LUND UNIVERSITY
School of Economics and Management

Risk Assessment

For Enterprise System Integration

Master thesis, 15 hp, Department of Informatics
Submitted: June, 2008
Authors: Narip Boonsiripant
Wacharawan Intayoad

Supervisor: Anders Svensson
Examiners: Erik Wallin
Linda Öberg

Lund University

Informatics

Risk Assessment

For Enterprise System Integration

Master thesis submitted June, 2008

Size: 74 pages

Supervisor: Anders Svensson

Resumé

Technology is playing a vital role for most companies to stay competitive over others. The global market has become very competitive so that it drives companies to adapt themselves to survive on this intense competition. Efficiency of an enterprise can be increased by integrating systems to business partners to create sustainable competitive advantage in the long run. System integration can be done by adopting the Business-to-Business e-commerce technology that will help connect linkages with external organizations. Due to the complication of system integrations, risk management is often overlooked because project managers are overwhelmed with the occurring problems and deadlines. In fact, if risks are properly identified and handled, the integration project can be even more smoothly implemented.

This thesis is to find out major risk areas for system integration and assess them in the context of enterprise risk management. The theoretical part provides understanding towards system integration and risk management while the empirical data is gathered via interviews with people who have experience and knowledge about the system integrating implementation. The results of the study present the major areas of risks that should be considered, including the assessment methods, when planning a system integration project. This will provide more understanding towards risk management in the area of extended-enterprise systems. Enterprises can use it not only to manage the IT system as a technical perspective, but also as an essential management function of the organization.

Keywords: Risk, Enterprise System, System Integration, Enterprise Risk Management, Business Partner Integration, Risk Management, Risk Assessment

Acknowledgements

This thesis would not have been possible without help and support from several people. We wish to thank all the respondents for their time and most valuable input; Surapol Sankasuban, Suchada Jariyaporn, Jirachchaya Suddee, Thitima Pungpibul, Tippawan Attajarusit, Surasin Tanchareon, and Sinchai Chanatokakul. We are grateful to their dedication of giving their valuable expertise, experience, and managerial skills that have been very constructive to the study. We would like to thank our friends and family for their support and encouragement during the study. We also thank to Erik Wallin and Linda Öberg for their helpful suggestions to the research. Finally we would like to thank our supervisor, Anders Svensson, for being supportive and generous with valuable criticism.

Thank you all

Lund University, June 2008

Narip Boonsiripant Wacharawan Intayoad

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Background and Problem Areas

Business-to-Business e-commerce technology has become a great factor driving enterprises to change their business environment in order to stay competitive over others. Organizations have re-engineered their business processes to exploit the tight integration of enterprise software with business processes, to maximize their efficiency and effectiveness. Business-to-Business e-commerce technologies have influenced the enterprise systems to jump into the power of that technology, and provide linkages between trading partners such as supply chain partners (Sutton 2006). In practice, IT governance and enterprise risk management strategies have not prepared to handle these rapid changes which result in causing vulnerabilities to unidentified risks derived from business partners. Corporate entities find themselves competing in the global market that focuses on cutting costs and general improvement of efficiency. The primary drive for these movements toward efficiency gains has been the use of enterprise systems to streamline internal operations and Business-to-Business e-commerce technologies that facilitate the tight linkages with external organizations. Quick application deployment, along with roughly planned implementations, led to widely reported failures of systems that either failed to adequately capture and process enterprise information, or failed to support critical business processes.

When an organization adopts a framework of enterprise risk management, the risk analysis will depend on the information, experience, and capability to handle problems already available in the business structure. To use the automating risk management processes, the business will have more precise and useful information for risk management which will improve both operating results and gain more support from the management in risk managing projects (Roland 2008). Nowadays, technology makes it easier to integrate risk management into critical business processes and improve performance. Technology solutions can provide several of the key features of a mature risk management program, including collaborative process support, audit and security, proactive automation, and integration with performance management.

1.2 Research Questions

The research question was founded to be used as a research guideline along the study. The investigation of the data collection was carried out in the area in question, and also the analysis of the findings was focused on the model of the research questions. The questions were formulated as the following:

"What are major risk areas inherited from inter-organizational system integration, in the context of enterprise risk management?"

After we knew the major risk areas, we investigated more on *"How to assess those risks from system integration?"*

1.3 Purpose

The aim of the thesis is to define a guideline for risk assessment in the area of system integration. The study will focus on risk assessment framework that can help assess level of risks in the major risk areas. Risk analysis framework can be used as a risk assessment model, which can be applied as an important part of the enterprise risk management. This framework will help key role persons to analyze risks inherited from system integration containing complexity in its system and difficulties from third party involvement. The framework will support the expanded boundaries of risks from external environment as well as the changing internal working environment of the extended enterprise system. We believe that the Business-to-Business integration will become more important for enterprises to stay competitive, especially in this globalized era. Thus it is crucial for key role persons to understand and properly assess these risks in order to develop effective strategy and manage the enterprise effectively.

1.4 Research Contribution

The research area will contribute to the risk management in the area of *risk assessment* in the extended-enterprise systems. The study will not only relate to the boundaries of the enterprise or company themselves, but also those impacts that might arise from inter-organizational relationship. It includes upstream and downstream trading partners in the supply chain, outsourcers, and other electronically connected business partners. In business, enterprise risk management includes the methods and processes used by organizations to manage risks (or seize opportunities) related to the achievement of their objectives. Enterprise risk management provides a framework for risk management, which typically involves

identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress (COSO 2006). By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

1.5 Delimitations

The study will focus on Business-to-Business enterprise model and its integrations such as connection to business partners. Enterprises of small size or Business-to-Customer e-commerce will not be covered. The framework is developed under investigation in Thailand but since Thai enterprises normally adopt Information Technology from abroad, it is most likely that there are no big differences in system infrastructure and integration techniques. Somehow, the framework may best match the cultural and working style of Thai enterprises.

This model can be used as fundamentals for the other procedures of enterprise risk management that we do not cover in this study, such as risk mitigation, risk response, control activities, or monitoring.

1.6 Research Structure

In this research, the theoretical framework is grounded by the knowledge areas of enterprise information system and enterprise risk management. The theory chapter explains the traditional enterprise system and its development to compete in the business world, the extended-enterprise system. The integration of the enterprise system is also illustrated to provide understandings towards its benefit for IT collaboration. A paradigm of risk management is exemplified to give insight of its role and use to the enterprise system. The research methodology illustrates the visibility and credibility of the study by showing the methods that the study was carried out. Also there is a note in regards to research ethics to provide the audience with the ethical perspective. The empirical study part is showing the information that is gathered from the data collection, which is categorized into major topics to help analyze the research question. The framework of analysis shows the study result, which is analyzed from the categorized data collection, which leads to the conclusion and future research in the last chapter. The thesis is divided into seven chapters which are detailed in the following:

Chapter 1 Introduction – Explains background and problem areas, with the relevant knowledge domain. The research question is formulated in this chapter, with the purpose and delimitation of the research.

Chapter 2 Enterprise Information System – Shows concepts of enterprise information system, its integration approaches, and its evolution to extended enterprise system.

Chapter 3 Enterprise Risk Management – Provide paradigm of risk management in the context of enterprise planning and strategy, with an emphasis on risk assessment. Risk management for extended enterprise is also described, with practical samples of risks from extended enterprise system.

Chapter 4 Research Methodology – Illustrates the methods for each research approach and its motivation of why and how the research is conducted.

Chapter 5 Empirical Findings – Categorizes the interview results into major implementation phases which are before integration phase, to-integration phase, implementing phase, and after integration phase. These results are used in analyzing the research question.

Chapter 6 Discussion – Findings in this research are discussed in comparison to the theoretical framework. The major areas of risks for extended enterprise system will be categorized from collected data, which will be used for risk assessment. Each area of analysis is explained in this chapter.

Chapter 7 Conclusion – Summarizes the study and present the final outcome of the thesis. Future research area is also mentioned in this section.

2 ENTERPRISE INFORMATION SYSTEM

Enterprise entities take advantage of the efficiency and effectiveness from Enterprise information system. The enterprise information systems are software packages, such as ERP system. Some of this enterprise information systems are relatively expensive to implement, and also inflexible and costly to customize (Sarkis & Sundarraj 2006). Enterprise entities find themselves competing in the global market either cutting costs or improving efficiency. However, sustainable competitive advantage cannot be obtained from cutting costs. Having integrated Business-to-Business e-commerce technologies to the enterprise systems, business environment tend to stay competitive over others. The primary drive for these movements toward efficiency gains has been the use of enterprise systems to streamline internal operations and Business-to-Business e-commerce technologies that facilitate the tight linkages with external organizations (Sutton et al 2006). The inter-organizational systems should be implemented to facilitate the integration business process such as the electronic exchange of information flows (Themistocleous et al 2002).

2.1 Type of Enterprise Information System

Integrating enterprise-wide information systems generally can be carried out in two ways: Enterprise Resource Planning (ERP), and Best-of-Breed (BoB). Enterprise resource planning software systems attempt to integrate all departments and functions across a company onto a single information system that can serve all those different departments' particular needs. Typically, a department with specialized functions and needs may have its own information system, customized to its particular procedures and duties. Nonetheless, the main effort of an ERP implementation is to combine as much functionality as possible into a single, integrated software program that runs on a single database, in order that the various departments can easily share information and communicate with each other (Tarantilis et al 2008).

Enterprise resource planning systems are a one big vendor software package that helps provide best-practice business process functionality running on a single database (Light & Wills 2001). Currently SAP and Oracle are globally accepted as leading Enterprise Resource Planning vendors on this market. Enterprise Resource Planning implementations normally come up with extensive business process reengineering (BPR) because even though Enterprise resource planning packages are usually configurable to meet the specific requirement of an organization's industry, geography, organizational structure, among other

requirements, they are, in the same time, considered non-flexible regarding the business processes (Hyvonen 2003; Themistocleous & Love 2004).

Most of the cases, organizations inevitably have to restructure their business processes to match the Enterprise Resource Planning software packages (Davenport 1998). Those organizations trying to customize Enterprise Resource Planning systems to use with their existing processes have always made themselves even more problems, such as delaying implementation, increasing staff requirements, and obstructing the upgradeability of the system (Light & Wills 2001). Enterprise Resource Planning implementations are usually time-consuming, costly and very troublesome to an organization (Davenport 1998).

Best-of-Breed systems are combinations of different software packages which provide more limited and focused functionality, such as one system for financials, one for accountings, one for human resource management, and so on. Organizations mix and match what they consider to be the best collection of software packages to match their organizational needs (Geishecker 1999). These packages are then integrated using some type of middleware. Best-of-Breed implementations are considered to be less troublesome to an organization, require less process reengineering, and providing more flexibility. However, because the packages come from different vendors there may cause compatibility problems and integration issues. In addition, maintenance and upgradability for Best-of-Breed system are likely to be more problematic than with a single vendor Enterprise Resource Planning system (William et al 2008).

Most of enterprises invest on their own systems in package, legacy systems and custom application which are complex and inflexible. It may lead to difficulties changing business requirement or operation process (Qureshi 2005). Thus enterprise information systems need to be flexible and adaptive to respond to the changing business needs. Evgeniou (2002) describes four types of organization that relate to their enterprise system types. The first one is standardized enterprise which is lack of inflexibility. The second one is steady state which has low requirement to be flexible, for example the monopolies and public sector organizations. The third one is decentralized enterprise which requires the flexibility to change in the organization but has limited of visibility to global business. Normally, these enterprises have those best-of-breed software. The last one is adaptive enterprise which has high visibility and flexibility. This type of enterprises has the system that can support internal process and also provide inter-organization processes such as electronic supply chain system.

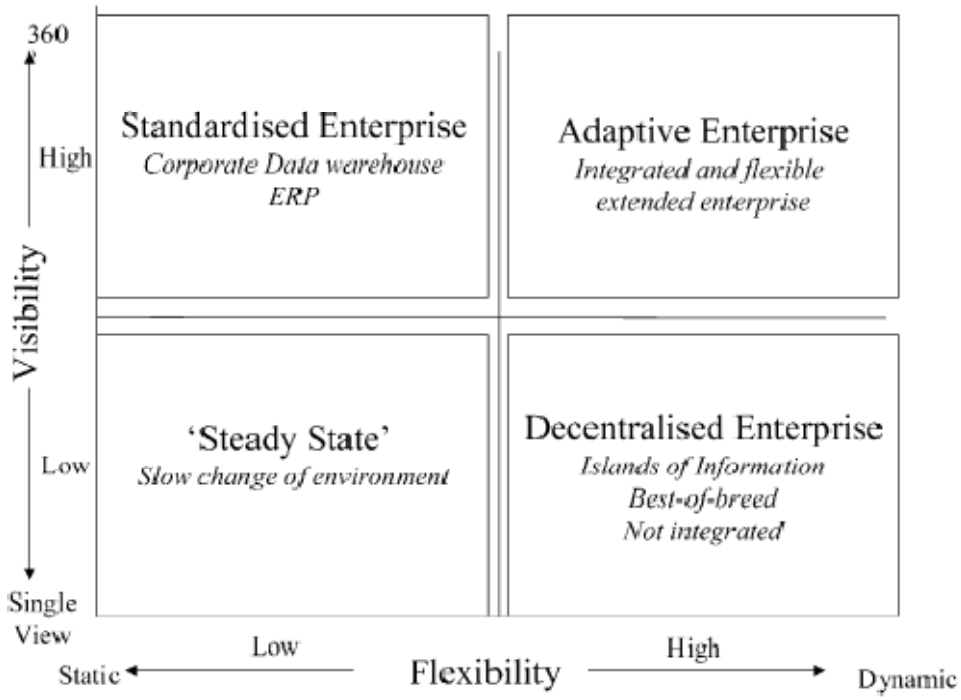

Figure 1 Type and infrastructure of Enterprise System (Evgeniou 2002, page 491)

The figure 1 describes four generic types of organization and general information technology infrastructure. Visibility on the vertical axis shows the number of views of management information an organization can have, ranging from a single perspective to multiple or global/regional, customer, and product. Flexibility on the horizontal axis ranges from static, which is inflexible to business changes, to dynamic, where change is considered a constant factor and the capability to respond the change is more likely to be possible (Evgeniou 2002).

2.2 Enterprise Integration

Recently many organizations use the process called enterprise integration as a key technique to transform their business processes to pursue the e-business benefits. For example, a company wants to offer its products or services on the Internet, so they implement Web-front-end systems and integrate with the enterprise legacy system. In this case, legacy system refers to any IT system already in operation. Integration is the organizations linkage of their systems to partner systems. For example, an emerging enterprise integration development is business-to-business (B2B) integration which also called extended enterprise model. The enterprise integrates its own business processes with those of its business partners to increase efficiency within a collaborative value chain (Wing & Venky 2004). The e-business current solutions mostly rely on enterprise integration requirements to integrate web-based systems

to each other and heterogeneous legacy systems which belong to the organization, its business partners, or other service providers.

Due to the complexity of new product lines and business processes, many projects need to collaborate with each other either intra-organization or inter-organization. The needs of enterprise integration may arise from many perspectives such as *integration of market* that enterprises adapt regional product consumptions and servicing as a response to the new free trade economic areas that are established around the world such as the European Union, the North America Free Trade, and Indonesian market. Another perspective of integration is *integration between several developments and manufacturing sites* which is the collaboration between remote enterprises is needed to produce complex products (e.g. Airbus). Hence the corporation such as exchange of technical and production data (information flow), project management (control flow) as well as distribution and logistics (material flow) are required to produce the product. Integration perspective can be also derived from *integration of multi-vender hardware and software* that systems need to integrate with various IT hardware and software solutions (Vernadat 2002).

The integration should provide the ability for an enterprise become more agile and flexible to continuously monitor market demand, quickly respond to provide new products, services and information, quickly introduce new technologies, and quickly modify business process. The technical and behavioral integration are the important factors to achieve agility and flexibility. The technical part concerns about software and hardware integrating. While the behavioral integration is the challenging part because if it is not properly managed, redistributed of roles and responsibilities among partners can impact an organization. Also the change management and transformation of an organization can be very difficult and sensitive issues (Jinyoul et al 2003). The entire project will fail if they only focus on the technical integration, but the organization is not going to internalize the enterprise system. So in order to maximize the benefits from the integration, it is required both successful technical and behavioral integration.

The figure 2 gives an overview of enterprise integration methodology. The three concentric rings represent the key management aspects of enterprise integration project which are inner, middle, and outer rings. The inner ring represents the *process* you follow to solve an EI problem, while the middle ring contains the *deliverables* you produce by following the process, lastly, the outer ring lists *risks* you must manage during the process to ensure the

project's success (Wing & Venky 2004). The six sectors overlaid the rings represent an enterprise integration project's phases.

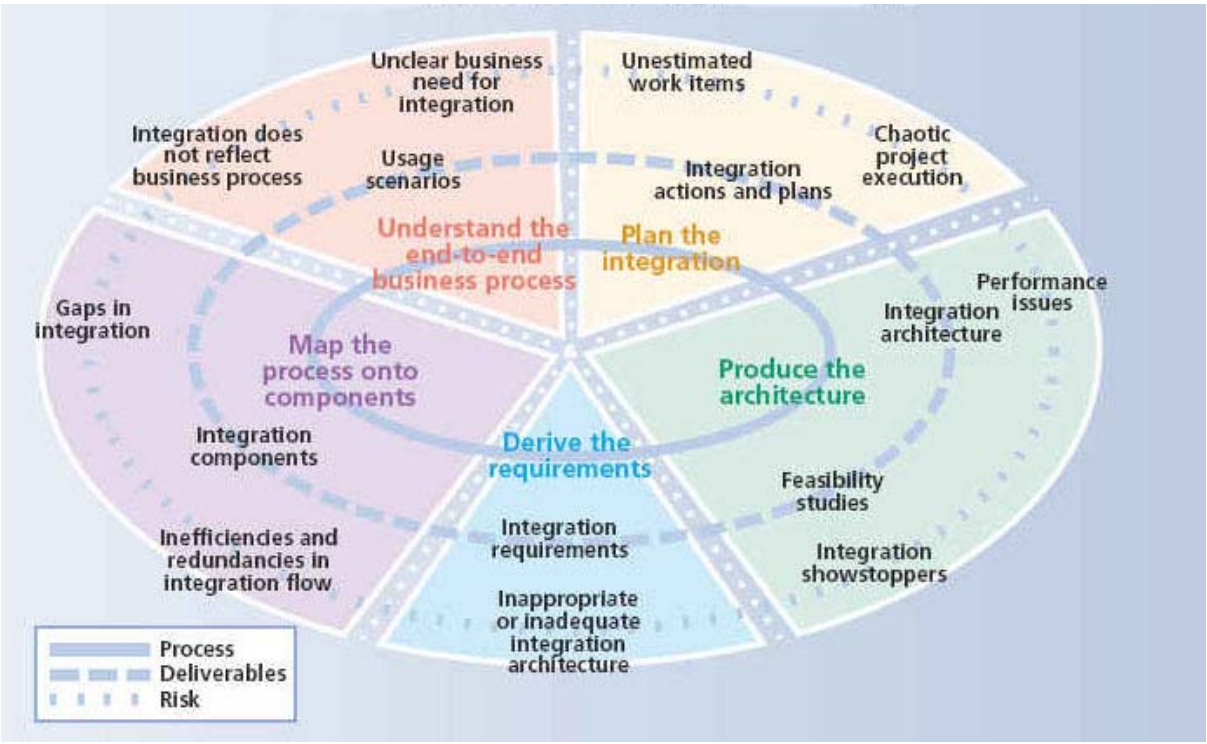

Figure 2 Overview of the enterprise integration methodology (Wing & Venky 2004, page 41)

2.2.1 Integration Compatibility

Enterprise systems are considered to be effective to handle the incompatible problems from different information systems of the departments in the same organization. Hence the needs for integrating intra-organizational information systems are established and accepted. Moreover, to handle business needs in the global markets, many organizations are now looking forward to further establishing integrated inter-organizational information systems. Enterprise Resource Planning systems were initially developed to provide internal integration (Lee et al 2003; Wang & Zhang 2005). Somehow, those organizations seeking to use Enterprise Resource Planning systems to establish integration, for example, with other supply chain stakeholders, found such integration difficult and risky (Themistocleous et al 2004). Unless those different firms were using the same Enterprise Resource Planning system, integration efforts were hampered by system incompatibilities. Recent advances by Enterprise Resource Planning vendors have addressed this need. For example, SAP now has added optional Supplier Relationship Management (SRM), and Customer Relationship Management (CRM) modules to enhance the functionality of its popular R/3 Enterprise Resource Planning system.

Even though integration systems among companies can create many benefits and advantages to business, it is not simple to achieve the best solution integration. The information system integration across organizations is a barrier to many companies. For example, in the supply chain system, business partners have their own independent systems, which in many cases cannot communicate to others. Problems also come from internal factors that not only different information is represented by different data in different sections across different business units and functions, but also duplicated in many areas, and errors are hiding everywhere (Themistocleous et al 2004; Theodoros 2002).

Application integration is a complex task because enterprise applications are composed of autonomous, heterogeneous and distributed components such as packaged, legacy, and custom applications. Those applications have been implemented for a long time to support the enterprise business process which they operate within complex, inflexible and mostly ad-hoc architecture. This will establish the difficulty to rapidly assemble and reassemble services to support new and challenging business requirements, and new internal and external business processes (Qureshi 2005). Therefore ineffectiveness technical integration of Business-to-Business systems indicates poor understanding towards integration with business processes. Moreover, failures of ineffective technical integration impact on business processes and application systems, and ultimately decrease reliability of transaction processing. These weaknesses have potential to increase risks of inter-organizational system integration (Sutton et al 2008).

2.2.2 Integration Technique

Enterprise Application Integration (EAI) technologies are also being used to create intra-enterprise and interenterprise integration (Banerjee et al 2005). Enterprise Application Integration software is typically a middleware solution which provides data and application translation and compatibility functions between heterogeneous enterprise software packages (Gabel 2002). All of the enterprise systems connect to the Enterprise Application Integration software rather than to each other in a point-to-point configuration, as seen in the figure 3.

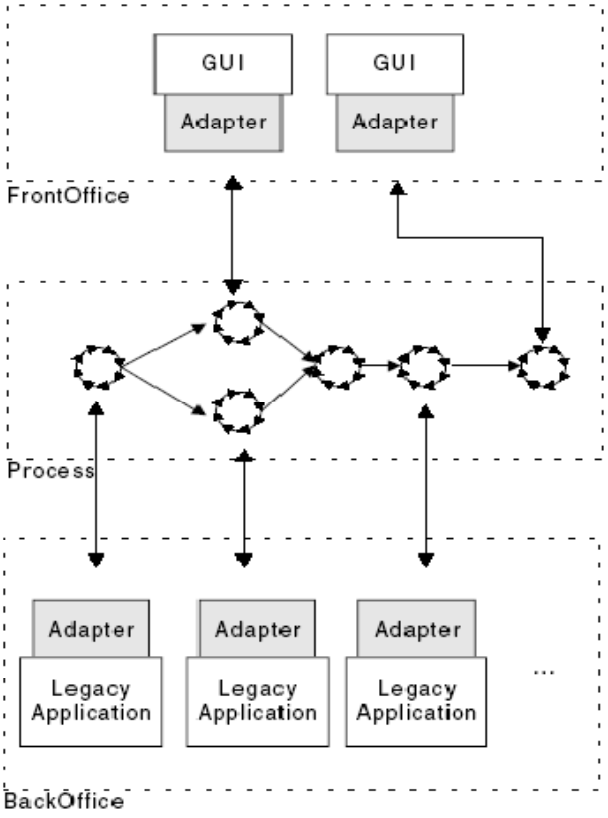

Figure 3 Integrating two disparate systems via adapters (Sutherland & Heuvel 2002, page 62)

Enterprise Resource Planning systems try to connect to other systems or inter-organization systems such as supply chain related functions. Extending systems can be done in many approaches, for example, through Web-Services reacted methodologies such as service oriented architecture (SOA) and web-development technique in general. Some international vendors like Oracle, SAP, PeopleSoft or small vendors like Exact Software Inc or Hyperion have realized the importance of these directions and revolutions (Dedrick et al 2008).

2.2.3 Type of System Integration

Many authors describe how important it is that companies have to choose between the degrees of incorporate when they integrated systems. Themistocleous & Irani (2002) have summarized the loose and tight integration application in the following table.

Loose integration	Tight integration
• Focuses on exchanging – sharing data among partners • Low degree of processes dependency • Low degree of integration • The development of a homogeneous integrated cross-enterprise infrastructure is not important • Asynchronous communication	• Focuses on integrating cross-enterprise business processes and systems • Highest degree of processes dependency • High degree of integration • The development of a homogeneous integrated cross-enterprise infrastructure is important • Synchronous communication

Table 1 Loose and tight Integration (Themistocleous & Irani 2002, page 161)

Themistocleous & Irani (2002) explain that loose integration generally refers to loose couple integration between partners. The partners have loose relationship that they will focus on the exchanging data. The degree of process dependency between two organizations is low which means that synchronous communication is not necessary. They do not need to immediately respond between systems. Hence the infrastructure issue integration is not important.

On the other hand, tight integration describes the tight relationship between partners. The process much relies on each other. For example when sending data to partner, the sender will wait for the response from the partner, this may cause of failure in the process if the receiver do not respond anything. This type of communication is called synchronous communication. The integrated cross-enterprise infrastructure is very significant part to this tight integration (Themistocleous & Irani 2002). An example is such some organizations share their production planning systems data with partners to decrease their own inventory stocks and move towards a just-in-time mode across the supply chain (Sutton et al 2006).

Themistocleous & Irani (2002) also mentioned the integration types that integrations application can be intra-organizational and inter-organizational. The list below is the integration types that associate with inter-organizational.

- Custom-to-e-business integration, Custom application and e-business sometimes collaborate to support each other. Custom application (e.g. stocks) may merge on e-business system to make the processes of an e-business automatic and integrate inter-organizational business. Similarly, e-business also supports custom application for an e-store updates that concerns with inventory in the stock.

- Packaged-to-e-business integration, the package application as enterprise resource planning systems, for example processes that deal with e-sales, e-procurement and e-supply chain management are integrated with packaged systems. The organization can use enterprise application integration (EAI) and e-commerce technology for integrating package application and e-business.
- E-business-to-E-business integration, the e-business application which has different process or task is integrated and supports each other. They can be integrated by message-based technology (e.g. XML) or distributed object technologies (e.g. CORBA), and database-oriented technologies (Java database connectivity, JDBC)
- Custom-to-packaged to-e-business integration, this approach focuses on integrating infrastructure which will integrate process and application together, such as department application level, enterprise or cross-enterprise level. So it is required integration technologies to support all integration levels. Therefore, technologies that facilitate the data, object, and interface and message level are required.

2.3 Extended-Enterprise System

Many of medium to large size organizations are quickly realizing that integrating electronic systems within and between physical locations is, more and more, a fundamental element of running their business. On the other hand, real-time communications and integration with both customers and vendors is also changing from competitive advantage to essential business requirement. In most of the cases, information technology is the main driver for the fundamental collaboration and integration changes taking place in industry. Up until now, much of the business transformation driven by Information Technology is led by companies in the United States; however, this trend of information integration across extended enterprise systems will soon be adopted by many organizations, regardless of their location and independent of the geographic addresses of business partners, plants, sales offices, customers, and/or vendors as shown in the figure 4 (Westone 2003). Physical boundaries will have less future business relevance except for issues of governance, taxes, and security. Information Technology is rapidly forcing enterprise systems beyond simply enabling change to become the drivers of business change.

Extended enterprises merge project and opportunity-based businesses that must react rapidly for changes in the market or the available technology. Partners should have collaboration and general agreement on a project framework, and one enterprise must lead the network which

usually is the most powerful ones. The partner who is the leader in the project should provide specific resources for operating the extended enterprise (Furst et al 2002). It is possible that any of the partners can be involved in multiple extended enterprises, such as two enterprises might be in the same time that cooperates in one business segment and compete in another.

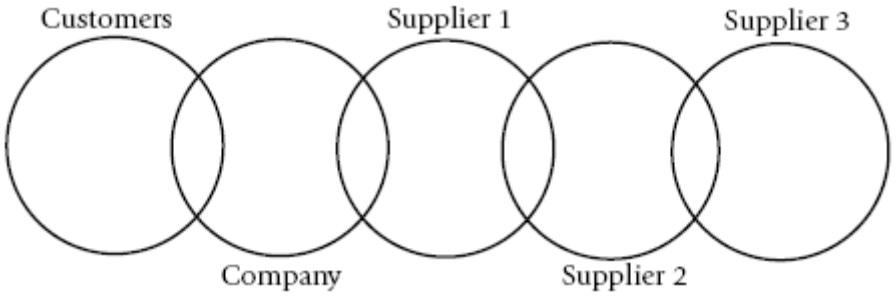

Figure 4 Integrated extended enterprise supply chain (Westone 2003, page 50)

The most important factors for extended enterprise business process are both security and flexibility of the system, especially in distributed environment that data is exchanged over the network. There are numerous issues about security concerns with extended enterprise such as authorization and authentication in order to establish trust, a necessary element in Business-to-Business transactions. Flexibility means that system should enable business network to react quickly to opportunities, the network infrastructure must be sufficient, and the mechanisms should be easy-to-access for incorporating new partners if needed (Furst et al 2002). Moreover when supporting the automated business process, each enterprise must have access to all the internet application components it requires.

The extended system integration needs to support the adaptability, flexibility and responsiveness. Adaptability means ability to change or reconfigure system to support the business process as it changes over time. It implies that business users should be empowered to reconfigure specific business processes when needed rather than IT personnels. The flexibility is the ability to integrate with new partners, branches, plants and their business processes. Responsiveness refers to the ability to respond the customer's needs, for instance when a customer asks for an order change, or a supplier signals a delivery problem. In sum, adaptability, flexibility, and responsiveness are adding power to the extended system by supporting the needs of the business process as it changes, internally and externally (Westone 2003).

2.3.1 Important Factors of System Integration

There are various risks that have potential to arise, such as losing or missing data, or the system processing failure. These risks come from the inconsistency of computer-based systems, for example, a system infrastructure is not properly planned by system architects and developers will lead to unsatisfied reliability of the Business-to-Business technologies (Dean et al 2003). However, factors that make the integration system failed are not only the technical issue, but also the business and management concerns. As Sutton et al (2006) stated that the integration of IT systems with business processes may have a direct impact on other members of the supply chain. Moreover, assurance over risks is related not only to technical and application issues, but also business integration, which are critical to consider.

Imed (2000) states that the criteria of the effective functioning of extended enterprise are as the following factors:

- Autonomy of partners - which supposes that each one is free to manifest and to take initiatives
- Added value - there is no exchange unless each partner finds it beneficial; the value added by each one must be appreciated precisely.
- Adapting to change - in so far as it privileges the functional links between its members, the network must facilitate their adaptation to change.
- Mutual aid - mutual aid between the members is fundamental.
- Reciprocity - is an essential rule that the network can only function if each partner receives and gives.
- Shared values - networks presuppose strong adhesion of each member to a system of values, network quality being a function of the quality of the values quality uniting its members.
- Common vision - poses many questions, for example, how members plan the future of the network, what the future collective goals are, etc.

There are some issues that should be examined for the larges-scale extended enterprise system implementation. Westone (2003) mentioned that these following issues have potential to cause failures of proceeding with an extended enterprise planning and execution of the system.

- Enterprises must provide training about system and management, such as training about cooperation with partners or deal with major customer, to potential users.

- The user acceptance testing (UAT) must be conducted to find errors, bugs and incomplete units, in integrating systems.
- Project scope, size, and plan for implementation module should be identified and agreed.
- There should be effective communication between people which involve in a project including project manager, sponsors, steering committees, and major stakeholders, with regular project updates.
- Unrealistic plan for milestones, deliverables or deadlines will lead to failures in scheduling which also makes it difficult to cooperate between partners.
- Misunderstanding of the data requirement for the system will lead to the wrong data or development.
- Adhesion to the old legacy system might be an obstacle for long term planning.
- The extended system should not only emphasis on technical goal, but also the business goal such as value added, revenue, cost and customer.

2.3.2 Extended Business Patterns

The extended enterprise business pattern in the e-business aspect is also known as business-to-business pattern. The extended business pattern illustrates the business process collaboration among enterprises. The information technology such as application integration enables connection between enterprise systems. The table 2 below describes about extended enterprise business pattern by cross-industry (Martin et al 2006).

Services	*Examples*
Buy Side	Direct Procurement Indirect Procurement Supply chain execution
Sell Side	B2B e-commerce (Distributors)
Trading Partner Modernization	Electronic data interchange (EDI) modernization

Table 2 Cross-industry examples of the Extended Enterprise pattern (Martin et al 2006, page 64)

Apart from the pattern by cross-industry, there are examples of extended enterprise system pattern by industries specific. Manufacturing industry is such supply chain planning, supply chain execution, and vendor-managed inventory. Travel industry is such checking flight or room availability, making or modifying reservations. Retail industry is such checking supplier inventory, placing replenishment orders, paying suppliers automatically. Financial industry is such transferring payments, checking account balances, obtaining credit

information. Finally telecommunication industry is such cross-organization order management managing service provider interconnections (Martin et al 2006).

2.3.3 Extended System Planning

The extended enterprise structures can be described as extended value chain. Enterprises join in the value chain to increase their business capability by receiving the value from the network such as suppliers and customers. Furthermore, enterprises can join in multi-extended value chain, but this might lead to more complexity in interacting with new partners in the value chain. To achieve business missions, enterprises must manage the complexity and changes which are inherited from multiple e-business applications. Each partner has its own stakeholders and shareholders that have their own specific goals. It is possible to have competitiveness in the chain which however, the partners should agree on the objectives and goals of the group. In some cases, there might be issues of intellectual property between partners, so the rules should be considered to ensure that each enterprise cannot display its expertise without compliance to these rules (IT Governance Institute 2005). The enterprise should keep in mind that the business environment is always changing and there is no legal cooperation solution for extended enterprise other than contract-based agreement for trading transaction.

Extended enterprise can be established only within a coherent business space. All partners must agree on the data criteria, a single ontology to describe data semantic, such as concepts (entities, attributes, processes, and so on), their definitions, and interrelationships. The extended system also needs collaborative business process and services among partners, as well as strong information security and efficient security mechanism. In the long term, extended enterprise should also support non-technical goals, such as building a common business culture, which help provide quick responses to unpredictable circumstances in the network (Furst et al 2002).

3 ENTERPRISE RISK MANAGEMENT

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Risk management is a framework to classify risks, assessing risks, and mitigate risks to a tolerable impact. This research is studied to guide effective risk assessment containing both the fundamental background and the practical guidance necessary for assessing risks identified, and planning to handle it, within extended enterprise systems for business partnerships. The aim is to help organizations to better manage IT-related mission risks (Stoneburner et al 2002).

Chapman and Ward (1997) have given the definition of risks as all projects involve risks in the way that the risk-free project is not worth investing. Organizations that better understand the risks and know how to handle them more effectively can not only avoid unexpected outcomes but also work with evenly-balanced margins and less contingency. This way will free up resources for other strategy, and seizing opportunities for better investment which might otherwise be rejected as too risky. Somehow, risks are distinguished from uncertainty as Bussey (1978) and Merrett and Sykes (1983) mentioned that outcomes from a risk can be expected with its probability, which is different from uncertainty in the way that the probability of each outcome can not be expected.

In business context these days, most of the decisions are made based on a financial consequence basis. Managements or decision makers need to understand and know whether the returns on a project rationalize taking risks and the extent of these repercussion or losses if the risks do occur. However, investors need some hint of whether the returns on an investment will meet up their minimum or tolerated point if the investment is fully exposed to the risks identified. So Merna (2002) suggests that risks should be assessed and provide the risk information to those investors of the project in order that they can have more understandings toward the investment. Therefore identifying risks and measuring them in relation to the returns of a project is important. By knowing the full coverage of their benefits and/or losses, business leaders and investors can then decide whether to endorse or cancel an investment or project (Al-Thani et al 2005).

Risk management for enterprise is important that it provides useful information for management levels. It is how to handle uncertainty and how risky the management should make a decision with fewest impacts on the business. Uncertainty can be either risk or

opportunity for the business, but opportunity can be maximized when strategy and goals are set by balancing growth, return of investment and risks. Enterprise risk management composes of aligning risk appetite and strategy, enhancing risk response decisions, reducing operational surprises and losses, identifying and managing multiple and cross-enterprise risks, seizing opportunities, and improving deployment of capital. These characteristics of enterprise risk management help management to achieve the enterprise performance and profitability targets and prevent loss of resources. They also ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the enterprise reputation and following consequences. In sum, enterprise risk management helps an enterprise obtain its goals easier and reduce mistakes or surprises along the way (COSO 2006).

Risk management can be perceived as the process that allows IT managers to balance the operational and economic costs of protective measures and achieve goals in each project by protecting the IT systems and data that support their organizations' missions. This process is actually not only for the IT environment, but also helps manage decision-making in many areas of our daily lives (Stoneburner et al 2002).

Management of risks is not only for the management levels, but also all levels of an enterprise need to be included in order for it to be effective. These levels are generally defined as corporate level (policy setting), strategic business level (business process) and project level. Risk management needs to take into consideration the communication of these levels and follow the processes that permit these levels to correspond and learn from each other. The aim of risk management is therefore including identifying risks, undertaking an objective analysis of risks specific to the organization, and responding to the risks in an appropriate and effective manner. These stages include being able to assess the prevailing environment, both internal and external, and to assess how any changes to that prevailing environment would impact on a project in hand or on a range of projects (Al-Thani et al 2005).

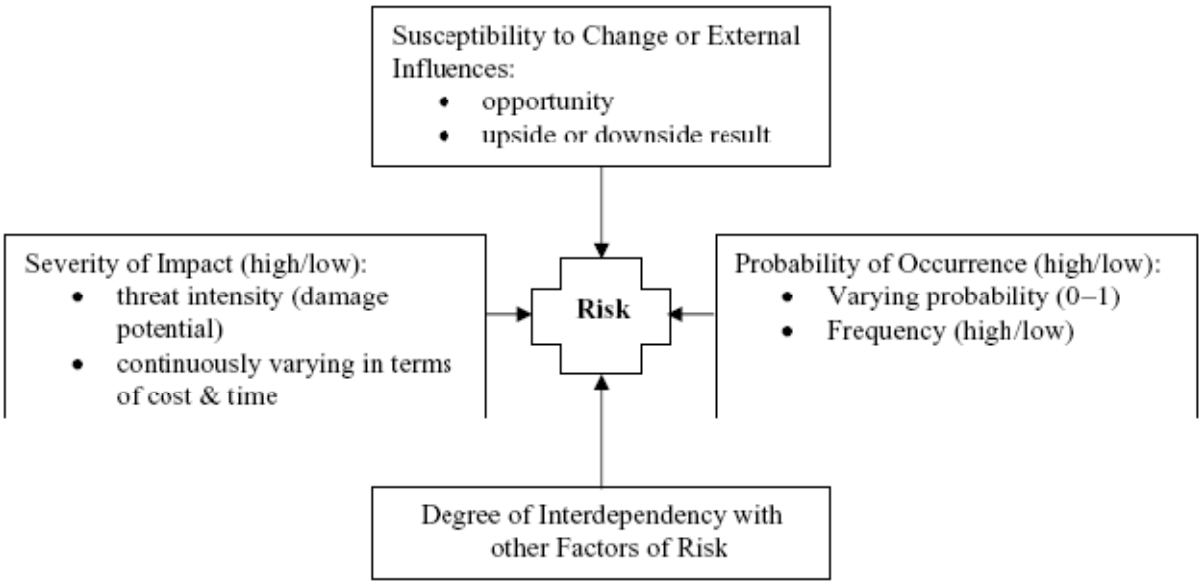

Figure 5 Typical risk parameter (Al-Thani et al 2005, page 10)

The model in the figure 5 shows that risk is generally composed of four essential parameters: probability of occurrence, severity of impact, susceptibility to change and degree of interdependency with other factors of risks (Allen 1995). If there is at least one of these four parameters, the situation or event can justly be considered risk. This model can be used to describe risk situations or events in the modeling of any investments for risk analysis.

3.1 Risk Management Models

In common, the process of risk management basically involves identification of risks or uncertainties, analysis of implications, response to minimize or mitigate risk, and allocation of appropriate contingencies. Risk management is rather a continuous loop than straight process. It makes an investment or project progresses, cycle of identification, analysis, control and reporting of risks is continuously undertaken (Smith 1995).

There are many effective risk management models that can be adopted, depend on suitability of each company or type of the implementing project. But still it is no big difference between them that there should be four major areas composing of assess risks and determine needs, implement policies and controls, promote awareness, and monitor and evaluate, which all the procedures should be managed by the responsible unit or team (U.S. GAO 1999). The model is illustrated in the figure 6.

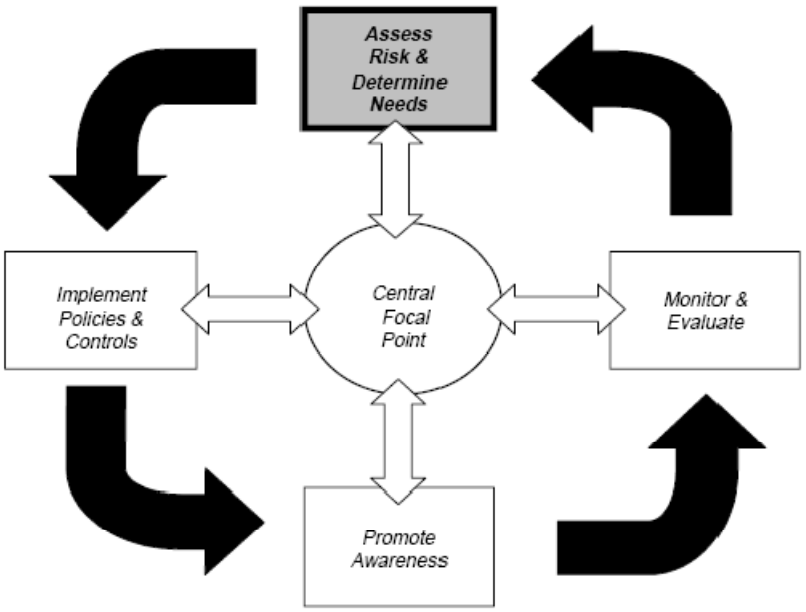

Figure 6 Risk Management Cycle (U.S. GAO 1999, page 6)

Not only the U.S. General Accounting Office that complies to the general risk management model, but also a famous consulting firm like Deloitte that practically adopt the model to work on the area of supply chain risk management. The major processes of their supply chain risk management are identify risk, determining the risk management strategy and actions, executing and implementing actions, and monitoring the risk management process and the results, as shown in the following figure (Deloitte 2008).

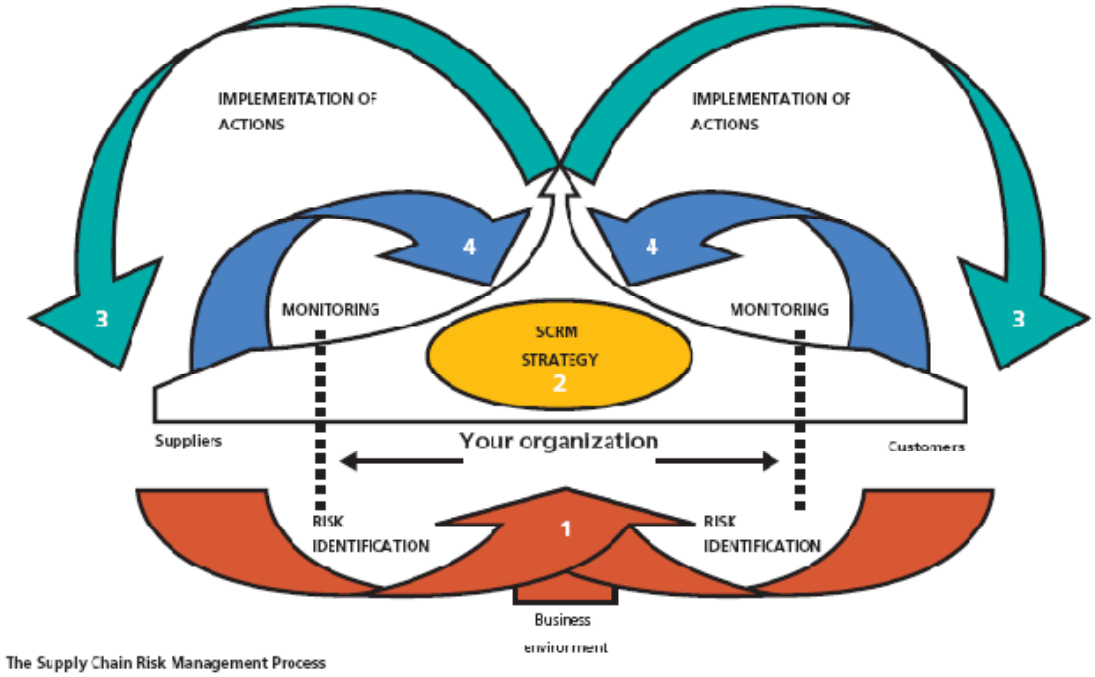

Figure 7 Supply Chain Risk Management Process (Deloitte 2008, page 4)

3.2 Risk Management in SDLC

In any system integration projects that adopt framework of system development life cycle (SDLC), risk management can be used efficiently and differently for each phase. It can be summarized as the following table:

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for system integration is expressed and the purpose and scope of the integration is documented	Identified risks are used to support the development of the integration requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The integration is designed, purchased, programmed, developed, or otherwise constructed	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development
Phase 3—Implementation	The security features of the integrated system should be configured, enabled, tested, and verified	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4—Operation or Maintenance	The integrated system performs its functions. Typically the systems are being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to the integrated system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

Table 3 Integration of Risk Management into the SDLC (Stoneburner et al 2002, page 5)

3.3 Risk Assessment

Risk assessments can be used as a means of providing decision-makers with information needed to understand factors that can harmfully impact operations and products, and giving concerns about the degree of actions needed to reduce risk. As the consequences of the growing technology, information security risks can be no longer overlooked by the government or business. Not considering any specific types of risk, the risk assessments generally include *identifying threats*, *estimating the possibility*, *estimating the potential losses or damage*, *and identifying cost-effective actions.* Documentation is recommended to those action plans (U.S. GAO 1999).

Risk assessment is one of the crucial components of the risk management. It provides the basis for many parts in the risk management circle. To be specific, it can be used to establish suitable policies and choose cost-effective techniques to implement them. Risks can be changed gradually so it is important that enterprises should occasionally assess risks and, if needed, adjust the strategy on policies and control to best handle the related risks (U.S. GAO 1999; Stoneburner et al 2002). A suggested methodology flowchart that can be used as a guideline along the risk assessment process is shown in the figure 8 (page 25).

The model of the risk assessment is various. The scope of the risk assessment determines the extent of analysis and resources. The quality of the risk assessment depends on the availability of data. The assessment process requires data of the risk likelihood, cost of the detriment, and cost of mitigating risk to determine the monetary cost of risk in the quantitative approach. But in many cases that no availability of the data such as risk likelihood and the impact losses cost, the qualitative approach will be applied for the risk assessment by identifying risk in more subjective and general term such as low, medium, and high. It is also possible to combine the two approaches to semi-quantitative approach in some cases (U.S. GAO 1999).

Cooper (2005) explains the descriptions of assessment approaches in the step of assigning priority to the risk as following:

- Qualitative analysis is based on descriptive scales such as low, medium, high for describing the likelihoods and impact of risk. This is approach useful when the enterprise wants to do quick assessment reviewed or initial review.
- Quantitative analysis uses numerical ratio scales for likelihoods and impact, rather than description scales.

- Semi-quantitative analysis is the combination between quantitative approach and qualitative approach. The number will be assigned for descriptive scale.

Stoneburner (2002) has illustrated a sample of risk assessment methodology for IT systems as the following steps. He has given the definition of the output from the 5th and 6th steps of the risk assessment methodology flowchart in the figure 8 (page 25) in the table 4 and 5 accordingly. Note that these definitions should be localized to best fit the business background or specifics when needed.

Likelihood Level	*Likelihood Definition*
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Table 4 Likelihood rating definition from the fifth step (Stoneburner et al 2002, page 21)

Impact Magnitude	*Impact Definition*
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Table 5 Impact rating definition from the sixth step (Stoneburner et al 2002, page 23)

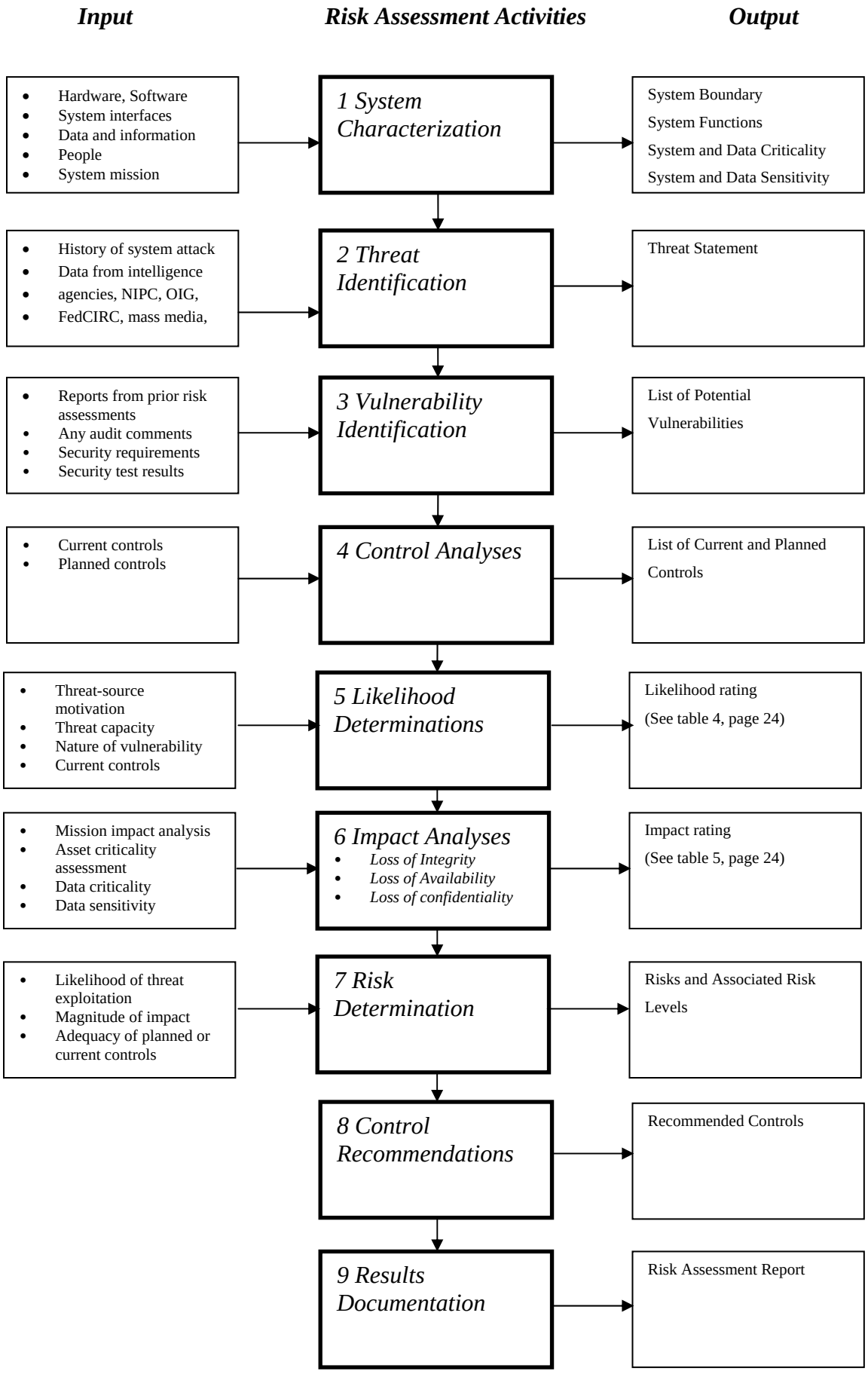

Figure 8 Risk Assessment Methodology Flowcharts (Stoneburner 2002, page 9)

System Characterization involves defining the boundary of IT system which encompass with information and resources. The characteristics of the IT system are the scope of risk assessment boundary. This is to ensure that participants have a common understanding of the system being assessed (Stoneburner et al 2002; ITSC 2001).

Threat is the inheritance from any particular threat-sources exercising a particular vulnerability. Vulnerability is a weakness that can be accidentally or intentionally exploited. A threat-source cannot create the risk when there is no vulnerability to attack (Stoneburner et al 2002). A threat is any agent such as person, activity or event that has potential to damage a system such as type of data processes, stored, and transmitted (ITSC 2001).

Vulnerability is a weakness in the information system design, implementation, internal controls, security control that could be exploited by threat which accidentally triggers or intentionally exploited (Stoneburner et al 2002). The vulnerability is the potential weakness in the system that may be attacked or exploited by threats. The vulnerability in the systems may be found in system design, physical layout, administrators, procedure, personnel, management, hardware, or software (ITSC 2001).

Control analysis procedure will identify and analyze control mechanism or the security policies that are currently implemented in the system or planed to implement which will protect the system from the threat that might exercise the vulnerability (Stoneburner et al 2002). This includes management controls, technical, physical, and operational security measures that are implemented to promote the security and integrity. The control analysis will apply with the likelihood of the potential risk. The effective safeguard can eliminate or reduce the level of harm from threats (ITSC 2001).

Risk Determination step will assign risk priority to each risk by comparing the likelihood level and impact level. To assign the risk level, the important things to consider are the likelihood and the impact scale. The scale depends on nature of the project, objective, criteria and anticipating risks. If we have three dimension of likelihood and impact then the matrix is a 3 x 3 matrix of threat likelihood (high, medium, and low) and threat impact (high, medium, and low). However, the size of the matrix depends on site's requirements and the specifics of risk assessment desired, some sites may need a 4 x 4 or a 5 x 5 matrix. After assigning the risk level, then we can determine necessary action to each risk (Stoneburner et al 2002; Cooper 2005).

The risk assessment matrix below is an example of Probability–Impact (P–I) tables which are used to assess the relative significance of risks. The probability of incidence and the potential impact of a risk are determined, for example, by selecting from a range of low/medium/high. The numerical meaning of each scale point should be predetermined for the project and investment (Allen 1995).

		Probability				
		V. Low 0.1	Low 0.3	Medium 0.5	High 0.7	V. High 0.9
Impact	V. Low 0.05	0.005	0.015	0.025	0.035	0.045
	Low 0.1	0.01	0.03	0.05	0.07	0.09
	Medium 0.2	0.02	0.06	0.10	0.14	0.18
	High 0.2	0.04	0.12	0.20	0.28	0.36
	V. High 0.8	0.08	0.24	0.40	0.56	0.72

Figure 9 Probability–impact tables (Al-Thani et al 2005, page 62)

Control Recommendation process will recommend control process to eliminate or mitigate the identified risk, as appropriate to the organization's operations. The recommend process will be the input for next process, mitigation of risk (Stoneburner et al 2002). It should be noted that not all the recommended controls can be implemented.

3.4 Key Role Persons

Technology is one of the important aspects that management levels need to understand, especially if they want to have effective management plans because IT impacts all aspects of the company. Risk management departments can function in misunderstood roles, leaving IT planned from an enterprise perspective and understood how the IT operation and its exposure bind with the business and shareholder value. In fact, the IT security plan, on the other hand, should be written by the chief information officer and the IT security team (Geisel 2007).

When the time of system implementation comes, normally companies are concerned mostly on their corporate governance practices, or what so called enterprise-centric, with only slight concerns in risks embedded in the IT-interconnected system. By the role of the chief executive officer (CEO) to take care of the internal controls which highly concerns on both criminal and civil actions for inadequate corporate governance practices, the IT-based systems are considered to be the next major area of focus and review in later phase. The

rising of extended system has been to re-shape the roles of management such as chief executive officers who have become much more focused on corporate governance and who have largely been directive that makes internal audit staffs focus almost all the reviews on internal control (Sutton et al 2006).

The chief executives assess the organization's enterprise risk management capabilities. In one approach, the chief executive brings together business unit heads and key functional staff to discuss an initial assessment of enterprise risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation (COSO 2006).

Chief information officers (CIOs) that have experienced a considerable change in their primary role and responsibilities as chief executive officers and board of directors mandate that chief information officers invest amount of effort by their IT staffs to integrate, enhance and document internal controls for IT-based systems. The chief information officers are responsible for the agency's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program (Sutton et al 2006; Stoneburner et al 2002).

3.5 Extended-Enterprise Risk Management

Risk management in extended enterprise systems composes of using risk sharing, control and prevention and financial instruments to lessen the effects of the integrated operational chain risks and their financial consequences. For example, operational risks concerning the direct and indirect unfavorable consequences of outcomes and events arising from operations and services that were not accounted for, that were unexpected from the weak and rough planning. These occur from many reasons, both stimulate internally and externally. For the internal case, consequences are the result of failures in operations and services sustained by the parties individually or communally because either from an exchange between the parties or some joint (external) risks that the firms are facing. The other case is that it is the consequence of unexpected events the supply chain was not ready for or is unable to manage (Tapiero & Kogan 2008).

3.5.1 Extended-Enterprise Case Studies

There are some examples of why risk management is important and should be included in the system planning and development. The samples also encourage the management to influence their employers to give attention to risk management.

In May 2002, Ford Motor Company revealed that someone posing as one of their employees "collected the work and home addresses, social security numbers, account numbers and credit histories of 13,000 people from one of their credit bureaus" (Vijayan, 2002). The imposter was a worker on the help desk for the software provider that served as the outsourcer for Ford's credit checking process for customer approvals. The imposter used user codes and passwords taken over the system to order credit histories. Ford's credit branch was billed for the credit reports and the imposter sold the reports to an identity theft ring leading to the then largest case of identity theft ever – totaling over US$10 million (Ghahremani, 2003). Ford turned to be a victim to the fraudulent act while having no real control over the processes that were circumvented.

Another example is on the supply chain failures and the impact that it can have on organizations. The failures are frequent in the literature with two of the more publicized being Nike Inc.'s May, 2001 crisis when reported sales for the prior quarter had to be reduced by $100 million because of confusion in its supply chain and the even larger hit taken by Cisco Systems Inc. when $2.2 billion was written off for unusable inventory resulting from problems in the supply chain. The impact on the financial statements is only part of the story, however, when one also considers Nike's stock dropped 20 percent in value after its announcement. Indeed, studies show that a drop of 7.5 percent upon announcement of supply chain interruptions is average and a drop of 18.5 percent is typical over the 12-month period following the announcement (Taylor, 2003).

3.5.2 Extended-Enterprise Risks

The integration between partners along the supply chain is a complex and difficult task. Because there is complexity of the exiting systems on both sides of partners which are complicated systems, in many cases they are fixed, reconfigured, or lacking of documents. Moreover, the incompatibility problem and integration problem among systems of those parties such as different standards, computing languages, or platform and operation systems also make it more difficult for integrating task (Themistocleous et al 2004). All the risks in extended enterprise system are relevant to each other. The risks that derive from the technical factors, has essential impact to other risks (Sutton et al 2008).

The following are examples of the risks that might arise from technical concerns:

- Losing or missing data, on the transfer data process or transmission can be errors such as sending to a wrong party or failures in sending. In some cases, senders require

acknowledgement from receivers before sending more information which sometimes waiting for events or messages that will never happen. This kind of event will make the data lost or queued somewhere, never happen, or might lead to process that will never terminate (Gleghorn 2005; Dean at al 2006).

- Accountability and security means that all data transmission should be logged or archived to enable availability for auditing. The system requires an appropriate level of security provisioning. Typical Business-to-Business integration needs data encryption while transferring process (Gleghorn 2005). To protecting data from modification in an improper way is very important because if unauthorized changes are made to data or system accidentally or intentionally, it may lead to inaccuracy, fraud, or erroneous decision (Stoneburner et al 2002). Also systems should be able to validate the received data whether it is complete, to ensure the validity of information and minimize errors (Gleghorn 2005).
- Business-to-Business projects concern with at lease two parties that they have to agree on the same details of implementation, such as file formats and encryption procedures to each field of data type. It generally takes longer to implement, maintain, and secure the system than internal integration projects. Sometimes partners might lack of technical capabilities that will lead to design change and potential project delays (Gleghorn 2005).

Inter-networking technology has become an effective tool to connect with business partners together. It brings significant benefits to the organization, but while integrating extranet partners can substantially enhance E-commerce, it also carries significant risk. Basically, organizations will need to expose to the hiring practices, values, code of conduct, and administrative practices of its partner that most probably be very different from those of theirs. It is assumable that managements understand this risk but need help articulating it, so they can secure the finding necessary to decrease that risk to a manageable level (Weiler 2001).

3.5.3 Risk Management in Extended-Enterprise Perspective

According to the World Economic Forum, the fast-rising supply chain risks are poorly understood and managed by most companies. Even the importance of supply chain risk is emphasized at company and government levels, the vulnerabilities to the chain are still not properly handled. Companies should understand, review, and measure supply chain risk (Adrian 2008).

The increasing global market also drives enterprise business models to be interconnected. However, there have been few studies on how this phenomenon impacts the enterprise risk management processes, and also the need to shift from an enterprise-centric view of risk management to an extended-enterprise risk management view. Moreover, in term of organizational systems control and risk assessment in the area of inter-organizational relationship, it should be further studied to handle risk complication and raise the awareness in IT planning and implementation, especially in management levels that they tend to overlook the importance of risk management as a business strategy. Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring (COSO 2006). Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation of the risk management plan.

Previously, in the traditional enterprise centric model the focus is on the enterprise, its information systems and Business-to-Business connections. An extended-enterprise risk management framework follow the assumption that risk must be managed across the entire supply chain. In the figure 10 (page 32) illustrates that, Company B reflecting the enterprise of concern, Company A being an upstream supplier, and Company C being a downstream customer. The circled area focuses on the extended-enterprise model of risk management and assurance (Sutton et al 2006).

Risk management in the context of extended enterprise system is capable of reducing the risks from external factors or controllable events such as human errors, mishaps of operating machines and procedures or due to the inherent conflicts that can occur when organization and persons in the integrated system may work at cross purpose. In such conditions, risk can be motivated, based on staff and company intentionality. It will help lessen information asymmetry, leading unpleasant selection and moral hazard that can lead to an opportunistic action by one of the parties which have particular implications for the management of the integrated system. Moreover, it may prevent a lack of information or the inefficient management of information and its exchange in the integrated system, such as forecasting the demands and needs in supply chain. Last but not least, it may express a perception, where a risk attitude may present risk to events that need not be risky or vice versa. Risk attitude is

then imbedded in a subjective perception of events that may be real or not (Tapiero & Kogan 2008).

Elliott (2001) recommends that those enterprises can achieve assurance over their own IT systems mainly through using existing Trust Services, for example, using SysTrust to assess the reliability of the IT systems together with security and information processing, and using an adapted form of WebTrust to assess the security and reliability of e-commerce linkages. (*Trust Services* are defined as a set of professional assurance and advisory services based on a common framework to address the risks and opportunities of IT. Trust Services principles and criteria are issued in 2006 by the Assurance Services Executive Committee of the American Institute of Certified Public Accountants or AICPA.) He further raises the issue that an enterprise may want assurance over the security and reliability of trading partners' systems with which the enterprise is connected. His vision is that this can be accomplished by extrapolating the Trust Services model to the systems of these connected enterprises (Elliott 2001).

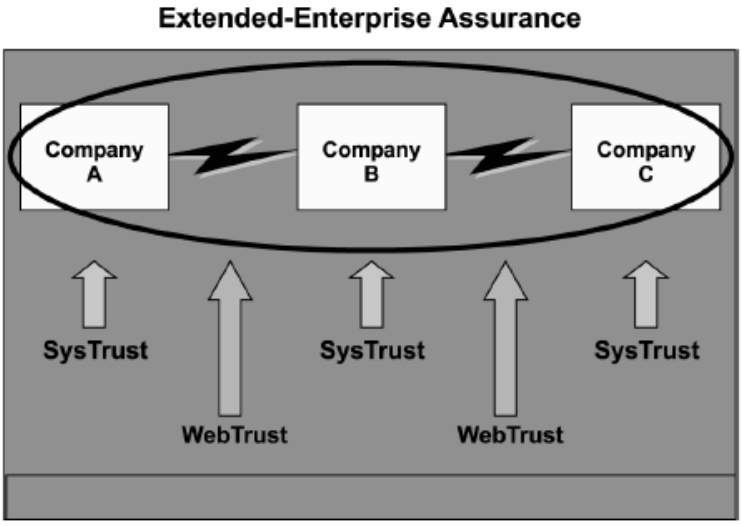

Figure 10 Extended-enterprise risk assessment model (Sutton et al 2006, page 108)

In an enterprise systems driven environment, the enterprise system influences the business processes and the business processes depend greatly on the specifications of the system. This integration is both an essential condition for effective and efficient business processes and a fundamental constraint to current IT governance and audit/assurance models. An organization can have highly reliable information processing, but poor integrating with the supported business processes which results in poor effectiveness within these processes than it should be (Sutton et al 2006).

4 RESEARCH METHODOLOGY

Data collection and analysis were conducted following the framework from Creswell (2007) in order to achieve quality of the research. Ethics were always considered as an important factor along the research, in order to avoid any ethical issues that might arise. The study was developed from reviewing related literatures from reliable and accessible sources, such as ELIN that provides thousands of e-journals and hundreds of databases. For the interview, as a data collection method, we had really good opportunities to interview leading organizations in Thailand, so we decided to carry out the investigation in Thailand. Interviews were selective to be arranged with those leading organizations in Thailand with good management reputation to ensure the reliability and validity of the research.

4.1 Literature Review

The study was started from literature review that summarizes and synthesizes sources within each paragraph as well as throughout the review. The literature review provides the foundation and framework for the research, and allows the investigator to be brought up to date regarding the state of the research in the field, and familiarizes with any contrasting perspectives and viewpoints on the topic. The research areas that are looked for are related to risk management, risk assessment in the e-commerce, Business-to-Business, e-business, system integration and supply chain. According to Oates (2005), data collection can be conducted from many sources of data such as books, journals, conference and workshop proceeding, reports, newspapers, magazine, resource catalogues and online database, and internet literature reviews. There are seven activities that we generally used to conduct literature reviews which are searching, obtaining, assessing, reading, critical evaluating, and writing a critical review. This information was used with the data we obtained from the interviews to analyze our study in the next phase.

4.2 Data Collection

According to Yin (2003), multiple sources of evidence methodology involves in the internal validity because the method provides data from many sources to analyze and discuss the research questions. Thus multiple sources of evidence were used along the data collection process of this research to ensure the validity. Document, archival records, open-ended interviews, focus interview, structured interviews and surveys, and observation (direct and participant) were considered to be the choices of investigation. Due to the limited timeframe and research location, some of the sources of evidence, such as observation or surveys, were

not suitable in the study. While not all the sources were ready, each possible source was intensively investigated to make sure that we had enough information to analyze, to be able to answer the research question reasonably.

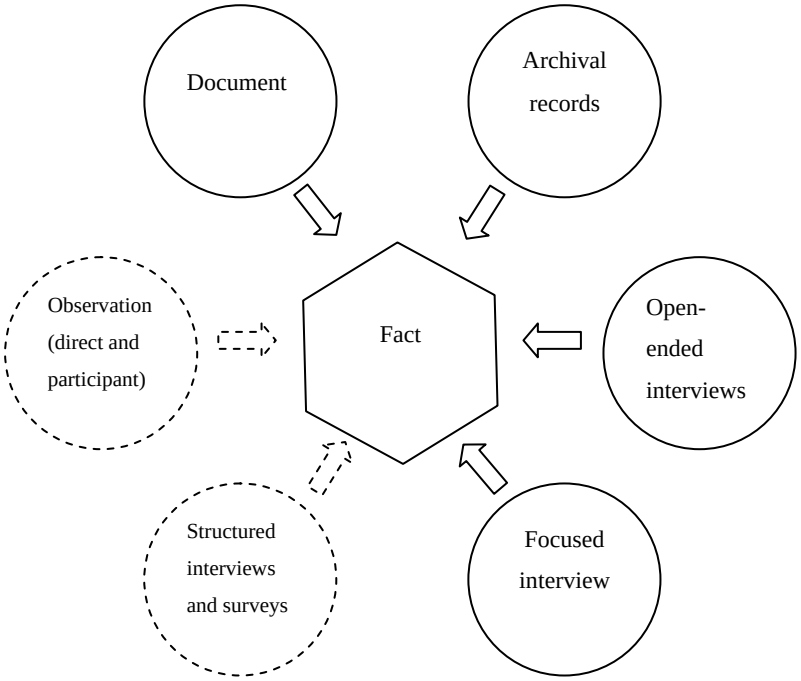

Figure 11 Multiple sources of evidence (Yin 2003, page 100)

4.3 Interviews

In order to investigate the study, interviews were used to gain information from people who have experience or knowledge about the system integrating implementation. The semi-structure interview is the interview type that we selected for this study. Themes to cover and questions to ask were prepared beforehand, but could be changed to best match the flow of conversations. The questions were open-end that will help explore the interviewees' experiences. The questions and interview guide will provide a direction of the interview conversation to focus on the system integration and risk management. In the same time we could get more additional data or issues from interviewee beyond our interview questions. As Oates (2005) describes about the semi-interview structure that additional questions might be asked when new issues or interesting topics were unexpectedly raised by the interviewees. Semi-structured interview framework was used along the interviewing research phase to capture various types of information we might get.

Companies in Thailand were contacted via e-mails to introduce our research and get contacted with the person whom we can interview. Feedbacks were given positively from many companies that they could provide their valuable time with the study. Names and

contact information were provided to conduct interviews with those recommended persons, which are responsible for the area of study we were interested in. E-mails were sent to those responsible persons to introduce more specifically about the study and what kind of information were needed. List of questions was sent to them before the actual interviews, to give them some time to think about the answers, and also to wait for the most convenient time of them to arrange the interview. Phone calls were a suitable and adequately effective way to conduct the interview with them. We conducted seven interviews from chosen persons who have experiences in system integration either inter-organizational or intra-organizational. The interviewees are from the different companies and also different positions which gave the various perspectives of the system integration and risk management. During the interview, we recorded the interview by the recorder and also note scripting. Each interview started from briefing the research background and area of studying. Interviews were followed with capturing the experience of the interviewees about implementing the system integration and/or related systems. Problems from each situation and several of solutions were captured and further investigated or analyzed to develop framework for the risk assessment in extended-enterprise system.

4.4 Data Analysis

Themes to conduct the research were identified for the data collection process. The needed theme was related to risk management and its role in the system integration and planning. According to Oates (2005), we grouped obtained data by their relevant to the research, data were sometimes not related to the current research such as technical details of the implementation project. Somehow these data help provide understandings to the specific situations or problems. Another group of data provides general descriptive information that was needed to describe the research context for the readers. Analysis took place differently in the following phase of implementation to find inter-connection between categories; which are *before integration phase, to-integration phase, integrating phase, and after integration phase,* which will be intensively discussed in the empirical findings chapter.

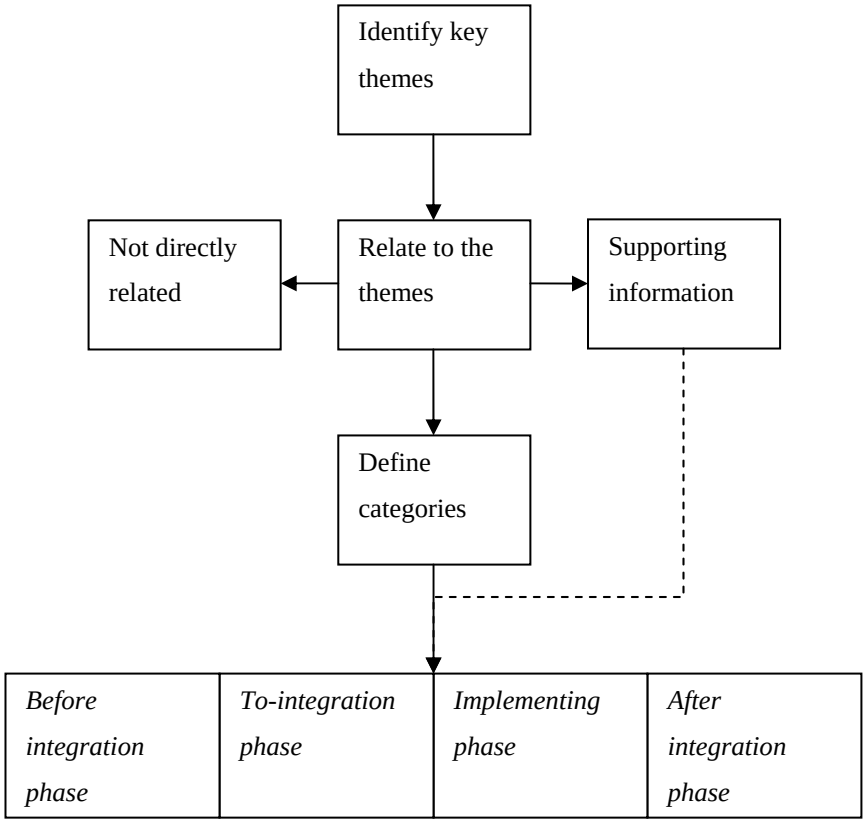

Figure 12 Data analysis methodology (adopted from Oates 2005)

4.5 Ethics and Research

There are two type of information from the interviews of this study. The first one is the general information of that knowledge domain that can be disclosed for academic purpose in the research. The other one is rather sensitive information that is private and was offered voluntarily to the research in confidence. Israel and Hay (2006) mentioned that the sensitive information might bring the bad consequences to the participants and also lead to difficulties to conduct research for the researcher. It is because the research framework was developed on the knowledge domain of risk management, so it was unavoidable to discuss with interviewees about problems that happened during the implementation phase, which most of the time referred to business partners or third parties. When discussing with those problems, it is noticeable or expectable from the context of the interview that whom or what companies are being mentioned. Some issues relate to trust between two enterprises which are considered sensitive issues that cannot let business partners know, especially in the context of Thai culture that some people might tend to care about what other people say. Also some names of the interviewed companies cannot be published in this thesis due to the details of the interview may affect the reputation of the company being criticized.

According to Oates (2005), participants in the research have the right that their identity and location will be protected. It was done by disguising where necessary such as using pseudonyms or changing gender during the writing-up. By doing so, it will prevent readers from guessing who said what; to make sure that there will be no harmful or embarrassing repercussion for them.

Apart from anonymity, confidentiality is also considered important in the context of ethics. Sometimes participants provided information in confidence that is required in order to explain the situation properly. Somehow, they did not want that information to be written in the research report. Similarly, an organization might allow researchers to carry out some data collection, but that findings should be kept confidential, so that its competitors cannot gain from the findings (Israel &Hay 2006). It is to be concluded that we, as a researchers, should respect participants' expectations of anonymity and confidentiality, and try not to coerce people into participating in the research by neither persuasive abilities nor connections from some position of power, and obtain informed consent and not deceive people about the research unless there is really no alternatives and no harm will follow (Creswell 2007; Oates 2005).

5 EMPIRICAL FINDINGS

Information gathered from all the data collection process can be categorized into several areas upon the implementation phases. Factors that can cause risks in each implementation phase was analyzed and summarized to be major risk areas. These areas can be used to help assess risks for enterprise system integration. All the risk areas and supporting information from the interviews will be illustrated in this part.

Literature reviews have paved the way for collecting data such as designing the interview questions, helping to identify risk areas, and so on. Interview results are categorized into the following areas to help analyze the framework; *before integration phase, to-integration phase, implementing phase, and after integration phase,* which each area will be explicitly explained in the following section.

5.1 Participant Presentation

Participant 1 - the interviewee is an IT director for a large scale construction company. His job is to plan and manage the IT strategy for the organization. He has been responsible for integration projects which his current project is to integrate a project management system for construction (Primavera) to the Enterprise Resource Planning System (SAP). (See 9.2.1)

Participant 2 - the interviewee is a senior unit manager/business analyst working in the department of electronic channel and sales and service network operation support, in the banking industry. One of her responsible project is to integrate a banknote inventory system with a money delivery company, for automatic teller machines. (See 9.2.2)

Participant 3 - the interviewee is an IT manager working in the franchise & restaurant industry. Her past experience is to implement an inventory management system that connects to branches in the coverage area. The project was carried out using logistic outsourcing. (See 9.2.3)

Participant 4 - the interviewee is an assistant manager/business process analyst working in the department of process development (internal consultant). She is responsible for a project that integrates customer information system with back-end and front-end system. (See 9.2.4)

Participant 5 - the interviewee is an assistant president for the department of consumer credit product operation for a large scale bank. Her past experience was to integrate Cardlink system for VISA product to the banking system. The system was implemented by outsourcing. (See 9.2.5)

Participant 6 - the interviewee is an IT manager in an IT company. His past experience was to implement the Electronic Data Interchange (EDI) by outsourcing in which the system was integrated with business partners. (See 9.2.6)

Participant 7 - the interviewee is a System Analyst for the application maintenance service department in a big IT company. His experience relates to system integration and testing. (See 9.2.7)

5.2 Interviews

5.2.1 Before Integration Phase

In this phase, skills of the integration team should be identified because organizations cannot, or normally do not, develop expertise or specific team for this area, especially in the area of integrating technology. In most of the cases, details of the integration, including legacy systems, adapters, implementing costs, will be studied thoroughly to choose the best alternatives for the integration project. (See 9.2.2, 9.2.4, 9.2.5)

Scope of the integration should be clearly identified. It is generally true that the more you pay, the better you get. However, when you select a suitable technology for the company, such as integrating method or adapter, you need to balance between efficiency and competitive advantage and incurring cost. The best alternative cannot come without considering all these three factors in the same time. (See 9.2.1, 9.2.3)

It is to be considered the long term maintenance of the system integration, especially when the system integration is implemented by the outsourcers. It is becoming more popular in Thailand that enterprises do not develop a specific team, like IT integration, that is not related to the core business. They tend to outsource a reliable company to do it for them. So sometimes it is a problem for an organization that has used a legacy system for 20 years and has a problem maintaining it. Thus it is important to set up fall-back procedures in such cases so that outsourcing is out-of-service. (See 9.2.4, 9.2.5)

It is normal for every organization to try and maximize their benefits, yet in terms of partner integration, we should bear in mind win-win solutions, in which agreement is best for both companies. This mutual benefit will dramatically minimize the conflict of interests for partner collaborations. (See 9.2.1, 9.2.2, 9.2.3)

5.2.2 To-Integration Phase

The to-integration phase is a term that enterprises use for the working procedure in the later phase of preparation to begin its implementation. In this phase, there should be a detailed plan for the information security. Data will be divided into two major parts. One is shared by the enterprise and the integrating company, while the other is data that contains confidentiality of the organization. Data that is private must be organized and stored differently than information of the shared ones. This will maximize the confidential level. Another major concern for implementing a system is the technical data protection. If data that are being shared are corrupted, it will impact all the parties involved. Thus an agreement among companies to use reliable and suitable data protection techniques must be made. (See 9.2.1, 9.2.2, 9.2.3)

5.2.3 Implementing Phase

While implementing the integration project, there are many problems with the scope and responsibility. Rarely does one specific team handle the responsibility for this type of projects. It is possible that responsible units do not really put the best effort for the outcomes, and sometimes even leave problems to be managed by their business partners. When a potential risk arises from the integration process, both parties should try to reduce and eliminate the risk altogether. They should also collaborate a counter plan to manage other risks that may occur in the future. (See 9.2.1, 9.2.3, 9.2.4, 9.2.6)

In terms of implementation that outsource by third parties, vendors who are not specialized in the core enterprise, the implementing technology may be chosen based on their expertise and preferences. Thus they do not rely on the technology trend which may help the operational process, and support the extendibility of the enterprise system. Each business will have a unique function or requirement, such as banking operations. Many managers have similar opinions towards the outsourcers that they should have business background related to their technical expertise, which will help them understand the right business process. This will eventually reduce the time it takes to gather required information for most of the implementation cases. Those managers also mentioned that they think the outsourcers can finally implement the project, but the problem is that enterprises cannot wait for too long if it will affect many departments which rely on that system. (See 9.2.2, 9.2.4, 9.2.5)

Trust and respect can always be an important issue while integrating the system with business partners. Low level of trust or respect may lead to unsuccessful integration, or incomplete

integrating functions. Tasks that need high level of security must be carefully planned through out the implementation. Lack of skills and experience of the implementers or outsourcers tend to erode the level of trust and reduce the scope of work. The reduced scope of integration will damage the benefits of the partner integration. (See 9.2.2, 9.2.3)

5.2.4 After Integration Phase

A thorough system testing is required after implementation phase before real deploying of the system. In large scale enterprises with tight system integration, there should be adequate testing on the *site acceptance test* (SAT) and *user acceptance test* (UAT) to prevent system errors or bugs after deployment. These tests will help to reduce risks that arise after deployment. The testing process should be collaborated between partners. (See 9.2.7)

After the integration, both the integrated companies may need access to disclosed information at some point; even they separate the confidential information from the shared data. It is necessary for both companies to sign an agreement not to share or disclose this information to any other party. This agreement should be applied to all the staff who work with this information, especially in the case of outsourcing. (See 9.2.2, 9.2.5)

Long term planning should be revised after the integration has been done, to make sure that it complies with the details of the implemented system. Documentation must be developed thoroughly, in order to maintain the system. Many companies that used complicated systems have problems maintaining and extending the system because they lack of people who can correctly and effectively perform those tasks. To hire specialists to handle this problem is costly and cannot be considered a sustainable solution. (See 9.2.1, 9.2.4, 9.2.5)

Data must be properly secured in a standard that agreed by both parties. Data backup must be performed regularly, which is normally recommended to use a hot swappable storage. A back up site can be implemented if needed, varied from cold sites to hot sites depending on the severity of the acceptable system downtime. (See 9.2.1, 9.2.5)

Outsourcing may lead a company to the dependency of the outsourced company. For example, when there is an error or bug in the process, the company has to depend on the outsourced company to handle the problem if they do not have a specific resource to take care of the problem. Moreover, when an application is developed by the outsourced company, it will be difficult to check for errors in the program because they might not allow the company to see the source code of the program. Therefore, if possible, in the case of outsourcing the

knowledge should be transferred from the outsourcing company after the implementation phase, to reduce dependency of the vendors. The knowledge should be transferred as much as possible, so the enterprise can handle the system by themselves and respond to problems quickly, or even monitor and audit the system to minimize problems. (See 9.2.6, 9.2.7)

6 DISCUSSION

In this section, the theoretical framework is related to the empirical data. In order to answer the research questions, we considered enterprise information system and its integration in the chapter 2, together with the enterprise risk management in the chapter 3, with the focus on risks inherited from partners as discussed in the section 3.5.1-3.5.2. We also extended the risk boundaries to cover business partners as suggested in the section 3.5.3. We analyzed the theoretical framework with the gathered data from empirical findings in the chapter 5 and found that there are six major areas of risk assessment that will be fundamental for the production of this study. The areas to discuss are shared goals and arbitrators, skill and experience, system compatibility, short term planning, trust and respect, and long term planning which are comprehensively illustrated in this chapter. These is also the foundation for the conclusions made in the next section. Moreover, for the second question, we adopted the risk assessment framework from the section 3.3 with the understandings towards enterprise risk management in the chapter 3 to make an assessment over the above-mentioned major areas of risks inherited from the partner integration.

6.1 Major areas for risk assessment

6.1.1 Shared Goals & Arbitrators

Results from the interviews show the similarities to the theoretical framework in the section 2.3.1 and 2.3.3 that each partner in the network has its own mission, own stakeholders with their own goals to achieve. So it is possible that the conflict might occur and also the competition in the values chain can happen. So the objective, goal and contract agreement for the extended system should be agreed to each partner. System integration between partners must add value or benefit to each partners, and all partners must share values that occur in the network. Moreover, they should share the vision about the future goals. These factors should be considered before implementing the system that it will maximize the value of the extended enterprise systems.

It is ideal for any collaboration projects to have both parties starting with goals that shared for both organizations. This minimizes the risks of conflicting interests that lead to failure of the integration. In order to do this, integration projects will need a great support from key role persons mentioned in the section 3.4. The role of key role persons is also relevant to the empirical findings in the section 5.2.1 indicating that both parties should always have shared

goals and look for a win-win solution when there is a problem. Moreover, it is recommended by many managers as the empirical findings in the section 5.2.3 shows that there should be a team that is responsible directly to the integration of a system, to avoid the risks of unhandled tasks and provide helpful support to projects. For example, a team of project coordinators can be founded to facilitate the project management. They involve in the development and administration of the project plan, and perform the project support. One way project coordinators help projects run smoothly is if the partner company has issues concerning about the project, they can contact the project coordinator for the initial information and support.

6.1.2 Skill & Experience

As discussed in the section 5.2.1, skills and expertise of the implementer impact directly to the implementing time of a project. In most of the cases, implementers can close the projects, but not in the allocated time. Problems will arise when projects are delayed which may turn to big risks for a large scale enterprise when products or service cannot launch in time, which also mentioned in the theoretical framework 3.5.2. Skills encompass implementation as well as skills in businesses that help provide understandings to the implementing system. The empirical data in the section 5.2.3 also shows that normally implementing will focus on technical functions, rather than the business function of the enterprise. This will lead to risks in the operational process that users cannot perform as well as they should, because of the technical constraints. This problem is also indicated in the theory section 2.3.1 that the important goals are not only technical goals, but also the business goals such as value added, revenue, cost and customers. This can be prevented by providing the business background to the implementation team, so that they have enough information to choose the most suitable technology for the users.

6.1.3 System Compatibility

The risks from incompatibility in integration are indicated in the section 3.5.2 as well as the findings in the section 5.2.1 and 5.2.3 that IT infrastructure of the two (or more) integrating parties should be clearly studied to make a thorough integration plan. Moreover extended enterprise system should support the business process to achieve the organization mission. It should provide the visibility and flexibility as shown by the figure 1 (page 7). Because flexibility enables enterprise to response rapidly with the business needs changing. And the visibility enables the sharing needed information between organizations or between units inside the enterprise. The table 1 (page 12) also shows degree of integration type needed to be considered before implementing the system. The degree of integration provides the guideline

in general about integration system characteristic. If we design the wrong systems, the inter-organizational system integration will fail in the term of supporting the business process requirement. Changes in the infrastructure might suitably integrate with the other system. Risks in unexpected cost, implementation complication, or long term maintenance can be one of the important factors to determine the solution or choice of technology to the implementation.

As discussed in the section 2.2.2 that integration of enterprise information systems between organization can be done in many approaches depending on the context of the business and application architecture, such as Enterprise Application Integration (EAI), Service Oriented Architecture (SOA), or middle ware solution. However, regardless of its size and context, an adapter's primary objective is to facilitate integration of the application for which it has been designed. Interview results in the section 5.2.1 also support that choosing the right adapter technology will effectively decrease the common problems of the system incompatibility.

Empirical findings in the section 5.2.4 also mentioned testing process that it is required before production deployment in order to find error, bugs or problem from the integration system. Theory section 2.3.1 mentioned the similar perspective that testing can be used on the risk assessment process. It can provide the IT system viewpoint of a threat sources and identify potential failures in the IT system protection, especially in the large extended enterprise system or the tight integration that has confidential data, it will require intensive testing to eliminate or reduce problems that might occur after system deployment.

6.1.4 Short Term Planning

Managers indicated similar opinions in the interview result section 5.2.1 that in the early stages of the project, scope of work must be discussed as detailed as possible in order to have a clear plan of what is to be done by the company and what is to be done by the other. Timelines must be possible for the implementers so it is to be agreed by all the related parties. Ideal timelines normally set by the organization always cause problems for the implementers or outsourcers. It is mentioned comparably in the section 2.3.1 that project scope, size, and plan for the implementation, realistic milestones, deliverables, and deadline should be identified and agreed.

A responsible team for integrating projects should engage at the very beginning stage to ensure there are fewest numbers of problems from both partiers and also be responsible for unassigned tasks. Resource analysis and budgets should be properly allocated by the key role

persons discussed in the section 3.4. It is to be correctly estimated the needs for the manpower of the project. Underestimating the resource required by the project will be risky for the deadline and cause delays for many related parties.

Data must be prepared to secure the confidential information of the organization as discussed in the section 5.2.2 as well as the theory 3.5.2 that mentioned the data modification prevention in the transferring process, file formats, and encryption procedures.

6.1.5 Trust & Respect

In the implementing phase, as discussed in the section 5.2.3, trust in business partners will provide more business opportunities and competitive advantage. However, without trust, it may affect the scope of work and level of involvement. Similarly, over trusted partners without proper assessment could be a risky implementation as well. Thus trust in terms of risk assessment can be looked in a way to properly assess the business partners in terms of background, knowledge, experience, resources, their capability and determination, and so on. There are case studies around the world, such as the Ford's credit checking process which is the largest case of identity theft ever which mentioned in the section 3.5.1, or outsourcing of banks from the interview result section 5.2.4 that customer information must not be disclosed.

Interview results further mentioned that respect of both integrated organizations play a vital role in implementation and integration. Interview results are showing that respect can reduce conflicts of the two different parties. Not paying respect to the partner may cause a loss in cooperation. It also means losses in support, suggestion, and expertise from the partner.

6.1.6 Long Term Planning

Interview results in the section 5.2.4 shows that integration is considered to be a long term project, unless there is a really big change to the business. Long term projects normally face problems in maintaining itself effectively with time as also discussed in the theoretical framework in the section 3.5.2. Risks in maintenance can be reduced by thorough documentation of the system and process which needs support from the key role persons to realize the importance of this specialized knowledge, and use more than one staff to retain a particular knowledge, to prevent knowledge loss from staff rotation.

The theoretical framework 3.5.2 discussed the data accountability and security that data should be carefully structured so that it can be used during long period. The empirical findings section 5.2.2 and 5.2.4 also regards security of the system as the most important

factors for extended enterprise business process, especially in distributed environment that data is exchanged over the network. Moreover, the theory section 2.3 mentioned the flexibility as an important issue because in the long term, because business processes always change as a result of the business environment changing over time. For example an enterprise must be able to add new system from new partners, so that the enterprise cannot depend on only a partner or supplier. Interviews further mentioned that data classification must be planned ahead of the integration. Data is to be classified into confidential and shared data, which will need different actions and plans for each. Data backup solution should be selected according to the business needs. Data back up can be varied from *cold sites to hot sites* depending on the severity of the acceptable system downtime (Records Management Services 2004).

The empirical findings section 5.2.4 and the factors of integration in the section 2.3.1 further mentioned the importance of outsourcing and knowledge transferring that it should be considered to be an important factor for the long term planning, especially a large scale of integration. Training is needed for extended enterprise system especially the large scale system. Trainings should be provided to potential users and should cover about the system and management over the value chain, such as how to cooperate with partners. The high dependency with the partner process and system might lead to inheriting risks from partners. If the partner system has errors or problems, the enterprise will be affected by the business process that is relying on the partner. For example, an enterprise shares data with their partners but the process to manage those data depends on the partner's side. When there is an error or change of that data but the enterprise do not properly obtain it, the enterprise may serve customers with wrong information which will impact the customer satisfactory.

6.2 Risk Assessment Method

From the six major areas of risks for system integration in the section 6.1, each area of risk should be assessed to see the area of the overall risks for the integration project. The Probability–Impact (P–I) table mentioned in the section 3.3 can be adopted as the level of risk is the *probability multiplies by impact level*, where the probability rating definition and impact rating definition is also given in the table 4 and 5 (page 24) of the section 3.3 accordingly.

According to Stoneburner (2002) and Cooper (2005), as discussed in the section 3.3, the important things to consider when assign the risk level are the likelihood and the impact scale. The scale depends on nature of the project, objective, criteria and anticipating risks. If we have three dimension of likelihood and impact then the matrix is a 3 x 3 matrix of threat likelihood (high, medium, and low) and threat impact (high, medium, and low). However, the size of the matrix depends on site's requirements and the specifics of risk assessment desired, some sites may need a 4 x 4 or a 5 x 5 matrix. After assigning the risk level, then we can determine necessary actions to each risk.

Suppose that a project manager assesses the integration risks by using the Probability–Impact (P–I) table in the figure 9 (page 27) for the area of shared goals and arbitrators as a medium impact (0.2) with medium probability (0.5), the risk level is the impact level multiplies by probability, which is 0.1. The project manager also thinks that the impact level and probability for the areas of skill and experience, short term planning, and trust and respect are the same, so that the project manager assesses the risk levels for those areas as 0.1 as well. Somehow, this project manager concerns about the high level of impact (0.8) with high probability (0.9) in the area of system compatibility and long term planning, so he assesses the risk level as 0.72 using the same (P-I) table in the page 27. An example of assessment can be illustrated in a spider chart in the figure 13.

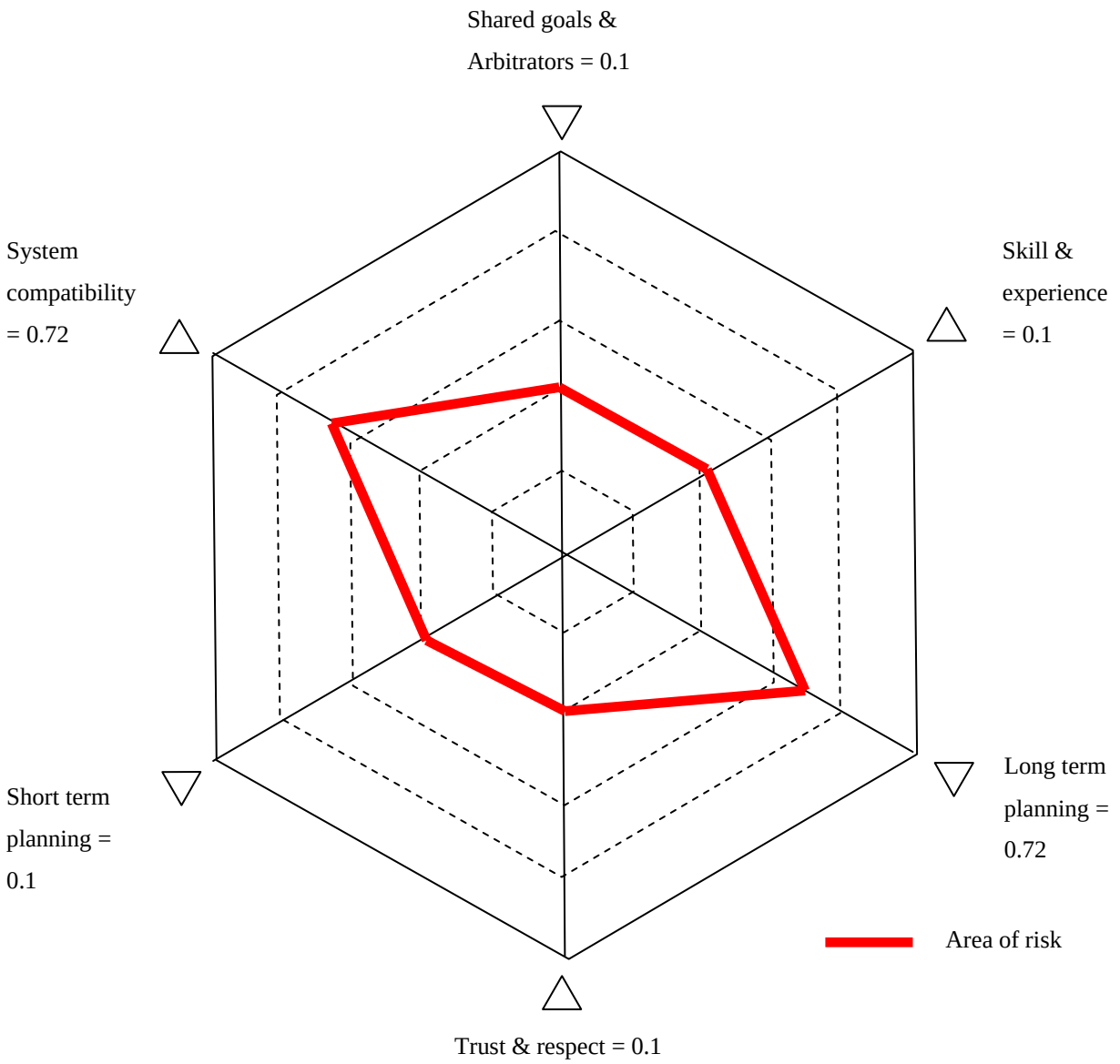

Figure 13 A Sample of Risk Assessment (authors' own creation)

The sample shows the risk sensitive areas of system compatibility and long-term planning of the system integration. This can be used as a *risk determination* output for the risk assessment methodology in the figure 8 (page 25).

7 CONCLUSION

In this chapter, we summarized our production of researching to the research questions and also discuss about future research areas.

7.1 What are major risk areas inherited from inter-organizational system integration, in the context of enterprise risk management?

This study was carried out to find the major areas of risks from system integration. The theoretical framework provides us with the perspective to analyze the empirical findings from the interviews in the data collection process. The various opinions from interviewees from the empirical findings together with the theory study are categorized and summarized to provide the major areas of risks from system integration as identified by the first research question. Those areas are shared goals and arbitrators, skill and experience, system compatibility, short term planning, trust and respect, and long term planning, as illustrated in the following section.

7.1.1 Shared Goals & Arbitrators

Objectives, goals and contract agreement for the extended system should be agreed to each partner. System integration between partners must add value or benefit to each partners, and all partners must share values that occur in the network. In order to do this, integration projects will need a great support from key role persons in the organization. Moreover, it is recommended that there should be a team that is responsible directly to the integration of a system to facilitate the project management.

7.1.2 Skill & Experience

Skills and expertise of the implementer impact directly to the implementing time of a project. Skills encompass implementation as well as skills in businesses that help provide understandings to the implementing system. The important goals are not only technical goals, but also the business goals such as value added, revenue, cost and customers.

7.1.3 System Compatibility

IT infrastructure of the integrating parties should be clearly studied to make a thorough integration plan. It should provide flexibility and visibility because flexibility enables enterprise to response rapidly with the business needs changing, and visibility enables the sharing needed information between organizations or between units inside the enterprise. The degree of integration provides the guideline in general about integration system characteristic.

Choosing the right adapter technology will effectively decrease the common problems of the system incompatibility. Testing process is also required before production deployment in order to find error, bugs or problem from the integration system.

7.1.4 Short Term Planning

Project scope, size, and plan for the implementation, realistic milestones, deliverables, and deadline should be identified and agreed. A responsible team for integrating projects should engage at the very beginning stage to ensure there are fewest numbers of problems from both partiers and also be responsible for unassigned tasks. Resource analysis and budgets should be properly allocated by the key role persons. Data must be prepared to secure the confidential information of the organization

7.1.5 Trust & Respect

Trust in terms or risk assessment can be looked in a way to properly assess the business partners in terms of background, knowledge, experience, resources, their capability and determination, and so on. Respect of both integrated organizations play a vital role in implementation and integration that it can reduce conflicts from the different parties. Not paying respect to the partner may cause a loss in cooperation. It also means losses in support, suggestion, and expertise from the partner.

7.1.6 Long Term Planning

Data should be carefully structured so that it can be used during long period. Data security is important as it is exchanged over the network. Data classification must be planned to be used properly by involved parties, and data backup solution should be selected according to the business needs. Data structure should be flexible because business processes always change as a result of the business environment changing over time.

Risks in maintenance can be reduced by thorough documentation of the system and process which needs support from the key role persons to realize the importance of this specialized knowledge, and use more than one staff to retain a particular knowledge, to prevent knowledge loss from staff rotation. Knowledge transferring should be considered as an important factor for the long term planning, especially a large scale of integration, to avoid high dependency with the partner process and system which may lead to inheriting risks from partners. Training is needed for extended enterprise system especially the large scale system that it should be provided to potential users and cover about the system and management over the value chain.

7.2 How to assess those risks from system integration?

These major risk areas are used with the risk assessment theory in order to properly assess the risks inherited from enterprise system integration following the second research question. The assessing areas of risk can be used with the probability-impact estimation that suits the type of enterprise. The threat likelihood and impact level should be evaluated following the definition given in the theory chapter of enterprise risk management, but it is to be customized based on the business specifics if needed. The important things to consider are the likelihood and the impact scale. The scale depends on nature of the project, objective, criteria and anticipating risks.

After the risks can be assessed, we will have the risk determination as we assigned risk priority to each risk by comparing the likelihood level and impact level. The risk determination will be used along the control process to eliminate or mitigate the identified risks. However, risk response may depend on each enterprise. Key role persons should consider the strength and weaknesses of the organization comparing with the area of risk. Each organization has different background and purpose, so it makes different resistance to risks. For example, company with little resource and capability to manage complications in IT system should not carry high risk of system compatibility. Large size enterprise with enormous numbers of staff should not take high risk from long term planning, such as weak plan for maintaining a big and complicated system. Companies with feeble business background, such as newly established ones, should look for business partners or outsourcers with strong and reliable background of skills and experience.

7.3 Future research

In the process of risk management, risk mitigation is the next important step in the risk management cycle. It composes of prioritizing, evaluating, and implementing the suitable risk controls which are guided from the risk assessment process. Because the removal of all risk is usually unfeasible or close to impossible, it is the responsibility of senior management and functional and business managers to use the cost-performance strategy, and implement the most appropriate controls to decrease integration risk to an acceptable level, with minimal undesirable impact on the organization’s resources and mission.

This research in the area of risk assessment can be used as fundamentals for the future research in the area of risk mitigation. As the system integration is becoming a vital part for

gaining competitive advantage to survive in the market. The effective risk mitigation strategy should be studied to complete the cycle of risk management process.

8 REFERENCES

Adrian, L., 2008. *Supply-chain risks misunderstood, mismanaged*. Report. Business Insurance, 42 (2), p. 23.

Al Thani, Faisal, F. & Merna, T., 2005. *Corporate risk management: An organizational perspective,* Subject: Economics Planning and surveying Provider. 1st ed. John Wiley.

American Institute of Certified Public Accountants. 2006. *Trust Services Principles and Criteria - an Overview* [Online]. Available at http://infotech.aicpa.org/Resources/System+Security+and+Reliability/System+Reliability/Trust+Services/Trust+Services+Principles—An+Overview.htm [accessed 25 April 2008]

Banerjee, N., Chordia, A. & Rajib, P., 2005. *Seamless Enterprise Computing Using Enterprise Application Integration (EAI).* Journal of Services Research, **5**(1), p. 171-196.

Bussey, L.E. , 1978. *The Economic Analysis of Industrial Projects*. Englewood Cliffs, NJ.

Chapman, C.B. & Ward, S.C., 1997. *Project Risk Management: Processes, Techniques and Insights.* Chichester: John Wiley & Sons.

Cooper, D., Grey, S., Raymond, G. & Walker, P., 2005. *Project Risk management guideline: Managing risk in the large projects and complex procurements*. Hoboken, NJ: J. Wiley

COSO (The Committee of Sponsoring Organizations of the Treadway Commission). 2006. *Enterprise Risk Management – Integrated Framework* [Online]. Available at http://www.coso.org/Publications/ERM/ [accessed 5 Mar 2008]

Creswell, J. W., 2007. *Qualitative inquiry and research design: choosing among five traditions*. 2nd ed., Calif.: Sage Publications.

Davenport, T.H., 1998. *Putting the Enterprise into the Enterprise System*. Harvard Business Review, 76(4), p. 121-131.

Dean K., Alan F., Paul G., Julian J. & Doug P., 2003. *Just What Could Possibly Go Wrong In B2B Integration?*. Computer Software and Applications Conference, 2003, COMPSAC 2003, Proceedings, 27th Annual International, p. 544-549.

Dedrick J., Xu S., & Zhu K., 2008, *Information Technology and the Number of Suppliers in a Supply Chain: Is There a Relationship?*. Journal of Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), p. 390-390.

Deloitte. 2008. *Enterprise Risk Services: Supply Chain Risk Management* [Online]. Available at http://www.deloitte.com/dtt/cda/doc/content/nl_eng_brochure_supply_chain_risk_management_070704x(1).pdf [accessed 8 May 2008]

Elliott, R., 2001. *21st century assurance*. AAA Auditing Section Mid-Year Meeting, Atlanta, GA.

Evgeniou, T., 2002. *Information integration and information strategies for adaptive enterprises*. European Management Journal, 20 (5), p. 486-494.

Farahmand, F., Navathe, S., Sharp, G. & Enslow, P., 2005. *A Management Perspective on Risk of Security Threats to Information Systems*. Information Technology and Management ,6 (2-3), p. 203-225.

Furst K., Schmidt, T., & Wippel, G., 2002. *Managing Access in Extended Enterprise Networks*. IEEE Internet Computing, 6(5), p. 67-74.

Gable, J., 2002. *Enterprise Application Integration*. Information Management Journal, 36(2),p. 48-50.

Geisel, R.W., 2007. *Enterprise risk manager needs technology grounding*. Business Insurance. Chicago, 41(21), pg. 24.

Geishecker, L., 1999. *ERP vs Best-of-Breed.* Strategic Finance, 80(9), p. 62-67.

Ghahremani, T., 2003. *Gremlin in the works*, CFO Magazine.

Gleghorn, R., 2005. *Enterprise Application Integration: A Manager's Perspective*. IT Professional Magazine, 7, p. 17.

Harikumar, A.K., Lee, R., Hae Sool, Y. , Haeng-Kon, K., & Byeongdo, K., 2005. *A Model for Application Integration using Web Services*, IEEE Computer Society. Journal of Computer and Information Science, Fourth Annual ACIS International Conference on, p. 468-475.

Hyvonen, T., 2003. *Management Accounting and Information Systems: ERP versus BoB.* European Accounting Review, 12(1). p.155-173.

Imed, B., Manuel, Z. & Nada, M., 2000. *Intercompany Cooperative Information Systems for Knowledge Management*, Citeseer. [Online] Available at: http://eric.univ-llyon2.fr/~pkdd2000/Download/WS5_05.pdf

Israel, M. & Hay, I., 2006. *Research ethics for social scientists: between ethical conduct and regulatory compliance*. London; Thousand Oaks, CA.: Sage.

IT Governance Institute (2005), *Governance of the Extended Enterprise: Bridging Business and IT Strategies*, New Jersey: John Wiley & Sons, Inc.

Jinyoul, L., Keng, S., & Soongoo, H., 2003. *Enterprise integration with ERP and EAI*. Journal of Association for Computing Machinery, Communications of the ACM, 46(2), p. 54-60.

Kvale, S. (1996): *Interviews: an introduction to qualitative research interviewing*. Thousand Oaks, CA.: Sage.

Lee, J., Siau, K. & Hong, S., 2003. *Enterprise integration with ERP and EAI*, Journal of Association for Computing Machinery, Communications of the ACM, 46(2),p 54-60.

Lang, J., Widjaja, T., Buxmann, P., Domschke, W., & Hess, T., 2008. *Information Technology and the Number of Suppliers in a Supply Chain: Is There a Relationship?*. Journal of Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), p. 89-88.

Lyons, T. & Molloy, O., 2003. *Development of an e-business skill set enhancement tool (eSET) for Business-to-Business integration scenarios*, Journal of Industrial Informatics, IEEE International Conference on, p. 118-123.

Light, B., Holland, C.P., & Wills, K., 2001. *ERP and Best of Breed: A Comparative Analysis*. Business Process Management Journal, 7(3), p. 216-224.

Martin, K. et al., 2006. *Patterns: Extended Enterprise SOA and Web Services*, IBM Corp: Red book.

Maurizio, A., Girolami, L. & Jones, P., 2007. *EAI and SOA: factors and methods influencing the integration of multiple ERP systems (in an SAP environment) to comply with the Sarbanes-Oxley Act.* Journal of Enterprise Information Management, 20(1), p. 14-31.

Merna, T., 2002. *Risk Management at Corporate, Strategic Business and Project Level*. Manchester: MPhil Thesis, UMIST.

Merrett, A.J. & Sykes, A., 1983. *The Finance and Analysis of Capital Projects*. 2nd ed. London: Longman.

Oates, B. J., 2005. *Researching information systems and computing*, Thousand Oaks, CA : Sage.

Records Management Services. 2004. *Vital Records: How Do You Protect and Store Vital Records?* , UW Records Management [Online]. Available at: http://www.washington.edu/admin/recmgt/vital.store.html [accessed 6 May 2008]

Reiersgaard, N., Salvesen. H., Nordheim, S. & Paivarint, T., 2005. *EAI Implementation Project and Shakedown: An Exploratory Case Study*. System Sciences, HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on, p. 227a-227a.

Roland, H., 2008. *Using IT to Drive Effective Risk Management*. Journal Risk Management, 55, Issue 1, p. 43

Sarkis, J. & Sundarraj, R.P., 2006. *Evaluation of enterprise information technologies: a decision model for high-level consideration of strategic and operational issues*. IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews), 36(2), p. 260-273.

Stoneburner, G., Goguen A., & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology, NIST Special Publication.

Sutherland, J. & Heuvel, W., 2002. *Enterprise Application Integration and Complex Adaptive Systems.* Communications of the ACM, 2002, 45(10), p. 59-64.

Sutton, G. & Steve, G., 2006. *Extended-enterprise systems' impact on enterprise risk management*. Journal of Enterprise Information Management, 19(1), p. 97-114.

Sutton, G., Khazanchi, D., Hampton C. & Arnold V., 2008. *Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships*. Journal of the Association for Information Systems, 9(3-4), p. 151-156,158,160,164-166,168-174.

Tapiero, C. & Kogan, K., 2008. *Supply Chain Games: Operations Management And Risk Valuation*, Publisher: Springer Science Business Media with SpringerLink.

Tarantilis, C.D., Kiranoudis, C.T. & Theodorakopoulos, N.D. , 2008. *A Web-based ERP system for business services and supply chain management: Application to real-world process scheduling*. Journal of European Journal of Operational Research, 187(3), p.1310-1326.

Taylor, D.A., 2003. *Supply chain vs supply chain*. Computerworld, 37, p. 44-5.

Themistocleous, M. & Iran,i Z., 2002. *Novel taxonomy for application integration, Benchmarking*. An International Journal, 9 (2), p. 154–165.

Themistocleous, M., Irani, Z. & Love, P. E., 2004. *Evaluating the integration of supply chain information systems: A case study*. Journal of European Journal of Operational Research, 159(2), p. 393-405.

United States General Accounting Office (U.S.GAO). 1999. *Information Security Risk Assessment - Practices of Leading Organizations*, A Supplement to GAO's May 1998 Executive Guide on Information Security Management [Online]. Available at http://www.gao.gov/special.pubs/ai00033.pdf [accessed date 30 Mar 2008]

Vernadat, F.B., 2002. *Enterprise modeling and integration (EMI): Current status and research perspectives*. Annual Reviews in Control, 26(1), p.15-25.

Vijayan, J., 2002. *Business partners, third parties can pose security risk*. Computerworld, 36 (26), p. 43-55.

Wang, M. & Zhang, S., 2005. *Integrating EDI with an e-SCM System Using EAI Technology*. Journal of Information Systems Management, 22(3), p. 31-36.

Weiler, R., 2001. *Integrating partners carries risk***.** InformationWeek. Manhasset, 837, p. 108.

Weston, F.C. Jr., 2003. *ERP II: The extended enterprise system*, Business Horizons [Online]. Available at http://balrog.sdsu.edu/~shu/Weston%20ERP%20II.pdf [accessed 15 Mar 2008]

William, M., Gerald, G. & David, C., 2008. *Enterprise Information Systems and Strategic Flexibility*. Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), p. 402-402.

Wing, L. & Venky, S., 2004. *Enterprise integration methodology*. Enterprise Information Management, 18(5), p. 511-530.

9 APPENDIX – INTERVIEWS INFORMATION

9.1 Interview Questions

Interviews are designed to be semi-structured interviews. Questions are used as a guideline towards the knowledge domain. Open-ended questions are asked to let the interviewees freely give opinions about their background, working problems and their variety of solutions. The list of interview questions is provided in this section.

- What project have you done that considered to be related to system integration or partner collaboration?
- What is the purpose of the project?
- What is the scope of the project?
- How do you plan the implementation phase and how do you handle risks? Is it based on the experience?
- What are risks and problems during the implementation?
- How do you manage to handle risks or solve those problems?
- How do you plan for partner collaboration or implementation outsourcing?
- What are risks or problems from partner collaboration or implementation outsourcing?
- How did you manage to handle confidential information of the company in order to work with your partners or outsourcers?
- What are problems from system integration which related to unexpected risks in the first place?
- What do you think they were success factors for the system implementation?
- Do you consider risk management for your IT strategic planning? And do you think it is useful or practical?

9.2 Interview Transcription

Due to the research ethics as described in the section 4.3, some names or companies will not be disclosed in the transcription. Answers from interviewees are italicized in the following section.

9.2.1 Enterprise Resource Planning System (SAP) Integrating With Primavera System (Project Management System for Construction)

Interviewee: Mr. Surapol Sungsuban

Position: IT Director

Department: Information Technology Division

Company: Ch-Karnchang Public Company Limited

Industry: Construction

Interview date: 24 April 2008

What project have you done that considered to be related to system integration or partner collaboration?

- *There are several integration projects such as connecting the system to the remote working site in Laos, for example. The types of connection and integration technique depend on the construction working method. Normally we have joint ventures and consortium projects. Joint venture is normally a short-term cooperation so we use an easy-to-implement approach with fair quality of connection and availability, while the consortium project types tend to use a more reliable system and so on. The latest project of integration is to integrate the company's enterprise system to the primavera system.*

What is Primavera system?

- *Primavera system is a project management system for construction that we use to manage our construction time, costs, resources, contracts and changes in the software. The aim is to maximize the resource allocation and business capacity and maintain clear visibility into the business performance at the project level.*

So why do you integrate to the enterprise system?

- *Because we have a number of engineers and management levels that access to this program but we do not need it for everyone at all times, so we decided to connect to the Primavera system at their office and buy a volume licensing. When we use it we will connect to their system remotely and this program does not use a lot of*

bandwidth so the system availability is pretty much ok even when the network is busy. Since we changed our enterprise system to SAP lately, we need to integrate this module to the enterprise resource planning system so they synchronize the resource management eventually.

How do you plan the implementation phase and how do you handle risks?

- *It is normal for cooperation project that we need to minimize the conflicts of interest and maximize the shared goals. Arbitrators are preferable for this type of project. They will work to minimize any kind of conflicts and manage the cooperation to gain benefits from each other. Normally they will negotiate to both sides to concern the shared goals, not ones goal, so that the cooperation can perform its best. By doing so, risks are handled in the same time.*

How do you plan for partner collaboration or implementation outsourcing?

- *Any projects with partner collaboration must be well planned who will do what until when. The schedule and scope of work must be discussed and agreed from both sides as much as possible.*

What are risks or problems from partner collaboration or implementation outsourcing?

- *Contracts are sometimes inadequately explained the details of the work or it can be said that it is practically possible that there might be something missing from the scope of work. So problems will arise when there are new tasks to do but they are not mentioned in the scope of work.*

How did you manage to handle confidential information of the company in order to work with your partners or outsourcers?

- *Non-disclosure contracts are applied to all those partners that obtain company's information from integration.*

What are problems from system integration which related to unexpected risks in the first place?

- *Well, sometimes adapters are not well compatible for both systems as we expected. Technical aspect of the integration should be well planed also.*

What do you think they were success factors for the system implementation? And do you consider risk management for your IT strategic planning? And do you think it is useful or practical?

- *Activity such as commerce and merchandising may lead to problems when ones only think of their benefits. Working with the partner with a win-win solution will*

eventually lead to the successful implementation and maximize benefits from each other. Currently we do not have a specific risk management plan but we always see it as an important factor that risks and consequences are concerned for all the plans.

9.2.2 Banknote Inventory System Integrating With Money Delivery Company (for Automatic Teller Machines)

Position: Senior Unit Manager/Business Analyst

Department: Electronic Channel and Sales and Service Network Operation Support

Industry: Banking

Interview date: 15 April 2008

What project have you done that considered to be related to system integration or partner collaboration?

- *There is an ongoing project about integrating banknote system to the company K that is currently outsourced for the money transfer. The project is still being studied and discussed about its feasibility and return of investment.*

What is the purpose of the integration?

- *Now our company has to manually manage the banknote inventory to be delivered at each automatic teller machine. Each machine has different consumption depends on its location. The more crowded people, such as business area, the more often we have to refill the banknotes, and vice versa. Even we can put a lot of money into those machines to easily get rid of the problem from insufficient banknotes in the machines, in fact, we try to leave the money in the machine as less as possible, but it must be enough for customers to use it without problems. We do not leave much money in the machines so that we can better manage the cash flow and maximize the benefits from that money. Now we have some staff working on that with some simple software to maintain the level of money in the machines, which of course not efficient enough for the country-wide scale. We believe that the integration will help optimize the cash flow for the company.*

What is the scope of the project?

- *Scope is still being discussed but it is most likely that we will have a pilot system in major areas first. If it goes well, we will expand to the rest. The requirement will be discussed for its feasibility between our company and the company K that is responsible for the money transfer, then when we have the final requirement, the IT*

work will be implemented by the company I (outsourcer) which now take care all the IT work for our company.

How do you plan the implementation phase and how do you handle risks?

- *Due to the fact that we outsource the work to many parties, both outsourcers that work for us and business partner that work with us, we have to be very precise for the scope of work, deadlines for each phase. We have set up a project management team that will be the center for the communication. It is to make sure that all the information will not be missing somewhere else. Also the project management officer will have a meeting with all the parties, including our management staff if decisions are needed. Once the project management team finishes the timeline, we will also discussed the possibility for each phase, with revising the requirement if there is any changes from the users.*

What are risks and problems during the implementation?

- *As a matter of fact that the company K has no strong IT background, it is why we still study the feasibility of integration because the system should have high availability for both companies, to maintain the service level for the customers. Our company still has concerns on the capability of the partner, and since this service needs high level of availability, we are revising the scope of work and feasibility study.*

How do you manage to handle risks or solve those problems?

- *We are studying all the feasibility to minimize risks before the implementation. We also develop more detailed requirements for discussion with the partners to avoid unexpected tasks.*

How do you plan for partner collaboration or implementation outsourcing?

- *We use the project management team to cooperate and handle all the work with the partners and third parties.*

What are risks or problems from partner collaboration or implementation outsourcing?

- *Skills and experience of the partner and outsourcer are difficult to evaluate. Lacking of strong background will lead to decreased trust between organization cooperation.*

How did you manage to handle confidential information of the company in order to work with your partners or outsourcers?

- *We exclude the shared data from all the data. Shared data is maintained separately. It is mentioned in the contract that the outsourcers or implementers cannot make use of those information.*

Do you consider risk management for your IT strategic planning? And do you think it is useful or practical?

- *We normally use the requirement as a central of discussion. When we review the requirement with users or outsourcers, we always brainstorm all the issues that might or used to happen, and find a solution together.*

9.2.3 Inventory Management: Logistic Outsourcing

Interviewee: Ms. Suchada Jariyaporn
Position: IT Manager
Department: Information System
Industry: Franchise & Restaurant
Interview Date: 28 April 2008

What project have you done that considered to be related to system integration or partner collaboration?

- *We have implemented the inventory system to manage raw material for branches in the coverage areas.*

What is the purpose of the project?

- *The system can help optimize the inventory that we do not have to contain raw foods for too much or too long in the inventory.*

What is the scope of the project?

- *Integrate system from the branches in the coverage area to use the inventory system.*

How do you plan the implementation phase and how do you handle risks?

- *First we have to identify skill of outsourcer, as the company cannot develop specific skill or carrier for this area, especially in term of technology aspects. Then we identify outsourcing scope that we need to balance between efficiency and competitive advantage, and the most important thing, cost.*

What are risks and problems during the implementation?

- *As we normally focus on how to finish the project, we sometimes lack of long term planning. We need more support from the outsourcers to introduce technology trend to help improve our operation or the recommendation for our system extendibility. Ownership of the project should be mentioned clearly as to make the best effort on outcome. Low level of trust and conflict of interests are the major problems for this cooperation project, for example, branches are normally concerned with the service*

level within the branch, and give little attention on the inventory project, as they thought it should be someone else's responsibility. One more problem is the skill of the outsourcers as outsourcer are specialized in technical more than business function so they focus on technical function, not business function to serve the business needs.

What are risks or problems from partner collaboration or implementation outsourcing?

- *When outsourcing is out-of-service such as they close their business, we do need a fall back procedure to make sure that we still have a system to serve the customers.*

How did you manage to handle confidential information of the company in order to work with your partners or outsourcers?

- *We develop a plan to control information security. The plan identified which data that can be shared and which is not. Non-Disclosure agreement must be applies to all the parties. Corporate information is identified what is critical and what is not, and disclose only those which is not critical. Technical protection techniques are selected to suit the type of data we have, including firewall for internal use and shared areas.*

What do you think they were success factors for the system implementation?

- *Both sides should respect each other and always concern the shared benefits, goals, and objectives. The readiness of infrastructure can tell whether the system can be implemented within time allocated. The skills of outsourcer play a vital role in the implementing time as well.*

9.2.4 Customer Information System Integrating with Back-end and Front-end system

Interviewee: Ms. Thitima Pungpibul

Position: Assistant Manager/Business Process Analyst

Department: Process Development (Internal consultant)

Interview Date: 21 April 2008

What project have you done that considered to be related to system integration or partner collaboration?

- *Now there is a big replacement of the legacy system of the company. So the new system must be smoothly connected to the other important systems.*

What is the purpose of the project?

- *The change happens to increase company's capability of business by replacing the core system of the company that has been used for almost 20 years. With the*

replacement, the new system is capable of operating at higher level of service, flexibility, and extendibility. The core system connects to almost everything in the company, including the front-end system for country-wide branches, and customer information system. While the management considers changing to front-end system in the same time, to maximize the capability of the new core system, integrating all these stuff together is to be carefully planned and implemented, to make the best sustainable system operation.

What is the scope of the project?

- *The replacement project considered to be a large scale project, which my team is taking care of the customer information system integration part.*

How do you plan the implementation phase and how do you handle risks?

- *We study all the system infrastructure and characteristics for all the related systems (core system, front-end system, customer information system), such as the database structure, Entity Relationship diagram (ER), fields of the database. There will be at least one system that has to be modified to be able to work all together, but which one to be modified is the one that is the least risky of modification, also with the cost of it. We calculate the price of modification for all the systems and compare each other, together with the risk in timeline (the bigger system, the more time they need to modify) that we cannot delay for too much since this project impact to most parts of the organization.*

What are risks and problems during the implementation?

- *We found out that the customer information system is using the old structure of database, that when a customer registers two or more products, there will be two or more registration of customers, rather than one single customer profile. This will make the size of the database grows dramatically in the future and make problems in maintenance.*

How do you manage to handle risks or solve those problems?

- *The problem of the database structure should be improved by using the relationship database type that all the registered products can be related to that customer. Having considered the cost of modification including the maintenance in the long term, we decide to modify the customer information system, that also most likely to finish in time, rather than the other systems.*

How do you plan for partner collaboration or implementation outsourcing?

- *First of all, we start all together with the structure of all the systems. We look for the solutions of integrating these stuffs together. Fields and entities are mapped to see the big picture of the system. Then we test all the functions whether it can perform at least what it can do previously (backward compatibility). After the function verification, we go through the services to test the same thing as we did in functions. Then we browse through all the functions and services to see which ones we should make an adjustment from the list of that we found not working. We map the fields of database for one last time before we send it to the implementer for the function development.*

What are risks or problems from partner collaboration or implementation outsourcing?

- *The scope of work is difficult to be identified as we work with many parties and systems. Also within our company, we also work with many departments for this project. Hence we spend a lot of time on meetings and meetings for the scope of work discussion. And that definitely impact the timeline for every party involved.*

How did you manage to handle confidential information of the company in order to work with your partners or outsourcers?

- *It is a must that all the vendors must sign the contract not to disclose or abuse the information. Somehow, vendors that we select are very reliable from their background and reputation. In a smaller project that vendors are not well-known this much, there will normally be some more procedures to control the information security.*

What are problems from system integration that you unexpectedly face during the implementation?

- *The customer information system is a tailor-made application, with a small purpose when first developed many years ago. So there has been insufficient documentation work for this system. Now the system is getting bigger and more complicated so to be able to understand the system and the structure, we have to manually test all the functions which is really time-consuming.*

What do you think they were success factors for the system implementation?

- *We need effective meetings that gain support from management to make a decision for the change that will impact to other departments or parties. Also skill of the vendors that they can understand our business so we spend less time on talking what it is, rather than just technical aspects.*

9.2.5 Cardlink (VISA) and system outsourcing

Interviewee: Ms. Tippawan Attajarusit

Position: Assistant President

Department: Consumer Credit Product Operation

Company: Kasikorn Bank Public Company Limited

Industry: Banking

Interview Date: 30 April 2008

What project have you done that considered to be related to system integration or partner collaboration?

- *The Cardlink project that connects our credit system to VISA retail electronic payments network (one of the most recognized global financial services brands).*

What is the purpose of the project?

- *To provide credit card service to financial institutions, merchants, consumers, businesses and government entities within the VISA network.*

What is the scope of the project?

- *The bank outsources the implementation of IT system in the bank to IBM, and the implementer of this integration to VISA is the specialist from a company that outsources to all the banks in Thailand.*

How do you plan the implementation phase and how do you handle risks?

- *The server is obtained from VISA, and is located at the bank. The system is then linked to the controlling and monitoring center in Singapore. The software of the system will be maintained by another company that is specialized in the application. The settlements with merchants are carried out by VISA. Cooperation is an important factor to work with many parties. Skills and expertise of the outsourcers can reduce risks of implementation failure. Testing is required to identify specific problems from integration.*

What are risks and problems during the implementation?

- *The specific knowledge of the business is sometimes bound to some certain staff that does not work there anymore. The lack of end-to-end process of the product impacts the completion of business requirement. There are some changes of the company that will impact the business requirements, and so delay the project as well. Directions and support from management are needed.*

How do you plan for partner collaboration or implementation outsourcing?

- *The finishing time of the project rely very much on the skill of the implementers. The implementers with strong background on the banking can definitely quicker understand the banking requirements than those who are not. Only the strong background of technical skills is not the only factor we concern when choosing the right implementers.*

What are risks or problems from partner collaboration or implementation outsourcing?

- *Lack of understandings in the business will increase time of implementation.*

How did you manage to handle confidential information of the company in order to work with your partners or outsourcers?

- *Non-disclosure agreement.*

What are problems from system integration which related to unexpected risks in the first place?

- *Changes in business requirement that derived from other departments that is product or service-related.*

What do you think they were success factors for the system implementation?

- *Software capability, product itself, IT infrastructure, and skill of the implementers.*

9.2.6 Electronic Data Interchange (EDI) Outsourcing and Partner Integration

Interviewee: Mr. Surasin Tanchareon

Work experience: IT manager

Company: Winstore Technology

Industry: Information Technology

Interview date: 1 May 2008

Please tell me about the integration system projects that you involved.

- *I have been involved in the integration system projects in Thailand. The first one is the EDI (Electronic data interchange) to manage the supply chain between partners. The company outsourced the EDI provider to implement the systems. And the company also implemented the middleware to connect the legacy system to EDI client.*

How did you plan for partner collaboration/outsourcing?

- *Before implementing we had to agree together about the mission, scope, and requirements for the process of integration and system itself. When we knew the*

specific requirements for the whole system, we designed the system and followed with an implementation phase. While implementing it always had collaboration to each other all the times, to make sure that everything will be achieved for the integration process goal. After the implementing phase, we also needed to test the system together to find the system bugs and errors.

What were problems from partner collaboration/outsourcing?

- *No we did not have many problems, because the EDI Provider always came to our company as an outsource duty.*

How did you manage to handle confidential information of the company in order to work with your partners/outsourcers?

- *The security issue is very important. In the implementing phase, we implemented on the test environment. We did not let their program connect to our legacy system directly; also we implemented the program to extract data from our database. Transforming it into the EDI client standard format file and then forwarded the data to the EDI client application.*

What are the securities for the system?

- *The security policy for the integrate system was derived from the system security in the company. All the servers were in the server room which authentication is needed to enter the room. The source code is backed up in many versions with Ms SourceSafe. Only developer who had authorization can check in and check out the source code and only IT manager has the authorization to deploy new version of application to production servers. Every transaction is backed up in the log file for auditing. An EDI provider connected with the company via virtual private network.*

What were problems from system integration?

- *Yes we had problems after the project was deployed for production. There was an error somewhere in the process which we were not sure. It could be our system EDI provider, or supplier system. We checked out program and log files. We were sure that it was not our failure. But we could not check the EDI Provider program and the supplier system also. The suppliers were upset because they had delivered the items and we had rejected to receive the items.*

So what did the partner company do when you reject to receive the items?

- *They were upset. But we did not agree to pay for it. The order was around 70,000 baht (approximately 14,000 sek).*

What about the other project?

- *The second one was the project in the same company but it was about an integration system with partners in Singapore to manage and use the same the customer's data. The in-house development was used for the project. This project has failed in the end because of too many problems after deploying.*

What were those problems to cause the failures?

- *That project was rapidly implemented. The problem was that is was a bad designed for the business requirement and the lack of collaboration between partners. We did not do much for system testing. And we had to depend on partner systems to manage these customer's data. The users of the system were another factor too. Because it was a rapid project, we did not provide good training for users and there are no documents after deployment.*

What do you think about risk assessment for integration system between partners?

- *I know about the risk assessment and risk management. I think it is a very good approach to conduct, to reduce and eliminate potential risk. But to be honest, in such a medium company we did not have time for that, but if we had time or enough people or resources to conduct the risk assessment, we will certainly do. The risk assessment should conduct together with the partners, because the process is crossed over the supply chain. If we found the potential risk and have likelihood to occur, we should find the control mechanism or policy to support when there is a problem. For example, in the EDI case, they should have a policy that if a duplicated order is sent to the system, the supplier should call the company for checking the problem or error.*

9.2.7 System Integration and Testing

Interviewee: Mr. Sinchai Chanatokakul

Position: System Analyst

Department: Application Maintenance Service

Company: IBM

Industry: Information Technology

Interview date: 2 May 2008

Please tell me about the integration system projects that you involved.

- *I worked with financial companies and had involved in a Credit Bureau systems. I worked as a system analyst in the data exchanging system project. Somehow, the*

partner company did not have experience on Credit Bureau and system integration. So we had agreed with the partner to implement system integration for them. We implemented middleware to retrieve data from database and transformed data into formatted files, and transfer those files via network to our company system on a monthly basis.

How did you manage the work at the partner site?

- *First we had a meeting together to get all requirements and then we design the system. Then we had to agree on the implementation details of the system. From the requirement phase to the implementation phase, we worked from our site. But in the late implementation phase, we had to work from both sites because we had to test the end-to-end system.*

How did you plan for partner collaboration/outsourcing?

- *We used meetings, phone calls, and e-mails to communicate to each other.*

What were problems from partner collaboration?

- *Sometimes we had communication problems because we did not have the same working time. And we did not have a project coordinator. When we were on the partner site, we had some problems because all the systems there were protected with high security policy. When we had a problem in different areas we needed to contact different persons. That was a slow process for us to know who we should contact and had to wait for permission.*

How did you manage to handle confidential information of the company in order to work with your partners?

- *Actually, it was the partner confidential information. But while in the implementation phase, the system was developed on the test environment.*

What are the securities for the system?

- *The organization had very intensive control and security policy including technical and non-technical policy to prevent, support, detect and recover. The server was kept in the server room which only authorized administrators can enter the room, and there were access controls to every system. The company had backed up system and data, such as keep log file for every transaction data. The transfer layer had the encryption method for confidential data while transferring data.*

What were the problems from system integration?

- *We have tested the system over and over again to make sure there will be no error when we deploy it on the production server. And we use both UAT (User Acceptance Testing) and SIT (System Integration Testing) procedures.*

What do you think about risk assessment for integration system between partners?

- *I think it is an advantage to perform risk assessment for IT projects. Now the company starts to conduct the risk assessment for new projects. And since it is the integration system between partners, they should do it on both sides.*