ICT Risk Management in Organizations: Case studies in Thai Business

Siridech Kumsuprom
School of Business Information System, RMIT University Melbourne Australia, siridech.kumsuprom@rmit.edu.au

Brian Corbitt
School of Business Information System, RMIT University Melbourne Australia, brian.corbitt@rmit.edu.au

Siddhi Pittayachawan
School of Business Information System, RMIT University Melbourne Australia, siddhi.pittayachawan@rmit.edu.au

Follow this and additional works at: http://aisel.aisnet.org/acis2008

Recommended Citation
http://aisel.aisnet.org/acis2008/98

This material is brought to you by the Australasian (ACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ACIS 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
ICT Risk Management in Organizations: Case studies in Thai Business

Siridech Kumsuprom
Brian Corbitt
Siddhi Pittayachawan
School of Business Information System, RMIT University
Melbourne Australia
Email: siridech.kumsuprom@rmit.edu.au; brian.corbitt@rmit.edu.au; siddhi.pittayachawan@rmit.edu.au

Abstract
Risks related to information communication and technologies (ICTs) still occur in organizations. In spite of development of ICT risk management methodologies that have been published in numerous frameworks and/or standards to help organizations deal with ICT risks, it has still been questioned about whether or not its methodology has manifested success. This research identifies the current profile of ICT risk management planning and investigates success in implementation in Thai organizations of both the Control Objectives for the Information and related Technology (COBIT) framework and the ISO/IEC 17799 standard for dealing with ICT risk management. The findings from three case studies indicate that successful ICT risk management planning focuses on the collaboration between the management level activities and the operational level activities in order to cope with ICT risks successfully.

Keywords
ICT risk management; COBIT; ISO/IEC 17799; Information security management

INTRODUCTION
The rapid development of information and communication technologies (ICTs) has effectively facilitated reorganizing a firm’s business processes and streamlining the provision of its products and services in today’s dynamic business environment (Lientz and Larssen 2004). Such adoption helps modern organizations develop and maintain their competitive advantage for ensuring their profitability and survivability in the market place. Their competitive advantage often brings organizations numerous benefits including fast business transactions, increasing automation of business processes, improved customer service, and provision of effective decision support in a timely manner (Mansell 1999; Ruddock 2006). However, the adoption of ICT applications has also brought organizations risks related to ICT such as strategic risk, financial risk, operational risk and technological risk. In order to minimize and control these risks successfully, ICT risk management policies and strategies have been developed and implemented in organizations.

In general, ICT risk management is referred to as the essential process to aid enterprise achieving “the new business changes, future investment in information and information system, an increasing ICT threats and an increasing dependence on delivering information in system” (Jordan and Silcock 2005; Lainhart 2000, P. 5; Lainhart 2001). Nevertheless, the success of ICT risk management in organizations has been questioned in the past 10 years (Coles and Moulton 2003; Segars and Grover 1996; Teneyuca 2001). For example, a computer security institute research shows that approximately $202 million were lost in computer crime in 2003 (McAdams 2004). ICT abuse and fraud are increasing in organizations, although organizations have concrete ICT governance arrangements in place as illustrated in a report by the Audit Commission of the United Kingdom (Audit commission 2005). Moreover, a government report in America demonstrates that over 80 percent of ICT development projects have failed in whole or in part due to poor ICT risk management (Center for Technology in Government 2007).

According to the reports above, two well-structured approaches including ICT governance and Information security (IS) governance have been developed for ICT risk management. In ICT governance, the management perspective is included in the management of ICT risks. Such an approach facilitates and encourages a top-down methodology for identifying, evaluating, minimizing, and controlling potential ICT risks in an organization (Lientz and Larssen 2004).

ICT governance, as a top-down strategy, is represented in the COBIT framework which is extensively used to describe the business functions, processes and tasks to support top management in developing and implementing ICT governance (Robinson 2005; Solms 2005). By adopting COBIT, the organization is concerned more with a business view than with technical solutions to ICT risk management. As a result, the emphasis is on the
organizational structure and content (Solms 2005), which often leads to lack technical capabilities in organizations (Hermanson et al. 2000; Viator and Curtis 1998).

Another standard that has been developed is IS governance which uses a bottom-up approach to ICT risk management. A representative of an IS governance standard is the ISO/IEC 17799 standard for effective ICT risk management. The ISO/IEC 17799 standard focuses on a detailed technical solution to risk management (Saint-Germain 2005; Solms 2005). This standard represents a bottom-up approach which explains detail technical processes coping with ICT risk management. The ISO/IEC 17799 standard provides organizations with the specific details on how the ISO/IEC 17799 standard can be used for controlling, preventing and mitigating ICT risks. This approach is, however, often criticized due to its over-emphasis on the technical implementation of risk management (Karabacak and Sogukpinar 2006; Mellado et. al. 2007; Solms 2005).

In order to investigate successful ICT risk management, empirically we have raised two questions to help understand the alternative perspectives on ICT risk management in organization. The questions are:

- What are the current profiles of ICT risk management in organization?
- How are ICT risk management concepts applied in organization?

**ICT RISK MANAGEMENT**

In general, ICT risk management is embedded in organizational internal control and audit which are widely used as part of the management control for risk management in organization (Speklé et al. 2007). However, this management control emphasises both business control and technological control which support business requirement and governance. Business and technological controls are involved in the policies, processes, systems and people in the organization (IIA 2006). Internal control and audit have played the main role of risk management. Internal control and audit can be used to “(a) provide risk management and control advice to relevant staff across the organization, (b) provide independent assurance to the board about the adequacy and effectiveness of key controls and other risk management activities across the organization, and (c) act as risk and control educators across the organization” (Pickett 2005, P. 41).

Internal control and the audit process control the entire range of interactive transactions and internal transactions across organization as well as monitor and manage risks including business risks and ICT risks (IIA 2006; Leuang et al. 2003). In an organization, internal control and audit is a process to help the organization manage and control its transactions, which is in the role of corporate governance (Leuang et al. 2003; Pickett 2005; Pickett and Pickett 2005). Pickett (2005) and Pickett and Pickett (2005) further mention that effective corporate governance reflects successful risk management in the organization. In term of governance itself, “there are three kinds of governance which should be considered in corporate environments: corporate governance, ICT governance and Information security (IS) governance” (Kim 2007, P. 235). The standard for corporate governance of ICT was recently released in Jun 2008, called ISO 38500 (ISO 2008). This standard is a conceptual approach to help organisations visualise effective ICT governance aligning with ICT management tools. The ISO 38500 standard provides guidelines to directors for directing, evaluating, and monitoring ICT (ITGI 2008). Moreover, the guidelines consist of “(a) defining and implementing clear responsibilities for ICT, (b) ensuring ICT strategy with the business, (c) acquiring ICT sensibility, (d) ensuring ICT performance, (e) ensuring ICT compliance with policies and law and (f) driving the human side of ICT” (The Quintica Group 2008). However, due to being a new standard, there is no literature regarding its implementation. Thus, this paper focuses upon the available standards and other frameworks by focusing on ICT governance, Information security (IS) governance and information security management.

Focusing on only an ICT perspective in the organization, corporate governance has less emphasis on risk management especially ICT. ICT governance is the responsibility of senior management to provide strategic direction of technology in order to achieve business goals and objectives (Bodnar 2003; Buckby et al. 2005; ISACA 2007; ITGI 2007; Korac-Kakabadse and Kakabadse 2001; Lainhart 2000; Ridley et al. 2004; Smith and McKeen 2006). One clear responsibility of executive management in ICT governance is ICT risk management (Buckby et al. 2005; Trites 2004). IS governance specifically is used to align with the ICT governance framework as an integrated strategy in order to achieve effective corporate governance (Solms 2001). Information security (IS) governance focuses on the leadership, organizational structures, and processes in order to help the organization provide superior relevant processes to safeguard information (Solms 2001). Significantly, its benefits lead to “(a) increased predictability and reduced uncertainty of business operation by lowering information security-related risk to a definable and acceptable level, (b) assurance of effective information security policy and policy compliance, and (c) a firm foundation for efficient and effective risk management, process improvement, and rapid incident response related to securing information” (ITGI 2006, P.14).
If ICT and IS governance are properly established in the organization, it will inevitably lead to effective corporate governance for ICT. Figure 1 shows the relationships between internal control and audit as well as corporate governance for ICT with respect to ICT governance and IS governance based on business orientation and technological orientation (IIA 2006; Pickett 2005).

**Figure 1: Internal control and audit for ICT risk management (Adapted from IIA 2006; Pickett 2005)**

**INTERNAL CONTROL AND AUDIT TOOLS FOR ICT RISK MANAGEMENT**

The COBIT framework is widely recognized as a key strategic tool in ICT governance for ICT risk management (Khan 2006). This framework provides general management guidelines for organizations to manage ICT assets and to facilitate ICT processes for effective ICT risk management (Bodnar 2006). It categorizes critical success factors into (1) plan and organize domain, (2) acquire and implement domain, (3) deliver and support domain as well as (4) monitor and evaluate domain (ITGI 2007). These four domains can be applied in an organization’s processes such as “processes and policies description, clear duty and task, management commitment, appropriate communication to concerned internal and external persons and consistent measurement practices” (Hawkins et al. 2003, P. 28).

Solms (2005a) in research on the effectiveness of the COBIT framework in ICT risk management shows that the COBIT framework is a high level control objective framework which is a superior ICT governance framework. COBIT gives more detailed instructions on “what” must be done in an organization with respect to ICT risk management. Lainhart (2000) shows that the COBIT framework is the main theme of overall business control for alignment with technological control in the organization. The COBIT framework, however, is less detailed on “how” it should be done in organizational ICT risk management that has a more technical orientation (ITGI 2005; Solms 2005). Moreover some researchers argue that top management lacks ICT security concerns (Byrd et al. 1995) and that this then may affect the level of technical planning for the annual plan in the ICT risk management.

Buchanan and Gibb (2007) further add that the role and scope of the information audit used in an organization are both often neglected or forgotten in developing an understanding of processes and practice. The three main problems of an information audit are: “Firstly, top-down approach itself still has a lack of clear top-down strategic direction. Secondly, there is less practical guidance on the scope of the information audit. Thirdly, there is no standard; agreed methodological approach to information audit” (Buchanan and Gibb 2007, P. 3). It can be argued then that information audit and control lack a clear scope and role which are the most important when organisations attempt to cope with ICT risk management. To address these shortcomings of the COBIT framework, the ISO/IEC 17799 standard can be used as it represents an alternative perspective on the ICT governance framework. The ISO/IEC 17799 standard ensures that a technical perspective is taken into account at the management level in order to strengthen management processes and procedures in an annual plan (Eloff and Eloff 2003). This standard was established to provide organizations with a holistic technical approach which refers to technical specifications such as a network system security, personnel security and organizational security (Kenning 2001; Theoharidou et al. 2005).

Groves (2003) demonstrates that the ISO/IEC 17799 standard provides more a technical orientation to risk management and includes generating a document of information security policy, assigning the responsibility for information security, training and educating information security, reporting security incidents and establishing a plan of business continuity management. The ISO/IEC 17799 standard is used to establish a process for...
protecting information in a collaborative effort by all employees in an organization. Capuder (2004) concludes that the processes of dealing with information security require commitment at all levels in the organization. The ISO/IEC 17799 standard concerns technical staff such as an internal auditor or security professionals and require them to deal with information security. Theoharidou et al. (2005) argue that using ISO/IEC 17799 helps organizations handle computer abuse from insider threats, threats derived from employees who have authorized access to IS and misuse it.

Both the COBIT framework and the ISO/IEC 17799 standard address both of the aspects of ICT governance and IS governance coping with ICT risk management - general ICT alignment with business orientation and technological security orientation. Jordan and Silcock (2005) and Sarens and Beelde (2006) suggest that ICT risk management should then focus on both top-down and bottom-up approaches. Such an effective integration of the COBIT framework and the ISO/IEC 17799 standard can be used, they argue, to enhance the needs of business by focusing on four key elements in the organizational ICT risk management: strategy and policy, roles and responsibilities, processes and approach, and people and performance (Jordan and Silcock 2005; Robinson 2005). Mena (2002) shows that close co-operation between senior management and the operational team can lead an organization to the attainment of optimal goals in ICT risk management. Each of the approaches alone is not comprehensive enough by itself. Hence, a focus on either business control or technical control alone is insufficient control for business requirements. This paper uses case studies to illustrate the advantages of using both standards.

RESEARCH DESIGN AND DATA COLLECTION

This research uses an interpretive perspective (Myers and Avison 2002) to explore belief, action and experience of the participants in particular ICT risk management areas in three organizations in Thailand. Inductive reasoning was employed by using the exploratory multiple case studies method (Shanks et al. 1993; Yin 1994). This method is appropriate for understanding and exploring ICT risk management in organizations. An exploratory research approach is used to explain and understand in detail the application of existing theory to what is happening (Scapen 1990).

Three Thai business case studies (a bank, a telecommunications company and a software development company) were purposively selected in Thailand to examine the application of both standards, COBIT and ISO/IEC 17799. Primary data was collected from semi-structured interviews using open-ended question with senior management and operational management levels at their organizations. The interview sessions were run for approximately one hour per person. Also, a digital voice recorder was used with the participants’ prior consent in order to ensure the accurate transcription of the interviewee’s perspectives. During the interviews, open-ended questions were asked of the participants to investigate their perceptions and experience in ICT risk management related to application of both the COBIT framework and the ISO/IEC 17799 standard. Short notes were also used to collect the participants’ feelings about whether they were sure about the meaning of the questions and the answers for a particular question or not. Secondary data was also collected from the organization to triangulate the interview data. These documents include their general ICT plans and their ICT security plans.

An interpretive analysis was conducted from three case studies along with eight interviews. The paper will refer to the three case studies and the participants as described in Table 1.

<table>
<thead>
<tr>
<th>Case study</th>
<th>Type of business</th>
<th>Number of Employees</th>
<th>Number of participant</th>
<th>Participant name</th>
<th>Position level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case study A</td>
<td>Telecommunication company</td>
<td>5,154</td>
<td>2</td>
<td>Khung Pol</td>
<td>Assistant Vice President (ICT audit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Khun Noy</td>
<td>Operation manager</td>
</tr>
<tr>
<td>Case study B</td>
<td>Bank</td>
<td>570</td>
<td>3</td>
<td>Khun Chai</td>
<td>Assistant Vice President (ICT)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Khun Nart</td>
<td>Division Director (ICT)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Khun Rong</td>
<td>Division Director (Internal Audit)</td>
</tr>
<tr>
<td>Case study C</td>
<td>Software development company</td>
<td>520</td>
<td>3</td>
<td>Khun Wat</td>
<td>Technical Director</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Khun Koy</td>
<td>Software developer manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Khun Kaow</td>
<td>Information Security (IS) manager</td>
</tr>
</tbody>
</table>

The interviews were conducted from July to October 2007 in Thailand with organizations which use both technological and accounting tools to deal with ICT risk management. The data was collected from the same management level view to enable real comparison of the data. Each interview was conducted using a proforma
of open ended questions which were uniformly asked of each participant. Interviews were conducted in Thai, transcribed and then translated into English with a check put in place to ensure accuracy of the translations.

Table 2. A comparison of handling ICT risk management in organization

<table>
<thead>
<tr>
<th>Main issue</th>
<th>Case Study A</th>
<th>Case Study B</th>
<th>Case Study C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organisational structure</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Setting committee to be responsible for ICT risk management</td>
<td>- Audit committee</td>
<td>- Audit committee</td>
<td>- Not specified</td>
</tr>
<tr>
<td>- Risk management committee</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Enterprise-wide security committee</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. ICT risk management treatment</td>
<td>- Corporate level</td>
<td>- Organizational level</td>
<td>- Project management</td>
</tr>
<tr>
<td>- Operational level</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Components of ICT risk management</td>
<td>- ICT control and audit</td>
<td>- General ICT</td>
<td>- ICT security</td>
</tr>
<tr>
<td>- ICT security control and audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Components of ICT control and audit</td>
<td>- ICT applications</td>
<td>- Applications</td>
<td>- Not specified</td>
</tr>
<tr>
<td>- Risk assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Operating system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Other ICT system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Components of ICT security control and audit</td>
<td>- Technical terms for security policy</td>
<td>- Developing security policy</td>
<td>- Security in a project management</td>
</tr>
<tr>
<td><strong>Organizational process</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. ICT risk management instrument</td>
<td>- A risk statement for an entire organization</td>
<td>- A risk statement for an entire organization</td>
<td>- A risk statement for a security function</td>
</tr>
<tr>
<td>- Specified risks for an entire organization</td>
<td></td>
<td></td>
<td>- Specified risk in project management</td>
</tr>
<tr>
<td>7. ICT risk management process</td>
<td>- COBIT is implemented</td>
<td>- Enterprise Risk Management (ERM) is implemented</td>
<td>- ISO is implemented</td>
</tr>
<tr>
<td>- ISO is implemented</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organizational control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. People</td>
<td>- ICT security awareness</td>
<td>- Access control</td>
<td>- Human resource protection and security</td>
</tr>
<tr>
<td>- Computer abuses</td>
<td></td>
<td>- Role and responsibility</td>
<td></td>
</tr>
<tr>
<td>- Educating and training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Rules and regulations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Human resource security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Information management</td>
<td></td>
<td>- Information management</td>
<td></td>
</tr>
<tr>
<td>- Security treatment</td>
<td></td>
<td>- Auditable area</td>
<td></td>
</tr>
<tr>
<td>- Setting the configuration</td>
<td></td>
<td>- Security management</td>
<td></td>
</tr>
<tr>
<td>- Penetration test</td>
<td></td>
<td>- Setting the configuration</td>
<td></td>
</tr>
<tr>
<td>- Security scanning tool</td>
<td></td>
<td>- Data authentication</td>
<td></td>
</tr>
<tr>
<td>- Auditable area</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Technology</td>
<td>- ICT application</td>
<td>- General control</td>
<td>- Application control</td>
</tr>
<tr>
<td>- ICT security</td>
<td></td>
<td>- Application control</td>
<td></td>
</tr>
<tr>
<td>11. System</td>
<td>- ICT infrastructure</td>
<td>- ICT infrastructure</td>
<td>- Communication link infrastructure</td>
</tr>
<tr>
<td><strong>Organizational ICT strategies</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Strategies</td>
<td>- The managerial focus</td>
<td>- The managerial focus</td>
<td>- The operation focus</td>
</tr>
<tr>
<td>- The operational focus</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. ICT risk management plan</td>
<td>- Corporate plan</td>
<td>- Corporate plan</td>
<td>- Operational plan</td>
</tr>
<tr>
<td>- Operational plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Revision of ICT department structure</td>
<td>- Not specified</td>
<td>- Not specified</td>
<td>- ICT department</td>
</tr>
<tr>
<td>- ICT security function</td>
<td></td>
<td></td>
<td>- ICT security function</td>
</tr>
</tbody>
</table>
A summary of comparisons between the three case studies with regard to each of the key elements of ICT risk management is listed in Table 2. There are thirteen main issues within organizational structure, organizational process, organizational control and organizational technical strategy with regard to ICT risk management for which data was collected. The findings are discussed in the next section.

DISCUSSION

According to the organizational profile relating to ICT risk management in the case studies, all three cases focus mainly on the application of ICT risk management concepts through the mapping of the four key areas of organizational structure, organizational process, organizational control and organizational ICT strategy.

Organizational Structure

Firstly, ICT risk management is governed by a separate committee which is responsible for different tasks in the organization relating to ICT risk management. Case study A has the clear responsibility of setting the ICT risk management strategy by monitoring and directing internal processes in the organization. The Audit committee mostly directs and monitors the internal operational transactions. The risk management committee is mainly concerned with several types of risk including business and ICT. Risks that occur as a result of information security problems are governed as an entire organization by an enterprise-wide security committee. In this organization several types of risk, including operational risk, business risk, ICT risk and IS risk, can be mitigated against, avoided and prevented simultaneously. By contrast the organisations in case studies B and C were concern with less setting of the responsibility for dealing with ICT risk management.

Secondly, the position level of ICT risk management treatment is considered within the entire three case studies but in each case from a different perspective. The organisations in case studies A and B control and audit ICT risk at both the corporate level and the operational level appropriately because ICT risk management treatment covers the origin of risk and the risk impact. This helps the department report back to the board to define the process of risk treatment to the other departments in order to mitigate, avoid and prevent the risk in the organization. The organisation in case study C is different from both A and B because it is a software hub. The major tasks of their operations are on computer programming or software development; as a result the process of risk treatment is in the application software embedded in each project produced.

Thirdly, the component of ICT risk management comprises ICT control and audit as well as information security control and audit. According to organisations A and B, ICT risk management relates to ICT activities and information security activities whilst dealing with ICT risk. Both organizations have set the term of ICT activities within ICT policy and information security activities as in IS policy. This means that the staff understand their role and responsibility when they react to any type of occurred risk from ICT and that they report back to the board. On the contrary, organisation C focuses on only the IS part because the entire work of their staff depends upon software development. Therefore, the staff always react to the risk via using the application software to fix the problem and mitigate against the negative impact.

Organizational Process

Firstly, the risk statement is seen from a different perspective according to the position level. However, the details on the risk statement cover the process for the both the entire organization and the specified function in the organization. In both organisations A and B, the risk statement is viewed as an ICT risk management instrument for the staff to follow at the corporate level and at the operational level. With regards to the meaning of the risk statement at the corporate and operational levels, ICT risk management is used to clarify the risk methodology in corporate and operational plans. For example, in the corporate plan regarding ICT risk management, the organization sets the scope of the overview of ICT risk management. Furthermore, in the operational plan, the organization sets the details of ICT risk management processes aligning with the corporate plan. This is a clear process statement for dealing with ICT risk in the organization. Conversely, organisation C mainly focuses on the specific function of each project produced, which means that the organization is concerned more with the operational level than the corporate level.

Secondly, in order to specify the processes in the organization, organisations A, B and C all follow the guidelines from the international accepted framework and standard of COBIT, of ISO 17799 and of Enterprise risk management (ERM) respectively. Organisation A complies with the COBIT and the ISO 17799 standard in order to specify the appropriate processes for ICT perspectives in both the corporate, top-down approach, and the operational bottom-up approaches. On the other hand, organisation B is concerned in addition with COBIT aligning with the ERM which is the methodology of business risk management in the organization by implementing the methodology from a business angle to direct, control, and monitor the ICT. This organization mainly focuses on a top-down approach as the mainstream approach at the corporate level, driving it to the operational level in order to mitigate, avoid and prevent risks from ICT. Organisation C considers only
information security to be part of a bottom-up approach to ICT risk which is the natural concern of the software development side.

Organizational Control

The common criteria are that each organisation emphasise are control of people, process, technology and systems in all three organizations. Organisation A, B and C concentrate on the control of business, service, ICT and IS functions simultaneously; although they emphasise those four functions from different perspectives. Due to these being different types of organization, each has to control and monitor the transaction generated from internal section and external section. For example, in organisations A and B, the entire transaction process relates to the operational process from routine and billing actions with customer. Thus business, service, ICT and IS functions are monitored concurrently. On the other hand organisation C operates each software development project as a job-order and as job-by-job which leads to ICT risk management being focused in each project by focusing on the application security management. Hence, the framework and the standards are considered accordingly to achieve successful ICT risk management in their organization in isolation. However, service functions, including both the internal and external parties involved, remain unaddressed in the organisation. Furthermore, it is not mentioned in detail at this level because it relates to another standard as ICT service management called The Information Technology Infrastructure Library (ITIL).

Organizational ICT Strategy

Organizational ICT strategy from the three case studies illustrates that they focus on ICT risk management in different ways. However, the case studies have raised common issues that an organization should consider about ICT strategy. Furthermore, both top-down and bottom-up approaches are considered relevant differentiated by the type of business. This can be clarified when an organization plans to deal with ICT risk management. An organization should consider risk planning at the corporate level within the overall ICT plan then leading to the operational plan by covering both ICT management and IS management. ICT risk management is considered at both corporate and operational levels as ICT risk management and ICT project risk management respectively. Moreover, different management levels in the studied organisations were concerned that the plan should be separated with the consensus agreement on the plan at both levels. This means that ICT risk management is planned at the corporate level as the scope of ICT risk management then drives the operational level to plan ICT project risk management in detail in each relevant department. However, both ICT risk management and ICT project risk management should be planned in the same direction as an entire organizational ICT risk management plan. As a result, successful ICT risk management planning focuses on the collaboration between the management level activities and the operational level activities in order to cope with ICT risks successfully.

In conclusion, in order to help an organization apply the framework and standard to map ICT risk issues properly, there is a need to investigate and apply both the COBIT framework and the ISO 17799 standard for dealing with ICT risk management planning in organization by following the guidelines from ITGI (ITGI 2005). The COBIT framework enables defining a strategic IT plan (PO1), defining the information architecture (PO2), determining technological direction (PO3), defining the ICT processes, organization and relationships (PO4), assessing risks (PO9), managing project (PO10), defining and managing services levels (DS1), managing performance and capacity (DS3), ensuring continuous service (DS4), ensuring systems security (DS5), managing service desk and incidents (DS8), managing the configuration (DS9), managing problems (DS10), managing data (DS11), managing the physical environment (DS12), managing operations (DS13), monitoring and evaluating ICT processes (ME1), monitoring and evaluating internal control (ME2), ensuring regulatory compliance (ME3), and providing IT governance (ME4). Aligning with the ISO 17799 standard, risk assessment, information security policy, organization of information security, human resources security, physical and environmental security, communications and operations management, access control, information security incident management, business continuity management and compliance are considered.

RESEARCH LIMITATION

There are limitations of this research. Firstly, the Basel II accord is not illustrated in this research, although it is a compulsory for banks around the world. In order to gain more information regarding the operational risk related to ICT, the researchers have noted that in future research the Basel II accord must be considered in ICT risk management to add-in to the process of data collection in order to understand the phenomenon whether the bank concerns with the Basel II accord along with the COBIT and the ISO 17799. Secondly, the new ISO 38500 standard for ICT corporate governance is also a main concern for dealing with ICT risk management in organizations. Because ISO 38500 is targeted at the highest level of governing ICT including ICT governance and IS governance while planning ICT risk management process. Lastly, ITIL is considered best practice for ICT service management and it is also recommended to supplement the COBIT and the ISO 17999 for dealing with ICT risk management (ITGI 2005).
CONCLUSION

ICT risk management in the three studies of Thai businesses is focused at both the corporate and operational levels. The corporate level sets the overall ICT risk management plan. The operational level is the specific technical security plan for ICT as ICT project risk management. Furthermore, both the corporate and operational levels in the three organizations reveal that organizational policy, organizational strategy direction, human resource management and planning, information security management and ICT management are the main factors to consider whilst dealing with successful ICT risk management. In order to achieve ICT risk management planning, these case studies have shown that any organization has to concentrate on both general ICT and security ICT simultaneously. The three companies use the two approaches to link together a complete pipeline (namely the two-way approach), in their view effective ICT risk management. The two-way approach works well as the COBIT framework lays the foundation of the top-down approach to risk management; on the other hand, the ISO/IEC 17799 standard focuses on the bottom-up risk management. Furthermore, the discussion shows that the four constructs evaluated in three cases in Thailand reflect use of both the COBIT framework and the ISO/IEC 17799 standard and report that the organizations perceive they are effective and efficient in putting risks under control.

REFERENCE


ACKNOWLEDGEMENTS

We would like to thank the track chair and the reviewers for their comments on the manuscript version.

COPYRIGHT

Kumsuprom Siridech, Corbitt Brian and Pittayachawan Siddhi. © 2008. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.