (Chen and Preston 2007). The information stewardship is therefore synonymous with the three security-control dimensions: technical controls, formal controls, and informal controls. In the case of the Indonesian banks, the role of an information steward is assumed by all divisions that own information systems and generate information, as demonstrated by the three case studies.

The case of Earl Capita Bank, for instance, depicts the dual control of information security with technical controls being an exclusive privilege of the institution's IT department. The IT department assumes the sole responsibility of controlling the technical aspects of the institution's information security. The Information Management Division however defines the role of information stewardship for all other divisions that own information systems. This assignment is an attempt to reduce the strong data ownership that hinders IT-governance centralization as well as security-governance centralization. The data-ownership issue in Earl Capita Bank is a major stumbling block for the Information Management Division to assume the logical-aspect primary leadership. For instance, the IT department has the full authority to announce and implement a new security patch for the institution's local area network and maintain its implementation. The Information Management Division, however, needs to discuss and request permission to reestablish the confidentiality context of a document published by another department within the institution.

In the three case studies, IT division as well as Information Security Division manages technical controls. The central theme of technical controls is technologies. Technologies are inscribed with particular symbols and material properties (Orlikowski 2000) and become a meaningful variable only when their use can be manipulated to assist any social actor in his work (Orlikowski et al. 1995). Technologies, particularly IT artifacts, are socially and cognitively altered by the social actors, and are always embedded in a fragment of an instance (e.g., time and place), consisting of interconnected components, emerging from continuous social and economic interactions, and are dynamic (Orlikowski and Iacono 2001). Many information systems lack security features which can be attributed to security underestimation during the systems analysis and design (Dhillon and Moores 2001). Such underestimation is due to the irrational optimism of management about the security features of an information system (Rhee et al. 2005). All respondents of the three case studies agree that information security is an organizational issue. Hence successful information risk management and control depends on sound information-security governance.

The Centro Metropolitan Bank case study and the Blue Sequoia Bank case study demonstrate the possession of formal controls and informal controls by divisions that process and disseminate information, and own information systems. These divisions, which act as information stewards, filter personnel who can access their information, how the information is accessed, and what information can be accessed. Information steward is the executor of information security governance since it seeks to accomplish the same objective as that of security governance. The emphasis is therefore on executives, controls, and information risk (Brotby 2009; Von Solms and Von Solms 2009). Information stewardship differs from information security governance in that stewardship focuses on data and information using the confidentiality, integrity, and availability concepts (Baldwin et al. 2012). While the three case studies have shown the existence of such a concept, the notion of information stewardship has been somewhat leaning towards the stronger notion of data ownership as apparent in the Earl Capita Bank case study. The concept of data ownership regards an entity as not only the protector of data, but also the owner of data, while the concept of information stewardship implies the steward as a data-security service provider (Baldwin et al. 2011). The data ownership has created small kingdoms of many information owners among divisions in Earl Capita Bank. A beginning is being made to eradicate this status quo now as a means to achieving data and information centralization.

Information stewardship, particularly as implemented in Earl Capita Bank, is an impeccable example of the interrelatedness of technical controls, formal controls, and informal controls. An institution's IT division uses its authority to regulate stakeholders of other divisions, including customers and the public, on the kind of data and information they are allowed to access and use, the method of such access (e.g., online access, hardcopy, etc.), and the purpose of such access. Despite each division owning the authority as an information steward, the IT division, or the Information Security Division, assumes the technical controls for data and information access in the institution. As such, divisions consult the IT division for technical access such as user privilege assignment.

7.4.3. Institutional Relationship

Institutional relationship is closely related to prudential supervision, is a functionality that aims to “preserve the safety and soundness of an institution,” (Schooner and Taylor 2009, p. 261). This is in line with the objective of preserving social order and stability. Institutional relationship is created due to the manifestation of the Central Bank’s powers to govern, monitor, and control the commercial banks and the commercial banks compliance, conformity, and adherence with the Central Bank. Institutional relationship emerges when there is a need for changing conditions that depend on the levels of individualism, power distance, masculinity, and uncertainty avoidance which are exhibited by the parties in the relationship (Shankarmahesh et al. 2003). An institutional relationship can be viewed as a relationship that involves two or more formal organizations bound by regulations and power. The Central Bank in general implements two types of power: deontic and constitutive (Hall 2008). These powers can be extended to include facilitative power (Silva and Backhouse 2003). Using these powers, the Central Bank formulates information security guidelines that are adopted by commercial banks and expanded according to each bank’s specific needs and organizational culture.

During adoption through implementation of security rules, the Central Bank exercises its deontic power (i.e., a power bestowed upon an entity due to its status in its social community) to govern and monitor the implementation. Deontic power also allows the Central Bank to exercise its constitutive power for formulating and enforcing regulations, including the information security guidelines. While such powers are undermined in developed countries to allow for creative implementation of such rules among commercial banks in developed countries, commercial banks in developing countries (e.g., Indonesia) endure sanctioning and penalties for failure to comply with regulatory adoption (Schooner and Taylor 2009). In developing countries, centralized, concentrated power exercised by the Central Bank serves "to compel a change in the culture of regulation" (Schooner and Taylor 2009, p. 272).

The core of institutional relationship is institutional authority. Institutional authority appears as a direct response to identify risks and to implement information security controls (Parrish 2000). Merely controlling critical infrastructures (i.e., technical controls) is inefficient and is beyond the direct control of organizations (Dutta and McCrohan 2002). Therefore the control of all security-control dimensions (i.e., technical, formal, and informal) is necessary to achieve efficiency. Due to the intricate nature of security-control dimensions, an internal control system is required to ensure security control. In general, the objective of an internal control is "to cover the aspects of quality and security as key control objectives in order to take care of ICT controls" (Omoteso et al. 2010, p. 160). Such internal control follows what is prescribed by the Central Bank. The internal control hence serves as a compliance authority in a commercial bank. Furthermore, the internal control manifests as an impact of the institutional relationship. The Compliance Division initiates this internal control to be implemented by all other divisions. While technical controls belong almost exclusively to IT division, formal controls and informal controls are implemented by all other divisions, particularly divisions that act as Information Stewards.

As discussed previously, each commercial bank assigns its Compliance Division to act as a single door for communication with the Central Bank. This division is a representative of its institution in matters related to the institutional relationship between a commercial bank and the Central Bank. All operational reports of a commercial bank are submitted to the Central Bank by the Compliance Division, including reports on Information Security and infrastructure. On the other hand, the Central Bank uses the Bank Supervision Division and the Accounting and Payment System Division to communicate with commercial banks. While the latter focuses on governing and controlling accounting and financial matters, the first deals with governing and controlling all matters other than accounting and finance. While technology and security infrastructure as well as information and communication issues are the responsibility of the Bank Supervision Division, the Accounting and Payment System Division assumes the responsibility to govern information systems that are used for accounting and financial issues.

7.5. Summary and Discussion

The final but important stage of this study is to review how synthesized concepts and emergent themes are used to answer research questions. The extent to which this study contributes to the body of literature depends on the interwoven concepts and themes. For example, this study has suggested that habitualized security routines emerge when social actors continue their daily, natural, activities involving information security governance and practices and strive to resist the impact of security breach as it is deemed to deviate from their routines.

The first issue that begs a response is the internalization of information security governance and practices in institutions. The key concept of security internalization is habitualization or ‘being accustomed to’. This study shows that there are two realms of security institutionalization based on Barley and Tolbert’s framework (1997). When implementing security governance and practices, social actors draw on the corporate information security culture through various processes. In addition, social actors also store their routines that involve information security governance and practices in the form of a conceptualized security culture[6]. Performing these activities creates a continuous internalization of information security governance and practices. The result of internalizing information security governance and practices is the formation of habitualized security routines. Vice versa, the habitualized security routines are an abstract component of information security culture since these presuppose knowledge and experience of information security as well as incorporate formal regulations about information security among others (Orlikowski 2000). This study demonstrates that security routines become security culture through script replication and patterned-actions objectification and externalization.

In a formal organizational setting, simply relying on unintentional principles enactment is not sufficient. Management that also acts as an authority is required to ensure that principles enactment of information security governance and practices is successful. While personnel are in general trustworthy, some may be unreliable and pose an internal threat (Dhillon and Moores 2001). In addition, management plays an important role in sound information security (Von Solms and Von Solms 2009). Information stewardship is assigned to each division management so as to safeguard information assets (Chen and Preston 2007) by enforcing all three security-control

[6] This instance is the objectification and externalization of information security practices and governance into the institutional realm.

dimensions. This is also true in the context of the intra-level institutionalization. The Central Bank as the central governance body overlooks minor aspects of information security governance and practices in commercial banks to ascertain the successful formation of habitualized security routines in these institutions.

The second issue looks at how the Central Bank affects the institutionalization of information security. In banking sector, the Central Bank plays a major and critical role. This role includes governing and controlling the implementation of information security governance and practices in commercial banks and other financial institutions. The fundamental concept behind this issue is the institutional relationship. This study demonstrates that institutional relationship stands on Scott's framework of multilevel institutional processes (Scott 2008). There are two processes in the institutional relationship: a top-down process from the Central Bank to commercial banks and a bottom-up process from a commercial bank to the Central Bank.

	Research Thematic		
	Security Internalization	*Central Governance Impact*	*Security Re-institutionalization*
Habitualized Security Routines	Routines are built from a collection of security culture through principles enactment. Actors reproduce routines during script replication and store routines during objectification and externalization.	The Central Bank ensures that routines are well implemented in commercial banks and become a habit.	Routines help prevent security breach as these serve as a basis for resistance to re-institutionalization.

Information Stewardship	Intentional principles enactment is used to implement technical controls, formal controls, and informal controls by management.	The Compliance Division acts as an intermediary of the Central Bank to assist information stewards in their attempt to implement the three security-control dimensions.	Security breach changes how information security is implemented as the victim institution assigns each division to improve its security controls.
Institutional Relationship	The Central Bank oversees the implementation of habitualized security routines through regular audit and requires regular reports from commercial banks.	The Central Bank governs and controls the implementation of information security while individual commercial bank reciprocates through conformity and reporting.	The Central Bank regularly audits security controls in each commercial bank and may conduct surprise audit when security breach hits. Similarly, commercial banks regularly report their security governance and practices to the central bank and implement any regulatory changes decreed by the central bank.

Table 7.1 – An Interpretive Framework for Information Security Institutionalization

The impact of the central bank's intervention and participation in security practices and governance in each commercial bank becomes obvious when security breach occurs. The central bank uses its power to change security rules and conduct surprise auditory visits to the premises of commercial banks, particularly any commercial bank which is the victim of the security breach. In doing so, the Central Bank manages the systemic risk (Van Greuning and Bratanovic 2000) that is caused by security failure in one commercial bank. During a normal condition, the Central Bank undertakes a regular, or annual, auditory visit to commercial banks and requires commercial banks to report their information security governance and practices. This study shows that the Compliance Division serves as a single door for communicating with the Central Bank and as an intermediary of the Central Bank. As an intermediary, this division assists each division that acts as an information steward to implement the three security-control dimensions.

The issue regarding information security re-institutionalization after a security breach relies on the very fundamental concept of an institution. Institutions never emerge from nothing and resist changes (Scott 2008) in order to retain social order and stability (Burrell and Morgan 1979). In an inter-level institutionalization, information stewardship proves to be a powerful tool in preventing security breaches. Institutional relationship is another safety feature from a intra-level institutionalization perspective.

The important issue in re-institutionalization is, however, the fact that security breach is merely an instance in information security. While it is viewed as a nuisance by most scholars and practitioners, security breach is a major incident that drastically changes and impacts how information security is handled and implemented in an institution. Computer crimes are considered subversive acts (Dhillon and Moores 2001) rather than an episode of information security institutionalization. In this study, security breach re-institutionalizes information security through script revision whereby social actors improve their information security governance and practices. Such improvement, for example, includes changes in technical controls (e.g., technologies and procedural upgrade), formal controls (e.g., new and improved security rules), and informal controls (e.g., increased security awareness). The objective of doing so is to prevent similar breach incidents from occurring and causing a damaging impact on the bank and on other commercial banks (i.e., systemic impact). Information stewardship in this study manifests through formal controls and informal controls in which each division controls the logical aspect of security and communicates information concerning such controls to personnel of other divisions.

8 CONCLUSION

8.1. Overview

This study has explored the internalization of information security governance and practices, involving collective individuals placed in a form of formal organization. Such a phenomenon is termed as the institutionalization of information security. Using theoretical frameworks by Barley and Tolbert (1997) as well as by Scott (2008), this study has demonstrated that there are many drives and considerations that affect security institutionalization. In this chapter, all previously discussed concepts and emergent themes are summarized and reviewed. Several important concepts are revisited: specifically- information security institutionalization and re-institutionalization, and the impact of a central governance body.

8.1.1. Information Security Institutionalization and Re-institutionalization

Central to this study is the institutionalization of information security. The argument presented in this study is that information security governance elucidates the interaction between knowledgeable human agents and the wider social system within which they exist. Another argument that merits consideration is that information security governance becomes institutionalized through social integration of routines and system integration of relevant technologies. This study conducts an overview of two commercial banks and the Central Bank of Indonesia as the unit of analysis.

The fundamental conception of this study is built on standard information security practices and information security governance. Kawaura (2004) has demonstrated a failure in corporate governance among Japanese banks, leading to systemic damage in the Japanese banking sector in the 1990s. Information security governance is a vital requirement, required to direct information security practices and to ensure sound information security. This study has shown how information security governance directs the following aspects in information security: Strategic and Risk Management, Resource Management and Business Process Management (Brotby 2009), which embody the strategic, tactical, and operational aspects of information security (Von Solms and Von Solms 2006a). Information security governance therefore redirects not only the human resources and formal organizational structure, but also the technical resources by virtue of managing the operational and environment aspects of security technical resources and ensuring business continuity (Da Veiga and Eloff 2007). Scholars have also recognized the importance of the role of executive and top management in information security governance (Dutta and McCrohan 2002; Khalfan and Alshawaf 2004; Knapp et al. 2006).

This study has depicted the significant impact of enforcing and adhering to information security policy. Information security policy as a set of regulations directing security behavior is necessary to promote sound information security (Cuppens and Cuppens-Boulahia 2008). Top management support is also a key factor that sustains good practices of information security (Hong et al. 2006; Fulford and Doherty 2003). In this study, key players such as the Central Bank, the Board of Directors, and the Bank Management are assuming the authority to formulate, enforce, and communicate Information Security Policy. The concept of principles enactment introduces the intentional, or consious, enactment, by which the bank's key players and personnel are coerced into complying with security policy, whether they are motivated or not, to do so (Bulgurcu et al. 2010). Scholars have denoted such phenomena as an impact of structuration sanctioning (Giddens 1984; Orlikowski 1992; Orlikowski 2000; Orlikowski et al. 1995; Walsham 1993; Walsham and Han 1991) whereby bank stakeholders face the consequences of compliance and compliance failure (Selznick 1969).

All such phenomena embody the three security-control dimensions: technical controls, formal controls, and informal controls (Dhillon and Moores 2001; Dhillon 2007). The institutionalization of information security depends on the intertwining of the three security-control dimensions (Dhillon 2007), that manifest into behavior and actions aimed at safeguarding information assets. In this study, security governance and practices that become a habit and a routine over time are internalized by members of an institution and get transformed into information security culture, which is built on experience and knowledge (Orlikowski 2000).

One of the highlights of this study is the impact of security breach on security institutionalization. The majority of scholars and practitioners regard security breach as a plight that results from unethical conduct (Dhillon and Moores 2001). This study contends that security breach is another episode in information security institutionalization. Security breach drives such institutionalization into a different direction through script revision that changes how technical controls, formal controls, and informal controls are implemented. Security breach forces an institution to upgrade its technologies and resources (i.e., changes in technical controls), improve security regulations (i.e., changes in formal controls), and increase security awareness (i.e., changes in informal controls). Security breach draws the attention of the Central Bank, which aims to mitigate systemic risk. Security breach is hence a variant mask of security institutionalization.

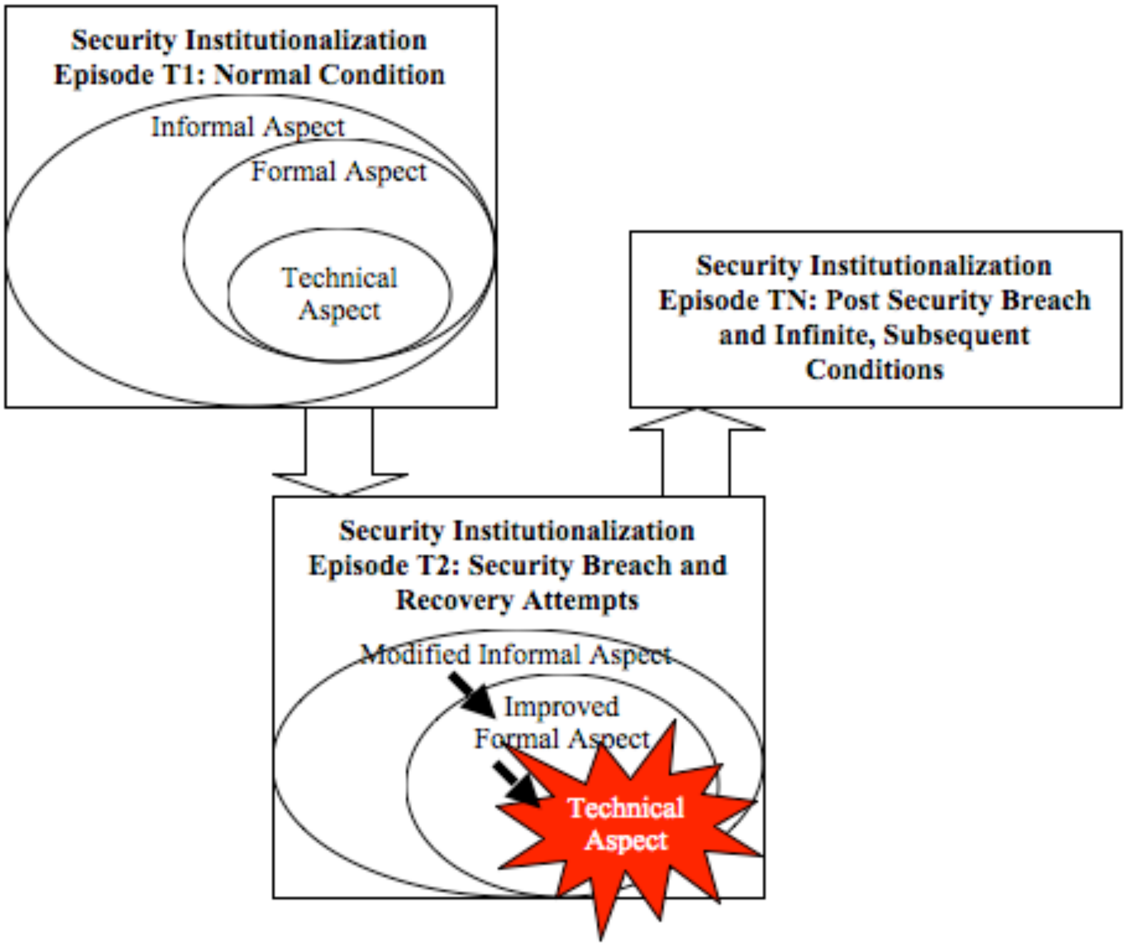

Security Institutionalization
Episode T1: Normal Condition
Informal Aspect
Formal Aspect
Technical
Aspect
Security Institutionalization
Episode TN: Post Security Breach
and Infinite, Subsequent
Conditions
Security Institutionalization
Episode T2: Security Breach and
Recovery Attempts
Modified Informal Aspect
Improved
Formal Aspect
Technical
Aspect

Figure 8.1 – A Simplified View of Different Episodes of Information Security Institutionalization Depicting Technical Controls, Formal Controls and Informal Controls

In this study, the institutionalization and re-institutionalization of information security in an institution are introduced as micro-level institutionalization. Each of the three case studies has brought forth a unique instantiation of information security institutionalization. Such an instantiation denotes the institution's unique identity in terms of information security governance and practices. Despite the intervention by the Central Bank, each commercial bank has proceeded to create its own unique security culture through different security features and procedures, different security rules, and different methods of security education. Except when an institution is intentionally disbanded, institutions in general do not emerge from nothing, do not disappear, and instead change facets (Powell and DiMaggio 1991; Scott 2008). The occurrence of such episodes resembles the concept of recursive structuration as introduced by Barley (1986), Barley and Tolbert (1997), Giddens (1984), Orlikowski (1992; 2000), Walsham (1993), and Walsham and Han (1991).

The emergent themes suggest that the different episodes of information security institutionalization are attributed to the habitualized security routines, which depict how information security governance and practices become a natural routine or habit and transform into security culture. In addition, such varying episodes can also be attributed to the Information Stewardship, which explains how an institution preserves its information assets by assigning each of its divisions to control such an asset technically, formally, and informally. While figure 8.1 depicts a simplified representation of information security institutionalization depicting the three security-control dimensions, figure 7.1 shows the synthesis of institutionalization concepts showing the comprehensive four processes: script encoding, principles enactment, script revision and script replication, and patterned-actions objectification and externalization.

8.1.2. Impact of Central Governance Body

The impact of the central governance body is another highlight of this study. The Central Bank that acts as the central governance body has been shown to have significant influences on every operational aspect of a commercial bank, including information security. As such, the Central Bank is one of the key bank players as portrayed in this study. The role of the Central Bank has been delineated to be very important in shaping and conditioning information security governance and practices in banking sector.

An essential concept of the Central Bank’s involvement is power. This study has elucidated the use and the impact of power on the institutionalization of information security. There are three types of power: deontic power, constitutive power (Hall 2008), and facilitative power (Silva and Backhouse 2003). The Central Bank uses this power to position itself as the highest authority in the banking sector. Such intervention, as has been delineated in this study, includes formulating security guidelines, enforcing the implementation of security guidelines among commercial banks and financial institutions, and controlling and auditing information security governance and practices in commercial banks and financial institutions.

From a constitutive-power perspective, this study has supported Hall’s (2008) assertion of the ways by which the Central Bank uses constitutive power to formulate security rules. In addition, the Central Bank also has the capacity to force commercial banks and financial institutions to implement such security rules using facilitative power as denoted by Silva and Backhouse (2003). The Central Bank utilizes these types of power due to its social status in banking sector, referring to the deontic power as introduced by Hall (2008). These types of power are used to sanction and reward commercial banks and financial institutions to comply with information security policy. Regulations are needed to maintain social order and stability (Berger and Luckmann 1966), which are the ultimate objective of safeguarding information asset. Figure 7.4 shows how these power types are placed to render the Central Bank the authority to govern and control information security in banking sector.

Equipped with these types of power, the Central Bank conducts the governance and control of information security in banking sector. Commercial banks and financial institutions reciprocate these actions by conforming to such actions and reporting their operational activities to the Central Bank. Such bidirectional relationships represent a top-down process and a bottom-up process of the multilevel institutional processes proposed by Scott (2008). Institutional relationship reflects this theoretical framework, embodying these two processes. In this study, institutional relationship is the basis for the prudential supervision, which is an authoritative privilege owned by the central bank. The core concepts of institutional relationship are relationships among formal organizations (i.e., institutions), power utilization, rules implementation and control, and regulatory conformity. Using this concept, the Central Bank is positioned as the highest authority that represents the government in banking sector, defined as the institutional authority. Figure 3.5 depicts the macro-level institutionalization that adopts Scott's (2008) multilevel institutional processes.

8.2. Implications for Theory

Despite the adoption of a descriptive framework to develop a theoretical framework for this study, this study highlights several major implications. Firstly, previous studies have singled out security breach as merely a plight and therefore do not consider it a factor that can improve the implementation aspects of information security. This study presents a radical position by introducing security breach as a driving force in institutionalizing information security governance and practices. This argument is built on one that is presented by Rhee et al. (2005). Information security is not taken seriously when all is safe, but gains attention when a security breach hits. As such, rather than fussing about security breach and various counteractions to it, this study suggests the acceptance of security breach as part of the implementation and governance of information security. Organizations put tremendous efforts into improving technical controls, formal controls, and informal controls once a security breach hits since organizations strive to resist changes (Scott 2008) and maintain stability and social order (Burrell and Morgan 1979).

Secondly, this study highlights how information security becomes internalized in organizations. Such an internalization cannot escape the interplay between technical controls, formal controls, and informal controls. This study is developed from a social science perspective. While the fundamental idea is the interaction between social actors and artifacts such as security artifacts and technologies, such an interaction requires complicated processes that explain how such interaction becomes internalized. Borrowing Barley and Tolbert's (1997) framework for institutionalization and structuration, this study portrays various formats of such interactions in an institutionalization as a process. Such interaction appears as an abstraction in some phases such as script encoding and emerges in its literal form when principles are successfully enacted. Furthermore, such interaction occurs for the attainment of certain objectives that are unique, and depend on the organization's objectives and culture. To conceptualize and simplify the various formats of such interaction, a terminology of habitualized security routines is introduced, focusing on how such an interaction becomes routine. Such phenomena are in line with the concept proposed by Berger and Luckmann (1966) that the interaction between social actors and artifacts is socially constructed and hence a social construction of reality. This study also supports socio-organizational security scholars who opine that information security is not a technical problem but rather a managerial issue. Moreover, this finding is a support for the argument that information security governance and practices become institutionalized through social integration of routines and system integration of relevant technologies.

Thirdly, this study supports the significant impact of power on information security governance and practices. Built on the structuration concept, this study shows how power can be used to facilitate the interaction between social actors and artifacts as well as to sanction such interactions. While some higher authority key players in an internal organization possess the power to govern and control information security implementation, a central governance body is required to explain different types of power needed to govern and control information security implementation. Such organization requires a valid admission in a social system in order to obtain the deontic power (Hall 2008) or dispositional power (Silva and Backhouse 2003), which finally endows the organization with the constitutive power that is used to formulate rules (Hall 2008) and facilitative power that is used to control and force such rules (Silva and Backhouse 2003).

Fourthly, this study provides a major implication for the theoretical lens, particularly the institutionalization and the structuration framework by Barley and Tolbert

(1997). In the context of information security, this study extends the notion of script and differentiates the application of and the causes for script replication and script revision. Barley and Tolbert (1997) and Barley (1986) have denoted a script as merely a link between actions and institutions and that a script contains patternized interactions. This study goes beyond such conceptualization by stating that the script contains information security culture formed over time through accumulated knowledge and experience of social actors pertaining to information security. In addition, this study combines institutionalization concepts from scholars such as Berger and Luckmann (1966), Scott (1987; 2008), and Powell and DiMaggio (1991). This study distinguishes script replication as one that represents a normal condition, from script revision that emerges as a result of attempts to survive after a security breach. The script revision is shown to ignite re-institutionalization as introduced by Powell and DiMaggio (1991). Last but not least, this study embeds the three security-control dimensions in the realm of action. The interrelated implementation of formal controls, technical controls, and informal controls has been proved to serve as the basis for organization's resilience against the impact of security breach.

Finally, another major highlight is the institutional relationship that depicts the interaction among organizations engaged in implementing information security. Information security studies have mostly placed emphasis on internal management issues, reiterating the importance of executives and top management in the successful implementation of information security.

This study moves beyond the internal management view by proposing that an organization plays the role and acts as an authority. This study has shown the importance of such an organization which can direct, govern, and control information security through certain key players placed in another organization which acts as a subordinate. Rather than looking at how groups of key players influence each other, this study proposes that formal collections of key players have the power to influence. Such a finding is a positive response to the argument that information security governance elucidates the interaction between knowledgeable human agents and the wider social system within which they are situated.

8.3. Implications for Practice

The findings of this study point towards several implications for practice, which are presented below. Information security is a managerial issue that requires commitment by not only the internal key players such as executives, top management, middle management, and employees, but also other similar organizations and the central governance body operating in the sector. This study has depicted the relationship between information security, information risk, and systemic risk, which resembles a domino effect. The central governance body and subordinate organizations need to maintain a mutually trusting institutional relationship in order to sustain sound information security. In this sense, the central governance body might benefit from an assessment of how much of its power is used to control and govern subordinate organizations into implementing sound information security governance and practices. Vice versa, practitioners at subordinate organizations might also benefit from carefully assessing the degree of control and governance by the central governance body.

Practitioners may also benefit from evaluating the importance of giving equal treatment to technical controls, formal controls, and informal controls of information security. Practitioners should realize that a routine implementation of these controls has the potential to transform into a corporate security culture unique to an organization, given the successful internalization of such controls in security implementation. While security breach has been said to be just another phase in information security implementation, any practitioner as a member of a social system should always be aware of any threat of information risk and make every effort to mitigate such a risk. This study has depicted that even when an organization is prepared, a security breach can affect that organization indirectly due to security failure in another organization. This is an example of the damaging impact of systemic risk.

Finally, information security should be made available to not only internal key players, but also to customers and other similar organizations in the sector. Hence, informal controls such as security education and awareness are as important as technical controls and formal controls of information security. This study has shown how customers can be gullible and may fall into a trap by perpetrators of unethical practices. Furthermore, this study has demonstrated that these unethical perpetrators are very creative and in fact do not even use state-of-the-art technology artifacts to breach security (Dhillon 2007). Perpetrators simply prey on customers in the hope of duping them on the basis of their gullibility and lack of security awareness of such customers. While customers need to be constantly educated about the importance of information security and the procedures for safeguarding information assets, other similar organizations in the sector also need to understand the security culture and procedures of an organization. The

EDC machine fraud has highlighted the lack of understanding and clarity of each other's security features, security artifacts and procedures amongst two banks.

8.4. Limitations and Future Research Avenues

Like any other scientific product, this study unfortunately does not come free from limitations. By presenting these limitations, exciting research avenues become available for exploration to other scholars. Firstly, this study is conducted in a developing country. An extant piece of literature by Schooner and Taylor (2009) has stated that too much power and control by the Central Bank may actually limit the freedom of commercial banks in exercising their information security governance and practices. Another similar study in a developed country such as the United States should be conducted to present an interesting parallel or comparison with this study.

Secondly, security policy and risk management are considered simply a component in the institutionalization of information security. Security policy and risk management are positioned as part of the formal controls of security that are automatically internalized along with technical controls and informal controls during information security institutionalization. A future study that places emphasis on the impact of internalizing security policy on information security institutionalization could throw up interesting findings. In addition, another study that focuses on risk management should be conducted to see how mitigating information risk and information assurance can re-institutionalize information security.

Thirdly, the commercial banks in the case studies are all large commercial banks that boast of strong information systems from among their counterparts in Indonesia.

There are in fact many other smaller commercial banks in rural areas using non-automated information systems. Hence there is a tendency that this study favors computerized information security that supports information security as a whole. Another study should be conducted for the purpose of comparing information security governance between commercial banks with automated information security, other commercial banks with weak automated information security, and commercial banks with non-automated information security. Furthermore, such a study needs to emphasize on the internalization of information security governance and practices when drawing such a comparison.

Finally, this study has introduced several important concepts such as systemic risk and micro-prudential supervision borrowed from the banking theory. This study however focuses on the internal information security institutionalization in each commercial bank and the Central Bank and also takes note of the relationship between the Central Bank and all commercial banks. The latter is a subject that merits a closer examination and another study should be conducted to focus mainly on the institutional relationship between the central bank and a commercial bank in terms of information security and highlight the impact of such relationship on other commercial banks using the systemic risk concept.

BIBLIOGRAPHY

Adeleye, B. C., F. Annansingh and M. B. Nunes (2004). "Risk Management Practices in IS Outsourcing: An Investigation into Commercial Banks in Nigeria." International Journal of Information Management **24**: 167-180.

Aguiar, A. and M. M. F. Martins (2008). "Testing for Asymmetries in the Preferences of the Euro-Area Monetary Policymaker." Applied Economics **40**: 1651-1667.

Albrechtsen, E. (2007). "A Qualitative Study of Users' View on Information Security." Computers & Security **26**: 276-289.

Aldhizer III, G. R. (2008). "The Insider Threat." The Internal Auditor **65**(2): 71-73.

Alfaro, J. G., N. Boulahia-Cuppens and F. Cuppens (2008). "Complete Analysis of Configuration Rules to Guarantee Reliable Network Security Policies." International Journal of Information Security **7**: 103-122.

Anderson, J. M. (2003). "Why We Need a New Definition of Information Security." Computers & Security **22**(4): 308-313.

Ansolabehere, S. and J. M. Jr. Snyder (1999). "Money and Institutional Power." Texas Law Review **77**(7): 1673-1704.

Baldwin, A., D. Pym, M. Sadler and S. Shiu (2011). Information Stewardship in Cloud Ecosystems: Towards Models, Economics, and Delivery. IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), Athens, Greece.

Baldwin, A., D. Pym, M. Sadler and S. Shiu (2012). Enterprise Information Risk Management: Dealing with Cloud Computing. Privacy and Security for Cloud Computing: Selected Topics. S. Pearson and G. Yee. New York, Springer.

Barley, S. R. (1986). "Technology as an Occasion for Structuring: Evidence from Observations of CT Scanners and the Social Order of Radiology Departments." Administrative Science Quarterly **31**: 78-108.

Barley, S. R. and P. S. Tolbert (1997). "Institutionalization and Structuration: Studying the Links between Action and Institution." Organization Studies **18**(1): 93-117.

Baskerville, R. (1993). "Information Systems Security Design Methods: Implications for

Information Systems Development." ACM Computing Surveys **25**(4): 375-414.

Baskerville, R. and M. Siponen (2002). "An Information Security Meta-Policy for Emergent Organizations." Logistics Information Management **15**(5/6): 337-346.

Batini, N. (2007). "Euro Area Inflation Persistence." Empirical Economics **31**: 977-1002.

Berger, P. L. and T. Luckmann (1966). The Social Construction of Reality: A Treatise in the Sociology of Knowledge. Garden City, Anchor Books.

Björck, F. (2004). Institutional Theory: A New Perspective for Research into IS/IT Security in Organizations. 37th Hawaii International Conference on System Sciences, Waikoloa, Hawaii.

Blakley, B., E. McDermott and D. Geer (2001). Information Security is Information Risk Management. 2001 Workshop on New Security Paradigms, Cloudcroft, New Mexico.

Bodin, L. D., L. A. Gordon and M. P. Loeb (2008). "Information Security and Risk Management." Communications of the ACM **51**(4): 64-68.

Botha, M. and R. Von Solms (2001). "The Utilization of Trend Analysis in the Effective Monitoring of Information Security. Part 1: The Concept." Information Management & Computer Security **9**(5): 237-242.

Botha, M. and R. Von Solms (2002). "The Utilization of Trend Analysis in the Effective Monitoring of Information Security. Part 2: The Model." Information Management & Computer Security **10**(1): 5-11.

Brenner, J. (2007). "ISO 27001: Risk Management and Compliance." Risk Management **54**(1): 24-29.

Brotby, K. (2009). Information Security Governance: A Practical Development and Implementation Approach. Hoboken, John Wiley & Sons, Inc.

Bulgurcu, B., H. Cavusoglu and I. Benbasat (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." MIS Quarterly **34**(3): 523-548.

Burrell, G. and G. Morgan (1979). Sociological Paradigms and Organizational Analysis. Burlington, Ashgate Publishing Co.

Castiglione, N. D. (2002). "My Social Security Number is…." ABA Banking Journal **94**(12): 57-59.

Cecchetti, S. G. and R. O'Sullivan (2003). "The European Central Bank and The Federal

Reserve." Oxford Review of Economic Policy **19**(1): 30-43.

Chandra, I. (2008). "The Five C's of IT Policy." The Internal Auditor **65**(6): 23-24.

Chang, S. E. and C. S. Lin (2007). "Exploring Organizational Culture for Information Security Management." Industrial Management & Data Systems **107**(3): 438-458.

Chen, D. Q. and D. S. Preston (2007). Understanding CIO Role Effectiveness: The Antecedents and Consequents. 40th Hawaii International Conference on System Sciences, Waikoloa, Hawaii.

Christiano, L., R. Motto and M. Rostagno (2008). "Shocks, Structures or Monetary Policies? The Euro Area and US After 2001." Journal of Economics Dynamic & Control **32**: 2476-2506.

Cuppens, F. and N. Cuppens-Boulahia (2008). "Modeling Contextual Security Policies." International Journal of Information Security **7**(4): 285-305.

Da Veiga, A. and J. H. P. Eloff (2007). "An Information Security Governance Framework." Information Systems Management **24**(4): 361-372.

Dhillon, G. (1997). Managing Information System Security. London, MacMillan.

Dhillon, G. (2001). "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." Computers & Security **20**(2): 165-172.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. Hoboken, John Wiley & Sons, Inc.

Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM **43**(7): 125-128.

Dhillon, G. and J. Backhouse (2001). "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives." Information Systems Journal **11**: 127-153.

Dhillon, G. and R. Torkzadeh (2006). "Value-Focused Assessment of Information System Security in Organizations." Information Systems Journal **16**: 293-314.

Dhillon, G. and S. Moores (2001). "Computer Crimes: Theorizing about the Enemy Within." Computers & Security **20**(8): 715-723.

Doherty, N. F. and H. Fulford (2005). "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis." Information Resources Management Journal **18**(4): 21-39.

Doherty, N. F. and H. Fulford (2006). "Aligning the Information Security Policy with the Strategic Information Systems Plan." Computers & Security **25**(1): 55-63.

Dos Santos Moreira, E., L. A. F. Martimiano, A. J. dos Santos Brandao and M. C. Bernandes (2008). "Ontologies for Information Security Management and Governance." Information Management & Computer Security **16**(2): 150-165.

Dutta, A. and K. McCrohan (2002). "Management's Role in Information Security in a Cyber Economy." California Management Review **45**(1): 67-87.

Dutta, A. and R. Roy (2008). "Dynamics of Organizational Information Security." System Dynamics Review **24**(3): 349-375.

Eisenhardt, K. M. (1989). "Building Theories from Case Study Research." Academy of Management Review **14**(4): 532-550.

Evans, J., R. Womersley, D. Wong and G. A. Woodbury (2008). "Operational Risks in Banks." JASSA – The Finsia Journal of Applied Finance **2**: 9-16.

Finne, T. (1996). "The Information Security Chain in a Company." Computers & Security **15**: 297-316.

Fixler, D. J. (1993). "Measuring Financial Service Output and Prices in Commercial Banking." Applied Economics **25**: 983-993.

Flannery, M. J. (1998). "Using Market Information in Prudential Bank Supervision: A Review of the U.S. Empirical Evidence." Journal of Money, Credit, and Banking **30**(3): 273-305.

Flores, F., E. Bonson-Ponte and T. Escobar-Rodriguez (2006). "Organizational Risk Information System: A Challenge for the Banking Sector." Journal of Financial Regulation and Compliance **14**(4): 383-401.

Fragniere, E., J. Gondzio and X. Yang (2010). "Operations Risk Management by Optimally Planning the Qualified Workforce Capacity." European Journal of Operational Research **202**(518-527).

Fulford, H. and N. F. Doherty (2003). "The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation." Information Management & Computer Security **11**(3): 106-114.

Giddens, A. (1984). The Constitution of Society. Berkeley & Los Angeles, University of California Press.

Gordon, L. A., M. P. Loeb and T. Sohail (2003). "A Framework for Using Insurance for Cyber-

Risk Management." Communications of the ACM **46**(3): 81-85.

Gupta, V. K. (2009). "Strategic Framework for Managing Forces of Continuity and Change in Risk Management of Banks in India." Global Journal of Flexible Systems Management **10**(2): 35-46.

Hall, R. B. (2008). Central Banking as Global Governance: Constructing Financial Credibility. Cambridge, Cambridge University Press.

Hazari, S., W. Hargrave and B. Clenney (2008). "An Empirical Investigation of Factors Influencing Information Security Behavior." Journal of Information Privacy & Security **4**(4): 3-20.

Hellier, J. (1999/2000). "Independence of the Central Bank, Growth, and Coalitions in a Monetary Union." Journal of Post Keynesian Economics **22**(2): 285-311.

Herath, T. and H. R. Rao (2009). "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations." European Journal of Information Systems **18**(2): 106-125.

Hone, K. and J. H. P. Eloff (2002). "Information Security Policy - What do International Security Standards Say?" Computers & Security **21**(5): 402-409.

Hong, K. S., Y. P. Chi, L. R. Chao and J. H. Tang (2006). "An Empirical Study of Information Security Policy on Information Security Elevation in Taiwan." Information Management & Computer Security **14**(2): 104-115.

Ising, O. (2009). "Asset Prices and Monetary Policy." Cato Journal **29**(1): 45-51.

Jarrow, R. A. (2008). "Operational Risk." Journal of Banking & Finance **32**: 870-879.

John, K., A. Saunders and L. W. Senbet (2000). "A Theory of Bank Regulation and Management Compensation." The Review of Financial Studies **13**(1): 95-125.

Jones, A. (2007). "A Framework for the Management Information Security Risks." BT Technology Journal **25**(1): 30-36.

Kaleem, A. and S. Ahmad (2008). "Bankers’ Perception of Electronic Banking in Pakistan." Journal of Internet Banking and Commerce **13**(1): 1-16.

Kawaura, A. (2004). "Deregulation and Governance: Plight of Japanese Banks in the 1990s." Applied Economics **36**: 479-484.

Khalfan, A. M. and A. Alshawaf (2004). "Adoption and Implementation Problems of E-Banking: A Study of the Managerial Perspective of the Banking Industry in Oman." Journal of

Global Information Technology Management **7**(1): 47-64.

Khoury, G. E. (2009). "Procyclicality of the Banking System: The Prudential and Accounting Framework of the Procyclicality of Bank Balance Sheet." The Business Review **14**(139-149).

Klein, H. K. and M. D. Myers (1999). "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems." MIS Quarterly **23**(1): 67-94.

Knapp, K. J., T. E. Marshall, R. K. Rainer and F. N. Ford (2006). "Information Security: Management's Effect on Culture and Policy." Information Management & Computer Security **14**(1): 24-36.

Knapp, K. J., R. F. Morris Jr., T. E. Marshall and T. A. Byrd (2009). "Information Security Policy: An Organizational-Level Process Model." Computers & Security **28**: 493-508.

Krauskopf, B. and C. Steven (2009). "The Institutional Framework of the European System of Central Banks: Legal Issues in the Practice of the First Ten Years of Its Existence." Common Market Law Review **46**: 1143-1175.

Kulczycki, G. (1997). "Information Security." Management Accounting **79**(6): 18-24.

Laeven, L. and R. Levine (2009). "Bank Governance, Regulation, and Risk Taking." Journal of Financial Economics **93**: 259-275.

Lam, W. (2005). "Barriers to E-Government Integration." Journal of Enterprise Information Management **18**(5/6): 511-530.

Lamy, R. E. and R. C. Moyer (1995). "Financial Services Marketing and Banking Regulation: The Case of the Community Reinvestment Act." Psychology & Marketing **12**(1-8): 721-733.

Lapke, M. S. (2008). Power Relationships in Information Systems Security Policy Formulation and Implementation. Information Systems. Richmond, Virginia Commonwealth University.

Larner, W. and R. Le Heron (2005). "Neo-Liberalizing Spaces and Subjectivities: Reinventing New Zealand Universities." Organization **12**(6): 843-862.

Lawrence, C. (2003). "Institutions and Organizations (2nd ed.). Review of Institutions and Organizations (2nd ed.)." Information Technology & People **16**(3): 374-383.

Lee, A. S. (1989). "A Scientific Methodology for MIS Case Studies." MIS Quarterly **13**(1): 33-50.

Lee, A. S. (1999). Researching MIS. Rethinking Management Information Systems: An Interdisciplinary Perspective. W. L. Currie and B. Galliers. New York, Oxford University Press**:** 7-27.

Lee, A. S. (2004). Thinking about Social Theory and Philosophy for Information Systems. Social Theory and Philosophy for Information Systems. L. Willcocks and J. Mingers. Chichester, John Wiley & Sons**:** 1-26.

Lee, A. S. and R. L. Baskerville (2003). "Generalizing Generalizability in Information Systems Research." Information Systems Research **14**(3): 221-243.

Lees, K. (2007). "How Large are the Gains to Commitment Policy and Optimal Delegation for New Zealand?" Journal of Macroeconomics **29**: 959-975.

Lewis, S. D., R. G. Colvard and C. N. Adams (2008). "A Comparison of the Readability of Privacy Statements of Banks, Credits Counseling Companies, and Check Cashing Companies." Journal of Organizational Culture, Communications, and Conflict **12**(2): 87-93.

Maguire, S. (2002). "Identifying Risks during Information System Development: Managing the Process." Information Management & Computer Security **10**(2/3): 126-134.

Malkawi, B. H. and H. O. Malkawi (2007). "Anti-Terrorist Finance Provisions in Jordan: Important Step but Insufficient." Journal of Money Laundering Control **10**(2): 180-188.

McFadzean, E., J. N. Ezingeard and D. Birchall (2007). "Perception of Risk and the Strategic Impact of Existing IT on Information Security Strategy at Board Level." Online Information Review **31**(5): 622-660.

McLaughlin, J. D. (1999). "There's More to "Financial" than Meets the Eye." ABA Banking Journal **91**(12): 12-14.

Miller, H. E. and K. J. Engemann (1996). "A Methodology for Managing Information-Based Risk." Information Resources Management Journal **9**(2): 17-24.

Mishra, S. (2009). Defining Value Based Information Security Governance Objectives. Information Systems. Richmond, Virginia Commonwealth University.

Moulton, R. and R. S. Coles (2003). "Applying Information Security Governance." Computers & Security **22**(7): 580-584.

Nana, E., B. Jackson and G. S. J. Burch (2010). "Attributing Leadership Personality and Effectiveness from the Leader's Face: An Exploratory Study." Leadership & Organization Development Journal **31**(8): 720-742.

Omoteso, K., A. Patel and P. Scott (2010). "Information and Communications Technology and Auditing: Current Implications and Future Directions." International Journal of Auditing **14**: 147-162.

Orlikowski, W. J. (1992). "The Duality of Technology: Rethinking the Concept of Technology in Organizations." Organization Science **3**(3): 398-427.

Orlikowski, W. J., J. Yates, K. Okamura and M. Fujimoto (1995). "Shaping Electronic Communication: The Metastructuring of Technology in the Context of Use." Organization Science **6**(4): 423-444.

Orlikowski, W. J. (2000). "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations." Organization Science **11**(4): 404-428.

Orlikowski, W. J. and C. S. Iacono (2001). "Research Commentary: Desperately Seeking the “IT” in IT Research – A Call to Theorizing the IT Artifact." Information Systems Research **12**(2): 121-134.

Orlikowski, W. J. and J. J. Baroudi (1991). "Studying Information Technology in Organizations: Research Approaches and Assumptions." Information Systems Research **2**(1): 1-28.

Page, V., M. Dixon and I. Choudhury (2007). "Security Risk Mitigation for Information Systems." BT Technology Journal **25**(1): 118-127.

Parrish, I. (2000). "Bridges to Excellence." The Internal Auditor **57**(6): 61-65.

Penn, B. (2005). "Commission Consults on Revision of the European Electronic Money Regime." Journal of Financial Regulation and Compliance **13**(4): 347-355.

Pennathur, A. K. (2001). "’Clicks and Bricks’: E-Risk Management for Banks in the Age of the Internet." Journal of Banking & Finance **25**: 2103-2123.

Post, J. E., L. E. Preston and S. Sachs (2002). Redefining the Corporation: Stakeholder Management and Organizational Wealth. Stanford, Stanford University Press.

Posthumus, S. and R. Von Solms (2004). "A Framework for the Governance of Information Security." Computers & Security **23**: 638-646.

Powell, W. W. and P. J. DiMaggio (1991). The New Institutionalism in Organizational Analysis. Chicago, The University of Chicago Press.

Quaglia, L. (2008). "Explaining the Reform of Banking Supervision in Europe: An Integrative Approach." Governance: An International Journal of Policy, Administration, and Institutions **21**(3): 439-463.

Rhee, H. S., Y. U. Ryu and C. T. Kim (2005). I am Fine, but You are Not: Optimistic Bias and Illusion of Control on Information Security. International Conference on Information Systems, Las Vegas, Nevada.

Rindfleisch, T. C. (1997). "Privacy, Information Technology, and Health Care." Communications of the ACM **40**(8): 93-100.

Rosenbaum, S. (2010). "Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access." Health Research and Educational Trust **45**(5p2): 1442-1455.

Ross, S. J. (2008). "Enforcing Information Security: Architecture and Responsibilities." Network Security **2**(7): 7-10.

Ryan, S. D. and B. Bordoloi (1997). "Evaluating Threats in Mainframe and Client/Server Environments." Information & Management **32**: 137-146.

Scandizzo, S. (2005). "Risk Mapping and Key Risk Indicators in Operational Risk Management." Economic Notes **34**(2): 231-256.

Schooner, H. M. and M. W. Taylor (2009). Global Bank Regulation: Principles and Policies. Burlington, Elsevier Inc.

Schutz, A. (1962-1966). Concept and Theory Formation in Social Sciences. Collected Papers. M. Nijhoff. Netherlands, The Hague.

Scott, D. F. Jr., W. G. Jens Jr. and R. E. Spudeck (1992). "Bank Reform: The Enduring Issues." Business Economics **27**(3): 7-12.

Scott, W. R. (1987). "The Adolescence of Institutional Theory." Administrative Science Quarterly **32**(4): 493-511.

Scott, W. R. (2008). Institutions and Organizations: Ideas and Interests. Stanford, Sage Publications.

Selznick, P. (1969). Law, Society, and Industrial Justice. Berkeley, Russell Sage Publications.

Shankarmahesh, M. N., J. B. Ford and M. S. LaTour (2003). "Cultural Dimensions of Switching Behavior in Importer-Exporter Relationships." Academy of Marketing Science Review **2003**(3): 1-17.

Shull, B. (2002). "Banking, Commerce, and Competition under the Gramm-Leach-Bliley Act." Antitrust Bulletin **47**(1): 25-61.

Silva, L. and J. Backhouse (2003). "The Circuits-of-Power Framework for Studying Power in

Institutionalization of Information Systems." Journal of the Association for Information Systems **4**(6): 294-336.

Singh, D. (2006). "Corporate Governance and the Interests of Depositors." Journal of Banking Regulation **7**(3/4): 189-190.

Smith, B. and J. Searle (2003). "The Construction of Social Reality: An Exchange." The American Journal of Economics and Sociology **62**(1): 285-309.

Smith, S. and R. Jamieson (2006). "Determining Key Factors in E-Government Information System Security." Information Systems Management **23**(2): 23-32.

Stern, R. N. and S. R. Barley (1996). "Organizations and Social Systems: Organization Theory's Neglected Mandate." Administrative Science Quarterly **41**(1): 146-162.

Stinchcombe, N. (2006). "How Administrative Managers Can Use Technology to Protect Their Organizations." The British Journal of Administrative Management **Apr/May**: 18-19.

Stone, D. L. and D. L. Marotta (2003). "Leveraging Risk Technology." The Internal Auditor **60**(6): 27-30.

Straub, D. W. and R. J. Welke (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making." MIS Quarterly **22**(4): 441-469.

Tsaih, R. H., W. Y. Lin and A. Chen (2008). "Safeguard Gaps and Their Managerial Issues." Industrial Management & Data Systems **108**(5): 669-676.

Tsoukas, H. and R. Chia (2002). "On Organizational Becoming: Rethinking Organizational Change." Organization Science **13**(5): 567-582.

Ullrich, K. (2007). "Introducing Instruments of Central Bank Accountability in a Monetary Union." Open Economies Review **18**(3): 239-262.

Van Greuning, H. and S. Brajovic Bratanovic (2000). Analyzing Banking Risk: A Framework for Assessing Corporate Governance and Financial Risk Management. Washington, D. C., The World Bank.

Von Solms, B. (2000). "Information Security - The Third Wave?" Computers & Security **19**: 615-620.

Von Solms, R. S. and S. H. Von Solms (2006). "Information Security Governance: A Model Based on the Direct-Control Cycle." Computers & Security **25**: 408-412.

Von Solms, R. S. and S. H. Von Solms (2006). "Information Security Governance: Due Care." Computers & Security **25**: 494-497.

Von Solms, S. H. (2001). "Corporate Governance and Information Security." Computers & Security **20**: 215-218.

Von Solms, S. H. (2005). "Information Security Governance – Compliance Management vs. Operational Management." Computers & Security **24**: 443-447.

Von Solms, S. H. and R. Von Solms (2009). Information Security Governance. New York, Springer.

Vroom, C. and Von Solms, R. (2004). "Towards Information Security Behavioural Compliance." Computers & Security **23**: 191-198.

Walsham, G. (1993). Interpreting Information Systems in Organizations. Chichester, John Wiley & Sons, Inc.

Walsham, G. (2006). "Doing Interpretive Research." European Journal of Information Systems **15**: 320-330.

Walsham, G. and C. K. Han (1991). "Structuration Theory and Information Systems Research." Journal of Applied Systems Analysis **17**: 77-85.

Ward, P. and C. L. Smith (2002). "The Development of Access Control Policies for Information Technology Systems." Computers & Security **21**(4): 356-371.

Whitman, M. E. (2003). "Enemy at the Gate: Threats to Information Security." Communications of the ACM **46**(8): 91-95.

Wibowo, K. and M. M. Batra (2010). "Information Insecurity in the Globalization Era: Threats, Governance, and Survivability." Competition Forum **8**(111-120).

Workman, M. and J. Gathegi (2007). "Punishment and Ethics Deterrents: A Study of Insider Security Contravention." Journal of American Society for Information Science and Technology **58**(2): 212-222.

Yang, T. C. and N. Zhang (2007). "China's New Rules on Anti-Money Laundering." Journal of Investment Compliance **8**(2): 58-62.

A INTERVIEW QUESTIONS

Theoretical Element	Research Question	Interview Question
		What is your position in your company? Briefly describe your task and duties.
Inter-Level: Script Encoding	Internalization of security governance and practices by an organization	Describe what you know about risk.
		Who is in charge of constituting risk policies and regulations in your company?
		Describe the policies and regulations of using your company's IT system.
		Is there any specific reference or guidance for risk policies and regulations?
	Impact of external governing body	Does your company devise risk-management policies and procedures to other commercial banks?
	Impact of security breaches	Describe what you know about a security breach.
Inter-Level: Principles Enactment	Internalization of security governance and practices by an organization	How is your company's IT security system maintained or enhanced?
		How are these practices reflected in a branch level?
		What action do management/controller personnel take to enforce security culture in your company?
		Who is in charge of enforcing and controlling risk policies and regulations?
	Impact of external governing body	What is the institutional relationship between your company and the central bank?

	Impact of security breaches	Has there been any security-breach incident in your company or its branches? To whom do you report any security breach incident?
Inter-Level: Script Replication and Revision	Internalization of security governance and practices by an organization	Are risk policies and regulations in your company periodically revised? How often? To whom are the risk policies and regulations revision reported? Who is in charge of receiving report and revision from your company's branches? Who is in charge of receiving report and revision in a branch level? Who is in charge of revising risk policies and regulations? Do branch personnel have the authority to constitute and revise risk policies and regulations? Why?
Inter-Level: Patterned-Actions Objectification and Externalization	Internalization of security governance and practices by an organization	Is your company's IT security system periodically maintained or enhanced? How often? Who is in charge of the IT security system maintenance? Who are the key players that enforce and control risk policies and regulations in a branch level? How are these policies and regulations enforced and governed in your company's branches? What are the penalties for security-breach incidents for employees? What are the penalties for compliance failure? What is the practice of information security governance in your company? What are the frameworks used for practicing information security governance in your company?

	Impact of security breaches	Describe the implementation of information security in your company and what your contributions are for such implementations? How do you handle any security-breach incident? How does/would your company handle security-breach incident?
Intra-Level: Governance and Control	Impact of external governing body	How do commercial banks comply? How do you expect commercial banks to comply? What penalties does your company implement for any security-breach incident in commercial banks? How often do you expect commercial banks to report their information-security practices? How do commercial banks report such practices?
Intra-Level: Governance and Control	Internalization of security governance and practices by an organization	How does your organization comply with the central bank's risk policies and regulations? How does your company report a security-breach incident to the central bank? How does your company report its information-security practices to the central bank? Has the central bank ever imposed any penalty over any incident or compliance failure? Examples?

B DATA COLLECTION: RECORDS AND SCHEDULE

Legend: EM: Executive Management
A: Authority
M: Management
OP: Operational Personnel

Date	Organization	Subject	Time Start	Time End	Duration	Interview?	EM?	A?	M?	OP?	Focus Area
05/24/2010	Centro Metropolitan Bank	Vice President of IT Security Dept.	12:10 PM	2:25 PM	1:15	Yes	No	Yes	Yes	No	Organizational background briefing and preliminary interview. Electronic copies of organizational structure obtained.
05/26/2010	Earl Capita Bank	IT Dept. Manager (Directorate of Information Technology)	2:00 PM	4:00 PM	2:00	Yes	No	Yes	Yes	No	Research presentation and preliminary interview.
05/31/2010	Earl Capita Bank	Head of Risk Management Team (Office of Governor)	8:10 AM	9:35 AM	1:25	Yes	No	Yes	Yes	No	Data collection: Interview on organizational structure (script encoding and principles enactment).

		Senior Analysts (Special Unit for Information Management)	2:20 PM	4:00 PM	1:40	Yes	No	Yes	Yes	No	Introduction and preliminary interview.
06/01/2010	Earl Capita Bank	Special Unit for Information Management	2:00 PM	3:35 PM	1:35	No	Yes	Yes	Yes	Yes	Sharing session with the UKMI's personnel: Dissertation-proposal presentation
06/02/2010	Earl Capita Bank	Senior Analysts (Special Unit for Information Management)	11:35 AM	1:45 PM	2:10	Yes	No	Yes	Yes	No	Data collection: Interview on technical control and organizational structure (script encoding and principles enactment).

		Head of Payment Information Systems Regulator (Directorate of Accounting and Payment System)	3:40 PM	4:35 PM	55 min.	Yes	No	Yes	Yes	No	Data collection: Interview on governance and control of macro-prudential supervision theory.
		Head of Payment Information Systems Supervisor (Directorate of Accounting and Payment System)	5:20 PM	5:45 PM	25 min.	Yes	No	Yes	Yes	No	Data collection: Interview on governance and control of macro-prudential supervision theory.
06/03/2010	Earl Capita Bank	Head of Payment Information Systems Licensing (Directorate of Accounting and Payment System)	8:25 AM	9:10 AM	45 min.	Yes	No	Yes	Yes	No	Data collection: Interview on governance and control of macro-prudential supervision theory.

		Senior IT Researcher (Directorate of Information Technology)	9:30 AM	10:50 AM	1:20	Yes	No	No	Yes	No	Data collection: Interview on technical control (principles enactment, script replication, and patterned-actions objectification and externalization).
		Analysts (Special Unit fot Information Management)	2:00 PM	4:08 PM	2:08	Yes	No	No	No	Yes	Data collection: Interview on information stewardship (principles enactment and patterned-actions objectification and externalization).

		Senior Analyst (Special Unit for Information Management)	4:10 PM	4:20 PM	10 min.	Yes	No	Yes	Yes	No	Data collection: Interview on information stewardship (principles enactment, script replication, and patterned-actions objectification and externalization).
06/04/2010	Earl Capita Bank	Senior Analyst, Analyst, Junior Analyst (Directorate of Bank Licensing and Banking Information)	2:25 PM	3:25 PM	1:00	Yes	No	No	Yes	Yes	Data collection: Interview on information systems management and use (script encoding, principles enactment, script replication, and patterned-actions objectification and externalization).

06/07/2010	Earl Capita Bank	Head of Risk Management Team (Office of Governor)	9:00 AM	10:05 AM	1:05	Yes	No	Yes	Yes	No	Data collection: Interview on risk policies (script encoding, principles enactment, script replication, and patterned-actions objectification and externalization).
		Senior Analyst of Public Relation Buerau (Office of Governor)	10:35 AM	10:45 AM	10 min.	Yes	No	No	No	Yes	Data collection: Interview on risk policies and management (script encoding).
		Head of Strategic Planning Bureau (Office of Governor)	10:50 AM	11:50 AM	1:00	Yes	No	Yes	Yes	No	Data collection: Interview on risk mitigation and implementation (principles enactment, script replication, and patterned-actions objectification

											and externalization).
		Senior Researcher (Directorate of Banking Research and Regulation)	1:45 PM	2:55 PM	1:10	Yes	No	No	Yes	No	Data collection: Interview on policies formulation, control, and implementation (script encoding, principles enactment, script replication, and patterned-actions objectification and externalization).

06/08/2010	Earl Capita Bank	Analyst (Directorate of Bank Licensing and Banking Information)	11:10 AM	11:45 AM	35 min.	Yes	No	No	No	Yes	Data collection: Interview on information systems management and use (script encoding, principles enactment, script replication, and patterned-actions objectification and externalization).
		Senior Analysts (Special Unit for Information Management)	2:10 PM	3:20 PM	1:10	Yes	No	Yes	Yes	No	Data collection: interview on information stewardship and security access and control (principles enactment and patterned-actions objectification and externalization).

06/09/2010	Earl Capita Bank	Head of IT Operational and Senior IT Researcher (Directorate of Information Technology)	8:00 AM	9:02 AM	1:02	Yes	No	No	Yes	No	Data collection: Interview on data recovery plan (script revision).
		Senior Bank Supervisor (Directorate of Bank Supervision 3: Private Banks)	11:00 AM	11:45 AM	45 min.	Yes	No	Yes	No	No	Data collection: Interview on governance and control of macro-prudential supervision theory.
06/10/2010	Earl Capita Bank	Head of Risk Management Team and Analyst (Office of Governor)	9:00 AM	10:17 AM	1:17	Yes	No	Yes	Yes	No	Data collection: Interview on risk management information systems (script encoding and principles enactment).

06/14/2010	Earl Capita Bank	Senior Bank Supervisor (Directorate of Bank Supervision 3: Private Banks)	2:00 PM	2:35 PM	35 min.	Yes	No	Yes	No	No	Data collection: Interview on governance and control of macro-prudential supervision theory.
		Head of Payment Information Systems Supervisor (Directorate of Accounting and Payment System)	9:15 AM	9:25 AM	10 min.	Yes	No	Yes	Yes	No	Data collection: interview on governance and control of macro-prudential supervision theory.
		Head of Payment Information Systems Regulator (Directorate of Accounting and Payment System)	12:00 PM	12:18 PM	18 min.	Yes	No	Yes	Yes	No	Data collection: Interview on governance and control of macro-prudential supervision theory.

06/15/2010	Earl Capita Bank	Bank Supervisors (Directorate of Bank Supervision 1: State Banks)	9:40 AM	11:30 AM	1:50	Yes	No	Yes	No	No	Data collection: Interview on governance and control of macro-prudential supervision theory.
	Blue Sequoia Bank	Head of Compliance, IT Analyst, and Head of Human Resource	2:45 PM	3:40 PM	55 min.	No	No	Yes	Yes	Yes	Organizational background briefing and dissertation-proposal presentation.
06/18/2010	Earl Capita Bank	Senior IT Researcher (Directorate of Information Technology)	3:25 PM	3:35 PM	10 min.	Yes	No	No	Yes	No	Data collection: Interview on security for intranet, internet, and email (script encoding, principles enactment, script revision and replication, and patterned-actions objectification and externalization).

06/21/2010	Centro Metropolitan Bank	Operational Group Head, Business Operation Improvement Dept. Head, and Domestic Payment Dept. Head (Central Operation)	11:10 AM	11:35 AM	25 min.	Yes	No	No	Yes	No	Data collection: Interview on information systems management and use (script encoding, principles enactment, script replication, and patterned-actions objectification and externalization).
		IT Audit Unit Head (Internal Audit Dept.)	4:43 PM	5:45 PM	1:02	Yes	No	No	Yes	No	Data collection: Interview on security implementation (script encoding, principles enactment, script replication, and patterned-actions objectification and externalization).

06/22/2010	Centro Metropolitan Bank	Assistent of Mass Banking Vice President	16:00	16:11	11 min.	No	No	Yes	Yes	No	Research introduction.
06/24/2010	Centro Metropolitan Bank	Vice President of IT Security Dept.	2:08 PM	3:15 PM	1:07	Yes	No	Yes	Yes	No	Data collection: Interview on security for debit card and ATM infrastructure, hardware, and software (principles enactment and patterned-actions objectification and externalization).
06/25/2010	Centro Metropolitan Bank	Operational Risk Management Team Leader	9:05 AM	9:25 AM	20 min.	No	No	Yes	Yes	No	Research introduction.

		Assistent of Mass Banking Vice President	3:35 PM	4:40 PM	1:05	Yes	No	Yes	Yes	No	Data collection: Interview on on security for debit card and ATM infrastructure, hardware, and software (script encoding, principles enactment, and patterned-actions objectification and externalization).

06/29/2010	Centro Metropolitan Bank	IT Audit Unit Head (Internal Audit Dept.)	8:50 AM	9:38 AM	48 min.	Yes	No	No	Yes	No	Data collection: interview on conformity and report of macro-prudential supervision theory and on security for debit card and ATM infrastructure, hardware, and software (principles enactment, script replication and revision, and patterned-actions objectification and externalization).
06/30/2010	Centro Metropolitan Bank	Operational Risk Management Team Leader	4:15 PM	5:15 PM	1:00	Yes	No	Yes	Yes	No	Data collection: interview on information risk management (script encoding, principles enactment, and script revision and replication).

07/01/2010	Centro Metropolitan Bank	Assistent of Mass Banking Vice President	5:33 PM	6:10 PM	37 min.	Yes	No	Yes	Yes	No	Data collection: Interview on debit-card transaction and security (principles enactment, script revision, patterned-actions objectification and externalization).
07/05/2010	Centro Metropolitan Bank	Vice President of IT Security Dept.	4:00 PM	4:53 PM	53 min.	Yes	No	Yes	Yes	No	Data collection: Interview on security policies (script encoding, principles enactment, script replication, and patterned-actions objectification and externalization).

07/08/2010	Centro Metropolitan Bank	E-Banking Product Manager	8:15 AM	9:26 AM	1:11	Yes	No	Yes	Yes	No	Data collection: Interview on electronic and card payment (principles enactment and patterned-actions objectification and externalization).
07/09/2010	Centro Metropolitan Bank	IT Audit Unit Head (Internal Audit Dept.)	9:18 AM	10:15 AM	57 min.	Yes	No	No	Yes	No	Data collection: Interview on security policies formulation and implementation (script encoding and script replication and revision) and conformity and report of macro-prudential supervision theory.

07/12/2010	Centro Metropolitan Bank	Operational Risk Management Team Leader	4:18 PM	4:56 PM	38 min.	Yes	No	Yes	Yes	No	Data collection: Interview on conformity and report of macro-prudential supervision theory.
07/13/2010	Centro Metropolitan Bank	Vice President of Head Corporate Center Audit	9:13 AM	9:40 AM	27 min.	Yes	Yes	Yes	Yes	No	Data collection: Interview on confidential data (principles enactment and patterned-actions objectification and externalization).
07/15/2010	Centro Metropolitan Bank	Vice President of Compliance Group	10:18 AM	11:25 AM	1:07	Yes	Yes	Yes	Yes	No	Data collection: Interview on conformity and report of macro-prudential supervision theory.

		IT Audit Unit Head (Internal Audit Dept.)	2:10 PM	2:50 PM	40 min.	Yes	No	No	Yes	No	Data collection: Interview on security breach and incidental case (script encoding, principles enactment, script revision, and patterned-actions objectification and externalization).
		Operational Risk Management Team Leader	4:20 PM	4:35 PM	15 min.	Yes	No	Yes	Yes	No	Data collection: Interview on security breach and incidental case (script encoding, principles enactment, script revision, and patterned-actions objectification and externalization).

07/16/2010	Centro Metropolitan Bank	Vice President of IT Security Dept.	2:23 PM	3:33 PM	1:10	Yes	No	Yes	Yes	No	Data collection: Interview on security breach and incidental case (script encoding, principles enactment, script revision, and patterned-actions objectification and externalization).
07/19/2010	Centro Metropolitan Bank	Assistent of Mass Banking Vice President	5:53 PM	6:25 PM	32 min.	Yes	No	Yes	Yes	No	Data collection: Interview on security breach and incidental case (script encoding, principles enactment, script revision, and patterned-actions objectification and externalization).

07/20/2010	Blue Sequoia Bank	Head of Enterprise Security Group	10:15 AM	11:23 AM	1:08	Yes	Yes	Yes	Yes	No	Data collection: Interview on information risk, control, and security policy (script encoding, principles enactment, and patterned-actions objectification and externalization).
07/29/2010	Blue Sequoia Bank	Head of Enterprise Security Group	10:08 AM	11:12 AM	1:04	Yes	Yes	Yes	Yes	No	Data collection: Interview on security implementation and security policies (script encoding, principles enactment, script replication, and patterned-actions objectification and externalization).

08/02/2010	Blue Sequoia Bank	Head of Electronic Banking Operation Group	3:32 PM	4:26 PM	1:06	Yes	Yes	Yes	Yes	No	Data collection: Interview on debit-card and electronic payment (principles enactment, script replication, and patterned-actions objectification and externalization).
08/10/2010	Blue Sequoia Bank	Head of Enterprise Security Group	2:13 PM	3:48 PM	1:35	Yes	Yes	Yes	Yes	No	Data collection: Interview on security implementation and security breach incident (script encoding, principles enactment, script replication and revision, and patterned-actions objectification and externalization).

08/12/2010	Blue Sequoia Bank	Head of Enterprise Security Group	2:13 PM	2:48 PM	35 min.	Yes	Yes	Yes	Yes	No	Data collection: Interview on technical controls and security technologies (principles enactment and patterned-actions objectification and externalization).
08/16/2010	Blue Sequoia Bank	Compliance Advisor	1:35 PM	2:28 PM	53 min.	Yes	No	Yes	No	Yes	Data collection: Interview on security policies formulation (script encoding) and conformity and report of macro-prudential supervision theory.

08/16/2010	Blue Sequoia Bank	Head of Electronic Banking Operation Group	3:05 PM	3:40 PM	35 min.	Yes	Yes	Yes	Yes	No	Data collection: Interview on debit-card payment (principles enactment and patterned-actions objectification and externalization).

VITA

Muhamad Faisal Fariduddin Attar Nasution was born on November 27, 1978 in Jakarta, Indonesia. He is the first son of Dr. Darmin Nasution and Salsia Ulfa Sahabi Manoppo. He visited France to accompany his father who was pursuing a masters and doctoral degree in developmental economic study at the *Université Paris 1 Panthéon-Sorbonne* and spent 5 years of his childhood living in Antony, a suburb of Paris. In the late of 1985, he returned to Jakarta, Indonesia, where he spent his remaining childhood and his adolescent period. He consistently ranked in the top 1% during his high-school career and was accepted to the prestigious *Universitas Indonesia* where he received his *Sarjana Ilmu Komputer* degree (equivalent to the U.S. Bachelor of Science in Computer Science) in 2002. He graduated with satisfactory predicate and subsequently worked at the Indonesian Bank Restructuring Agency (IBRA) in 2002 as a contract web-based systems analyst programmer for one year.

Fari soon received the Indonesia's Upstream Oil and Gas Executive Agency Scholarship in 2003 and embarked on his graduate study in the United States. He enrolled at the University of Missouri at Saint Louis where he received his MBA degree in general business administration in 2005. Upon graduation, he was hired as an external temporary consultant with the World Bank Group at Washington, D.C., where he assisted data collection for the South-East Asia National Single Window project.

In 2006, Fari was accepted to the doctoral program in information systems at Virginia Commonwealth University School of Business. During his tenure at VCU, Fari was awarded a graduate assistantship that covered his tuition costs and stipend. Employed as an adjunct instructor, Fari gained a significant experience in teaching technical-subject courses and managerial-subject courses such as computer hardware and software, database systems, fundamental data communications, and systems analysis and design. He also received his first taste of teaching a large class when he taught business information systems.