Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2011 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

9 July 2011

Managing Security Requirements: Towards Better Alignment Between Information Systems And Business

Azmat Ullah
La Trobe University, a.ullah@latrobe.edu.au

Richard Lai
La Trobe University, lai@cs.latrobe.edu.au

ISBN: [978-1-86435-644-1]; Full paper

Recommended Citation
Ullah, Azmat and Lai, Richard, "Managing Security Requirements: Towards Better Alignment Between Information Systems And Business" (2011). *PACIS 2011 Proceedings*. 195.
http://aisel.aisnet.org/pacis2011/195

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2011 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

MANAGING SECURITY REQUIREMENTS: TOWARDS BETTER ALIGNMENT BETWEEN INFORMATION SYSTEMS AND BUSINESS

Azmat Ullah, Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, Vic. 3086, Australia, A.Ullah@latrobe.edu.au

Richard Lai, Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, Vic. 3086, Australia, lai@cs.latrobe.edu.au

Abstract

Information Systems are increasingly becoming essential to the success of business organizations. They play a central role in the success of almost all components of the organization such as business decision-making, business strategy formulation, business goal modeling, managing organizational resources, structure, managing organizational data etc. However, protecting information systems and organizational resources from security threats is a critical task in the management of the business, which alternately, negatively affects the alignment process between business and information systems. Managing information security within business organizations calls for a clear understanding of the viewpoint of business and the architecture of the system that is being used in the organization. This paper presents a requirements engineering based approach to modeling and maping the issue of information security at an early stage of the system's development life cycle in the context of alignment between business and information systems.

Keywords: information security, risk management, risk analysis, business-IS alignment, requirements engineering.

1 INTRODUCTION

Today, an information system (IS) plays a pivotal role in the growth of the business organization. However, this growth often demands quick action on the implementation of the organization's requirements and may result in weak alignment between business and IS. Alignment can be defined as the optimized synchronization between dynamic business objectives and respective technological support by IS (Ullah & Lai 2010a). The concept of alignment first appeared in the early 1970s (Luftman et al. 1993); McKeen & Smith 2003) and since then, researchers have tried to understand the issue by studying various organizational factors such as: structural differences between business and IS (Pollalis 2003), cultural variations between business and IS (Luftman et al. 1999), strategic differences between business and IS (Kearns & Lederer 2000), and variations in social aspects between business and IS (Reich & Benbasat 2000). Recently, researchers have diverted their attention from business-driven solutions for alignment to IS-driven solutions, where they consider the organization's factors: business goal modeling and business requirements of its underlying IS (Ullah & Lai 2010a; 2010b)

One way of achieving successful alignment is the management of information security risk requirements within the business organization. Over the last 25 years, security problems (e.g. cyber attacks, human error, system failure, organizational data confidentiality, integrity, unauthorized access of organizational resources, etc.) have increasingly adversely affected the implementation and deployment of IS in both public and private business organizations (Laney et al. 2004; Liu et al. 2003). According to the ISO/IEC (1999) and Castano et al. (1995), information security refers to the ability of IS to protect data information from unauthorized individuals or systems which try to read or change data and only allows access only to authorized staff.

Through the use of requirements engineering methods, this paper proposes an approach to manage information security requirements in the early stages of system development in relation to alignment between business and IS. The paper suggests how to model and map security goals with IS requirements to guarantee the protection of the business organization and its resources from different threats as well as to guarantee a long term alignment between business and IS. The paper is structured as follows: in section 2, we review the context of our paper which includes the theoretical concept of alignment and information security. Section 3 presents the proposed methodological framework which is further categorized into: the identification of the organizational environment, the derivation of information security goals, the detection of security requirements from goals, the detection of constraints and security requirements at the IS level, and the analysis of risks at the system architecture level. Finally, section 4 presents the conclusion of the paper.

2 THE CONTEXT OF OUR WORK

This paper presents an approach to manage security-related issues within the business organization in context of the Business-IS alignment research area. Therefore, it is important to describe the theoretical concept of both alignment and information security in the business organization prior to discussing the idea of security management in the alignment domain.

2.1 Business and IS Alignment

Alignment between business and information systems (IS) is the degree of fit and integration between business strategy, IS strategy, business infrastructure, and IS infrastructure (Henderson & Venkatraman 1993).The concept of alignment emerged early in the 1970s (Luftman et al. 1993; McKeen & Smith 2003). Since this time, alignment scholars have struggled to tackle the issue through linking the business plan with the IS plan. But the early approaches were ad hoc, given the level of dissatisfaction in organizations regarding their respective IS departments. These theories have

expanded over time and nowadays, researchers point out many issues and challenges, and have developed different and suitable alignment techniques and models.

Alignment can be measured in various directions. These directions are characterized with respect to an organization's strategy (Kearns & Lederer 2000; Byrd et al. 2006); Campbell et al. 2005), structure (Pollalis 2003; Chan 2002), culture (Luftman et al. 1999); Silvius et al. 2009; Campbell 2005), and social direction (Reich & Benbasat 2000). In regard to an organization's strategic directions, researchers normally consider a "formal strategy" and an "informal IS strategy" in order to measure alignment. On the structural side, researchers focus on "structure complexity", and "rapid changes in organizational structure". On the organizational culture side, researchers investigate the "lack of communication between business and IS", "weak relationships between business and IS" and "low IS belief within the organization". Finally, in relation to the social direction of the organization, factors such as a "lack of shared domain knowledge", a "lack of business knowledge of IS" and a "lack of IS knowledge in the business" are considered. Alignment has several phases, where each phase represents a specific part of the business organization, for example, internal and external phases of alignment. In the external phase, the business organization is aligned with the business partner or with other similar business organizations including clients, dealers, competitors etc. In the internal phase of alignment, business aligns with their own internal departments. This kind of alignment could be organizational phase alignment, departmental phase alignment, upper and lower phase alignment, project phase alignment, system phase alignment, etc (Ullah & Lai 2010a).

2.2 Information Security

Today, information technology has penetrated almost all aspects of business organizations in a huge variety of ways and has had a great impact on business performance. However, it has also increased security threats for business organizational data information. Data information is a resource like any other business resource and it can exist in many forms such as: in writing, soft files, emails, film, etc. Information security is the process of protecting organizational resources. Ensuring the security of organizational resources can be achieved through the implementation of a set of controls which include: procedures, processes, business policies, enterprise structure, software and hardware functions etc. These controls need to be properly established, developed, examined, evaluated and improved, where essential, to guarantee that the security and business organizational objectives are met. This can be done by linking with other business processes (Gilliam & Feather 2004).

Moreover, achieving successful security is important to both public and private organizations, as many important organizational resources such as information, business processes, systems and networks are facing threats from several sources, including computer viruses, fraud, fire, espionage, and flood. Damage from system hacking, and denial-of-service attacks have recently become more common and increasingly sophisticated. Engineering security within the business-IS alignment domain is a specialized area of concern for both business organizations and their related IS departments. If security is not a part of the development life cycle of the system which meets the needs of the business, the quality of the developed system could be impacted, and the result could be loss of trust and organizational image, which means alignment suffers. In addition, system requirements engineering and managing security issues are both important parts of software engineering and failure to these can result in the failure of the system (Demarco & Lister 2003).

3 THE PROPOSED METHODOLOGY FRAMEWORK

Many information security problems arise when there is a need to protect organizational resources from threats/attacks. However, protecting organizational resources is a critical task in this rapidly changing business environment. Organizations consist of complex business structures that are continually being evaluated and updated with consumer demands and structures that contain strategies, policies, models, processes, commonly-shared values, coordination, sets of organizational activities that work together to achieve a common business goal etc. In alignment between business and IS domains, security-related problems can be addressed by managing security in the form of

identifying/modeling, mapping, and analyzing the attacks to IS and to specifying the suitable requirements in order to respond to those attacks in early stages of IS development.

The aim of this paper is to present a requirements engineering-based approach for business and IS analysts to better understand security-related issues and identify their associated security goals, the detection of security requirements from the goals, the detection of constraints and security requirements at the IS level, and analyze the risks at the system architecture level in the context of alignment between business and IS. The proposed approach is structured in two parts as shown in Figure 1. Part 1 describes the specifications of the business organizational environment in the form of infrastructure and resources, which is based on the already accepted methodology called requirements engineering approach for Business/IT alignment proposed by (Ullah & Lai 2010a). Part 1 is further divided into two levels: level 1 details the organization's stakeholders (e.g. business and IT executives), the organizational aims, strategy, mission, and objectives. Level 2 describes the organizational resources. On the business side, resources are anything that has economic value to the business organization, are things that the organization owns or are things which are central to the organization in the realization of its business goals. For example, in our case study, business resources are the management of automobile company processes, personal information of company staff and customers, and management of company data information and knowledge. On the IS side, resources are anything that is part of the information technology department and provide support to the business resources. For instance, in our case, IS resources are software, hardware, network, people etc. The protection of these resources is important for the survival of the business organization.

.

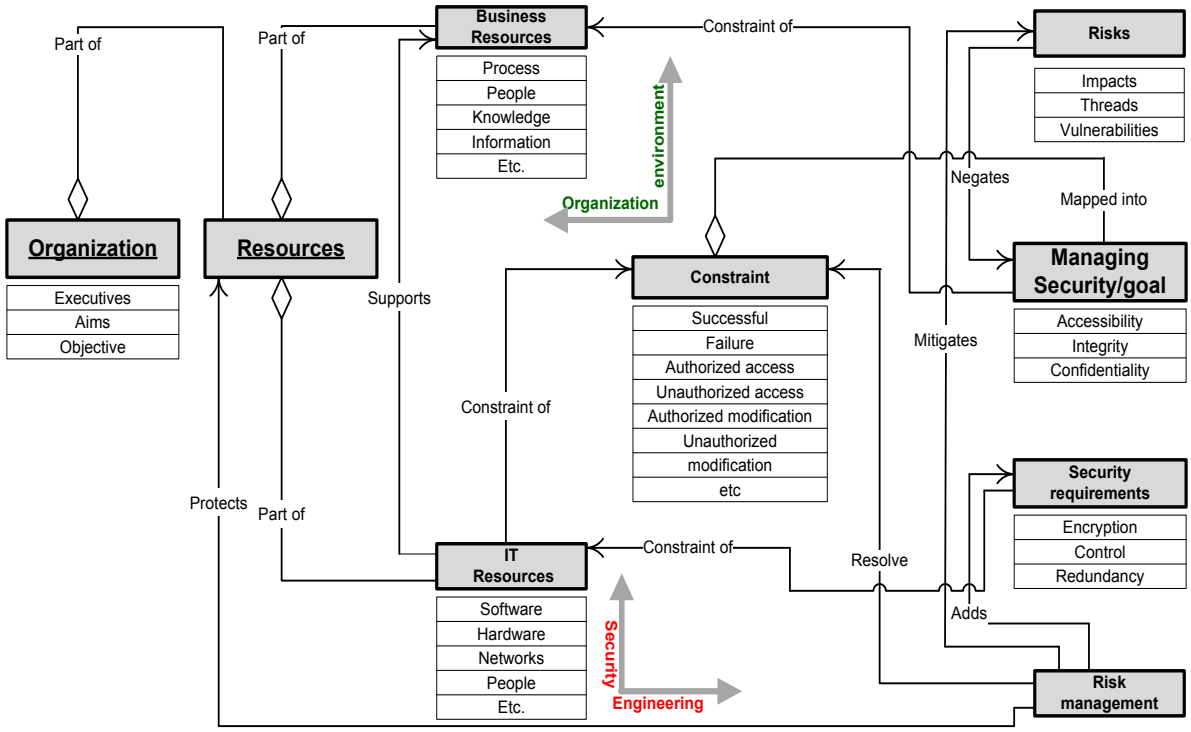

Figure 1. Information security framework in the context of IT-Business alignment (Ullah & Lai 2010a)

Part 2 describes the way to identify/model and analyze the attacks on IS and the overall business organization, as shown in figure 1, as security is the main concern of IS for the scope of this proposed approach. It defines the qualities expected from IS such as safety, usability, reliability etc. Part 2 is further divided into five levels: level 1 presents how to model the business process using *i** language so that security requirements can be linked with it. Level 2 describes the way to identify information security goals and defines how to link them with business processes. Level 3 depicts the derivation of security requirements from the goals. Level 4 illustrates the identification of constraints and security

requirements. Finally, level 5 describes the method of risk analysis at the system architecture level, as analysis of risks is the key issue to keep in mind when dealing with different kinds of security qualities.

3.1 Identification of Organizational Environment (Level 1)

To validate this proposed approach, we extend already accepted case study on the order management process in an automobile company (Ullah & Lai, 2010b). To identify and analyze the business process, we used the *i** framework (Yu 1995), as shown in figure 2. This framework was developed for modeling and reasoning the business organizational environment and the environment of the related information system. The framework is divided into two main modeling components: the strategic dependency (SD) model that is used to define the dependency associations between the organizational actors; and the strategic rationale (SR) model that is used to describe the stakeholder's interests in terms of what they need, what is their main concern, and how these concerns might be addressed in the organizational and system environments. The framework is well accepted in the fields of business process modeling, process redesigning, information systems process modeling and reengineering (Yu & Mylopoulos 1994).

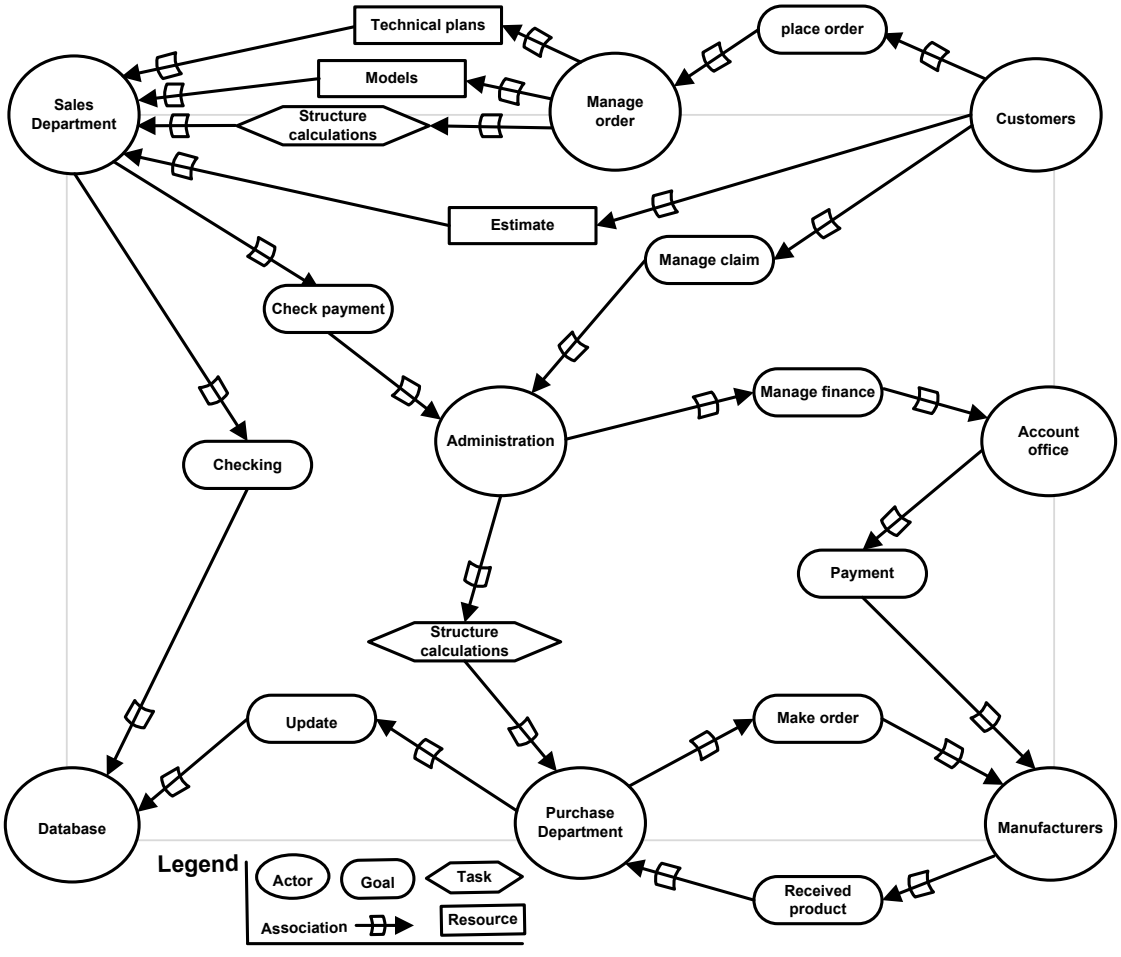

Figure 2. Automobile company process model (Ullah & Lai, 2010b)

The primary goal of the automobile company is to make possible the supply of auto parts to different cities around the country. The company order management process has been divided into several activities through an *i** diagram. The company process is made up of different organizational *actors* which include: administration, sales, managers, customers, account office, manufacturers, databases, and the purchasing department. All these actors are represented in terms of *i** concept. There are four

types of dependencies: (1) *business goal* dependency, (2) *task* dependency, (3) *resources* dependency, (4) *soft goal* dependency. The *business goal* dependency can be further categorized into nine sub dependencies, as shown in figure 2: *Place order* – supports the customer to place the order, *manage claim* – defines the way customers can lodge a claim with the company, *check payment* - the administration checks the customer's chosen payment method after the order has been placed, *manage finance* – the account office is responsible for managing finance-related queries*, checking* - checks the product availability with the company database, *payment* – responsible for making payments to the manufacturers, *update* – database need to be updated after a sale or purchase of a product, *make order* - orders new items when there is no stock, and *received product* - responsible for receiving the product from the manufacturers.

The *task* dependencies can be used when organizational actors perform any activity. For instance, in our case study, the *manage order* actor does "structured calculations" for the sales department, and the *purchase department* actor does "structured calculations" for the administration. The *resources* dependency is used to describe the organizational actor's dependency. For example, managing the *customer order* actor in the case study depends on resources such as: the *manage order* actor should provide technical plans and models to the sales department, and the sales department should provide estimates to their customers. Finally, the *soft goal* dependency is different from goal dependency. Soft goals refer to goals for which there are no straightforward criteria to determine whether the condition is fulfilled.

3.2 Derivation of Information Security Goals (Level 2)

Once it has been decided which business processes need to be implemented and once all business process-related resources are identified, there is a need to derive and identify the security objectives to protect the resources in the proposed business process. Several methodologies have appeared in the literature to protect business resources. The most prominent ones are integrity, availability, and confidentiality (ISO/IEC 2005), where the term *integrity* is used to define the accuracy and completeness of the business resources, the term *availability* is used to represent the accessibility and usability of business resources upon request from the business authorities, and the term *confidentiality* defines the information which will not be disclosed or will not be made available to unauthorized authorities, entities, processes etc.

After the identification of the business process, it is important to add security goals to the process. Security goals at this stage confirm the definition of soft goal in *i**. Requirements engineering literature shows that it is possible to map security goals into the business requirements (Liu et al. 2003; Mouratidis et al. 2003; Lamsweerde & Letier 2000). Figure 3 shows soft goals in our case study where the method of defining security or soft goals is different from business resources, for instance, confidentiality is the soft goal for the estimates, structuring identified business goals into the organizational hierarchy that describes the specifications of all included goals, and their contribution to the higher level components of the business, which are either part of the organization's business strategy or related to the organizational external factors.

Figure 3 depicts the security-related goals showing how to secure the business process and important information on customers. For example, the *measurement of confidentiality* security goal directly contributes to customer *trust* and *confidence*, the *technical plans confidentiality, accessibility activity model* security goals contribute to company *confidence* etc. Moreover, in some cases security goals can be represented as security dependencies, where actors indicate security issues rather than the soft goals of the company. In our case study, we introduce a new actor called *regularity body* in order to satisfy the *structural reliability* of the automobile company or identify a stakeholder who has a security concern, as shown in figure 3.

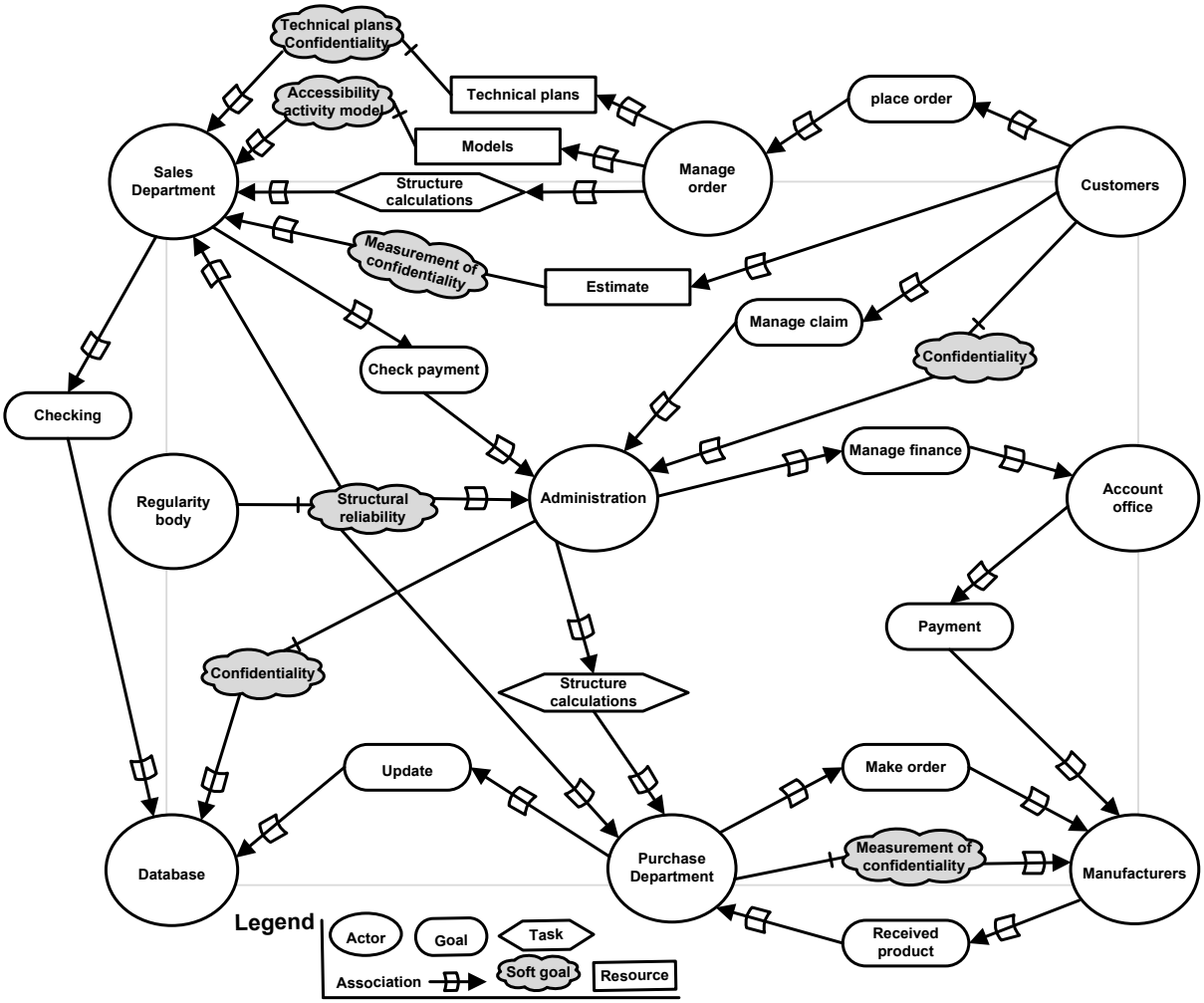

Figure 3. Identification and mapping security goals

3.3 Detection of Security Requirements from Goals (Level 3)

In the previous section, we described how information security objectives can be mapped with business requirements. In this section, we illustrate how these security goals can be refined in the context of information systems requirements. Once the security goals are identified, there is a need to map the goals at the business domain level, in terms of security requirements in the development of IS. For example, *confidentiality of the customer's personal information* goal can be mapped into the *unauthorized access to the customer* record constraint, as shown in figure 1. Figure 3 shows IS at this stage still requires a further detailed description on how security requirements can be implemented in terms of the underlying IS infrastructure. For example, the system provides several services which include: managing the account office, managing the customer order, managing the company database, etc, but the implementation of these services in terms of the underlying system are not clear.

An intermediate level of system requirements is of utmost importance in order to overcome problems with the properties of a system. With respect to the existing information security methodologies, the concept of constraint presents in the context of requirements engineering that provides a detailed description on security goals and supports alternative design decisions for future changes in the system. When articulating an *unauthorized access* or *unauthorized modification* constraint on IS, there is no further information on how the constraint is going to be operationalized. On the other hand, figure 1 also presents a taxonomy associated with security requirements. The idea of security requirements varies from domain to domain; in some cases, they are used as technical requirements

associated with different components of IS: network, hardware, software, telecommunication, database, etc. In some other taxonomies, security requirements correspond to generic non-functional requirements that can help to define the system architecture. However, commonly, the literature shows two different types of requirements (ISO 2004): (1) generic security requirements, where important security requirements can be accessed but requirements cannot be implemented due to a lack of information on security requirements; and (2) technical security requirements which are related to the length of the key that is used in the encryption mechanism. In this analysis stage, the non-technical requirements are more significant than the generic ones. Moreover, there is a need to establish the link between security requirements and a constraint, where constraints are used to describe security problems that need to resolved, and security requirements are used to implement methods in order to find a solution to these security problems**.**

3.4 Detection of Constraints and Security Requirements (Level 4)

Once the security goals have been detected, there is a need to detect constraints and security requirements at the system architecture level. To implement security requirements, in our case study, we only provide detailed information on the *sales department* actor in our proposed case study and its interactions with the *information system (IS) plan* as shown in figure 4. The IS plan proposes collaborative support for a set of services used by several departments of the automobile company and also supports the *structure calculations* activity in the company. The first *structure calculations* task dependency identified at the business organizational level is between the *sales department* and the *senior manager*. But the second *structure calculations* task dependency is defined at the IS level, where two agents, the *junior manager* and *store manager,* manage this task. A *junior manager* uses the *IS plan* structure calculations service on the basis of *technical plan estimations*. However, for authorizing structure calculations that need to be conveyed to the *sales department*, a *store manager* authenticates the results that the calculation tool generates. After authentication, the *store manager* gives feedback on item availability and payment confirmation to the *sales department* by using the *feedback* goal in the *store manager* actor, as shown in figure 4. Moreover, our model for the implementation of security requirements at the system level also introduces a new actor called *IS Analyst*, which is an expert in calculating structure tools, and in updating technical plans according to the demands of the system. It can be seen that the model at this stage clearly defines how security goals can be described at the business level and how goals can be transferred into constraints at the system level.

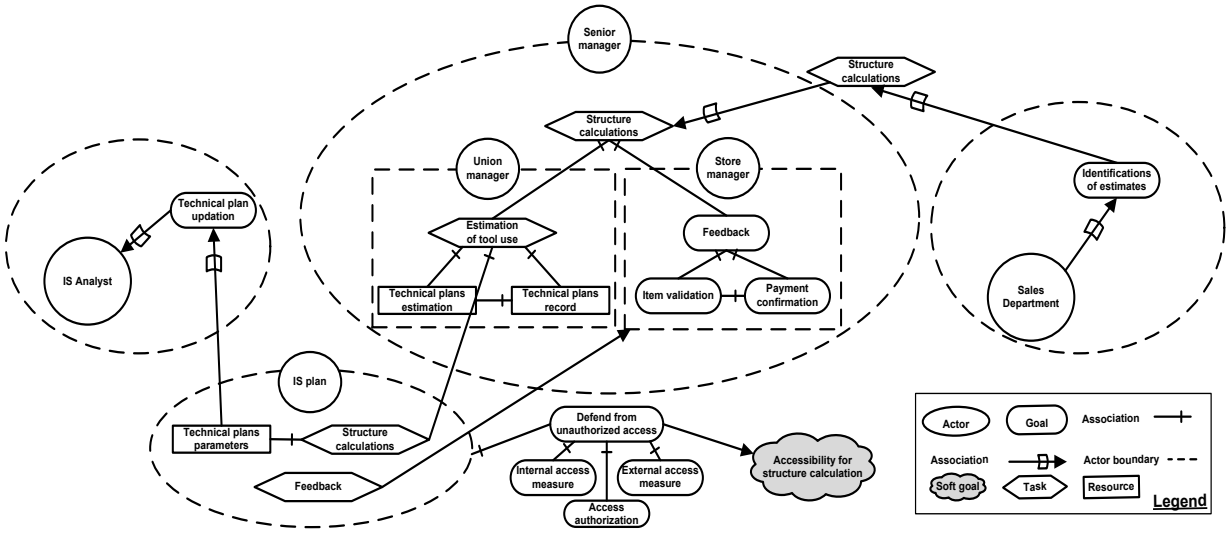

Figure 4. Constraints and security requirements

Additionally, figure 4 show that the *defend from unauthorized access* constraint can be derived from the fact where *accessibility for structure calculation* is used to represent information system resources and the resource that needs to be defended from unauthorized access. The pattern of three information security requirements is defined in this proposed case study and the pattern which contributes to the reengineering of the constraint: internal access measure, which defends the internal components of the business process such as controlling access and modifications; external access measure, which is a defense measure to ensure that external components are not able to access the information system; access authorization, which is a defense measure that acts on the system user's authentication component. These three requirements are not only suitable for the proposed case study constraints, but can also be used for others constraints in other situations.

3.5 Risks Analysis at System Architecture Level (Level 5)

The concept of managing risk analysis is well known in the literature (ISO 2004; ISO/IEC 2006; COSO 2004; ISO/IEC 2002). Risk management is a process which is continually identifying, analyzing, treating, and monitoring risk throughout the product life cycle (ISO/IEC 2006). In this section, we focus on the method of analyzing risk at the system architecture level. At this stage of our discussion, several architectural components are identified for example, the counter measures that can be used to fulfill the security requirements, as shown in figure 1 and the counter measures that can be used to identify the most adequate security requirements that are central to the method of security risk management. At this stage, we are dealing with the specific *history of managing risk* security requirement identified in the *detection of constraints and security requirement* sections. Figure 5 shows that the security requirements could be completed with the solution based on *monitoring risks through video* as well as with information technology-based solutions installed in the network, hardware, and applications for software.

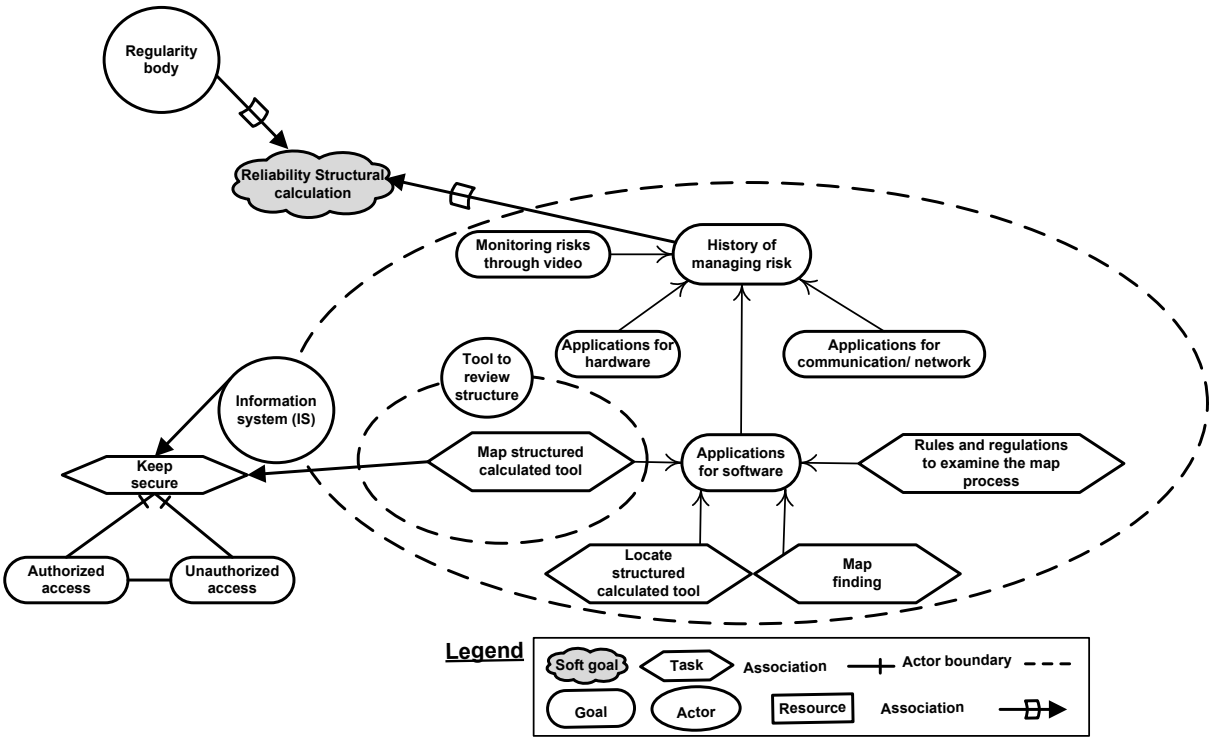

Figure 5. Risk analysis at the IS architecture level

Each control in the risk analysis model presented in figure 5 can further be categorized into sub-levels, such as control for software applications which is made up of four tasks: examine the mapping structure calculation tool; locate the data analysis tool that is used to analyze an examined event; define the rules and regulations to analyze the examined events according to possible security violations; and maintain the data analysis records after the examined event. Each control in the case study has value and cost in terms of implementation, deployment, and maintenance activities. Therefore, the security of each goal is important. The *keep secure* task in figure 5 is used to guarantee that the system activities in this proposed business process are only being used by the authorized person and to ensure the activities are secure from unauthorized access. At this stage, the security requirements have been cleared and completed at the requirements engineering level of IS development, which guarantees strong alignment between business and IS.

4 CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Information security and managing risk is a critical task in the development of secure systems and in order to protect business organizational resources in the context of alignment between business and IS. The term *alignment* refers to a process where both activities of business and IS are interrelated, with IS providing services at all levels of the business organization to enable it to effectively achieve its goals and objectives. However, this increasing use of IS at every level of the business organization increases the security threats for the organization due to the following: electronic communication between the organizational departments, storage of organizational data in the form of soft files, use of the World Wide Web, and the lack of information on security goals at the requirements engineering level of the IS. Our focus in this paper is to tackle the issue of information security at the earliest stage of IS development. The case study on the process of order management in an automobile company (Ullah & Lai 2010b) has been extended in order to validate this proposed approach. The results indicate: (1) requirements engineering in the field of software engineering is suitable to model the information security goals within the business organization. (2) It is better to model and to map the security requirements at early stage of the IS development that could guarantee a long term alignment between business and IS as well as the protection of organizational resources. (3) Security requirements must be generates from the business processes, as processes are the stable key element where the success of all others organizational components are based.

The approach has two limitations. Firstly, the approach is limited through validation of only on business process in one type of business organization, so there is a need to authenticate it with different business processes from different organizational types, as processes vary from organizational objective to objective and from organizational type to type. Secondly, the approach is limited only on identifying some important security goals and constraints due to limited space. Thus, further investigation is required in both assessing the approach with one or more industry processes in order to improve the sustainability of the approach and to enlarge the approach in regard with complete identification of security goals and constrains within the complete business organization.

REFERENCES

Byrd, A., Lewis, B.R. and Bryan, R.W. (2006). The Leveraging Influence of Strategic Alignment on IT Investment: An empirical examination. *Information & Management,* 43(3), 308–321.

Campbell, B. (2005). Alignment-Resolving ambiguity within bounded choices. *PACIS*, Bangkok, Thailand.

Campbell, B., Kay, R. and Avison, D. (2005). Strategic Alignment: A practitioner's perspective. *Journal of Enterprise Information Management*, 18(6), 653–664.

Castano, S., Fugini, M., Martella, G. and Samarati, P. (1995). *Database security.* Addison-Wesley.

Chan, Y.E. (2002). Why Haven't we Mastered Alignment? The importance of the informal organization structure. *MIS Quarterly Executive,* 1(2), 97–112.

COSO. (2004). *Enterprise Risk Management - Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission, Retrieved 05 April, 2010, from http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

Demarco, T. and Lister, T. (2003). Risk Management during requirements. *IEEE computer science*, 99-101.

Gilliam, D.P. and Feather, M.S. (2004). *Security engineering: systems engineering of security through the adaptation and application of risk management*. Pasadena, CA: Jet Propulsion Laboratory, National Aeronautics and Space Administration.

Henderson, J.C. and Venkatraman, N. (1993). Strategic Alignment-Leveraging information technology for transforming organizations. *IBM Systems Journal*, 32(1), 4–16.

ISO 15408. (2004). *Common Criteria for Information Technology Security Evaluation.* Retrieved 01 April, 2010, from http://www.commoncriteriaportal.org

ISO/IEC 17799. (2005). *Information Technology – Security techniques - Code of Practice for Information Security Management.* Geneva, Retrieved 01 December, 2010, from http://www.iso.org/iso/catalogue_detail?csnumber=39612

ISO/IEC. (2002). *Risk Management-Vocabulary-Guidelines for Use in Standards*. ISO/IEC Guide 73, Retrieved 05 June, 2010, from http://www.iso.org/iso/catalogue_detail?csnumber=34998

ISO/IEC. (2006). *Systems and software engineering - life cycle processes - risk management*. ISO/IEC 16085, Retrieved 24 April, 2010, from http://webstore.iec.ch/preview/info_isoiec16085%7Bed2.0%7Den.pdf

ISO/IEC 15408-1. (1999). *Information technology. Security techniques. Evaluation criteria for TI security. Part I: introduction and general model*. Switzerland, Retrieved 20 December, 2010, from http://webstore.iec.ch/preview/info_isoiec15408-1%7Bed3.0%7Den.pdf

Kearns, G.S. and Lederer, A.L. (2000). The Effect of Strategic Alignment on the use of IS-Based Resources for Competitive Advantage. *Journal of Strategic Information Systems*, 9(4), 265–293.

Lamsweerde, A.V. and Letier, E. (2000). Handling Obstacles in Goal-Oriented Requirements Engineering. *IEEE Transactions on Software Engineering, Special Issue on Exception Handling,* 26(10), 978-1005.

Laney, R., Barroca, L., Jackson, M. and Nuseibeh, B. (2004). Composing Requirements Using Problem Frame. *RE'04*, Kyoto, Japan.

Liu, L., Yu, E. and Mylopoulos, J. (2003). Security and Privacy Requirements Analysis within a Social Setting. *Proc. of the 11th IEEE International Requirements Engineering Conference (RE'03)*, 151-161.

Luftman, J.N., Lewis, P.R. and Oldach, S.H. (1993). Transforming the Enterprise: The Alignment of Business and Information Technology Strategies. *IBM Systems Journal,* 32(1), 198–221.

Luftman, J.N., Papp, R. and Brier, T. (1999). Enablers and inhibitors of business-IT alignment. *Communications of the Association of Information Systems,* 11(1), 1–33.

McKeen, J.D. and Smith, H.A. (2003). *Making IT Happen: Critical issues in IT management*. John Wiley & Sons, England.

Mouratidis, H., Giorgini, P. and Manson, G. (2003). Integrating Security and Systems Engineering: Towards the Modelling of Secure Information Systems. *Proceedings of the 15th Conference on Advance Information Systems (CAiSE '03)*, p. 16-20, Austria.

Pollalis, Y.A. (2003). Patterns of co-alignment in information-intensive organizations: business performance through integration strategies. *International Journal of Information Management*, 23(6), 469-492.

Reich, B.H. and Benbasat, I. (2000). Factors that Influence the Social Dimension of Alignment between Business and Information Technology Objectives. *MIS Quarterly,* 24(1), 81–113.

Silvius, A.J.G., Haes, S.D. and Grembergen, W.V. (2009). Exploration of cultural influences on Business and IT alignment. *Proceedings of the 42nd Hawaii International Conference on System Sciences*, p. 1-10, Waikoloa, Big Island.

Ullah, A. and Lai, R. (2010). A requirements engineering approach to improving IT-Business alignment, *Proceedings of ISD, 19th International Conference on Information Systems Development*, p. 1-9, Prague, Czech Republic: published in Springer Computer Science Lecture Notes.

Ullah, A. and Lai, R. (2010). Modeling Business Goal for Business/IT Alignment Using Requirements Engineering, *accepted by the Journal of Computer Information Systems (JCIS),* Will appear in an issue of 2011.

Yu, E. (1995). *Modelling Strategic Relationships for Process Reengineering, Ph.D. thesis, also Tech. Report DKBS-TR-94-6*, Dept. of Computer Science, University of Toronto.

Yu, E. and Mylopoulos, J. (1994). Understanding 'Why' in Software Process Modelling, Analysis, and Design. *Proc. 16th International Conference on Software Engineering*, p. 159-168, Sorrento, Italy.