2010

Collaborative risk method for information security management practices: A case context within Turkey

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Sevgi Ozkan
Middle East Technical University

Recommended Citation

Karabacak, B., & Ozkan, S. (2010). Collaborative risk method for information security management practices: A case context within Turkey., *30* (6), 567-572. https://doi.org/10.1016/j.ijinfomgt.2010.08.007

International Journal of Information Management xxx (2010) xxx–xxx

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Case study

Collaborative risk method for information security management practices: A case context within Turkey

Bilge Karabacak[a,b], Sevgi Ozkan[a,*]

[a] Informatics Institute, Middle East Technical University, Ankara, Turkey
[b] Scientific and Research Council of Turkey, Ankara, Turkey

ARTICLE INFO

Article history:
Available online xxx

Keywords:
ISO/IEC 27001:2005
ISO/IEC 27002:2005
Information security
Risk analysis
Flow chart
Case process approach
Information security governance

ABSTRACT

In this case study, a collaborative risk method for information security management has been analyzed considering the common problems encountered during the implementation of ISO standards in eight Turkish public organizations. This proposed risk method has been applied within different public organizations and it has been demonstrated to be effective and problem-free. The fundamental issue is that there is no legislation that regulates the information security liabilities of the public organizations in Turkey. The findings and lessons learned presented in this case provide useful insights for practitioners when implementing information security management projects in other international public sector organizations.

1. Introduction

Public organizations in Turkey have been showing an increasing interest in information security standards since 2005 with ISO/IEC 27001:2005 and ISO/IEC 27002:2005 as the two most widely available and adopted. ISO 27001 provides a model for setting up and managing an effective Information Security Management System (ISMS). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. Thus, the most crucial step to fulfill these requirements is to perform a risk analysis with respect to business risks. ISO 27001 does not recommend a specific risk analysis method; rather it just states it to be a mandatory process by the requirement to "define a systematic approach to risk assessment".

Previous research emphasize that information security is not only a technical matter as Solms notes "Not realizing that the protection of information is a business issue and not a technical issue" (Solms & Solms, 2004). Therefore, to achieve information security, organization culture must be changed and executives must take part in processes related with information security. ISO 27001 has been developed considering these issues, where it is not a technical standard but rather a business standard that helps establishing an infrastructure for improving information security continuously in an organization.

According to Solms (2001), information security is a multi-dimensional discipline incorporating *corporate governance*. The information possessed by organizations is among its most valuable assets and is critical to its success. The top level management, which is ultimately accountable for the organization's success, is therefore responsible for the protection of its information (Solms, 2001).

The important aspect of information security governance, which is crucial for enterprise wide effectiveness of information security, is the responsibility of top level management. Information security governance must be an integral and transparent part of corporate governance and should be aligned with the corporate governance framework.

Legal dimension, without which information security governance cannot be achieved properly, is another important dimension (Solms & Solms, 2004; Solms, 2001). In developed countries, required legislation for information security that affects the public organizations has already been enacted. However, Turkey does not have a legislation that obligates the public organizations to obey information security principles. Due to the lack of legislation, the interests to ISO 27000 series standards are not enterprise wide; rather they originate – as a result of the need to operate more securely – from the Information Processing Departments (hereafter IPDs) of public organizations.

Efforts of the IPDs on their own to establish enterprise-wide information security management are not sufficient. In this study, a collaborative information security risk management method is proposed for IPDs of public organizations. This method has been developed based on the findings from eight ISO/IEC 27001:2005

* Corresponding author.
E-mail address: sozkan@ii.metu.edu.tr (S. Ozkan).

0268-4012/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ijinfomgt.2010.08.007

based information security management projects. These eight cases reveal a common outcome: the lack of the information security legislation in Turkey affected the projects negatively. It is believed that the proposed risk management method would be useful for public organizations in other countries where, similar to Turkey, effective information security management legislation is not enacted. The proposed method is applied to a case in Turkey.

2. Information security management projects within public organizations in Turkey

In Turkey, there is no legislation that regulates the information security liabilities of public organizations. As stated in the OECD e-government studies report, a comprehensive regulatory approach to electronic data and transactions is needed in Turkey (OECD Report Turkey, 2007). Turkey's public sector has a tradition of passing legislation rather than using secondary regulations to interpret basic legislation. The legislative approach to ensuring proper functioning, equity and fairness in the public sector is slower and more difficult to change – and thereby less responsive – than using a framework of secondary regulations to guide e-government implementation in a context of technological and process change. According to the OECD survey, 75 percent of the respondents that are the workers of central government think that Turkey has regulatory challenges for e-government (OECD Report Turkey, 2007). Respondents believe that legislation prevents collaboration, it is complex and burdensome and it lacks of recognition of e-government processes. Consequently, information security governance principles cannot be fully applied within the public agencies where top level management does not have any formal, regulatory and explicit roles and responsibilities for information security. Generally, top level managers do not obey due care principles of information security (Solms & Solms, 2004).

One of the most important negative impacts of lack of legislations is that there is no formal human resource infrastructure for information security management in most of the public organizations in Turkey. In some of the public organizations, IPDs of have been the only initiatives of enterprise-wide information security implementation. Since IPDs do not have this role by legislation, approximately five percent of Turkish public organizations understand the need for, and therefore accept to implement enterprise-wide information security. Consequently, the scope and affect of these implementation efforts of IPDs reveal many problems.

The authors of the paper have been conducting information security management projects for public organizations in Turkey since 2005. In this paper, eight projects are investigated together with the discussion of problems that were encountered during the project implementation process. IPDs of these eight organizations (names have been kept anonymous due to confidentiality agreements) initiated enterprise-wide information security implementations under the guidance of ISO 27001. These eight cases have common problems and they all failed to perform an enterprise-wide information security implementation.

In all of the organizations, the project owners were IPDs. This means project requests originated within these departments and the projects were conducted by IPD staff. In four of these projects, the scope was the whole organization and in the rest four, the scope was the IPDs only. The top level managers of the four public organizations were aware of the project, whereas top management of the other four organizations was not even informed about the project. Four of these public organizations were financial institutions and the remaining four are active in the following domains: justice, ministry, regulatory body, auditing.

The projects have been conducted following the eight common implementation steps of ISMSs. ISO 27001 adopts the "*Plan-Do-Check-Act*" (*PDCA*) model, which is applied to structure and to ensure continual improvement of all ISMS processes. "*Plan*" of PDCA model comprises first five steps: (1) Determination of scope, (2) The determination and valuation of assets within the scope, (3) The determination and valuation of threats that exploits vulnerabilities, (4) The determination of vulnerabilities of assets, (5) The determination and prioritization of risk. The remaining three are as follows: "*Do*" corresponds to step (6) The determination and application of countermeasures; "*Check*" corresponds to step (7) The determination and application of corrective and preventive actions; and "*Act*" corresponds to step (8) Checking the effectiveness of countermeasures and performing internal audit.

The authors of this paper have given consultancy on each step of the project and the employees of the organizations were the main executers of the projects. In all of these organizations, core business processes are implemented by IT systems with more than one database and application servers. For most of the critical applications, servers are accessible via the Internet. All of the organizations have standard security products like firewall and antivirus software.

3. Problems encountered

IPD was the project owner in all of the organizations, which was a problem especially for the projects having a scope of the whole organization. This additionally caused a number of potency problems during the projects. One problem was that in all of the organizations, IPDs did not have sufficient and needed power to implement most of the security countermeasures. Another problem was, because core business processes are implemented by IT systems, a clear distinction between the IPD and the other business departments could not be achieved. Thus, similar potency problems occurred in the organizations.

Even for the organizations in which top level managers were aware of the projects, management support and involvement could not be achieved both for the project itself and for the procurement and application of the countermeasures. It has been identified that top level management and even the owner of the projects, i.e. IPDs, had the misunderstandings such as:

1. Information security management is a technical concept and totally related with IT.
2. Information security management should be confined with IPDs only.
3. The head of the IPD should be responsible for enterprise-wide information security.
4. Information security management can and should be achieved by the consulting firm.

In all of the eight cases, the information security management process could not be implemented effectively mainly due to the lack of support and involvement of top level management. In all eight cases, there was no *formally appointed* staff for the projects. Informal participation of staff was not sufficient due to low staff-hours (i.e. approximately 6 person-hours) per week allowed. The percentages of countermeasures that are applied during the project are quite low (5% or lower in three organizations and between 10% and 50% in the other five) because only the ones that had no or minimal cost to organization and that did not impact the whole organization could be applied.

Apart from these fundamental problems, a number of secondary problems were confronted in projects. During the determination and valuation of assets, authors realized that only tangible assets

Please cite this article in press as: Karabacak, B., & Ozkan, S. Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management* (2010), doi:10.1016/j.ijinfomgt.2010.08.007

like hardware and software are listed in almost all of these eight projects. For the "information" security projects, the most crucial assets are "information" assets, which are intangible. Without taking "information" into consideration, the asset inventory cannot be established reliably and the values of assets cannot be determined correctly. The vulnerabilities in assets, the threats that exploit these vulnerabilities are determined by using asset inventory. Thus, a tangible asset inventory would cause an incomplete risk analysis focusing only on technical dimensions of information security disregarding the social and non-technical dimensions.

In fact, the above-mentioned problems were consequences of a more fundamental issue in all eight cases: all of the organizations had their IT processes undocumented. Furthermore, both the technical staff and the managers of IPDs were not neither aware nor knowledgeable about the intersection of business processes and IT processes.

Due to these problems, in none of the eight projects, all implementation steps were accomplished. Only the first five steps, which belong to the "planning" phase of PDCA cycle, were implemented. At the sixth step, some of the countermeasures identified would have some cost and top level management did not allow spending for these countermeasures. For example, most of the organizations have weak password policies. Implementing strong password policy is an easy configuration from the perspective of IPD. However, the effects of this change would require some extra effort by computer users including top level managers. These changes could not be made due to the pressure from other departments and managers of the organization. Since most of the crucial countermeasures could not be implemented in step 6, the projects discontinued at this step leaving steps 7 and 8. The initial aims of the projects were not achieved and an information security management system (ISMS) could not be established in any of the cases.

Information security management projects within eight public organizations in Turkey have proved that, standards like ISO/IEC 27001:2005 does not ensure the establishment of an ISMS by itself. In order to have an effective ISMS that covers the whole organization, information security governance principles should be in place in the organization. ISO 27001 comprises what to do about the constitution of information security management and assumes that information security governance exists in the organization. Therefore, existence of information security governance, whose principles can be applied by enacting required legislation, is a prerequisite of ISO 27001.

It is important to mention that there are some positive issues: these eight institutions were the first eight public organizations that requested to establish ISMS, pioneering the realization of information security governance in public institutions in Turkey.

4. Risk analysis methods for information security

Risk analysis, which is defined as the systematic use of information to identify sources and to estimate the risk, is a preliminary to risk management. If risk analysis is not performed properly, the selection of countermeasures will fail, and risk management process cannot be successful. Generally, risk analysis is a rather complicated process because the risks are based on probability. The complexity of the risk analysis process has become much more pronounced when information and communication technologies became widely used. In terms of information technologies, risk is not a simple probabilistic value. It is the probability of a threat successfully attacking an asset via a particular vulnerability. Thus, risk depends on three inputs, asset, vulnerability and threat.

$$\text{Risk} = f(\text{asset, vulnerability, threat}) \quad (1)$$

Function f given in the formula (1) shows an abstract risk model, it has three inputs and one output; risk. There are some other reasons for the particular complexity of information security risk analysis. First of all, information is one of the most fundamental and important assets for companies. Thus, peculiar attention should be given to information assets while performing risk analysis. However, information is an abstract asset. Information can exist in many forms, electronic, hard copy, verbal etc. Information does not have the capability of protecting itself against malicious actions. Apart from information, hardware, software, storage media, humans and hardcopy documents are assets as well. Another reason for the difficulty of information security risk analysis is the correlations between these asset categories. Vulnerability in an asset may turn into a threat for the other assets. As an example, a computer virus may use the vulnerability of outdated computer virus database. However, information, software, humans and company reputation may suffer from computer viruses. Reputation is just another abstract asset like information. Its value cannot be measured in monetary terms. Risk analysis methods for information security would need to answer all of these challenges.

There are two types of risk analysis methods; quantitative risk analysis methods contain mathematical instruments to evaluate risk, qualitative risk analysis methods do not contain any mathematical instruments. Some of the quantitative tools, which can be used in a risk analysis process, use complex mathematical tools like Bayesian networks, fuzzy logic, simulation and fault trees; which are advanced and comprehensive to model specific risk situations in depth. Generally, these tools require tremendous mathematical calculation to be fit into the information security area that spans wide risk scenarios. There are a number of quantitative methods proposed for the information security risk analysis process in the academic studies which usually detail into specific problem areas and try to solve problems by suggesting specific and effective solutions for the specified problem area. However, public organizations require simpler, more generic and collaborative methods (Tong, Fung, Huang and Chan, 2003).

The foremost requirement to ensure information security management in public organizations is *staff involvement*. It cannot be assured by a third party company or a consulting firm; rather it is a continual process. Information security plan must be based on the identified risks (Solms & Solms, 2004) 0. The risks and their levels are determined within the risk analysis process. Thus, qualitative tools or quantitative tools that do not have complicated mathematical instruments would be best suitable for public organizations. Further, risk analysis methods for information security management should have the capability of determining the processes within the scope, the assets within the processes, the vulnerabilities of the assets, the threats and finally the risk. The methods that have heavy quantitative tools may fail during the modeling process.

5. Proposed information security risk management method

The actual remedy for the aforementioned problems is to have information security legislation that urges the top level management to take responsibility on information security issues. In Turkey, the IPDs of public organizations show interest in information security management and specifically in information security risk analysis projects. However, in the short term, the information security legislation is not expected to be enacted in Turkey. Therefore, an effective and problem-free risk management method is necessary for public organizations willing to implement information security management projects.

"Information security is not a technical issue, rather it is a social/business/regulatory issue" (Solms & Solms, 2004; Solms,

Please cite this article in press as: Karabacak, B., & Ozkan, S. Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management* (2010), doi:10.1016/j.ijinfomgt.2010.08.007

2001). However, in practice, as evident from the eight cases investigated, information security is perceived as solely technical concept confined within the IPDs. The authors have come across a number of vulnerabilities at IT services in these cases. Although all of the eight organizations have standard firewall and antivirus products in place, the security policies of firewall were not strict and virus databases were out-of-date. This is one of the many outcomes of not having an enterprise-wide ISMS which ensures continuous improvement of security processes. However without clearly defined roles and responsibilities including top level management's, establishing and maintaining an enterprise-wide information security management system is almost impossible without legislations and corporate governance as it has been observed during the eight projects. In that regard, the proposed method aims to establish an information security management system within IPDs of public organizations, not targeting the whole organization.

The problems that are directly related with the lack of information security governance principles can be solved by the enactment of information security legislation. As a workaround solution to these problems, the scope of the information security management project should be "the activities of the IPD". These activities are directly related with the IPD and do not have strong relation with the core business processes. By doing so, the IPD can conduct a risk analysis process, take countermeasures and finally establish an information security management system by itself. At the beginning of the project, the scope should be determined carefully so that IPD can implement PDCA cycle by itself. Within this scope, the activities of IPD may have relations with the other business processes; for example, managing user accounts in LDAP server, configuring routers and switches, managing databases, etc.

Another problem observed is related with the features and ease of use of the risk analysis method within risk management. This can be solved by modeling the activities of information processing department, in other words by enabling process modeling within the scope. Risk analysis method for ISO 27001 based information security management projects should have the capability of determining the processes within the scope, the assets within the processes, the vulnerabilities of the assets, the threats and finally the risk by using simple qualitative tools. A method which has these properties will also contribute positively to the participation of the staff. In the light of these findings, in the proposed method, the first of eight ISMS implementation steps has been replaced by two steps: (1) The scope: the activities of IPD and (2) The determination and modeling of the processes. This helps IPD to take countermeasures easily and run PDCA cycle by itself.

6. Case analysis

The organization's information technology infrastructure comprises the following. Employees use thin clients. All of the applications and files are hosted at terminal servers. Database servers, e-mail servers and domain controllers use disk arrays. The data at disk arrays are backed up by backup server. There is one firewall, one intrusion detection system and one antivirus server for the security needs. There is one web server at the DMZ section. Web server is accessed from the Internet. This information system is operated by five system administrators. One for database server, one for disk array and backup server, one for domain controllers, web servers, one for network devices and security services and one for terminal servers and thin clients. Information security was not considered systematically in the design of this system like the PACS (Tong et al., 2003).

The implementation of the proposed risk analysis method lasted about four weeks from scratch. Initially, a risk analysis team comprising five system administrators was formed. The team members were trained before starting the project so that they worked without any ambiguity during the entire process. They were involved with the determination and valuation of the assets, vulnerabilities, threats; and with the risk assessment process and countermeasure selection.

Scope is the area in which the risks are identified. The determination of scope is a requirement of ISO/IEC 27001:2005. The scope defines the activities, functions and services to be provided to internal and/or external customers. Thus, scope draws the frame of the risk analysis. In our case study, the scope is selected as "the activities of the IPD" as stated in the proposed method.

In the second step, *processes are determined and modeled*. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. The design and implementation of an organization's ISMS is influenced by the processes within the organization. A process can be seen as a value chain by contributing to the creation or delivery of a product or service. Seven processes are determined within the scope: (1) *Network*, (2) *Substructure*, (3) *Security*, (4) *Terminal*, (5) *Storage*, (6) *Backup*, and (7) *Database*. *Network* process includes operation and maintenance of switches, routers, communication cables. *Substructure* process composed of active directory, DNS, DHCP, WINS and web server. *Security* process composed of firewall, intrusion detection system and antivirus. *Terminal* process includes terminal servers and thin clients. *Storage* process composed of disk arrays. *Backup* process composed of backup software and hardware. Finally, *database* process includes database servers and corresponding client side applications.

Fig. 1 depicts details of the *database* process only. The remaining six processes were modeled using a similar approach.

Database process is modeled by using flowchart techniques. The basic flowchart (Level 1) depicts the following activities visually: computer user enters data to database server by using web application. While performing this operation, he uses his computer/thin client. The data goes through the transmission lines. Data goes through the application server before written onto the database. Level 1 is composed of seven assets within the process. Thus, *assets are determined while modeling the process*. The flowchart at Level 1 shows what information processing elements are used within the database process. The processes of IPDs can be easily modeled as in Fig. 1 by using flow chat techniques since IT processes are not as complicated as core business processes. Because the method is collaborative, a complicated process modeling technique is not preferred. Flow charting is a well-known and widely used modeling technique. The advantages of flowcharts center on their ability to show the overall structure of a system; to trace the flow of information and work; to depict the physical media on which data are entered, produced, and stored; and to highlight key processing and decision points (Giaglis, 2001) 0. These are important features for information security management.

In the proposed method, two independent *asset valuation* criteria are used. The first one captures qualitative information and determines the impact of the abuse of the asset on confidentiality, integrity and availability scaled in four levels from "low" to "very high". The other criterion depicts quantitative information and it is the total monetary loss if the asset is abused where each of these four levels corresponds to monetary values. The value of an asset is the "total" monetary cost if it is abused. For instance, when the backbone switch is damaged, both the cost of the switch and the cost of unavailable business activities during interruption should be considered. The value of an asset is totally independent from the confidentiality, integrity and availability values. One asset may affect the confidentiality and integrity significantly, but its value may be low.

Please cite this article in press as: Karabacak, B., & Ozkan, S. Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management* (2010), doi:10.1016/j.ijinfomgt.2010.08.007

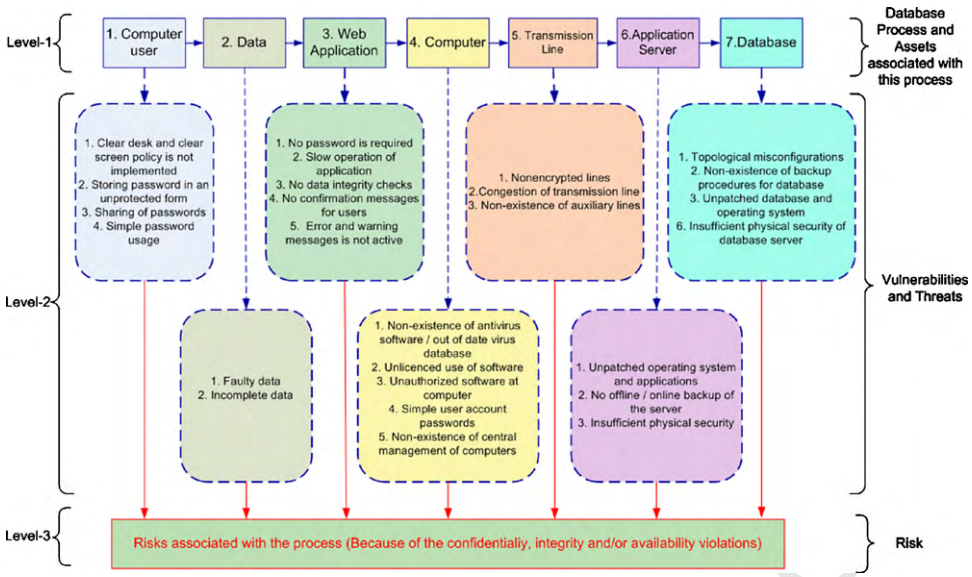

Fig. 1. Assets, vulnerabilities and threats for the database process.

These monetary values have been determined by the representatives of the organization and are dynamic in content as they can be altered according to the budget of the organization. Also, the security requirements of the organizations may vary. All of the results of asset determination and asset valuation processes have been entered in spreadsheets and an asset classification report is produced.

After determining and valuation of assets, *the vulnerabilities of assets within each process and the threats that exploit the vulnerabilities are determined*. This is shown as Level 2 in Fig. 1. By taking the values of assets, the criticality of vulnerabilities, the strengths of already used countermeasures and the nature of threats into consideration, the likelihoods and impact levels of threats are determined. Depending on the *likelihood* (e.g. "low" if 'less than once per year', "very high" if 'greater than once per day') and the *impact* (e.g. "very high" if 'damage caused may not be compensated and it is organization wide'; "low" if 'damage caused may be compensated in the short term and the threat prevalence is the department') of the threat, *risk values are determined*. This part of the method corresponds to the Level 3 of Fig. 1. The risk method for determining the risk level is shown in Formula 2, which is a well-known and widely used risk basic model. "*Likelihood of threat*" and "*the impact level of threat*" parameters are shown explicitly in Formula 2. The other parameters "*asset value*" and "*vulnerability level*" are implicit parameters. These parameters change the levels of explicit parameters shown in the Formula 2, hence they change the risk value as well. The values of risk are dynamic and may be altered in order to reflect the specific security requirements of the specific organization.

$$\text{Risk} = \text{likelihood of threat} * \text{the impact level of threat} \quad (2)$$

The risk values that are determined together with the representatives of the organization are raw values and are unrefined, which cannot be interpreted in their current form. These risk values need to be prioritized according to the predefined criteria of organization. The criteria to be considered for *risk prioritization process* were the security requirements of organization, the cost of countermeasures, the budget of organization and the usability and the operability of the countermeasure – these were determined collaboratively with the involvement of employees of the organization. There are two fundamental explicit inputs for determining priority: the *cost* and the *importance* of the countermeasure. The importance is determined by taking the risk analysis result and the security requirements into account. The cost includes the price of the planned countermeasure, and the operation and setup costs. The budget of the organization also contributes to this value. Priority level is determined by assessing these parameters. For example, if both the cost and the importance of the risk are "very high" than its priority is assigned as "very high" and vice versa. Risk prioritization – done in line with the organization's needs – stands between risk analysis and determination of countermeasures. After risks are prioritized, countermeasures were determined collaboratively with the involvement of the organization staff.

Upon the completion of the risk analysis and prioritization processes, a total of 115 risks have been identified in all of the seven processes within the scope of this case study. Three percent of these risks are very high. The majority of the risks are high (35%), medium (27%) and low (35%) level risks. The risks with very high values are: "the existence of shared administrator accounts", "the lack of password policy within the active directory system" and "the existence of a server behind the firewall instead of the DMZ, which is accessed from the Internet". Countermeasures for two of these can be implemented by the IPD. "The lack of password policy" is not implemented because the affects of corresponding countermeasure spans the whole company. Countermeasures are implemented for most of the risks within processes – i.e. ranging from 60 to 100% for each process. In total, for all seven processes, 82% of the determinate countermeasures are applied. The remaining 18% of countermeasures are not implemented due to high costs or countermeasure's wide range of effect. When compared with the common eight-step ISMS implementation method where at most 50% of the countermeasures were implemented, the proposed risk assessment method proves itself as more effective.

Countermeasures selection is one of the most crucial steps of the ISMS establishment process, because countermeasures help either to decrease the risk level or to eliminate the risk. Security countermeasures may be established for formulating an effective overall security solution to address threats at all layers of the information infrastructure (Kim & Lee, 2005). Kim and Lee (2005) propose a method for the selection of countermeasures. In their method, information value, threat level, security services, the scope of security services are considered for selection of both technical and non-technical countermeasures. In our case study, the same factors were taken into consideration for the selection of countermeasures.

Please cite this article in press as: Karabacak, B., & Ozkan, S. Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management* (2010), doi:10.1016/j.ijinfomgt.2010.08.007

Additionally, ISO 27002 was an important resource utilised. This standard has 133 high level countermeasures that cover both internal and external threats. Yeh and Chang (2007) also emphasize the importance of this standard. Except for externally requested regulations, such as privacy laws or government regulations, firms mostly determine their security policies and procedures internally (Yeh & Chang, 2007). The selection process took as much time as the other steps of case study, during which both the staff of the organization and the consultants as external factors were involved.

As final remarks of the case study, ISO 27004 has been referred to for validation of the effectiveness of countermeasures. After setup and application of countermeasures, an internal audit is performed by a team whose members were not involved in the implementation project. After completion of the internal audit, corrective and preventive actions have been determined and taken.

7. Discussion and conclusion

The case study implementation has demonstrated that, the proposed risk analysis method is in line with the nature of information security risk analysis. It brings a systematic and structured approach to risk analysis. More importantly, it is *collaborative* allowing effective involvement, i.e. discussions, decisions, etc. of the employees in the information security risk analysis process. As discussed previously, complicated mathematical and statistical tools would have limited use in modeling the risks of information security in public organizations.

Unlike most of the information management projects where asset inventory is performed right after the determination of the scope; the proposed method suggests determining and modeling processes before creation of asset inventory. Because processes are composed of assets, having well-defined processes beforehand enables determining assets easily and completely, capturing all tangible, i.e. hardware/software, and intangible, i.e. information assets.

The proposed method provides a "suggested scope". The experiences from the eight public cases show that requests arise from the IPDs and that scope has to be determined carefully. Thus, "the activities of IPD" is a well-refined scope in order to establish a PDCA cycle within the IPD.

The official ISO/IEC 27001:2005 route can be very difficult because of its "all-or-nothing" design and an incremental approach to certification is suggested (Solms & Solms, 2001). It is believed that it would be possible to cover all of the sections of ISO/IEC 27002:2005 with the proposed method within the scope of "the activities of the IPD".

Our collaborative process-based risk analysis reveals crucial IT processes within its scope and analyzes the risks associated with these processes. Traditionally, a great deal of attention is focused on efforts that address the risks affecting business information from an IT infrastructure point of view (Posthumus & Solms, 2004). The proposed method does not put an emphasis on technical items such as servers and software, rather, it accents business processes.

It is believed that the proposed risk management method would be useful for public organizations in countries where effective information security management legislation has not yet been enacted like Turkey. This method may be beneficial for the adaptation of the IPDs to new governance principles after possible enactment of legislation in the near future.

References

Giaglis, M. G. (2001). A taxonomy of business process modeling and information systems modeling techniques. *The International Journal of Flexible Manufacturing Systems*, *13*, 209–228.

Kim, T., & Lee, S. (2005). Design procedure of IT systems security countermeasures. *Computational Science and its Applications*, *3481/2005*, 468–473.

(2007). *OECD e-Government Studies – Turkey*. , ISBN 978-92-64-02844-9.

Posthumus, S., & Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*, 638–646.

Solms, B., & Solms, R. (2001). Incremental information security certification. *Computers & Security*, *20*(4), 308–310.

Solms, B., & Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*, 371–376.

Solms, B. (2001). Information security – A multidimensional discipline. *Computers & Security*, *20*, 504–508.

Tong, C. K. S., Fung, K. H., Huang, H. Y. H., & Chan, K. K. (2003). *Implementation of ISO17799 and BS7799 in picture archiving and communications system: Local experience in implementation of BS7799 Standard*. International Congress Series 1256. pp. 311–318.

Yeh, Q., & Chang, A. J. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, *44*, 480–491.

Please cite this article in press as: Karabacak, B., & Ozkan, S. Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management* (2010), doi:10.1016/j.ijinfomgt.2010.08.007