LITERATURE BASED REVIEW - RISKS IN ERP SYSTEMS INCLUDING ASIAN COUNTRIES

Samantha Mathara Arachchi #1, Siong Choy Chong#2 , A.D.S.M Lakshanthi #3
1,2 Management and Science University (MSU)
University Drive, Off Persiaran Olahraga, Section 13, 40100 Shah Alam,
Selangor Darul Ehsan, Malysia, Malaysia
3 University of Colombo School of Computing
35, Reid Avenue, Colombo 7, Sri Lanka

ABSTRACT: *Enterprise Resource Planning (ERP) systems are widely used in nowadays to manage resources, communication and data exchange between different departments and modules with the purpose of managing the overall business process of the organization using one integrated software system. Due to the large scale and the complexity nature of these systems, many ERP implementation projects have become disasters in the history of ERP. Since an ERP requires many resources such as financial, human resources, time, computer hardware and software, a failure can menace the entire business organization. The aim of this survey is to identify risks associated with the ERP projects, general and security within the Asian region, so that the parties responsible for the project can take necessary precautions to deal with those risks for a successful ERP implementation.*

KEYWORDS: ERP, Risk factors, Security risks

INTRODUCTION

Enterprise Resource Planning is a business management software which is used to integrate different functions and departments of a company such as human resource, financial management, sales and distributing, financial, marketing. Market for these systems have increased, since these systems are developed to manage the organizational resources effectively and efficiently.

But, most of the ERP projects are proven to be unsuccessful due to various facts such as inadequate requirements gathering, lack of commitment from management, inadequate training, improper package selection, large scale, complex nature of the system etc. According to a research, there are fifty four percent of cost overruns, seventy two percent of schedule overruns and sixty six percent of organizations had fifty percent or less benefits developing ERP projects in the year 2013. These percentages are higher than the year 2012 which was fifty three percent of cost overruns, sixty one percent of schedule overruns and sixty percent of companies having less benefits [1]. With these increasing rates, identifying risks in ERP projects that might lead to failures, before implementing a project becomes a crucial fact. So that, the parties responsible for the implementation of the system can take necessary actions and controls to prevent or minimize the impact of those risks and be able to achieve a success- full ERP implementation.

Risk management mainly consists with three activities, risk identification, risk evaluation and risk control [2]. This survey is focused on identifying risk factors and security risks that an organization needs to consider when investing or migrating to an ERP system.

ERP Overview

Enterprise Resource Planning systems are frequently used in present day with the purpose of integrating business processes and managing organizational resources in an effective and efficient manner. As one study has defined ERP as "an integrated, configurable, and tailor able information system which plans and manages all the resources and their use in the enterprise, and streamlines and incorporates the business processes within and across the functional or technical boundaries in the organization"[3], another study has defined ERP as "ERP is a descriptor assigned to integrated computer software systems designed to connect multiple parts of the business together and enable data gathered in one area to be accessible to other business units, enabling finer degrees of analysis" [4]. When the origin of ERP systems is considered, it dates back to 1960s when organizations were started to develop centralized computer systems for automatically manage and control the inventories of business organizations. As the next generation of manufacturing business system and manufacturing resource planning software, ERP systems were first introduced by the Gartner group in 1990s [3].

ERP systems differ from MRP II systems from both system requirements aspect as well as technical requirements aspect. Graphical user interface, use of fourth generation language, relational database, and computer aided software engineering tools in development, open systems portability and client/server architecture can be identified as some of the technical requirement differences in comparison to MRP II. Modern vendors have added more modules

and functions such as Supply Chain Management (SCM), Sales Force Automation (SFA), Advanced Planning and Scheduling (APS), Customer Relationship Management (CRM), Business Intelligence (BI) and e-business capabilities as add-ons to the core modules of ERP systems. Thus the Extended ERP is born by making the ERP systems some of the most complex and risky information systems available in today [5].

Thus we can see that an ERP system integrates all functions and departments across an organization into a single, integrated computer system based on a centralized common database, so that the requirements of various departments of a business organization can be achieved [5].

Drawbacks of ERP Systems

Even though there are large numbers of benefits of using an ERP system, there exist some drawbacks as well. Following are some of them [5].

- High cost of planning, customization, testing, implementation, configuration etc., of ERP systems.
- Cost savings/payback may not be realized immediately after an ERP implantation.
- Difficulty in learning and using ERP systems.
- Possibility of indirect costs such as new IT infrastructure cost of upgrading WAN links etc.
- Difficulty in migrating existing data into the ERP system.
- Difficulty in integrating ERP with standalone software systems.
- Time consumption for implementation of ERP systems can be range from several months to many years.
- Time consumption for training employees.

– Facts such as changes associated with ERP, need of adopting business processes to match the software etc., result in a difficult and a complex implementation.
– Difficulty in changing organizational structure or changing the vendor once an ERP system is established.
– ERP systems require well defined hierarchical structure for the organization.
– Competitive advantage of an organization can be lost due to the re-engineering of business process.

Risk Overview

A risk can be defined as uncertainty concerning loss, which is estimated in advanced, is caused by deficiencies of designing and management [2]. When a risk becomes a reality, it is treated as an issue.

Risk management process is used to deal with risks before they become issues [7]. Risk management can be defined as avoid or minimize the adverse effects of unforeseen events by avoiding risks or drawing up contingency plans for dealing with risks [7]. It mainly includes risk analysis and risk control. Risk analysis can be further divided into risk identification and risk estimation, whereas risk control involves drawing up contingency plans, risk monitoring and risk controlling.

Risk Identification

Following factors that need to be considered in the risk identification step [7]. Those are Application, Staff, Project, and Project methods, Hardware/software, Supplier and Environment.

Identification and evaluation of risks can be achieved through various techniques such as expert investigations, scenario analysis, trouble tree analysis, AHP (Analytic Hierarchy Process), OCTAVE, and risk matrix. It is important to identify relevant exposure risks, potential risks as well as uncertainty causes when identifying risks [2].

The project has categorized into risks in technical aspect, organizational aspect, project management aspect or external risks. These categories have further divided into subcategories. For an example, when project management is considered, there can be risks in estimation, planning the project, controlling or in communication. Project dependencies, resources, funding and prioritization are organizational risks. Likewise, risks associated in various aspect of a project can be identified through a risk breakdown structure.

ERP Risks

Due to various advantages such as competitive advantage, improvement of management level, financial benefits etc., many organizations worldwide have adapted ERP systems. Even though some of them appear to be successful, most of the projects have resulted in failures [2]. Large size and the high complexity of ERP systems mainly contribute to these failures. Below here are some of the examples for failures of ERP projects [8].

– Hershey’s ghastly problems with its SAP ERP, Siebel CRM and supply chain applications
– FoxMeyer Drug’s ERP system
– General Motor’s locomotive division
– Sony Germany

- Russ Berrie and Coperations three year failed implementation
- Nike's Supply Chain Issues
- HP's centralization of its disparate North American ERP systems onto one SAP system
- Waste Management's ERP System from SAP

Since most of the failures of ERP projects can be avoided or minimized through identification of risks associated with ERP at the beginning, it is crucial to carrying out studies to identify various risks associated with ERP. Note that this paper defines a risk as "a problem that has not yet happen, but which could cause some loss or threaten the success of the project if it did" [9].

ERP Risk Factors

Some research studies have identified risk factors in Information Systems (IS) projects such as organizational fit, skill mix, management structure and strategy, software systems design, user involvement and training, technology planning, project management and social commitment [9]. In addition to these risk factors, there are other unique risk factors that are presented in the context of ERP.

Previous research studies which focused on identifying these risk factors have categorized them into different categories. As one study has categorized them into risks in decision stage, risks in implementation stage and risks in application stage [2], another study has categorized into people related issues, process risks, technological risks, implementation risks and operation and maintenance risks [6].

People Related Risks

Managers, employees, development team, vendors and external consultants are the most important people related to an ERP project. It is important that these people have a better understanding of the system and the benefits of having an ERP system. Otherwise, non-cooperation of these people can result in a failed ERP system [6].

a. Change Management

It is inevitable that a business process and how people work to be changed when an ERP system is in play in an organization. These changes will result in changes in the job profile of employees as some jobs will be no longer needed and some new job profiles will be created. Automation of new processes, integration of information, improvement of decision making etc. will also be occur due to adopting an ERP system. These changes should be carefully handled; otherwise system can be resulted in failure [6].

b. Internal Staff Adequacy

Implementation team and the post implementation team of an ERP system is mostly consist of internal employees. If these employees do not have relevant knowledge and skills required to develop and maintain an ERP system, the organization will have to recruit external consultants. This will result in a higher implementation cost [6], [9] and [10].

c. Project Team

Since an ERP project development is a complex task, it is important to have a right team who can take the responsibility for the project. Team members of a right team should possess excellent team skills, excellent communication skills, initiative ideas, dedication etc.

and a balance should be there between internal members and external expertise hired for the project. One of the crucial mistake the management can make is, appointing members for a team just because they are the only employees available [6] and [11].

d. Training

Training is one of the most important aspects of any project. Confusion and inaccuracy can be occurred if users are not trained to use the system in a proper way. Therefore, the organizations will not be able to gain intended befits form the ERP system. One crucial mistake organizations can make is, proving the training to a selected set of employees and expects them to share the knowledge with the others [6], [11] and [12].

e. Employee Re-location and Re-training

Changes in the job description and emergence of new jobs are inevitable with the ERP systems. Employees should be handled in a friendly manner if they are uncomfortable with these changes [6].

f. Staffing

Skilled employees are a crucial fact for ERP implementation, operation and maintenance. If employees with necessary skills are to leave the organization in implementation and transition phase, it could result in schedule and cost overruns [6].

g. Top Management Support

Since ERP systems are complex, they require a lot of resources for the implementation team. It is necessary that top management should attend to providing these resources and support accomplishing the project goals and objectives [2], [6] and [9].

h. Consultants

When an ERP system is in the process of implementing, many organizations tend to seek the guidance from external consultants who are experts in ERP systems. These consultants can cause issues if they are not familiar with the organization culture and policies. It is important that a senior manager to act as an intermediate between consultants and implementation team until they familiarize with the organization [6].

i. Discipline

It is important that employees and management of the organization have discipline to learn and practice what they learn. Without discipline it is nearly impossible to meet the schedules. Also system should not compromise its standard specification. [6] and [9].

j. Resistance to Change

Employees may resist changing mainly because of their misconception of the ERP systems. It is important that senior management should provide proper understanding to the users of the benefits of ERP for the company as well as well as for themselves. Also, a proper change management mechanism should be incorporated when ERP project planning is carried out [6] and [12].

k. Insufficient Training and Reskilling in IT Staff

It is important for an implementation team to possess required skills; otherwise senior management have a responsibility of providing existing IT staff a proper training [9].

l. Recruit and Retain Qualified ERP Systems Developers

Due to the high market rate, many organizations are reluctant to recruit qualified ERP system developers. It is important that the top management pay attention to this regardless of the initial cost, since it is important to have a qualified implementation team for a successful ERP implementation [9].

m. Proper Management Structure

Since ERPs are centralized systems, it is important to have a centralized management structure. Without a proper central leadership work duplication can occur. A leader should be someone who is able to take responsible for the project [9] and [10].

n. Business Analysts

It is a crucial fact that an organization to recruit analysts with both business and technology knowledge. An expert analytic can analyze and identify the requirements of the organization and communicate those requirements to the implementation team [9].

o. Communication

Communication takes an important role in any project implementation. It is required that the people involved in the ERP project to know progress, issues etc., related to the particular project. Ineffective communication can lead to duplication of workload, unnecessary problems between team members etc., which ultimately cause a failure of a project [9] and [11].

Process Risks

One of the main purposes of implementing an ERP system is to improve the business process and make it more effective, efficient and productive. An ERP system will eliminates some business processes and introduce new business process to the organization. So it is important that the implementation of business processes to be closely managed [6].

a. Program Management

An ERP system manages different modules of an organization such as financial, material management, supply chain management, order tracking, procurement planning, human resource management etc. It is required that the organization should have up to date information regarding these modules and programs. Therefore, an ERP system should be able to protect data integrity and provide information at the right time in a right manner [6] and [11].

b. Business Process Re-engineering (BPR)

ERP systems require that the business process of the organizations to be changed or improved to suit the systems. These changes can be huge and can be achieved through changing organizational structure, management, using information systems, training, changing job descriptions, changing performance measures etc. There is a probability that these changes may sometimes lead to failure of the entire business organization, since it will become more dependent on the ERP system. Also, since BPR affects the whole organization, it is difficult to move back to the previous state once the changing occurred [6], [9] and [13].

c. Stage Transition

Stage transition can be defined as who takes the responsibility once the system is up and running. This is an important fact and top management should give high consideration when appointing employees for this task [6].

d. Benefits Realization

Implementing a successful ERP system and realizing the benefits from it are two different things. It is much important to plan and organize operational phase; otherwise the success of the ERP system will not be matter. Employee participation, training and top management support will have a crucial effect on this fact [6].

Technological Risks

Since technology is improving day by day, it is important for an organization to move with the technology in order to gain competitive advantage. But certain risks are associated with the technology as well [6].

a. Software Functionality

ERP systems provide variety of functions and features. Since all these functions can be overwhelming for users, it is important for an organization to consult with ERP experts and vendors to customize the system and install only the features and functions that are only necessary for the organization [6] and [12].

b. Technological Obsolescence

Since new, efficient and fast technologies are developed every day, any technology that is present today can be obsolete in few years. Therefore, any organization that wishes to adopt a new ERP system should select packages, vendors and technology that will not be obsolete in the near future. In this case architecture of the product, ease of upgrading, support of vendor etc., are some of the important facts [6] and [14].

c. Application Portfolio Management

Any organization which provides ERP systems to other companies, usually spend most of its resources and human effort maintaining those systems and supporting their infrastructure. If this process is not handled properly, many resources will be needed to allocate to this. Hence, productivity of the organization will be reduced [6].

d. Upgrades or Enhancements

Every ERP system needs to be kept up to date to get the maximum benefits. Therefore, it is the responsibility of the maintenance team to be in contact with the vendors and updates the system if updates are available. It is important to select trusted vendors. Proper contracts should be signed when the system is deployed, to avoid risks such as vendor stops supporting the system or close its operations [6] and [13].

e. Technological Bottleneck

Technological bottleneck can occur when different technological environments exists within one organization. This can cause delays in database management systems as well. One of the instances this will occur is, when designers of ERP systems try to map ERP modules with existing legacy systems. This can cause significant time and cost overruns [9] and [11].

Implementation Risks

Since many ERP projects have a tenancy of failing, it is important to have a clear understanding what could go wrong in the implementation process [6].

a. Project Size

The main difference between normal IS projects and ERP projects are the scope and the size. Typical ERP project involves a lot of people, cover the whole business organization and effect all the employees and lasts for a long period of time. Therefore, the project should be carefully handled and precautions should be taken such as handling uncertainties [6] and [12].

b. Implementation Length

Since ERP implementations can last for a long time, keeping employees enthusiastically and devoted to the project becomes a major issue. If top management does not treat this issue, that could increase the employee turnover [6] and [11].

c. High Initial Investment

ERP projects require high initial investment and its benefits can be realized only after a successful implementation. If the project is to be failed, the company will face a tremendous financial loss [6].

d. Unreasonable Deadlines

In some situations, top management may demand unreasonable project deadlines. It is important to be highly careful when agreeing to these since taking short cuts to meet deadlines can cause harm to the quality of the system [6], [14] and [12].

e. Insufficient Funding

ERP projects require huge funding. When allocating budget for the project, it is important to have insights from experts. Otherwise, it is inevitable that the project be stopped due to lack of funding. Allocating a contingency budget additionally to the required budget is a safe practice [6].

f. Interface

Even though an ERP system becomes the center of the organization once deployed, it may need to interact with external partners, handle complex data sources and legacy data types etc. It is a necessity for an ERP project to have relevant interfaces to handle these tasks [6].

g. Organizational Policies

Since every organization has their own policies it is important that implementation team, external vendors and consultants not to be caught in internal fights. For an example, recruitment policies differ from organization to organization. Therefore, the system should be customized to match the policies when buying from a vendor. [6] and [14].

h. Scope Creep

Changing the scope of the project constantly, increasing or decreasing can cause confusion to the implementation team. Therefore, it is important to clearly define the scope of project [6], [11] and [14].

i. Unexpected Gaps

There can be a gap between what is expected from the ERP system and what it actually provides. Senior management should carry out gap analysis from time to time to overcome this problem. The actions taken can result in costs and schedule overruns [6].

j. Configuration Difficulties

When an ERP system is bought, it is usually customized to get only the required features. But there can be some areas that is difficult or cannot be customized [6].

k. Lack of prototyping

Prototyping aids developers to have a clear and better understanding of the requirements of any system. Since ERP systems are large and complex, development of prototypes are usually skipped [14].

Operation and Maintenance Risks

An ERP system is never over after the implementation phase. Its benefits can only be gained when the system is in use. Therefore, installing new features and versions, embracing new technology, training new end users etc. should be carried out throughout the lifetime of the system. So the top management and the users of the system should give their lifelong commitment to the operation and maintenance of the system [6]. Among these risks, some factors are unique to the ERP systems [9]. They are Business Process Re-engineering, Business analysts, insufficient training and reskilling of IT staff, internal staff adequacy, attempting to build a bridge between legacy systems

And also some of these risk factors are inter related and have a hierarchical relationship among one another [4]. For an example, it is identified that lack of senior management can lead to insufficient training to end users and ineffective communication. That ultimately led to users' resistance to the system.

ERP Security Risks

Even though, the word ERP is usually heard in the context of businesses, variety of areas such as health care, intelligence and defense have adopted ERP systems at the present. Since these areas including finance are highly sensitive, having excellent security becomes a crucial fact [3]. Therefore, it is important that any organization which have an interest of ERP to have a proper understanding of the security risks.

Security risks of an ERP system can mainly be divided into three categories; security of network layer, presentation layer and application layer [3].

Network Layer Security Risks

These risks are occurred when an employee communicates with the ERP system or different modules of the systems communicate with one another. Managing and controlling these types of risks are fall within the responsibilities of network security administrators and ERP administrators are usually not involved [3].

Presentation Layer Security Risks

Presentation layer includes personal computers, browsers and graphical user interfaces. It is difficult to secure the system by limiting user access to the GUI since it is not possible to restrict the transmission of GUI packets. Security can be achieved for some extent by placing a CITRIX server between clients [3].

Application Layer Security Risks

Application layer security is mainly focusing on the security of data and process. The security functions provided by database vendors may activate or deactivate according to the security solution used in the system [3].

a. Security Policies

Since security policies includes rules and constraints for granting or revoking permissions to users and processes, it is important that any organization with an ERP systems to have well defined security policies [3].

b. **User Authentication**

Since an ERP system is used by large number of employees of an organization, it is necessary to have a proper and accurate user authentication mechanism to identify whether the person actually himself or someone claiming to be that person. If this process is not handled carefully, outsiders can easily access the system [3] and [15].

c. Separation of Duties

It is important that authority to execute some tasks should be given to selected employees or selected roles. For an example, if every employee is given the permission to access and change sensitive data, there can be employees who misuse that right for their own personal gain [3] and [15].

d. Authorization

When a user request to perform some tasks or access some data, system should check whether the access has given for that person. If not, employees can misuse the system [3] and [15].

e. Time Restriction

Sometimes, certain situation can occur where a user needs to access resources that per- son have not entitled. It is security administrators' responsibility to grant permission and revoke that permission just after the situation is handled [3] and [15].

f. Loggings

Logging and tracing is required to check on the events that have occurred. These log files should be protected from tampering and breaching [3] and [15].

g. **Security Administrator**

Granting and revoking access, define capabilities of users and roles are some of the highly sensitive tasks that should be handled carefully. Since these tasks are responsibility of the security administrator, organizations should give extra attention when an employee is appointed to this role [3] and [15].

h. Database Security

Since an ERP system integrates whole business organization and has a centralized database, it is crucial to handle the security of the database. An unprotected database can be subjected to many external attacks [3], [13] and [15].

In addition to previously mentioned risks, following are some other risks that an organization needs be considering with respect to the security.

i. Legacy Systems

In some organizations, communication between ERP system and the legacy system is inevitable. These communications must be handled carefully, since there is a possibility of legacy system introducing new bugs and security issues to the system [16].

j. Standard and Metrics

There should be clearly specified standards for a security team to know when to stop. Trying to make the system to secure can result in new issues [16].

k. Breaches and Incidents

Every software has its own vulnerabilities. Therefore, responding to security breaches and incidents appropriately is equally important as developing a secure system [16].

l. Knowledge on Vulnerabilities, Attacks, Attackers etc.

Every organization needs to spend a certain amount of resources on intelligence gathering of the security related aspects such as previous attacks, attackers etc. These aspects can be categorized into seven aspects, principles, guidelines, vulnerabilities, exploits, rules, attack patterns and historical risks. Developing systems without having the knowledge what went wrong in the past, can make same mistakes of those previously attacked systems [16].

m. Tools

Sometimes, to automate the security tasks during the development process, tools such as ASET, AUTOCRYPT are used. It is important to select an effective set of tools in these situations [16].

n. Continuous Improvement

Since security is a field that is moving forward day after day, system developers should constantly improve and reinvent the security procedures that are used for various tasks in the system such as handling breaches, reporting issues, monitoring and logging, data security and integrity. Older security procedures are more vulnerable to attacks [16].

Security Risks in the Cloud ERP

Cloud ERP systems are the ERP systems that have deployed in a cloud environment. Since these systems provide flexible, efficient, adaptable, scalable and affordable solution, they have provided big success to deliver business critical data [17]. Even though cloud ERP provides such benefits, it is important for an organization to have a clear understanding of the risks associated with the cloud architecture.

a. Confidentiality

Many number of parties, applications and devices involved in a cloud environment leads to increased number of access points. Therefore, there is a probability that unauthorized par- ties may try access the data [18].

b. Multitenancy

Multitenancy is the characteristic of resources such as memory, network, pro- grams and data. In a cloud environment, resources are shared in at network, host and application level. Even though users are separated in a virtual level, hardware is not separated. This can cause serious vulnerability issues, if the reusable objects are not handled properly [18].

c. Data Remanence

This refers to residual representation of erased or removed data. Since there is no sep- aration of hardware between users within a single cloud infrastructure, data remanence can lead to unwilling disclosure of private data [18].

d. User Authentication

User authentication is verifying whether a person is who he/she is claiming to be. Lack of strong user authentication can lead to unauthorized access to user accounts which may ultimately cause breaches in the privacy. [18].

e. Software Confidentiality

In a cloud environment, the user has to trust the applications provided by the cloud owner will maintain and protect data in a secure manner [18].

f. Privacy

When adopting to cloud, company data is stored in a service providers servers rather than in an organizations servers. Those severs can locate in any location. This can cause conflicts with various legal requirements. For an example, European law indicates that an organization needs to know where its data is located [18].

g. Integrity

Integrity refers to protecting data from unauthorized deletion, modification and fabrication. Lack of string authentication and authorization mechanism can cause harm to integrity of data [18].

h. Availability

Data, software and hardware should be available for the authorized users whenever they demand. Therefore, the system should be able to operate even when there is a possibility of a security breach [18].

CONCLUSION

Through the findings of the survey, we can agree that many risk factors are associated with an ERP project. These risks can be classified into categories as people related, process, and technological, implementation and operation and maintenance. Among these risks, some risks such as business process reengineering, attempt to build a bridge between legacy systems are unique to ERP systems.

Furthermore, we can see that they are many ERP risk factors that are people related. Among them top management support, internal staff adequacy, training to the end users and end users resistance to the new system are risks that have been identified by many previous researches. Another risk that many researchers have identified is the reengineering of business process to suit the ERP system. This should be handled very carefully since it affects the entire business organization. Overall, we can see that having a supportive top management, qualified staff and consulting external experts where necessary can minimize many of these risks.

Security is another aspect of ERP that involve high risks. Since security is an essential aspect of any application, identification of these risks will be beneficial for any organization who wishes to adapt an ERP system. Cloud environment is associated with many risks such as confidentiality, privacy, integrity. Even though cloud ERP has many benefits, organizations needs to consider those security risks associated with the cloud before moving into a cloud based environment.

Therefore, any organization that wishes to adopt an ERP system must consider these risks and take necessary actions to prevent risks or minimize the effect of the risks.

REFERENCES

[1] A. P. Consulting, “2014 ERP REPORT,” Tech. Rep., 2014. [Online]. Available: http://panorama-consulting.com/resource-center/2014-erp-report/

[2] J. Deng and Y. Bian, “Constructing a risk management mechanism model of ERP project implementation,” Proceedings of the International Conference on Information Manage- mentProceedings of the International Conference on Information Management, Innova- tion Management and Industrial Engineering, ICIII 2008, vol. 2, pp. 72–77, Dec. 2008.

[3] W. She and B. Thuraisingham, “Security for Enterprise Resource Planning Systems,” Information Systems Security, vol. 16, no. 3, pp. 152–163, Jun. 2007.

[4] M. Vanderklei, “RISK FACTORS IN ERP IMPLEMENTATIONS: HIERARCHICAL AND LINEAR RELATIONSHIPS,” in 21st European Conference on Information Sys- tems, pp. 1–7.

[5] Y. Zeng, “Risk Management for Enterprice Resource Planning system Implemenations in Project Based Firms,” Ph.D. dissertation, 2010.

[6] A. Leon, Enterprise Resource Planning. Tata McGraw-Hill Education, 2008. [Online]. Available: http://books.google.lk/books?id=pTGDy2GX s UC&printsec =frontcover& source=gbs ge summary r&cad=0#v=onepage&q&f=false

[7] . Silva, “Risk management, scs3001, planning and management of software projects,” University of Colombo School of Computing, 2014.

[8] S. Mathar Arachchi, “Erp fail, ict3001, enterprise resource planning,” University of Colombo School of Computing, 2014.

[9] M. Sumner, “Risk factors in enterprise-wide/ERP projects,” Journal of Information Tech- nology, vol. 15, no. 4, pp. 317–327, Dec. 2000.

[10] Grabski, Leech, and Lu, “Risks and Controls in the Implementation of ERP Systems,” The International Journal of Digital Accounting Research, vol. 1, no. 1, pp. 47–68, 2001.

[11] G. Seo, “Challenges in Implementing Enterprise Resource Planning (ERP) system in Large Organizations : Similarities and Differences Between Corporate and University Environment,” Ph.D. dissertation, 2013.

[12] R. Ghosh, “A Comprehensive Study on ERP Failures Stressing on Reluctance to Change as a Cause of Failure,” Marketing and Management, vol. 3, no. May, pp. 123–134, 2012.

[13] Y. Song, M. Yin, F. Meng, and X. Ding, “Enterprise internal controlling risks and preven- tion within ERP system,” Proceedings - 2011 4th International Conference on Information Management, Innovation Management and Industrial Engineering, ICIII 2011, vol. 2, pp. 41–44, Nov. 2011.

[14] R. Ray, Enterprise Resource Planning. Tata McGraw-Hill Education, 2011. [Online]. Available: http://books.google.lk/books?id=52KPTrtm QC&printsec =frontcover& source=gbs ge summary r&cad=0#v= onepage&q&f =false

[15] R. V. D. Riet, W. Janssen, and P. D. Gruijter, “Security moving from database systems to ERP systems,” Proceedings Ninth International Workshop on Database and Expert Systems Applications (Cat. No.98EX130), 1998.

[16] A. Brian and C. Brad, “Software Security in Practice,” IEEE Security and Privacy, no. April, 2011.

[17] G. F. H. Raihana, “Cloud erp a solution model,” vol. 2, no. 1, pp. 76–79, 2012.

[18] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, Mar. 2012.