DEVELOPING AN INFORMATION SECURITY MANAGEMENT FRAMEWORK: CASE STUDIES ON REGISTRATION OFFICE AND COMPUTER CENTER OF A STATE UNIVERSITY

Thesis submitted to the
Institute for Graduate Studies in Social Sciences
in partial satisfaction of the requirements for the degree of

Master of Arts
in
Management Information Systems

by

Gökhan Ergen

Boğaziçi University
2007

The thesis of Gökhan Ergen

is approved by:

Associate Professor, Birgul Kutlu …………………………………………...
(Thesis Advisor)

Professor, Meltem Özturan ……......……………………………………….

Professor, H. Levent Akın……..................……………………………………

September 2007

ACKNOWLEDGEMENT

I would like to thank to my thesis advisor, Birgül Kutlu for her encouraging calmness, unlimited patience and admiring kindness.

I would also like to thank to my lecturer and my manager Tamer Şıkoğlu, for his support and leading.

I would like to my Seyhan Sertoğlu, my soul mate, for her continuous but necessary pokiness and for her priceless efforts.

I feel very lucky for myself to have such a supporting family. Their support was essential for me.

I would like to dedicate this study to my former advisor Tolga Ulus. His undying spirit has provided me the courage throughout two years to complete this thesis.

ABSTRACT

Developing an Information Security Management Framework: Case Studies on Registration Office and Computer Center of a State University

by

Gökhan Ergen

Information Technology (IT) provides a wide range of benefits for the companies as well as organizations and institutions. Obtaining fast, efficient and effective operations are among the main benefits. On the other hand, the workflow of business in companies, organizations and institutions are mainly handled via computers; the data are recorded, processed by state-of-art systems and distributed to individuals via fully integrated networks. However, since all data is electronically stored and transferred, maintaining the security of data has become a primary subject for the owners and users of the data. Security breaches, resulting in huge amounts of financial losses and eventually in enforcement of several regulations force information owners to build sound information security systems as well as IT infrastructures. Concurrently, the managerial aspects of these systems have also become one of the main topics for the top management. The aim of this study is to constitute a basic information security management framework based on the standards BS 7799/ ISO 17799 and to apply it via case studies. For the application of the framework, two case study subjects are selected; one registration office and one computer center of a state university. Based on the framework proposed, the information security practices of these two entities are evaluated.

KISA ÖZET

Bir Bilgi Güvenliği Çerçevesi Oluşturmak: Bir Devlet Üniversitesinin Kayıt Bürosu ve Bilgi İşlem Merkezi üzerine Vak’a Çalışmaları

Gökhan Ergen

Bilgi Teknolojisi (BT) şirketlere olduğu kadar organizasyonlara ve kurumlara çok geniş faydalar sağlar. Hızlı, etkin ve etkili operasyonların elde edilmesi bu geniş faydalar arasında sayılabilir. Öte yandan günümüz şirketlerinde, organizasyonlarında ve kurumlarında bulunan çalışma ortamındaki iş akışları bilgisayarlarla takip edilmekte; veriler son teknoloji sistemlerle kaydedilmekte, işlenmekte ve ilgili bireylere tümüyle entegre ağlarla dağıtılmaktadır. Öte yandan, tüm veriler elektronik olarak kaydedilmekte ve transfer edilmekte olduğundan, verilerin güvenliğinin sağlanması, veri sahipleri ve kullanıcılar için en önemli konu haline gelmiştir. Yüksek miktarlarda finansal kayıplara ve sonunda bir çok kanunun yürürlüğe konmasına neden olan güvenlik ihlalleri, bilgi sahiplerini BT altyapıları kadar sağlam bilgi güvenliği sistemleri kurmaya da zorlamıştır. Aynı zamanda, bu sistemlerin yönetimiyle ilgili durumlar da üst yönetim için en önemli konulardan biri haline gelmiştir. Bu çalışmanın amacı BS 7799/ ISO 17799 standartlarına bağlı olarak bir bilgi güvenliği yönetimi çerçevesi oluşturmak ve bunu vak’a çalışmaları ile uygulamaktır. Çerçevenin uygulanması için iki vak’a çalışması hedefi belirlenmiştir. Bunlar bir devlet üniversitesine ait kayıt bürosu ve bilgi işlem merkezidir. Öne sürülmüş çerçeve ile bu iki kurumun bilgi güvenliği uygulamaları değerlendirilmiştir.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Today's daily life, as well as the business life, mostly depends on two main assets; information and technology. The former provides the insight and method to reach at a desired result, while the latter provides the backbone for the means to the end. These two assets may unite in most of the cases and called as "Information Technology" or as "IT" which is a term whose importance is well known by most companies.

Mainly IT has two facilitating roles in business life; one as a facilitator of business operations and the other as a facilitator of competitive advantage. It is crucial for this study to expand the meanings under these two roles.

It's been a great jump from paperwork to computerized systems for the business since the very first development of computers. Execution of most of the time consuming operations has been transferred to sophisticated software systems and nearly all of the business operations are integrated with each other by deployment of computer hardware, databases, networks, telecommunications, data warehouses and centralized accounting systems such as Enterprise Resource Planning (ERP) systems (Cerullo et al, 2003). The more the departments are integrated, the more the business operations became effective.

Since IT increase the effectiveness of the companies and render them more profitable, the second facilitating role of IT becomes clearer; companies with complex and integrated IT systems have more competitive advantage over the ones that don't have. This competitive advantage is not only fed by the internal information and knowledge generated by the companies themselves; the successful companies also utilize global network infrastructures in order to gain access to more information relevant to their business. Global network infrastructures, such as the Internet, have led to instantaneous business communications and the utilization of high volume databases are observed more frequently, in parallel to the memory storages becoming more common and cost effective (Eloff et al, 2005).

However, most of the companies which did not pay enough attention to the use of security systems for their IT have suffered from serious security incidents, resulting in non-operative systems and even loss of critical business data. In PWC's Global State of Information Security Survey (Lobel, 2006), it is found out that 22 percent of the 7791 companies surveyed respond that they lost more than $100,000 due to cyber attacks. This is an indication of the fact that without implementing solid and effective information security solutions, IT itself is of no good to companies and may even cause harm to them.

It should be noted that, this study approaches the concept of information security from a managerial perspective. Therefore, although the proposed framework controls include some technical issues (such as digital signatures, antivirus software, etc), the aim is not to bring forward technical solutions, but to harmonize the management related literature studies in order to propose a management framework.

In this study, the definitions related to information security are given first. Afterwards, the need for information security is summarized and supported with two main instances of regulations, one global regulation and one local regulation. Then, information security related standards are presented at the conclusion of the literature survey.

An ‘Information Security Management Framework’ is developed based on the information obtained through the literature review and based on the ISO/IEC 17799 / BS 7799 standards which are going to be referenced as BS 7799/ ISO 17799 hereafter. In order to test this framework, a questionnaire is prepared. As case studies, this questionnaire is applied to two different entities of a state university; registration office and computer center. Lastly, the results which show the conformance level of these two entities to the proposed framework are compared and discussed.

CHAPTER II

LITERATURE REVIEW

Definitions

In order to comprehend the content of information security and establish a framework based on the practices and theories behind, it is crucial to mention about definitions related to it. Three main concepts are going to be explained, including 'Information Security' itself, with contribution of several articles on the subject.

Information Security

Information Security can simply be defined as "the preservation of confidentiality, integrity and availability of information" (ISO/IEC, 2000, p 1). The details of this definition lie under the definitions of the components of information security, which are 'Confidentiality', 'Integrity' and 'Availability'.

Confidentiality ensures that information is provided to the parties on a need-to-know basis (Ezingeard et al, 2005) and is not accessible by or disclosed to unauthorized individuals, entities or processes (ISO/IEC, 2004).

Integrity ensures that the accuracy and completeness of information is protected against deletion or corruption (ISO/IEC, 2004), either intentionally or unintentionally (Ezingeard, et al, 2005).

Availability ensures that authorized individuals, entities or processes can access information on a timely manner upon demand (ISO/IEC, 2004), hence the information provides the organization the ability to perform operations and accomplish its objectives (Ezingeard, et al, 2005).

Even though the definition of Information Security is well accepted and used by many, Anderson (2003) states that this definition is too broad that it covers some activities that are not among the parts of ‘computer security’ or ‘information security’. Anderson has proposed a different definition to Information Security; ‘a well-informed sense of assurance that information risks and controls are in balance’ (p 310).

On the other hand, Landwehr (2001) has added two more components to Information Security; ‘authentication’ and ‘non-repudiation’. He explains in his study that authentication (or sometimes so-called identification and authentication) ensures that each principal involved in a transaction is who they claim to be and non-repudiation ensures that a neutral third party can be convinced that a particular transaction or event did (or did not) occur.

Lichtenstein (1997) also states that, the term ‘information security’ is often used inter-changeably with ‘computer security’. He references to Baskerville (1988) as Baskerville defines ‘information security’ as a broader range of issues. Lichtenstein points out that Baskerville states the information security concept covers related issues like ‘computer security’- which is defined by Baskerville as pure safeguarding of electronic computer and communication systems, manual information systems, systems analysis and design methods, information security issues at managerial level and societal and ethical issues.

Tryfonas et al. (2001) broaden the debate and while defining the appliance area of information security as ‘Information Systems (IS)’, they emphasize that it includes set of principles, regulations, methodologies, techniques and tools that are developed or purchased in order to protect an IS or any of its parts from potential vulnerabilities.

The information security framework proposed by this study is based on the first definition among the ones mentioned above, i.e. Information Security is based on the components of ‘Confidentiality’, ‘Integrity’ and ‘Availability’.

Information Security Management

While ‘Information Security’ is a concept that is to be defined before acting accordingly, ‘Information Security Management’ is the method or set of methods to be applied to provide ‘Information Security’. More detailed and organized definitions on Information Security Management are also available within the literature.

Von Solms (1999) stresses that technical protection systems will always have an outstanding importance in securing an IT-environment, and appropriate administrative and managerial controls are to be in place to orient and direct the actions and behaviors of the information system users. Logan (2002) references Suydam (1999) noting that information security professionals are increasingly demanded to own well-developed managerial, cognitive and communication skills, and strong technical knowledge and specialization. Von Solms (2000) defines the ‘Management’ phase in his analysis of the phases of information security, as characterized by a growing management realization of and involvement with the importance of information security. He also defines the ‘Technical’ phase as having only technical solutions in order to maintain information security (mainframe operating systems, access control lists, user-ids, and passwords) and proposes an 'Institutional' phase as having best practices and codes of practice, certification, corporate culture of information security and continuous information security measurement. In alignment with the former two definitions of information security management, Nyanchama states that "information security management involves visioning, planning and execution of a security management program with a purpose of minimizing information security risks" (2005, p 30).

Although there are several definitions in place, studies that compare and combine the information security management approaches are not common. Hong et al. (2003) have combined five information security management related theories in their study (information policy theory, risk management theory, control and audit theory, management system theory and contingency theory) to develop an integrated theory of information security management which may be used as a basis for further understanding managerial bottlenecks, forecasting the effectiveness of managerial level and altering managerial strategies. BS 7799/ ISO 17799, which is a standard referenced by two of these theories (control and audit theory, and management system theory) will be the subject of further chapters in this study.

Information Security Governance

Moulton et al. defines information systems governance as "the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems" (2003, p 581).

Von Solms (2001) stresses the importance of information security governance in another article and states that there are different dimensions of information security, among which are the human (personnel) dimension, the awareness dimension, the legal dimension, the policy dimension, the measurement and monitoring dimension. Von Solms also points out in his study that the senior management should implement and conduct an enterprise-wide information security plan in the company, taking into account all the different aspects of information security mentioned above. Andersen (2001) emphasizes the same issue and states that boards and executive management in companies should understand the need for information security governance and achieve its harmony with IT governance framework.

As combining information security to business perspective, von Solms et al. notes that information security governance has an enterprise wide risk mitigating effect, and that "the risks mitigated by an information security governance plan, are risks which have an enterprise wide business implication" (2005, p 272). Von Solms et al. also count 'not realizing that information security is a corporate governance responsibility' as one of the ten deadly sins of information security management in another study (2004, p 372). Poore (2005) brings the understanding of information security governance one step forward and claims that the major goal of governance in corporations is management accountability to the stakeholders; therefore the information security governance must give priority to the goal of achieving management accountability for safeguard and ethical use of information assets.

The Need for Information Security

The awareness on the need for information security is increasing in most organizations today. In parallel, studies that emphasize the need for information security are also available in the literature.

Posthumus et al. (2004) indicates that IT has an important role in storing, processing and transmitting valuable business information assets. Haworth et al. also points out that, since "the data used in financial reporting is captured, verified, stored and reported mainly by computer based systems, senior management has turned to computer security officers to implement needed controls on those systems" (2000, p 73).

Saint-Germain points out in his study that today there are a number of information security related risks to be mitigated by the organizations. These risks range from terrorist attacks to fires, from earthquakes to other possible disasters, all of which may lead to the destruction and devastation of information processing facilities and business-critical documents. Saint-German also points out that not only destruction of information assets is a risk, but also losing competitive advantage in commercial activities due to stealing of business related confidential data and loss of integrity of data due to unexpected system shutdowns is also another risk that organizations may confront. (2005). Little et al. also agree with Saint-Germain in their study and underline that "computerized information systems, whilst providing many benefits to organizations, are also vulnerable to many threats including internal and external intruders attempting to access sensitive information, modify data, make fraudulent changes to programs, enter fraudulent transactions and perform other undesirable acts within the system" (2003, p 419).

Poole also states that “Corporate governance requirements place increasing demands on organizations to demonstrate that they have effective internal control arrangements in place which in the end result in the inclusion of information security as part of operational risk in the wider corporate governance definition” (2006, p 1).

Whitman (2004) notes in his study that, the results of the Computer Crime and Security Survey carried out by Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) in 2003 indicate that 90 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months of the survey. Deloitte Global Security Survey (2006) also shows that the 82 percent of respondents indicated that they had experienced some form of successful breach, either internally or externally.

Apart from the business requirements mentioned above, there are regulatory issues to be considered by the companies to ensure the security of their information assets as well. One global (Sarbanes Oxley Act) and one local (Information Security Auditing for Banks in Turkey) regulatory requirement examples will be introduced in order to demonstrate the legal need for information security for companies.

Sarbanes Oxley Act of 2002

Shareholder confidence has been abated due to the occurrence of financial disclosure distortion scandals in companies like Enron, Tyco and WorldCom. In 2002, US government passed the Sarbanes Oxley Act (shortly called as SOX), in order to safeguard the shareholders against inaccurate and unreliable corporate financial disclosures and closing the legal loopholes in the available regulatory infrastructure (Dhillon et al., 2006). Sarbanes Oxley regulation renders executives of publicly traded companies “explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting and disclosure” (Damianides, 2005, p 78).

Compliance with Sarbanes Oxley Act is not only necessary for the public companies; compliance may be sought for other companies as well. For example, Canadian companies that are in trade relations with publicly traded US companies, and banks may be required to comply with SOX (Miller, 2005).

Goins points out that Sarbanes Oxley Act is applicable for the accounting and reporting principles and financial environment in public companies, but the contribution of an information technology with proper and sufficient controls in place, to a reliable financial reporting environment cannot be overlooked (2005). Luthy et al. also underline a similar point and state that today information technology is commonly used in companies; and although Sarbanes Oxley does not specify a standpoint about utilization of it in corporations, an IT environment with appropriate controls in place is a requisite to obtain a reliable financial reporting environment. Hence, an information technology environment with appropriate controls is essential for SOX (2006).

In order to obtain assurance on the capability of information technology environment to comply with SOX, IT assets should be available to the Sarbanes-Oxley compliance team (Goins, 2005).

Information security is not directly referred to in Sarbanes Oxley. Gordon et al. points out that “the definition of internal control provided by the US Security and Exchange Commission (SEC), combined with the fact that the reporting systems in all firms required to comply with SOX are based on sophisticated computer-based systems, does imply that more focus on information security is a necessary, though not sufficient, compliance requirement" (2006, p 504). In fact, in addition to the detailed examination of corporate financial data, SOX also covers the IT processes behind the financial systems (Hardy, 2006). Volonino et al. stresses that "Key to achieving sustainable compliance with SARBOX is an IT infrastructure that satisfies mandated levels of internal control, corporate governance, and fraud detection" (2004, p1). Schneider et al. (2006) also state in their study that the financial data and administration systems are becoming more and more IT supported, in parallel, the people with the knowledge on the design and execution of these systems are becoming IT professionals. As SOX evolves, IT controls are becoming an even more important element in helping companies meet the stringent corporate governance regulations, since generating reliable reports is key to proving that a company is meeting the requirements of the Act (Hardy, 2006). A recent study on the companies that are subject to SOX shows that SOX is having a significant impact (increased over 100 percent) on the voluntary disclosure of information security activities (Gordon et al., 2006).

Information Security Auditing for Banks

At 2003, Banking Regulation and Supervision Board Vice President declared that corruption confronted has never been experienced before in the banking sector. It is stated that the banking information system is configured as to cover the real figures from the authorities and the difference between real deposit and official deposit amounts are debited to the bank's former and current managers (Haber Vitrini, 2003). It is stated that the Imar Bank case does also stand as an international example for information security incident (Şenyüz, 2007). As a result of this incident, the government bodies understood the importance of information systems for banking operations and the importance of information security. In order to prevent such incident to happen again, Banking Regulation and Supervision Board has released a regulation (BRSA, 2006), on auditing of information systems of the banks. According to the regulation, the bank management is liable for providing information systems, relevant documentation concerning the financial information formation processes, any record, information, document, application and maintaining any means necessary for the general controls of IT environment.

Standards

Information Technology Infrastructure Library (ITIL)

ITIL was first developed in the late 1980s as a catalog of best practices for government IT departments by the Central Computer and Telecommunications Agency, which is also a branch of British government today (Worthen, 2005). The library provides a full bunch of best practices for IT processes (Schlarman, 2007) as well as management and exploitation of the IT infrastructure (Violino, 2005) in a service oriented approach. Instead of having distinct features of a standard, ITIL provides enhancements in IT Service quality, business/IT alignment and IT cost management covering divergent set of concepts and frameworks (Marquis, 2006). Using the set of best practices, ITIL also supports the business efforts in effective and efficient use of Information Systems (IT Governance Institute, 2005).

The practice-based origin of ITIL facilitates the recognition of it, while providing more concrete solutions for companies to align their IT and business goals (Le Roux, 2005). To put it more specifically, ITIL can provide increased system uptime, faster problem resolution and better security (Worthen, 2005). ITIL's best practice framework could also be customized in order to be used in various kinds of IT structures (Lonsdale et al., 2006).

Today, ITIL is mostly used as an enterprise-infrastructure standard and as a way for most of the service providers to certify their capabilities (Violino, 2005).

Control Objectives for Information and Related Technology (COBIT)

CobiT is an acronym for Control Objectives for Information and Related Technology and is an open standard for control over IT. Latest version of CobiT (4.1) is published by the IT Governance Institute in 2007 and the institute was also the primary publisher of CobiT 3rd edition in July 2000.

CobiT is an 'IT governance framework and supporting toolset' that enables managers to handle the control requirements, technical issues and business risks at the same time (ISACA, 2007) by bringing together business control models and IT control models (Saint-Germain, 2005). Basically, CobiT does not directly address Information Security. On the other hand, it provides the set of tools and framework for establishing an Information Security practice in a company while laying more emphasis on IT governance (von Solms, 2005).

CobiT has fundamental benefits to IT related practices; being a baseline for Sarbanes Oxley compliance, covering most relevant IT processes, providing specific key performance indicators (KPI's) and sufficient information for implementation of these KPI's (Schlarman, 2007).

Luthy et al. (2006) visualize the CobiT framework in three dimensions: "IT processes, including domains and processes; IT resources including human resources, software, technology, physical structures and data; and information criteria including quality, owner of information, and security.

CobiT include 34 generic processes under 4 domains in order to deliver relevant information to business considering both business and governance requirements (IT Governance Institute, 2007). These four domains are;

PO: Plan and Organize

AI: Acquisition and Implementation

DS: Delivery and Support

ME: Monitor and Evaluate

Brown et al. (2005) also mention about the four domains of CobiT, including IT processes with a set of high level control objectives, which in the end provide a framework of good practices. Hawkins et al (2003) define the purpose of four domains in a comprehensive way: 'Plan and Organize' domain is the source the strategic plan developed by the management of IT environment. 'Acquisition and Implementation' domain provides necessary guidelines and practices in order to implement the plan. The effectiveness of the processes that are in place for implementing the strategic plan is examined with the help of 'Delivery and Support' domain. 'Monitor and Evaluate' domain enable managers to update the current processes in order to increase efficiency.

CobiT also includes a management guideline component in order to expand and enhance its focus on IT governance. The management guidelines are comprised of;

- maturity models, providing a benchmark opportunity;
- critical success factors, providing key elements in order to control IT processes;

- key goal indicators, providing monitoring points for the IT process goal achievement; and
- key performance indicators, providing monitoring points for IT processes performance achievement within each of 34 IT processes (Bodnar, 2006).

Among these, maturity models could help the management in order to position the organization, with respect to best practice in the industry and to international (Hardy, 2006).

ISO/IEC 17799 - Code of Practice for Information Security Management

First version of BS 7799 consisted of two main parts; 'The Code of Practice for Information Security Management – BS 7799 Part 1 Code of Practice' is developed by the support of many leading companies like BT, Marks and Spencer, Shell and Unilever and it is published as ISO/IEC 17799 Part 1 Code of Practice for Information Security Management in December 2000. The second part; The Specification for Information Security Management Systems was published in February 1998 (Kenning, 2001).

BS 7799/ISO 17799 provides necessary controls (Sweren, 2006) and a baseline approach (Barnard et al., 2000) for information systems security used by both production and finance companies, varying from small to large organizations. The standard facilitates the companies' efforts in avoiding the predictable security risk by providing 'a common basis for companies to develop, implement, and measure security management practice' (Chang et al., 2006, p 348). In addition, BS 7799/ISO 17799 provides critical advantages such as speeding up the information access, introducing concepts like risk management, recordkeeping and tools and methods for management of information (Thorp, 2004). Briefly BS7799/ ISO 17799 provides companies a solid business perspective while handling information security without only focusing on the technical solutions (Saint-Germain, 2005).

Saint-Germain (2005) separates the purpose of ten domains of BS 7799/ISO 17799 into five compliance levels being managerial, organizational, legal, operational and technical. The ten domains are also presented under three aspects in the same study, as Organizational, Physical and Technical. In the Figure 1, the proposed pyramid of BS 7799/ISO 17799, the ten domains are sorted from Organizational level of management to Operational level.

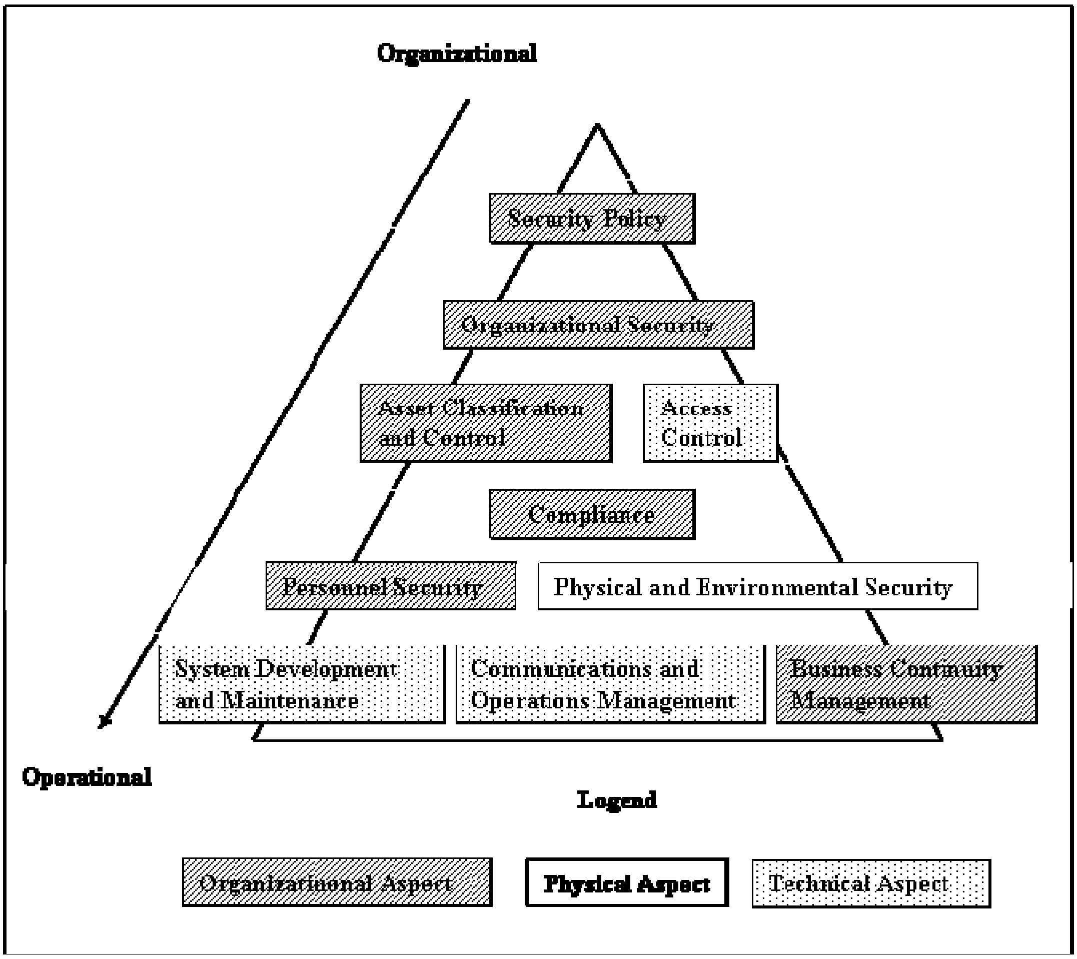
Organizational
Security Policy
Organizational Security
Asset Classification and Control
Access Control
Compliance
Personnel Security
Physical and Environmental Security
System Development and Maintenance
Communications and Operations Management
Business Continuity Management
Operational
Legend
Organizational Aspect
Physical Aspect
Technical Aspect

Fig. 2.1 Ten domains of ISO 17799 and their suggested aspects (Saint-Germain, 2005, p 61)

BS 7799/ISO 17799 provides 127 detailed controls under 36 control objectives within ten domains (Saint-Germain, 2005), in order to facilitate the efforts of the companies in search of an effective information system (Eloff et al., 2000).

BS 7799/ISO 17799 security domains are as follows (Saint-Germain, 2005);

Security Policy: Necessary actions must be taken in order to include and encourage management towards the attempts of information security

Organizational Security: Ensure the proper coordination and management of information security while allocating necessary responsibilities.

Asset Classification and Control: Take necessary actions in order to protect critical or sensitive assets.

Personnel Security: Perform training and awareness activities within the organization regarding information security.

Physical and Environmental Security: Take necessary precautions in order to protect the information, information processing facilities and organization's premises.

Communications and Operations Management: Maintain proper and secure use of information processing facilities and develop incident response procedures for handling incidents.

Access Control: Locate necessary controls in order to protect the access to information system and to detect unauthorized activities.

Systems Development and Maintenance: Take necessary actions in order to protect the information the operating systems and applications.

Business Continuity Management: Build up a proper contingency plan for the organization in order to prepare it minimally affected from the interruptions resulting from disasters.

Compliance: Consider the laws and regulations regarding the information security while ensuring the compliance of the security policy with the policies already in place.

Barnard et al. (2000) suggest three main steps for companies in order to apply solid information security practices with the help of BS7799/ISO 17799; (1) analysis of dependency and impact of IT on business, (2) identification of the security requirements based on the analysis and (3) selection of the necessary controls from BS 7799/ISO 17799 for the coverage of the security requirements.

CHAPTER III

METHODOLOGY

Information Security Management Framework

As it is mentioned in the previous sections of this study, maintaining information security in an organization is both technical and managerial issue. Since technical details of information security is not presented, the framework that is to be proposed will be based on managerial details, hence the name of the framework. The target of this framework is limited with the organizations in Turkey.

The framework is mainly based on BS 7799/ISO 17799 standard, using the 9 domains instead of 10. 'Compliance' domain is not applicable in most of the organizations in Turkey therefore it is not included in the framework.

The framework first consists of 61 controls under the 9 domains. These controls stand for conformance points for organizations regarding information security framework. For the base of the controls, the BS 7799 checklist that is located on the SANS website is selected (Thiagarajan, 2005). Other controls are formed based on the literature survey conducted. The list of the controls could be seen on the questionnaire provided in the 'Appendix' part of this study.

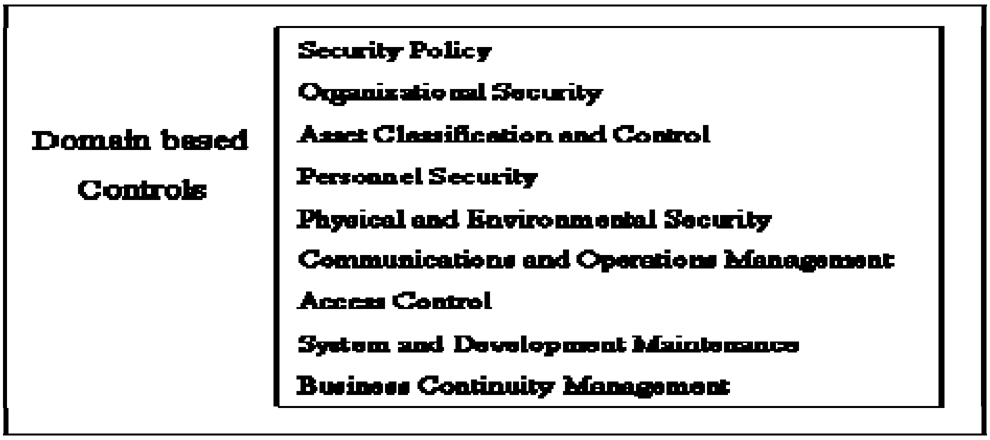
Domain based Controls
Security Policy
Organizational Security
Asset Classification and Control
Personnel Security
Physical and Environmental Security
Communications and Operations Management
Access Control
System and Development Maintenance
Business Continuity Management

Fig. 2.2 List of the domains considered for the controls in the framework

The conformance of the organizations regarding the controls is defined in three levels:

Effective: If the control is in place with all the aspects included in the control definition.

Gap: If the some part of the control definition is in place but the whole area of the control is not covered.

Deficiency: If none or very little part of the control definition is covered.

These conformance levels are defined in a judgmental approach with the help of personal expertise during in-depth interviews performed.

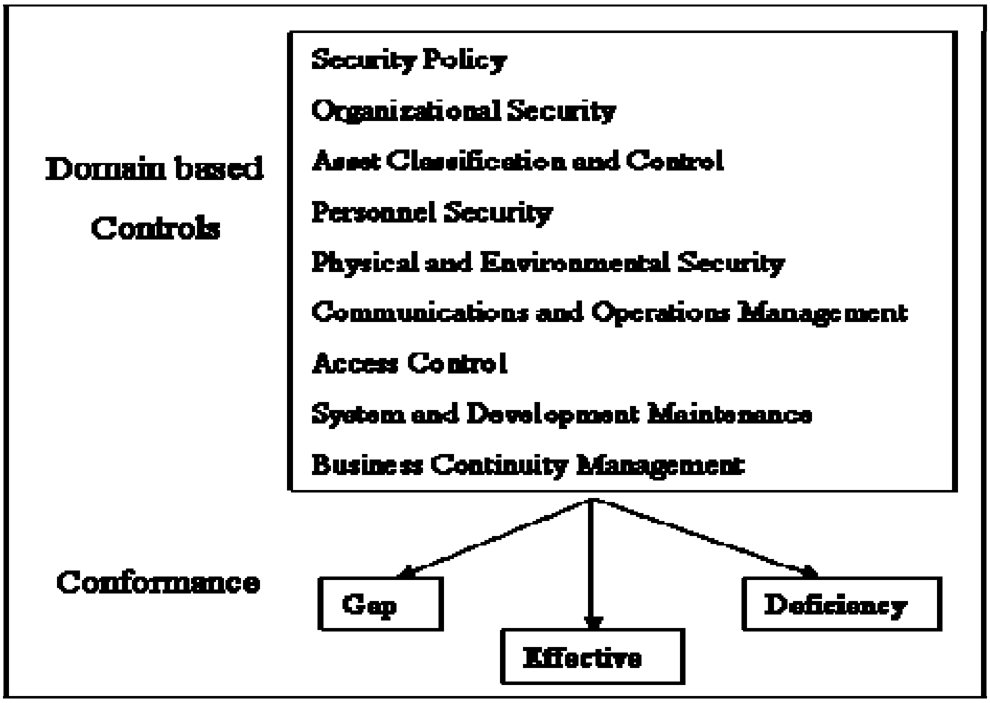
Domain based Controls
Security Policy
Organizational Security
Asset Classification and Control
Personnel Security
Physical and Environmental Security
Communications and Operations Management
Access Control
System and Development Maintenance
Business Continuity Management
Conformance
Gap
Effective
Deficiency

Fig. 2.3 Conformance levels originating from the domain based controls

If the conformance level is 'Gap' or Deficiency', a risk and a recommendation based on the risk is defined for the related control. 'Risk' stands for the possible events or incidents that may occur if the requirements of the related control is not met. 'Recommendation' includes suggestions that will help the organization to conform with the requirements of the related control.

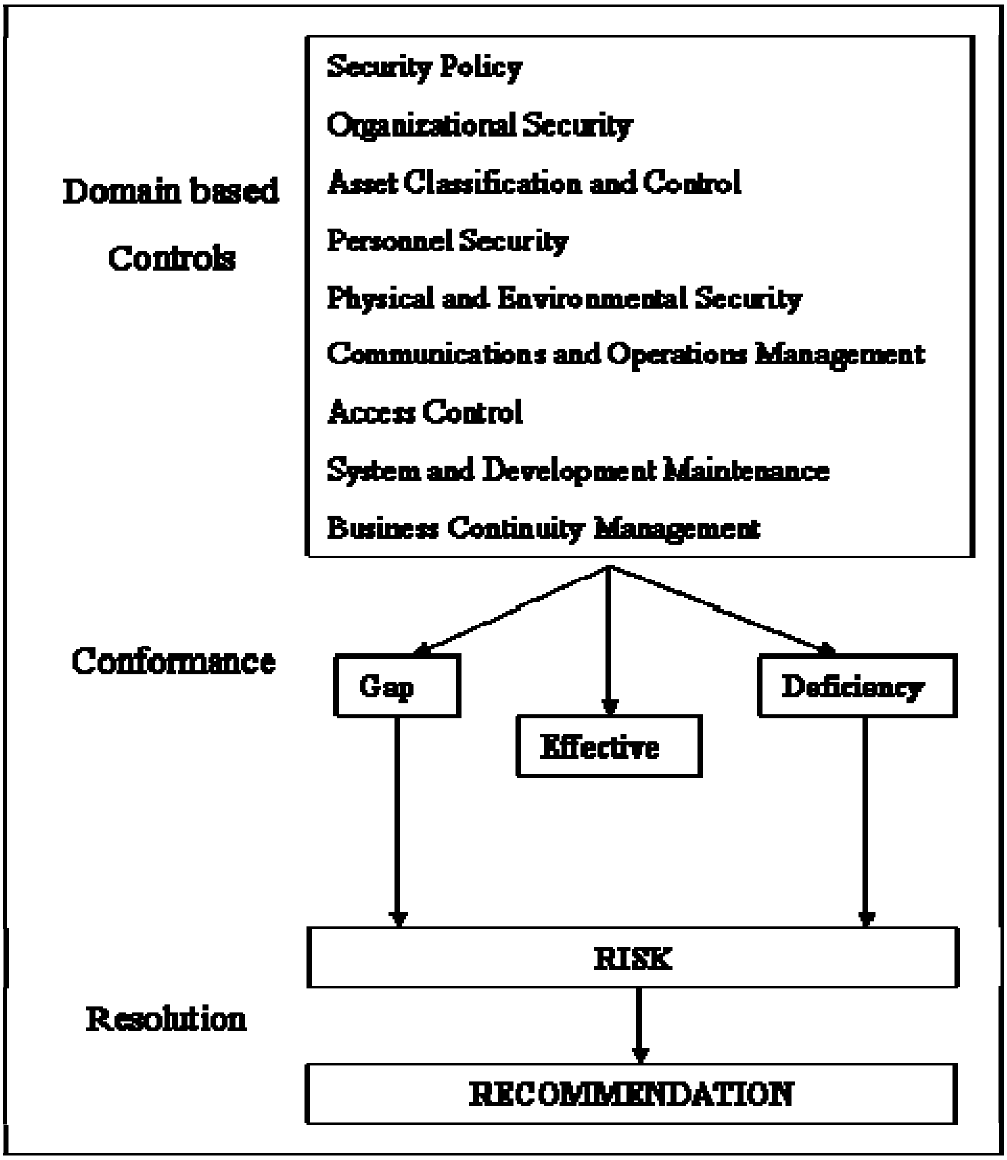
Domain based Controls
Security Policy
Organizational Security
Asset Classification and Control
Personnel Security
Physical and Environmental Security
Communications and Operations Management
Access Control
System and Development Maintenance
Business Continuity Management
Conformance
Gap
Effective
Deficiency
RISK
Resolution
RECOMMENDATION

Fig. 2.4 Resolution based on the gaps or deficiencies identified

A questionnaire is prepared based on the proposed information security management framework. The questionnaire is composed of 61 'should be' sentences, in other words 'controls' related to 9 domains of BS 7799/ISO 17799.

The questionnaire includes both management level related and operational level related topics. Therefore, in order to obtain most relevant and most detailed information using the questionnaire, the interviews should be performed with at least one person from IT top management and one or more high level representatives from IT operations department or division.

Case Studies

In order to apply the framework constructed, case study method has been used. Computer center and the registration office of a state university in Turkey are selected as subjects of the case study. Two interviews are scheduled with representatives of each of these offices and the prepared questionnaire is asked during these interviews to obtain information on whether the controls in the questionnaire are in place. The details of the controls are obtained if the related answer is positive.

The answers obtained from interviewees are evaluated based on the 'conformance levels' in the proposed framework. In this way, the number of controls that are 'effective', controls that have 'gaps' and controls that have 'deficiencies' is identified for each domain of each entity.

As a next step of the framework, risk and recommendations related to the controls with gaps or deficiencies are defined. A comparison is made between these two entities and a conclusion is reached according to the framework.

CHAPTER IV

ANALYSIS OF DATA

This section reports the analysis results. After performing the questionnaire and obtaining the findings, the categorization of the findings based on the conformance levels are applied. The categorization is also applied by 9 domains of BS 7799/ISO 17799. The results are compared between entities based on the conformance levels and domains covered.

Registration Office

During the interview, most significant finding was the lack of control over the 3rd party service provider. Since most of the security services are outsourced to the 3rd party service provider and since they are not monitored, the number of the gaps and deficiencies identified is high. The categorization of the findings according to the 9 domains investigated is presented in Table 4.1. The numbers represents the number of controls for each domain and each conformance level.

Table 4.1 Summary of the Findings Identified for Registration Office

Category	Questions Asked	Effective	Gap	Deficiency
Security Policy	2	0	0	2
Organizational Security	7	0	0	7
Asset classification and Control	6	2	1	3
Personnel Security	4	0	2	2
Physical and Environmental Security	8	2	3	3

Category	Questions Asked	Effective	Gap	Deficiency
Communications and Operations Management	13	5	1	7
Access Control	11	3	6	2
System Development and Maintenance	4	0	0	4
Business Continuity Management	6	0	0	6
Total	61	12	13	36

Security Policy

Under Security Policy domain, there are 2 questions asked and both answers indicate deficiencies for related controls. During the interview performed, it is noted that there is no formal written information security policy in place. Furthermore, university strategy does not address IT strategy, specifically IT strategy related to the registration office. The risks and recommendations related to these findings is stated in Table 4.2

Table 4.2 – Registration Office Risks and Recommendations for Security Policy Domain

Findings	Risks	Recommendations
There is no formal written information security policy in place	In absence of an information security policy, the methods for securing the university operations, critical systems, critical information may not be sufficient and may not include every critical systems in place.	The Information Security Policy constitutes a security framework for the organizations.
University strategy does not adress IT strategy	Not incorporating the IT strategy with the organizations (hereby 'University') may lead to insufficient implementation of the IT strategy because of lack of management support. That could result in IT Strategy to be remained out-dated or insufficient for latest threats and/or opportunities.	Both the university strategy and IT strategy should adress the other in order to support each other and to remain updated. Management support would facilitate the implementation of IT Strategy and would in return provide the safety of the university's information assets.

Organizational Security

There are 7 questions asked and all of the answers indicate deficiencies for related controls under Organizational Security domain. It is noted that the risks from third party access are not identified and appropriate security controls are not implemented since the third party itself established and monitors the access to the production system. The remote access is initiated by the third party. Vendor accounts are not disabled and under control of the third party. The password control related to vendor accounts is performed by the third party. As a final finding, there is not information security offices function in place. The risks and recommendations related to these findings is stated in Table 4.3

Table 4.3 – Registration Office Risks and Recommendations for Organizational Security Domain

Findings	Risks	Recommendations
The risks are not identified and appropriate security controls are not implemented since the third party itself established and monitors the access to the production system.	Not classifying the possible types and reasons of accesses may result in unidentified acccess to crtitical data and security breaches that could not be identified at the firewall level.	The types of access related to the third parties should be identified, justified and classified. According to every type of access, necessary security controls should be designed and implemented. At least one officer should be responsible for the access of the third parties.
The remote access is initiated by the third party.	Not monitoring the remote access of vendors could lead into unauthorized access to critical information. Unauthorized remote access could also pose a threat to RO's information systems letting them vulnarable to security attacks.	Immediate action must be taken in order to restrict the remote access of third parties. Necessary policy and procedures must be documented and applied and remote access connection must be monitored starting from initiation till termination.

Findings	Risks	Recommendations
Vendor accounts are not disabled and under control of the third party.	Although the firewall is configured not to allow unauthorized access, enabled accounts could be compromised internally to access to critical systems files.	Vendor accounts should be disabled during inactivity. The activities performed by the vendor account should also be logged and reviewed as an additional control.
The password control is performed by the third party	Unchanged vendor passwords increases the risk of unauthorized use of the vendor accounts for accessing critical system files.	Vendor passwords should be changed after each usage and they should be change by RO.
There is no information security offices function in place	Not having a seperate information security officer in place decreases the attention given to the security of the information systems. That could result in unauthorized exposure of the critical data, manipulation and even deletion of the critical data.	There should be information security officer in place seperate from the IT department. IS officer should directly report to the management about the security strategy, security operations and security actions planned to be taken. The information security officer funtion should be seperated from IT department. The responsbilities of the function should be defined on the corporate level. Information security officer should define the security policies as well as monitor the compliance of the operations with those policies. IS officer should report and non-compliance issues and security breaches to the management.

Asset Classification and Control

There are 6 questions asked having 1 gap and 3 deficiencies identified for related controls under Asset Classification and Control domain. It is noted that there is no formal definition of the security levels and no formal information classification scheme or guideline in place. Furthermore data owners are not identified. Finally although the IT equipment is traced and logged by the central university equipment registration, there is no formal list kept by the RO. The risks and recommendations related to these findings is stated in Table 4.4

Table 4.4 – Registration Office Risks and Recommendations for Asset Classification and Control Domain

Findings	Risks	Recommendations
There is no formal definition of the security levels. They are reviewed on necessity	Not defining the security levels to the specific information may result in unauthorized access to the sensitive data. That could even result in not recognizing this kind of security breach.	Management should first consitute an information repository regarding the university information systems and data related to the university operations. Then the security levels of the information shoule be defined. Finally necessary procedures should be designed to sustain the security of critical information.
Data owners are not defined.	Not assigning data owners may result unexpected exposure of the critical and sensitive data to unauthorized users.	After defining the system inventory and related security levels to be preserve, data owners should be assigned for these systems. The data owners should be provided the roles and responsibilites related to the systems they are responsible of based on the criticality of the systems and measures that are defined to preserve the security
The IT equipment is traced and logged by the central university equipment registration. There is no formal list kept by the RO.	IT equipments could be stolen or damaged and they cannot be noticed until there is a necessity. Further more there may be a risk in place that the equipment is somehow logged mistakenly and this would go unnoticed for a long time.	A central log for the IT equipment should be designed. There should be a perodic reconciliation of the log with the physical asset for the integrity of the log.
There is no formal information classification scheme or guideline in place.	In absence of information classification scheme or guideline, the sensitive data may be compromised without knowledge of the IT personnel. IT personnel	A formal information classification scheme should be in place, defining levels of data and data handling procedures related to these levels. Access to the data in the systems should be restricted in line with the levels defined in the scheme.

Findings	Risks	Recommendations
	may lack awareness of handling method of the sensitivie information.	

Personnel Security

There are 4 questions asked having 2 gap and 2 deficiencies identified for related controls under Personnel Security domain. It is noted the employees do not sign a separate confidentiality or non-disclosure agreement or these terms are not included in the contracts they sign when they are employed. Terms and conditions of the employment do not cover the employee's responsibility for information security. Furthermore the job descriptions of the personnel are not documented as a personnel base but rather as a division base and the scope of each division is briefly explained. Finally, although the staff attends to the internal training of the university on a regular basis to update or revise their technical skills, these trainings do not cover information security related topics. The risks and recommendations related to these findings is stated in Table 4.5

Table 4.5 – Registration Office Risks and Recommendations for Personnel Security Domain

Findings	Risks	Recommendations
The job descriptions are not documented as a personnel base but rather as a division base. The scope of each division is brifly explained.	Undefined role and responsbilities may result in lack of appropriate skills and knowledge identifying and handling security incidents.	Specific job descriptions for personnel should be in place, covering responsibilities and accountabilities of personnel. Personnel should be provided with a clear description of accountability areas.

Findings	Risks	Recommendations
The staff attends to the internal training of the university on a regulare basis to update or revise their technical skills.	Lack of adequate training of the IT personnel may result in inproper planning of the security systems and inadequate handling of the security incidents.	IT personnel should be provided with regular trainings on IT systems and IT security. The trainings should be provided in line with a training program accepted by the management. IT personnel should be provided by the means to increase their level of experience in IT systems.
The employees do not sign a seperate confidentialiy or non-discosure agreement or these terms are not included in the contracts they sign when they are employed.	Not signing a confidentiality aggreement may result in lack of awareness about the usage of information systems. That could increase the risk of unintended misuse of the systems in place.	Personnel with access to critical data sources should sign a confidentiality aggreement with the university.
Terms and conditions of the employment does not cover the employee's responsibility for information security.	If the responsibilities of the personnel for information systems is not properly delivered to the personnel, the risk of unintended systems disruptions/misuse may increase.	The responsibilities of personnel for IT security should be clearly communicated. Terms and conditions of employment may obtain security related responsibilities. Personnel may be required to sign a declaration indicating being acknowledged on security related responsibilities.

Physical and Environmental Security

There are 8 questions asked having 3 gap and 3 deficiencies for related controls under Physical and Environmental Security domain. It is noted that the system room is access via standard door and key and there is no keypad or card-reader mechanism in place for the system room entry. Only security precaution in place is that the outer room door has a keypad equipped with a password entrance but the keypad is activated only during non-work hours. The key to the system room is kept only one personnel and no record is kept for the visitors to the room.

Unauthorized individuals are escorted by an authorized individual during visit. No visitor log is kept.

For the system room conditions, it is noted that Fire detectors are in place but conventional fire extinguishers are used, there is no humidity controller in place, the water and drainage pipers are routed away from IT systems but no raised floor or lowered ceiling is used. As a final point there is periodic preventative maintenance of computer components. The risks and recommendations related to these findings is stated in Table 4.6

Table 4.6 – Registration Office Risks and Recommendations for Physical and Environmental Security Domain

Findings	Risks	Recommendations
The system room is access via standard door and key. There is no keypad or card-reader mechanism in place for the system room entry. The outer room door has a keypad equipped with a password entrance. The keypad is activated during non-work hours.	Not maintaining a security mechanism for the access to sensitive IT areas could result in unauthorized access to the system resources. Unauthorized individuals could steal, manipulate or even destroy ciritical information without dealing with security measures applied on the software level. The security of the critical physical assets would also be in danger without proper access restrictions.	The system room access must be restricted only authorized personnel by using a keypad or other security mechanism.
The key to the system room is kept only one personnel	Restricting access to the system room to one personnel may seem a good practice but it would create a risk of making the access to the system room difficult in case of emergencies if that personnel is not available. The critical system resources may be partially or totally lots in case of disasters or similar	There should be security mechanism in place to restrict the access to the system room to authorized individuals. The list of the authorized individuals should be managed and approved by the necessary level of management.

Findings	Risks	Recommendations
	incidents.	
No record is kept for the visitors to the room.	Logging of access to the system room enables proper tracking of access to the room. In absence of access logs, unauthorized access and/or abnormal access to the system room may go unrecognized and responsible people in case of an unauthorized access may remain unidentified.	Logging of card reader mechanism should be enabled and logs should be retained for a period specified by the management. The logs should be reviewed periodically in order to identify any abnormal accesses made to the system room.
Unauthorized individuals are escorted by an authorizd individual during visit. No visitor log is kept.	Although the visitors are escorted by the authorized individuals, absence of a visitor log decreases the traceability of access to the system room.	System room access of the visitors, who are not among the responsible personnel of RO, should be registered in a visitor log. The visitors should sign in a visitor book in order to enhance tracking of the visitors accepted in the system room.
Fire detectors are in place but conventional fire extinguishers are used. There is no humidity controller in place. The water and drainage pipers are routed away from IT systems but there is no raised floor or lowered ceiling is used. There is one UPS in the system room There is air conditioning in place. Power Generator is shared with the rest of the university	Not maintaining necessary environmental controls for system room could result in unexpected damages on the physical assets in case of fire, flood, electricity cuts, etc.	Fire extinguishers that contains material which would not harm electronic equipment (i.e. FM-200) must be used. Humidity detectors must me in place. Use of raised floor or lowered ceiling for cabling must be considered.

Findings	Risks	Recommendations
There is periodic preventative maintenance of computer components	Preventive maintenance held for the critical equipment decreases the risks of unexpected hardware failures and interruption of the university operations resulting from hardware failures. Hence, in absence of preventive maintenance, the risk related to unexpected failures and/or major defects resulting from minor failures in hardware increases.	Preventive maintenance should be performed periodically to cover the critical hardware equipment of RO. For the equipment for which technical knowledge of the personnel is not adequate, third party services should be provided. For the services provided by third parties, the service levels and responsibilities of sides should be clearly stated in SLAs that are signed by both parties.

Communications and Operations Management

There are 13 questions asked having 1 gap and 7 deficiencies for related controls under Communications and Operations Management domain. It is noted the software developers monitors and reviews the system capacity but not in regular basis. All of the changes applied to the programs on production system are handled by the third party. The registration office interferes only at the testing phase. There is no formal and documented incident management procedure and no operating procedures identified. There is no policy in place for the acceptable use of electronic mail. There is no control in place for malicious software and since there is no formal and documented security policy in place, software licensing issues are not properly addressed. Although backups are taken regularly, the backup CD's are kept on site in a file cabinet and the backup CD's are not tested. The risks and recommendations related to these findings is stated in Table 4.7

Table 4.7 – Registration Office Risks and Recommendations for Communications and Operations Management Domain

Findings	Risks	Recommendations
The software developers monitors and reviews the system capacity but not in regular basis.	Not reviewing the systems capacity might result in not meeting the required level of resourced on sudden or regular demand increases. This could not only decrease the satisfaction level of the users but could also result in unexpected systems problems and event security breaches.	Management should request montly and yearly capacity analyssis of the information systems and should review them. The review results and possible actions to be taken should be communicated to the related personnel and be formally documented for further use.
There is no formal and documented incident management procedure in place.	Creating effective responses to security incidents confronted requires a definition of security incidents, incident escalation procedures and incident handling management procedures. In absence of an Incident Management procedures, problems may be encountered in identifying security incidents, the required analysis steps and resolution means. Hence, the action steps taken may be insufficient to minimize the business effects of possible security incidents.	Formal incident management procedures should be in place in order to identify and manage any security incidents that may be confronted. The procedures should be periodically reviewed in order to keep up to date with the university operations requirements.
The backup CD's are kept on site in a file cabinet	Offsite storage of backup tapes protects system data against disaster affecting the local offices of RO. Therefore, only onsite storage of backup tapes is in place, the risks related to business interruption in case of a disaster affecting RO and inability to recover the systems using the backup dates increases.	At least one copy of backup tapes should be kept at an offsite location.
The backup CD's are not tested.	Unless the backup tapes are tested regularly, the required recovery times may be misestimated. Another possible risk is that, any defects in backup tapes affecting the ability of recovering them may go undetected and tapes may be	Backup tapes should be tested regularly in order to review recovery procedures performed, required recovery times and to observe whether the hardware equipment is compatible for the recovery of the backup tapes.

Findings	Risks	Recommendations
	not functioning with the equipment set utilized for the recovery.	
Since there is no formal documented security policy in place, operating procedures are not identified.	Absence of such procedures may lead to problems in communicating the security-related operational steps to be performed and gaps between what is done to perform the job and what is done. Therefore such procedures are required in order to minimize the grey areas between responsibilities of the related employees and steps to be performed.	Operating procedures should be completed as soon as possible to provide guidance on the operational jobs performed and responsibilities of personnel for these jobs.
All of the changes applied to the programs on production system is handled by the third party. The registration office interferes only at the testing phase.	In absence of a formally established change management process, the risk related to intended/unintended migration of unauthorized and/or erroneous program changes to production environment increases. Thus, applications may function other than expected, erroneously and/or inefficiently.	A formal change management process should be in place, defining change initiation, development and testing of changes, migration steps and the required approvals taken at several milestones of change management process. Changes, their approvals and related information should be centrally registered in order to provide a traceable past data on the changes performed in systems.
There is no control in place for malicious software. Since there is no formal and documented security policy in place, software licensing issues are not properly addressed.	Lack of controls over malicious software and unauthorized software may result in expose of critical information to unauthorized individuals.	Necessary security practices must be implemented to control malicious software usage(i.e. Anti-malware software). Information Security policy must address the software licencing isssues including usage of unauthorized software. Periodic controls must be in place to prevent usage of unauthorized software.
There is no policy in place for the acceptable use of electronic mail.	Usage of e-mail without having enough awareness of the possible dangers may result in expose of critical data to unauthorized individuals and lloss of information resources.	There should be a seperate policy in place and published to all of the users regarding the acceptable use of e-mail. This policy could refer to main information security

Findings	Risks	Recommendations
		policy for broader comprehension of the information security dangers.

Access Control

There are 11 questions asked having 6 gap and 2 deficiencies for related controls under Access Control domain. It is noted that there is no central anti-virus solution in place; anti virus application is installed on only some of the computers and although the third party performs penetration testing, the results are not disclosed to the Registration Office. The third party can access to the applications of the Registration Office at any time and it maintains the logs of the systems in place. There is no control of the Registration Office on the log system.

There is a formal rule for providing Registration ID to the students. The ID and the password are provided to the student with a sticked paper on their file which is not a best practice. Furthermore there is no formal and documented procedure for allocating and reallocating the passwords. The only password controls in place are not using specific characters in the password which are provided at the web site and not using passwords with more than 10 characters. There is no password management system in place. Finally, there is no authentication mechanism in place except for User ID and password. The risks and recommendations related to these findings is stated in Table 4.8

Table 4.8 – Registration Office Risks and Recommendations for Access Control Domain

Findings	Risks	Recommendations
There is no central anti-virus solution in place. Anti virus application is installed on some of the computers.	Todays sophisticated viruses could harm system resources in short periods of times. Viruses that go unnoticed could manipulate or delete critical data or even let unauthorized individuals gain access to these resources.	A central anti-virus solution should be implemented. The maintenance of this software and update of the definitions must be controlled by documented procedures and practices. Whole systems resources including individual computers must be scanned for viruses periodically (min. weekly)
The third party performs penetration testing. The results are not presented to the Registration Office.	Third parties may not pay attention on all of the security vulnarabilities in the systems or may not share this information with RO. That could lead to unauthorized access to critical information and damaging of the system resources.	Penetration testing must be performed periodically by an authorized third party with a contact in which necessary requirements and obligations are addressed. The results of the testing must be evaluated and necessary actions must be taken.
There is a formal rule for providing Registration ID to the students. The ID and the password is provided to the student with a sticked paper on their file.	In absence of a formal user registration and deregistration process, unauthorized people may gain access to system resources. This in return leads to the risk of intended malicious transactions in the system performed by unauthorized people. Data integrity and confidentialy may be compromised in absence of this process as well.	A formal user registration and deregistration process should be established. In addition to this, compliance to these procedures should be regularly assessed and results should be provided to the high level administration.
There is no formal and documented procedure for allocating and reallocating the passwords.	Printing passwords on papers in the allocation process may lead to the risk that unauthorized people may obtain other people's passwords.	Allocation of e-mail account passwords should be performed on the basis of personal application of the users, as in the reallocation process.

Findings	Risks	Recommendations
There is no authentication mechanism in place except for User ID and password.	Although external connections are secured with firewalls and HTTPS protocol, not utilizing tokens increases the risk of exposure to security vulnerabilities.	Tokens should be utilized for remote connection to the systems.
The third party can access to the applications of the Registration Office at any time.	Lack of nesessary security mechanism in order to protect network of RO could lead to unauthorized access to the system resources. Even though third party is allowed to access to system resources, insuffficient access rules may increase the risk of accesing these resources without authorization of RO.	Firewalls must be in place and access rules must be configured appropriately so that third party access is monitored and unauthorized attempts of accesses are blocked.
The only password controls in place are not using specific characters in the password which are provided at the web site and not using passwords with more than 10 characters. There is no password management system in place.	If a formal password management system is not in place, security vulnerabilities related to sharing of passwords and acquisition of passwords by unauthorized people increases. Therefore, unauthorized people may gain access to systems.	A formal password management process should be established. Users should be forced to select strong passwords by the system. Minimum and maximum password ages should be forced as well.
The third party is maintaining the logs of the systems in place. There is no control of the Registration Office on the log system.	If exception logs are not reviewed periodically, several exceptions and security related events may remain unrecognized.	The exception logs should be reviewed periodically in order to identify any suspicious exceptions and log review results should be reported to management.

System Development and Maintenance

There are 4 questions asked and all of the answers indicate deficiencies for related controls under System Development and Maintenance domain. It is noted that all system development is maintained by the third party and there is no strict controls in place over access to program source libraries. Digital signatures are not used. The risks and recommendations related to these findings is stated in Table 4.9

Table 4.9 – Registration Office Risks and Recommendations for System Development and Maintenance Domain

Findings	Risks	Recommendations
All system development is maintained by the third party.	In absence of a formal system development life cycle, needs of the university units may not be met within the allocated time frame in an efficient and cost effective manner and the required outputs at the required quality level may not be produced.	A formal and documented system development methodology should be adopted in RO. The required approvals in 'Analysis', 'Development' 'Testing' and 'Migration' phases should be clearly communicated and obtained. Documentation related to these phases should be retained in order to serve as a future reference.
Digital signatures are not used.	Digital signatures are utilized for authenticity and integrity of electronic documents. Without digital signatures, the source of the electronic document can not be verified and possible impairments made in the electronic document may be unrecognized.	Digital signatures should be utilized in order to obtain assurance on the authenticity and integrity of the electronic documents and compliance with current regulations.
There is no strict controls in place over access to program source libraries.	Lack of strict controls over access to program source libraries could lead to unauthorized access to the source libraries which could lead to potential corruption of programs used. A malicious user could alter the program source in order to gain benefit from the program.	Access to the program source libraries must be restricted to the individuals who could only migrate developed codes from test or development environment to production environment.
All system development is maintained by the third party.	In absence of formal control procedures over implementation of changes, the risk related to intendedly/unintendedly performed changes in information system increases. Thus, applications and systems may function other than expected, erroneously and/or inefficiently.	Implementation of changes should be performed only if required testing of changes is performed and approvals are obtained for the implementation. Testing results and obtained approvals should be retained. The changes performed should be reported

Findings	Risks	Recommendations
		to management reporting or communicated to the relevant users of the IT systems.

Business Continuity Management

There are 6 questions asked and all of the answers indicate deficiencies for related controls under Business Continuity Management domain. It is noted that there is no specific Business Continuity Plan in place for the computer systems at the Registration Office. The office is subject to the general building directives in case of a disaster. The evacuation plan of the university facilities includes general information about the possible disasters and common emergency plans against them. However these possible disasters and their impact on the information systems are not identified and systems are not priotized. The risks and recommendations related to these findings is stated in Table 4.10

Table 4.10 – Registration Office Risks and Recommendations for Business Continuity Domain

Findings	Risks	Recommendations
There is no specific Business Continuity Plan in place for the computer systems at the Registration Office. The office is subject to the general building directives in case of a disaster.	In absence of a business continuity plan, the university may not be able to react properly in case of an emergency. This could result in partial or total loss of the information systems as well as the critical system room.	There should be a process in place for developing and maintaining the business continuinty. The process should include defining a Business Continutiy Plan, reviewing and testing of the plan and applying necessary updates on the plan.

Findings	Risks	Recommendations
Systems are not priotized.	If the systems are not priotized and scheduled for recovery in accordance with work impact, less critical systems which have less affect on the healt of the information systems are recovered while critical systems may remain damaged.	Information systems should be priotized according to the their impact on the university operations. Based on the prioritized systems, a recovery strategy should be constituted.
There is no formal contingency plan in place	If the continuity plans are not tested, they might include insufficient information about the updated/changes systems in place which could result in inappropriate/improper methods for providing continuity to the university operations.	The contingency plans should be tested at least annually in order to reflect the current status of the information systems in place. The test should also applied in order to see if the plans are applicable and sufficient for the systems.
The evacuation plan of the university facilities includes general information about the possible disasters and common emergency plans against them. However these possible disasters and their impact on the information systems are not identified.	In absence of identifying possible disasters that could cause interruptions to the university operations may result in insufficient response to these disasters. In absence of a strategy plan based on the risk assessment results could lead to total or partial loss of the information systems during times of disasters.	In order to define and implement Disaster Recovery Plans, risk assesment must be performed. Durign risk assessment phase, possible causes of business interruptions must be defined. The results of the risk assesment should be used to direct or update the overall business continuity plans in place.
There is no BCP in place	The lack of defining a time frame for recovery of the information systems may result in significant disruptions in the university operations and may even result in unauthorized access to the critical systems. Recovery plans might include insufficient information about the updated/changes systems in place which could result in inappropriate/improper methods for recovery.	Within the disaster recovery plans, time frames should be defined for the systems' recovery durations. This time frames should be based on the priotization of these systems related to their criticality level. The DRP's should also be tested at least annually and updated if necessary.

Findings	Risks	Recommendations
There is no BCP in place	In case of a disaster, the location where the information systems reside may partially or totally damaged and may become unreachable. In absence of the BCP and DRP storage off-site, on-site plans may not be reached and applied.	The BCP's and DRP's should be stored off-site and the location of these plans should be included in the plans.

Computer Center

During the interview, it is been noted that, although Computer Center seems to be conforming to the controls, still there were critical points such as not having adequate operating procedures, a Business Continuity or Disaster Recover Plan in place.

The categorization of the findings according to the 9 domains investigated is presented in Table 4.11. The numbers represents the number of controls for each domain and each conformance level.

Table 4.11 Summary of the Findings Identified for Computer Center

Category	Questions Asked	Effective	Gap	Deficiency
Security Policy	2	1	1	0
Organizational Security	7	1	2	4
Asset classification and Control	6	2	2	2
Personnel Security	4	0	2	2
Physical and Environmental Security	8	4	2	2
Communications and Operations Management	13	5	1	7
Access Control	11	6	4	1
System Development and Maintenance	4	1	1	2
Business Continuity Management	6	0	0	6
Total	61	20	15	26

Security Policy

Under Security Policy domain, there are 2 questions asked and only one answer indicate gap for related controls. During the interview performed, it is noted that although the information security policy in place contains adequate information about the usage of the information technology systems, it does not state the management commitment and set out organizational approach to managing information security. The risks and recommendations related to this finding is stated in Table 4.12

Table 4.12 – Computer Center Risk and Recommendation for Security Policy Domain

Findings	Risks	Recommendations
There is a policy published at the web site of Computer Center. The policy includes information about the usage of several parts of information systems. Although the policy contains adeqauate information about the usage of the information technology systems, it does not state the management commitment and set out organizational approach to managing information security.	The lack of management commitment and setting of organizational approach may cause the policy to stay un-updated for a long period. That could result in unexpected exposure of the information systems due to non-protection againts latest security threats.	The information security policy should include management statement of commitment, approach on information security and responsibilities for reviewing and approving the policy.

Organizational Security

There are 7 questions asked having 2 gap and 4 deficiencies identified for related controls under Organizational Security domain. It is noted that there is no information security officer function in place. Employees are responsible for ensuring the security of their responsibility areas. Furthermore vender passwords are not regularly changed and although vendor access is restricted at the firewall, Vendor accounts are not disabled when not in use and there is no formally documentation of the types and classification of accesses. The risks and recommendations related to these findings is stated in Table 4.13

Table 4.13 – Computer Center Risks and Recommendations for Organizational Security Domain

Findings	Risks	Recommendations
The organization acquires services from third parties. The access of third party service providers to the resources of Computer Center is restricted at the firewall level. Recenlty, security software is been purchased for securing access to the information systems. However there is no formally documentation of the types and classification of accesses.	Not classifying the possible types and reasons of accesses may result in unidentified acccess to critical data and security breaches that could not be identified at the firewall level.	The types of access related to the third parties should be identified, justified and classified. According to every type of access, necessary security controls should be designed and implemented. At least one officer should be responsible for the access of the third parties.
Vendor accounts are not disabled when not in use but the access is restricted at the firewall.	Although the firewall is configured not to allow unauthorized access, enabled accounts could be compromised internally to access to critical systems files.	Vendor accounts should be disabled during inactivity. The activities performed by the vendor account should also be logged and reviewed as an additional control.
Vender passwords are not regularly changed	Unchanged vendor passwords increases the risk of unauthorized use of the vendor accounts for accessing critical system files.	Vendor passwords should be changed after each usage and they should be change by CC.

Findings	Risks	Recommendations
There is no information security officer function in place. Employees are responsible for ensuring the security of their responsibility areas.	Not having a seperate information security officer in place decreases the attention given to the security of the information systems. That could result in unauthorized exposure of the critical data, manipulation and even deletion of the critical data.	There should be information security officer in place seperate from the IT department. IS officer should directly report to the management about the security strategy, security operations and security actions planned to be taken.
There is no information security officer function in place.	same as above	The information security officer funtion should be seperated from IT department. The responsbilities of the function should be defined on the corporate level.
There is no information security officer function in place.	same as above	Information security officer should define the security policies as well as monitor the compliance of the operations with those policies. IS officer should report and non-compliance issues and security breaches to the management.

Asset Classification and Control

There are 6 questions asked having 2 gap and 2 deficiencies identified for related controls under Asset Classification and Control domain. It is noted there is neither information classification scheme or guideline nor formally documented data classification scheme in the organization. The data stored in systems is not classified as public, secret, confidential, etc. Instead, access to sensitive sources, like servers, is protected and restricted with firewall settings. Although a manual list of IT equipment is kept by the Computer Center, there is no process of periodic reconciliation of physical assets to the log. The risks and recommendations related to these findings is stated in Table 4.14

Table 4.14 – Computer Center Risks and Recommendations for Asset Classification and Control Domain

Findings	Risks	Recommendations
There is no formally documented data classification scheme in the organization. The data stored in systems is not classified as public, secret, confidential, etc. Instead, access to sensitive sources, like servers, is protected and restricted with firewall settings.	Not defining the security levels to the specific information may result in unauthorized access to the sensitive data. That could even result in not recognizing this kind of security breach.	Management should first consitute an information repository regarding the university information systems and data related to the university operations. Then the security levels of the information shoule be defined. Finally necessary procedures should be designed to sustain the security of critical information.
There is no formal data ownership structure in the organization.	Not assigning data owners may result unexpected exposure of the critical and sensitive data to unauthorized users.	After defining the system inventory and related security levels to be preserve, data owners should be assigned for these systems. The data owners should be provided the roles and responsibilites related to the systems they are responsible of based on the criticality of the systems and measures that are defined to preserve the security.
The IT equipment log is kept with the physical asset list of university properties. A manual list is also kept by the CC. There is no process of periodic reconciliation of physical assets to the log.	IT equipments could be stolen or damaged and they cannot be noticed until there is a necessity. Further more there may be a risk in place that the equipment is somehow logged mistakenly and this would go unnoticed for a long time.	A central log for the IT equipment should be designed. There should be a perodic reconciliation of the log with the physical asset for the integrity of the log.

Findings	Risks	Recommendations
There is no information classification scheme or guideline in place.	In absence of information classification scheme or guideline, the sensitive data may be compromised without knowledge of the IT personnel. IT personnel may lack awareness of handling method of the sensitivie information.	A formal information classification scheme should be in place, defining levels of data and data handling procedures related to these levels. Access to the data in the systems should be restricted in line with the levels defined in the scheme.

Personnel Security

There are 4 questions asked having 2 gap and 2 deficiencies identified for related controls under Personnel Security domain. It is noted that no separate confidentiality agreement is signed by the personnel apart from the general officer agreement signed by every employee in the university and terms and conditions of the employment does not cover the employee's responsibility for information security. Furthermore the roles and responsibilities are defined at the division level. Specific job descriptions are not defined. Finally there is no formally documented plan of the training and experience necessary for the IT personnel. The risks and recommendations related to these findings is stated in Table 4.15

Table 4.15 – Computer Center Risks and Recommendations for Personnel Security Domain

Findings	Risks	Recommendations
The roles and responsibilities are defined at the division level. Specific job descriptions are not defined.	Undefined role and responsbilities may result in lack of appropriate skills and knowledge identifying and handling security incidents.	Specific job descriptions for personnel should be in place, covering responsibilities and accountabilities of personnel. Personnel should be provided with a clear description of accountability areas.

Findings	Risks	Recommendations
When a group of IT personnel attends a course provided by a third party, they give the same training to the other IT personnel. However there is no formally documented plan of the training and experience necessary for the IT personnel.	Lack of adequate training of the IT personnel may result in inproper planning of the security systems and inadequate handling of the security incidents.	IT personnel should be provided with regular trainings on IT systems and IT security. The trainings should be provided in line with a training program accepted by the management. IT personnel should be provided by the means to increase their level of experience in IT systems.
No seperate confidentiality aggreement is signed by the personnel apart from the general officer aggrement signed by every employee in the university.	Not signing a confidentiality aggreement may result in lack of awareness about the usage of information systems. That could increase the risk of unintended misuse of the systems in place.	Personnel with access to critical data sources should sign a confidentiality aggreement with the university.
Terms and conditions of the employment does not cover the employee's responsibility for information security.	If the responsibilities of the personnel for information systems is not properly delivered to the personnel, the risk of unintended systems disruptions/misuse may increase.	The responsibilities of personnel for IT security should be clearly communicated. Terms and conditions of employment may obtain security related responsibilities. Personnel may be required to sign a declaration indicating being acknowledged on security related responsibilities.

Physical and Environmental Security

There are 8 questions asked having 2 gap and 2 deficiencies for related controls under Physical and Environmental Security domain. It is noted that no record is kept for the card reader mechanism. Although unauthorized individuals are escorted by an authorized individual during visit to the system room, no visitor log is kept. The servers have a heat alarm mechanism that sends an e-mail, which is not sufficient for the personnel to be alerted when the heat exceeds a level. Also, power generators are shared by the other facilities of the university. There is no preventative maintenance of computer components. The risks and recommendations related to these findings is stated in Table 4.16

Table 4.16 – Computer Center Risks and Recommendations for Physical and Environmental Security Domain

Findings	Risks	Recommendations
No record is kept for the card reader mechanism. On the other hand the system room is monitored by the cameras inside the system room.	Logging of access to the system room enables proper tracking of access to the room. In absence of access logs, unauthorized access and/or abnormal access to the system room may go unrecognized and responsible people in case of an unauthorized access may remain unidentified.	Logging of card reader mechanism should be enabled and logs should be retained for a period specified by the management. The logs should be reviewed periodically in order to identify any abnormal accesses made to the system room.
Unauthorized individuals are escorted by an authorized individual during visit to the system room. No visitor log is kept.	Although the visitors are escorted by the authorized individuals, absence of a visitor log decreases the traceability of access to the system room.	System room access of the visitors, who are not among the responsible personnel of CC, should be registered in a visitor log. The visitors should sign in a visitor book in order to enhance tracking of the visitors accepted in the system room.
There is a smoke detector and manual fire extinguishers in place. There are motion sensors and an alarm system in place. Air conditioning is in place. The servers has a heat alarm mechanism that sends e-mail when the heat exceeds a level. UPS is in place. Power generators	The heat alarm mechanism in place informs the responsible personnel by e-mail. In case of a situation where the responsible personnel are unable to access their e-mails, the delivered heat alarm e-mails may not reach their targets. The sharing of power generators with the other facilities of the university may result in power shortage for the critical servers in the system room in case of a long power failure.	The heat alarm should deliver the alert messages via SMS. It is planned in computer center to switch to SMS-messaging as well. There should be a power generator allocated only for the critical servers in computer center in order to decrease university operations interruption risk due to power failures.

Findings	Risks	Recommendations
are shared by the other facilities of the university.		
There is no preventative maintenance of computer components.	Preventive maintenance held for the critical equipment decreases the risks of unexpected hardware failures and interruption of the university operations resulting from hardware failures. Hence, in absence of preventive maintenance, the risk related to unexpected failures and/or major defects resulting from minor failures in hardware increases.	Preventive maintenance should be performed periodically to cover the critical hardware equipment of CC. For the equipment for which technical knowledge of the personnel is not adequate, third party services should be provided. For the services provided by third parties, the service levels and responsibilities of sides should be clearly stated in SLAs that are signed by both parties.

Communications and Operations Management

There are 13 questions asked having 1 gap and 7 deficiencies for related controls under Communications and Operations Management domain. It is noted a periodical review of the current systems capacity is not preformed. There is no formally documented operating procedure in place but they are planned to be established. There is no change management in place.

It is also noted that there is no formally documented Incident Management procedure in place. There is a system in use by the university by which IT users may convey their IT requests to Computer Center. But, this system is not utilized for central registration of the IT problems encountered. IT problems are neither prioritized nor reported to the management. The issues resolved are not documented.

For backup operations, it is noted that the backup tapes are kept at the cabinets inside the system room. The backup tapes are tested but testing does not take place regularly.

The risks and recommendations related to these findings is stated in Table 4.17

Table 4.17 – Computer Center Risks and Recommendations for Communications and Operations Management Domain

Findings	Risks	Recommendations
A periodical review of the current systems capacity is not preformed. Instead, a review of the system capacity is performed in cases of new acquisitions.	Not reviewing the systems capacity might result in not meeting the required level of resourced on sudden or regular demand increases. This could not only decrease the satisfaction level of the users but could also result in unexpected systems problems and event security breaches.	Management should request montly and yearly capacity analyssis of the information systems and should review them. The review results and possible actions to be taken should be communicated to the related personnel and be formally documented for further use.
There is no formally documented Incident Management procedure in place.	Creating effective responses to security incidents confronted requires a definition of security incidents, incident escalation procedures and incident handling management procedures. In absence of an Incident Management procedures, problems may be encountered in identifying security incidents, the required analysis steps and resolution means. Hence, the action steps taken may be insufficient to minimize the business effects of possible security incidents.	Formal incident management procedures should be in place in order to identify and manage any security incidents that may be confronted. The procedures should be periodically reviewed in order to keep up to date with the university operations requirements.

Findings	Risks	Recommendations
There is a system in use by the university by which IT users may convey their IT requests to Computer Center. But, this system is not utilized for central registration of the IT problems encountered. IT problems are neither prioritized nor reported to the management.	In absence of a formal prioritization of the IT problems, limited IT resources may be allocated to resolve the problems with lower priorities or less severe university operations impact. Hence, business priorities may be unmatched and the IT satisfaction provided may decrease. Management reporting increases management awareness of the IT problems. If management reporting of the encountered IT problems is not in place, awareness of the IT problems (both repeated and first-time problems) may be insufficient and delays in identifying potential solutions for the IT problems may be confronted.	Prioritization conditions should be clearly stated in a formally documented prioritization procedure. Management approval might be sought in prioritization process. IT problems should be reported to management periodically in order to increase awareness of the IT problems.
The issues resolved are not documented.	Creating a repository of the past issues increases the ability to identify the confronted IT issues and represents a reference for the resolution steps. If documentation of the resolved issues is not in place, several delays and/or erroneous actions may be encountered in the identification of the problems encountered and definition of the resolution steps to be followed. Absence of documentation of issues also contribute to difficulties in identifying trends of the problems.	The definition, analysis and resolution steps and results of IT issues should be registered in a central repository to serve as a future reference.
The backup tapes are kept at the cabinets inside the system room.	Offsite storage of backup tapes protects system data against disaster affecting the local offices of CC. Therefore, only onsite storage of backup tapes is in place, the risks related to business interruption in case of a disaster affecting CC and inability to recover the systems using the backup dates	At least one copy of backup tapes should be kept at an offsite location.

Findings	Risks	Recommendations
	increases.	
The backup tapes are tested but testing does not take place regularly.	Unless the backup tapes are tested regularly, the required recovery times may be misestimated. Another possible risk is that, any defects in backup tapes affecting the ability of recovering them may go undetected and tapes may be not functioning with the equipment set utilized for the recovery.	Backup tapes should be tested regularly in order to review recovery procedures performed, required recovery times and to observe whether the hardware equipment is compatible for the recovery of the backup tapes.
There is no formally documented operating procedures in place but they are planned to be established.	Absence of such procedures may lead to problems in communicating the security-related operational steps to be performed and gaps between what is done to perform the job and what is done. Therefore such procedures are required in order to minimize the grey areas between responsibilities of the related employees and steps to be performed.	Operating procedures should be completed as soon as possible to provide guidance on the operational jobs performed and responsibilities of personnel for these jobs.
There is no change management in place.	In absence of a formally established change management process, the risk related to intended/unintended migration of unauthorized and/or erroneous program changes to production environment increases. Thus, applications may function other than expected, erroneously and/or inefficiently.	A formal change management process should be in place, defining change initiation, development and testing of changes, migration steps and the required approvals taken at several milestones of change management process. Changes, their approvals and related information should be centrally registered in order to provide a traceable past data on the changes performed in systems.

Access Control

There are 11 questions asked having 4 gaps and 1 deficiency for related controls under Access Control domain. It is noted there is no formal management process for allocation and reallocation of e-mail passwords and no formal password management system. Before the recent purchase of Intrusion Prevention System, penetration testing is performed. However the test was not regularly performed during normal times. Although the audit logs are kept for security exceptions, they are not regularly reviewed. There is no token usage in place. The risks and recommendations related to these findings is stated in Table 4.18

Table 4.18 – Computer Center Risks and Recommendations for Access Control Domain

Findings	Risks	Recommendations
There is an Intrusion Prevention System purchased recently. Before the purchase, penetration testing is performed. But the test is not regularly performed during normal times.	Unless penetration tests are not regularly performed, the potential vulnerabilities of network and systems may remain undetected.	Penetration tests should be performed regularly at an interval that is specified by the management.
There is no formal management proces for allocation and reallocation of e-mail passwords. During the allocation process, the passwords are delivered to the users on a printed page during the registration. For reallocation, users are asked to apply to computer center personally in order to obtain a new password.	Printing passwords on papers in the allocation process may lead to the risk that unauthorized people may obtain other people's passwords.	Allocation of e-mail account passwords should be performed on the basis of personal application of the users, as in the reallocation process.
Secure connection is used for web page. (HTTPS protocol is used.) There is no token usage in place.	Although external connections are secured with firewalls and HTTPS protocol, not utilizing tokens increases the risk of exposure to security	Tokens should be utilized for remote connection to the systems.

Findings	Risks	Recommendations
	vulnerabilities.	
There is no formal password management system.	If a formal password management system is not in place, security vulnerabilities related to sharing of passwords and acquisition of passwords by unauthorized people increases. Therefore, unauthorized people may gain access to systems.	A formal password management process should be established. Users should be forced to select strong passwords by the system. Minimum and maximum password ages should be forced as well.
The audit logs are kept for security exceptions. The logs are, though not regularly, reviewed .	If exception logs are not reviewed periodically, several exceptions and security related events may remain unrecognized.	The exception logs should be reviewed periodically in order to identify any suspicious exceptions and log review results should be reported to management.

System Development and Maintenance

There are 4 questions asked having 1 gap and 2 deficiencies for related controls under System Development and Maintenance domain. It is noted that there is no formally documented system development methodology in place. But 'Analysis', 'Development' 'Testing' and 'Migrating' phases are performed. Furthermore there is no formal strict control procedure in place over implementation of changes to the information system. Digital signatures are not used to protect the authenticity and integrity of electronic documents. The risks and recommendations related to these findings is stated in Table 4.19

Table 4.19 – Computer Center Risks and Recommendations for System Development and Maintenance Domain

Findings	Risks	Recommendations
There is no formally documented system development methodology in place. But 'Analysis', 'Development' 'Testing' and 'Migrating' phases are performed.	In absence of a formal system development life cycle, needs of the university units may not be met within the allocated time frame in an efficient and cost effective manner and the required outputs at the required quality level may not be produced.	A formal and documented system development methodology should be adopted in CC. The required approvals in 'Analysis', 'Development' 'Testing' and 'Migration' phases should be clearly communicated and obtained. Documentation related to these phases should be retained in order to serve as a future reference.
Digital signatures are not used to protect the authenticity and integrity of electronic documents.	Digital signatures are utilized for authenticity and integrity of electronic documents. Without digital signatures, the source of the electronic document can not be verified and possible impairments made in the electronic document may be unrecognized.	Digital signatures should be utilized in order to obtain assurance on the authenticity and integrity of the electronic documents and compliance with current regulations.
There is no formal strict control procedures in place over implementation of changes to the information system.	In absence of formal control procedures over implementation of changes, the risk related to intendedly/unintendedly performed changes in information system increases. Thus, applications and systems may function other than expected, erroneously and/or inefficiently.	Implementation of changes should be performed only if required testing of changes is performed and approvals are obtained for the implementation. Testing results and obtained approvals should be retained. The changes performed should be reported to management reporting or communicated to the relevant users of the IT systems.

Business Continuity Management

There are 6 questions asked and all of the answers indicate deficiencies for related controls under Business Continuity Management domain. It is noted that although the roles and responsibilities in case of a business discontinuity are known by the Computer Center employees, there is no formally documented business continuity plan in the organization; testing of the plan is not applicable as well. The evacuation plan of the university facilities includes general information about the possible disasters and common emergency plans against them. However these possible disasters and their impact on the information systems are not identified and systems are not prioritized. The risks and recommendations related to these findings is stated in Table 4.20

Table 4.20 – Computer Center Risks and Recommendations for Business Continuity Domain

Findings	Risks	Recommendations
The roles and responsibilities in case of a business discontinuity are known by the Computer Center employees. But, there is no formally documented business continuity plan in the organization; testing of the plan is not applicable as well.	In absence of a business continuity plan, the university may not be able to react properly in case of an emergency. This could result in partial or total loss of the information systems as well as the critical system room.	There should be a process in place for developing and maintaining the business continuinty. The process should include defining a Business Continutiy Plan, reviewing and testing of the plan and applying necessary updates on the plan.
There is no BCP in place	If the systems are not priotized and scheduled for recovery in accordance with work impact, less critical systems which have less affect on the healt of the information systems are recovered while critical systems may remain damaged.	Information systems should be priotized according to the their impact on the university operations. Based on the prioritized systems, a recovery strategy should be constituted.
There is no BCP in place	If the continuity plans are not tested, they might include insufficient information about the updated/changes systems in place which could result in inappropriate/improper methods for providing continuity to the university operations.	The contingency plans should be tested at least annually in order to reflect the current status of the information systems in place. The test should also applied in order to see if the plans are applicable

Findings	Risks	Recommendations
		and sufficient for the systems.
The evacuation plan of the university facilities includes general information about the possible disasters and common emergency plans against them. However these possible disasters and their impact on the information systems are not identified.	In absence of identifying possible disasters that could cause interruptions to the university operations may result in insufficient response to these disasters. In absence of a strategy plan based on the risk assessment results could lead to total or partial loss of the information systems during times of disasters.	In order to define and implement Disaster Recovery Plans, risk assesment must be performed. Durign risk assessment phase, possible causes of business interruptions must be defined. The results of the risk assesment should be used to direct or update the overall business continuity plans in place.
There is no BCP in place	The lack of defining a time frame for recovery of the information systems may result in significant disruptions in the university operations and may even result in unauthorized access to the critical systems. Recovery plans might include insufficient information about the updated/changes systems in place which could result in inappropriate/improper methods for recovery.	Within the disaster recovery plans, time frames should be defined for the systems' recovery durations. This time frames should be based on the priotization of these systems related to their criticality level. The DRP's should also be tested at least annually and updated if necessary.
There is no BCP in place	In case of a disaster, the location where the information systems reside may partially or totally damaged and may become unreachable. In absence of the BCP and DRP storage off-site, on-site plans may not be reached and applied.	The BCP's and DRP's should be stored off-site and the location of these plans should be included in the plans.

Comparison of Registration Office and Computer Center

The conformance levels of two entities based on the controls under nine domains are compared in Table 4.21. Based on the results obtained from both entities, first the similarities than the differences on conformance levels are summarized. The numbers represents the number of controls for each domain and each conformance level.

Table 4.21 – Domain Based Statistics of Registration Office and Computer Center

Category	Effective		Gap		Deficiency	
	RO*	CC**	RO	CC	RO	CC
Security Policy	0	1	0	1	2	0
Organizational Security	0	1	0	2	7	4
Asset Classification and Control	2	2	1	2	3	2
Personnel Security	0	0	2	2	2	2
Physical and Environmental Security	2	4	3	2	3	2
Communications and Operations Management	5	5	1	1	7	7
Access Control	3	6	6	4	2	1
System Development and Maintenance	0	1	0	1	4	2
Business Continuity Management	0	0	0	0	6	6
Total	12	20	13	15	36	26

* RO: Registration Office
**CC: Computer Center

Similarities on Conformance Levels

By looking at the number of conformance levels, it could be said that although Computer Office has greater number of 'Effective' controls, in some domains the numbers are equal or near to equal (having both 'zero' in two domains). In the 'Communications and Operations Management' both entities have same number of controls under each conformance level. Although not all the controls have same conformance levels for both entities it could be said that both entities have equal level of conformance in proper and secure use of information processing facilities. This similarity is also applicable for 'Personnel Security' domain, this time having the same conformance levels for the same controls. This result could be explained as applying the same procedures that the university encourages. Another significant similarity between two entities is that both have six deficiencies out of six controls for 'Business Continuity Management' domain.

Difference in Conformance Levels

In general, Computer center tend to have more controls with 'Gaps' while Registration Office has ten more 'Deficiencies' then Computer Center in its controls. In particular, Registration Office has more 'Gaps' and 'Deficiencies' for 'Access Control' and 'Organizational Security' domains, while Computer Center has more 'Effective' controls. This could be explained with outsourcing of the security services to the 3rd party service provider without effective monitoring of the actions performed by this service provider.

CHAPTER V

CONCLUSION AND IMPLICATIONS FOR FURTHER RESEARCH

Conclusion

The aim of this study is to propose an information security management framework based on the BS 7799/ISO 17799 standard and apply this framework on two selected entities in a state university. Literature survey has been performed in order to provide detailed information about information security and its need for today's business life. BS 7799/ISO 17799 standard is also mentioned in the literature survey to support the framework proposed. In the framework development section, the controls are prepared in accordance with the nine domains of the BS 7799/ISO 17799 standard. Afterwards, interviews are performed in two entities of a state university and the status of these entities with respect to the controls identified is appraised. Based on the appraised status of the entities, conformance levels are identified and risk and recommendations are documented accordingly. Then, the conformance levels are compared and details of similarities and differences are discussed.

Based on the conformance levels identified, it is clear that the registration office lacks more 'effective' conformance levels while having more 'deficiencies' due to level of control on the 3rd party service provider activities in the systems. Most of the security operations are outsourced to a 3rd party service provider and neither adequate monitoring of activities performed by the 3rd party service provider is available, nor regular reviews are requested / performed by the registration office. The only bounding document in place is the agreement made with the third party, which does not contain any security related clauses either.

Since the most valuable information related to the registration office is the ‘grades’ of the students, it is not necessary to apply critical security measures. However, maintaining an information security management framework will certainly increase efficiency of the methods used for handling the confidentiality issues. The proposed framework in this study also indicates the critical action points to be taken into consideration and provides detailed information about the risks and recommendations related to these points.

Although computer center has more ‘effective’ conformance levels and less ‘deficiencies’, it still lacks important points of maintaining information security. Regarding information security, the ‘confidentiality’ concept is the main concern of the registration office, whereas the ‘availability’ concept is probably the main concern of the computer center since it provides the infrastructure of network throughout the whole university premises. On the contrary, the computer center lacks proper and formal plans for business continuity and disaster recovery. These plans should immediately be developed and put into effect as soon as possible in order to provide the actions to be performed for obtaining business continuity in the university and the computer center itself. The risks and recommendations related to these and other controls are provided with the proposed framework.

The proposed information security management framework could be used as an initial point of assessing the information security controls of an entity. Since it is based on the BS 7799/ISO 17799 standard, it would also help the entity to comply with the standard or standards accordingly. It would provide preliminary as well as detailed roadmap for developing and maintaining information security practices.

Limitations

The proposed information security management framework is applied only to two case studies as an initial point. Furthermore, these two case studies are different entities; they are under the organization of only one state university. Application of these case studies at least five entities in five different organizations may lead to obtainment of more sufficient and comparable results. Different sectors may also be compared with different firms or organizations.

Implications for Further Research

The interviews performed with the responsible people are mainly based on questions and answers and no evidence has been obtained. In order to support the responds obtained and detail the study, documents related to the questions asked may be obtained from the organizations. This would also help the researcher to decide on the conformance level in a more efficient way and with a less judgmental approach.

The conformance levels are identified by personal judgment in a qualitative approach. Further studies may handle the levels in a more quantitative approach, scaling the conformance levels based on the efforts needed for full conformance with the controls. A scale with five or seven levels may be utilized, having ‘effective’ in one end and ‘deficiency’ in the other. This method would also help the researcher to perform further quantitative analysis based on the numerical results.

After the realization of the interviews and analysis of the results, a report may be produced. This report may include the whole responds received with statistical information based on the analysis on the results. Furthermore, the risks and recommendations may be documented in a pre-determined format which may change based on the case studies selected as well. The final part of the report may also include the summary of the study, stressing the critical points and findings based on the results.

The study is performed according to the BS 7799/ISO 17799 standard. However in 2007, ISO is planning to develop a new series of information security standards, after which BS 7799/ISO 17799 will lose its validity. The tentative plan includes information security management system requirements, code of practice, implementation guidance, information security management metrics and measurement and information security risk management (Sweren, 2006). Any or all of these standards may be taken as basis for further researches and studies.

Furthermore, main approach of this study to the information security is from a management perspective; mostly giving emphasis on policies and procedures. A further study may be implemented in order to analyze the technical aspects of information security and harmonize the results related to technical aspects with the results of this study.

APPENDIX

Questionnaire

Security Policy

1) There should be an Information security policy, which is approved by the management, published and communicated as appropriate to all employees. It should state the management commitment and set out the organizational approach to managing information security.
2) University strategy should address IT strategy

Organizational Security

1) Risks from third party access should be identified and appropriate security controls implemented. The types of accesses should be identified, classified and reasons for access are justified.
2) Remote access by vendors should be initiated by the University not the vendor
3) Vendor accounts should be disabled when not in use
4) Vendor password should be regularly changed
5) Information Security Officer should report to a senior level
6) The function should be appropriately separated from the information systems department.
7) The Information Security Officer should monitor compliance with the policy and report breaches

Asset Classification and Control

1) Management should define and implement security levels related to the sensitivity of specific information.
2) Data owners should be assigned for all systems
3) There should be a central log of IT equipment and this should be reconciled to physical assets on a periodic basis
4) All movements of IT equipment should be logged
5) Disposal of IT equipment must be authorized by management.
6) There should be an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.

Personnel Security

1) Job description should detail scope of role and accountabilities
2) Staff should have sufficient experience and training for role
3) Employees should be asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment. This agreement should cover the security of the information processing facility and organization assets.
4) Terms and conditions of the employment should cover the employee's responsibility for information security. Where appropriate, these responsibilities might continue for a defined period after the end of the employment.

Physical and Environment Security

1) Access to sensitive IT areas should be restricted to IT staff by keypad or other security mechanism.
2) Physical access into the computer room should be limited to those individuals whose primary functions require them to have access
3) A record should be kept of visitors to the data room
4) Unauthorized individuals should be escorted by an authorized individual during visit.
5) "Fire suppression equipment should be installed
Temperature and humidity controllers should be in place
Water and drainage pipes should be routed away from IT systems
Uninterruptible power supply (UPS)
Emergency Power System (EPS) (e.g., generators, transformers)"
6) Periodic preventative maintenance of computer components
7) The rooms, which have the Information processing service, should be locked or should have lockable cabinets or safes.
8) The power and telecommunications cable carrying data or supporting information services should be protected from interception or damage.

Communications and Operations Management

1) Management should review systems capacity on a regular basis to ensure that there are sufficient resources for demand increases
2) Incident Management procedure should exist to handle security incidents.
3) IT problems should be logged and tracked for resolution.
4) IT problems should be prioritized and subject to summary reports to management.
5) Issues which have been resolved should be documented for future reference
6) Back-up of essential business information such as production server, critical network components, configuration backup etc., should be taken regularly. Example: Mon-Thu: Incremental Backup and Fri: Full Backup.
7) The backup media along with the procedure to restore the backup should be stored securely and well away from the actual site.
8) Backup tapes should be properly labeled and organized to facilitate recovery
9) The backup media should be regularly tested to ensure that they could be restored within the time frame allotted in the operational procedure for recovery.
10) The security Policy should identify any Operating procedures such as Back-up, Equipment maintenance etc.
11) All programs running on production systems should be subject to strict change control i.e., any change to be made to those production programs need to go through the change control authorization.
12) There should a control against malicious software usage. The security policy should address software licensing issues such as prohibiting usage of unauthorized software.
13) There should be a policy in place for the acceptable use of electronic mail or does security policy does address the issues with regards to use of electronic mail.

Access Control

1) Firewall, Internet Connection and E-Mail service should work fast, secure and should be reliable
2) Anti-virus software should be implemented and regularly updated for all users
3) Penetration testing should be considered
4) There should be a formal user registration and deregistration procedure for granting access to multi-user information systems and services.
5) The allocation and reallocation of passwords should be controlled through a formal management process.
6) There should be guidelines in place to guide users in selecting and maintaining secure passwords.
7) There should be authentication mechanisms for challenging external connections. Examples: Cryptography based technique, hardware tokens, software tokens, challenge/ response protocol etc.
8) The network (where business partner's and/ or third parties need access to information system) should be segregated using perimeter security mechanisms such as firewalls.
9) There should be network connection controls for shared networks that extend beyond the organizational boundaries. Example: electronic mail, web access, files transfers, etc.
10) There should be a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form,
11) The audit logs recording exceptions and other security relevant events are should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

System Development and Maintenance

1) Systems developments should be undertaken in a structured way, using systems development lifecycle:
- Project planning, feasibility study
- Systems analysis, requirements definition
- Systems design
- Implementation
- Integration and testing
- Acceptance, installation, deployment
2) Digital signatures should be used to protect the authenticity and integrity of electronic documents.
3) Strict controls should be in place over access to program source libraries. This is to reduce the potential for corruption of computer programs.
4) There should be strict control procedures in place over implementation of changes to the information system. This is to minimize the corruption of information system.

Business Continuity Management

1) There should be a managed process in place for developing and maintaining business continuity throughout the organization. This might include Organization

wide Business continuity plan, regular testing and updating of the plan, formulating and documenting a business continuity strategy etc.,

2) Systems should be prioritized and scheduled for recovery in accordance with work impact

3) Contingency plans should be tested on a regular basis to ensure they work.

4) Events that could cause interruptions to business process should be identified example: equipment failure, flood and fire. A risk assessment should be conducted to determine impact of such interruptions. A strategy plan should be developed based on the risk assessment results to determine an overall approach to business continuity.

5) Plans should be developed to restore business operations within the required time frame following an interruption or failure to business process. The plan should be regularly tested and updated.

6) Copies of the contingency/ disaster recovery plan and restart/recovery procedures should be stored off-site.

Table 1 – Questionnaire Results of Registration Office

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Security Policy	There should be an Information security policy, which is approved by the management, published and communicated as appropriate to all employees. It should state the management commitment and set out the organisational approach to managing information security.	There is no formal written information security policy in place	In absence of an information security policy, the methods for securing the university operations, critical systems, critical information may not be sufficient and may not include every critical systems in place.	The Information Security Policy constitutes a security framework for the organizations.	Deficiency
Security Policy	University strategy should address IT strategy	N/A	Not incorporating the IT strategy with the organizations (hereby 'University') may lead to insufficient implementation of the IT strategy because of lack of management support. That could result in IT Strategy to be remained out-dated or insufficient for latest threats and/or opportunities.	Both the university strategy and IT strategy should adress the other in order to support each other and to remain updated. Management support would facilitate the implementation of IT Strategy and would in return provide the safety of the university's information assets.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Organizational Security	Risks from third party access should be identified and appropriate security controls implemented. The types of accesses should be identified, classified and reasons for access are justified.	The risks are not identified and appropriate security controls are not implemented since the third party itself established and monitors the access to the production system.	Not classifying the possible types and reasons of accesses may result in unidentified acccess to crtitical data and security breaches that could not be identified at the firewall level.	The types of access related to the third parties should be identified, justified and classified. According to every type of access, necessary security controls should be designed and implemented. At least one officer should be responsible for the access of the third parties.	Deficiency
Organizational Security	Remote access by vendors should be initiated by the University not the vendor	The remote access is initiated by the third party.	Not monitoring the remote access of vendors could lead into unauthorized access to critical information. Unauthorized remote access could also pose a threat to Registration Office's information systems letting them vulnarable to security attacks.	Immediate action must be taken in order to restrict the remote access of third parties. Necessary policy and procedures must be documented and applied and remote access connection must be monitored starting from initiation till termination.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Organizational Security	Vendor accounts should be disabled when not in use	Vendor accounts are not disabled and under control of the third party.	Although the firewall is configured not to allow unauthorized access, enabled accounts could be compromised internally to access to critical systems files.	Vendor accounts should be disabled during inactivity. The activities performed by the vendor account should also be logged and reviewed as an additional control.	Deficiency
Organizational Security	Vendor password should be regularly changed	The password control is performed by the third party	Unchanged vendor passwords increases the risk of unauthorized use of the vendor accounts for accessing critical system files.	Vendor passwords should be changed after each usage and they should be change by Registration Office.	Deficiency
Organizational Security	Information Security Officer should report to a senior level	There is not information security offices function in place	Not having a seperate information security officer in place decreases the attention given to the security of the information systems. That could result in unauthorized exposure of the critical data, manipulation and even deletion of the critical data.	There should be information security officer in place seperate from the IT department. IS officer should directly report to the management about the security strategy, security operations and security actions planned to be taken.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Organizational Security	The function should be appropriately separated from the information systems department.	N/A	same as above	The information security officer funtion should be seperated from IT department. The responsbilities of the function should be defined on the corporate level.	Deficiency
Organizational Security	The Information Security Officer should monitor compliance with the policy and report breaches	N/A	same as above	Information security officer should define the security policies as well as monitor the compliance of the operations with those policies. IS officer should report and non-compliance issues and security breaches to the management.	Deficiency
Asset Classification and control	Management should define and implement security levels related to the sensitivity of specific information.	There is no formal definition of the security levels. They are reviewed on necessity	Not defining the security levels to the specific information may result in unauthorized access to the sensitive data. That could even result in not recognizing this kind of security breach.	Management should first consitute an information repository regarding the university information systems and data related to the university operations. Then the security levels of the information shoule be defined. Finally necessary	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
				procedures should be designed to sustain the security of critical information.	
Asset Classification and control	Data owners should be assigned for all systems	Data owners are not defined.	Not assigning data owners may result unexpected exposure of the critical and sensitive data to unauthorized users.	After defining the system inventory and related security levels to be preserve, data owners should be assigned for these systems. The data owners should be provided the roles and responsibilites related to the systems they are responsible of based on the criticality of the systems and measures that are defined to preserve the security	Deficiency
Asset Classification and control	There should be a central log of IT equipment and this should be reconciled to physical assets on a periodic basis	The IT equipment is traced and logged by the central university equipment registration. There is no formal list kept by the Registration Office.	IT equipments could be stolen or damaged and they cannot be noticed until there is a necessity. Further more there may be a risk in place that the equipment is somehow logged mistakenly and this would go unnoticed for a long	A central log for the IT equipment should be designed. There should be a perodic reconciliation of the log with the physical asset for the integrity of the	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
			time.	log.	
Asset Classification and control	All movements of IT equipment should be logged	The movements are manually logged by the university.	No risks identified.	N/A	Effective
Asset Classification and control	Disposal of IT equipment must be authorized by management.	The equipment to be disposed is sent to related university office by the approval of the management.	No risks identified.	N/A	Effective
Asset Classification and control	There should be an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.	There is no formal information classification scheme or guideline in place.	In absence of information classification scheme or guideline, the sensitive data may be compromised without knowledge of the IT personnel. IT personnel may lack awareness of handling method of the sensitivie information.	A formal information classification scheme should be in place, defining levels of data and data handling procedures related to these levels. Access to the data in the systems	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
				should be restricted in line with the levels defined in the scheme.	
Personnel Security	Job description should detail scope of role and accountabilities	The job descriptions are not documented as a personnel base but rather as a division base. The scope of each division is brifly explained.	Undefined role and responsbilities may result in lack of appropriate skills and knowledge identifying and handling security incidents.	Specific job descriptions for personnel should be in place, covering responsibilities and accountabilities of personnel. Personnel should be provided with a clear description of accountability areas.	Gap
Personnel Security	Staff should have sufficient experience and training for role	The staff attends to the internal training of the university on a regulare basis to update or revise their technical skills.	Lack of adequate training of the IT personnel may result in inproper planning of the security systems and inadequate handling of the security incidents.	IT personnel should be provided with regular trainings on IT systems and IT security. The trainings should be provided in line with a training program accepted by the management. IT personnel should be provided by the means to increase their level of experience in IT	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
				systems.	
Personnel Security	Employees should be asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment. This agreement should cover the security of the information processing facility and organisation assets.	The employees do not sign a seperate confidentialiy or non-discosure agreement or these terms are not included in the contracts they sign when they are employed.	Not signing a confidentiality aggreement may result in lack of awareness about the usage of information systems. That could increase the risk of unintended misuse of the systems in place.	Personnel with access to critical data sources should sign a confidentiality aggreement with the university.	Deficiency
Personnel Security	Terms and conditions of the employment should cover the employee's responsibility for information security. Where appropriate, these responsibilities might continue for a defined period after the end of the employment.	Terms and conditions of the employment does not cover the employee's responsibility for information security	If the responsibilities of the personnel for information systems is not properly delivered to the personnel, the risk of unintended systems disruptions/misuse may increase.	The responsibilities of personnel for IT security should be clearly communicated. Terms and conditions of employment may obtain security related responsibilities. Personnel may be required to sign a declaration indicating being acknowledged on security related responsibilities.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Physical and Environment Security	Access to sensitive IT areas should be restricted to IT staff by keypad or other security mechanism.	The system room is access via standard door and key. There is no keypad or card-reader mechanism in place for the system room entry. The outer room door has a keypad equipped with a password entrance. The keypad is activated during non-work hours.	Not maintaining a security mechanism for the access to sensitive IT areas could result in unauthorized access to the system resources. Unauthorized individuals could steal, manipulate or even destroy ciritical information without dealing with security measures applied on the software level. The security of the critical physical assets would also be in danger without proper access restrictions.	The system room access must be restricted only authorized personnel by using a keypad or other security mechanism.	Deficiency
Physical and Environment Security	Physical access into the computer room should be limited to those individuals whose primary functions require them to have access	The key to the system room is kept only one personnel	Restricting access to the system room to one personnel may seem a good practice but it would create a risk of making the access to the system room difficult in case of emergencies if that personnel is not available. The critical system resources may be partially or totally lots in case of disasters or similar incidents.	There should be security mechanism in place to restrict the access to the system room to authorized individuals. The list of the authorized individuals should be managed and approved by the necessary level of management.	Gap
Physical and Environment Security	A record should be kept of visitors to the data room	No record is kept for the visitors to the room.	Logging of access to the system room enables proper tracking of access to the room. In absence of access logs, unauthorized access and/or abnormal access to the system room may go unrecognized	Logging of card reader mechanism should be enabled and logs should be retained for a period specified by the management. The logs	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
			and responsible people in case of an unauthorized access may remain unidentified.	should be reviewed periodically in order to identify any abnormal accesses made to the system room.	
Physical and Environment Security	Unauthorized individuals should be escorted by an authorized individual during visit.	Unauthorized individuals are escorted by an authorizd individual during visit. No visitor log is kept.	Although the visitors are escorted by the authorized individuals, absence of a visitor log decreases the traceability of access to the system room.	System room access of the visitors, who are not among the responsible personnel of Registration Office, should be registered in a visitor log. The visitors should sign in a visitor book in order to enhance tracking of the visitors accepted in the system room.	Gap
Physical and Environment Security	Fire suppression equipment should be installed Temperature and humidity controllers should be in place Water and drainage pipes should be routed away from IT systems Uninterruptible power supply (UPS) Emergency Power System (EPS) (e.g., generators,	Fire detectors are in place but conventional fire extinguishers are used. There is no humidity controller in place. The water and drainage pipers are routed away from IT systems but there is no raised floor or lowered ceiling is used. There is one UPS in the system room	Not maintaining necessary environmental controls for system room could result in unexpected damages on the physical assets in case of fire, flood, electricity cuts, etc.	Fire extinguishers that contains material which would not harm electronic equipment (i.e. FM-200) must be used. Humidity detectors must me in place. Use of raised floor or lowered ceiling for cabling must be considered.	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
	transformers)	There is air conditioning in place. Power Generator is shared with the rest of the university			
Physical and Environment Security	Periodic preventative maintenance of computer components	There is periodic preventative maintenance of computer components	Preventive maintenance held for the critical equipment decreases the risks of unexpected hardware failures and interruption of the university operations resulting from hardware failures. Hence, in absence of preventive maintenance, the risk related to unexpected failures and/or major defects resulting from minor failures in hardware increases.	Preventive maintenance should be performed periodically to cover the critical hardware equipment of Registration Office. For the equipment for which technical knowledge of the personnel is not adequate, third party services should be provided. For the services provided by third parties, the service levels and responsibilities of sides should be clearly stated in SLAs that are signed by both parties.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Physical and Environment Security	The rooms, which have the Information processing service, should be locked or should have lockable cabinets or safes.	The servers, the network equipment is keps in locked and/or lockable cabinets.	No risks identified.	N/A	Effective
Physical and Environment Security	The power and telecommunications cable carrying data or supporting information services should be protected from interception or damage.	There is a seperate cover for the cables in the system room and during the corridors which prevents the cables to exposed to critical dangers.	No risks identified.	N/A	Effective
Communications and Operations Management	Management should review systems capacity on a regular basis to ensure that there are sufficient resources for demand increases	The software developers monitors and reviews the system capacity but not in regular basis.	Not reviewing the systems capacity might result in not meeting the required level of resourced on sudden or regular demand increases. This could not only decrease the satisfaction level of the users but could also result in unexpected systems problems and event security breaches.	Management should request montly and yearly capacity analyssis of the information systems and should review them. The review results and possible actions to be taken should be communicated to the related personnel and be formally documented for further use.	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Communications and Operations Management	Incident Management procedure should exist to handle security incidents.	There is no formal and documented incident management procedure in place.	Creating effective responses to security incidents confronted requires a definition of security incidents, incident escalation procedures and incident handling management procedures. In absence of an Incident Management procedures, problems may be encountered in identifying security incidents, the required analysis steps and resolution means. Hence, the action steps taken may be insufficient to minimize the business effects of possible security incidents.	Formal incident management procedures should be in place in order to identify and manage any security incidents that may be confronted. The procedures should be periodically reviewed in order to keep up to date with the university operations requirements.	Deficiency
Communications and Operations Management	IT problems should be logged and tracked for resolution.	Problems and requests are obtained via a form page on the web site. They are sent to the registration commission of the university. They are discussed and necessary actions are taken according to the decisions taken in the commission meeting. The results are kept in hard copy format	No risks identified.	The logs related to IT security should be reviewed on a periodical basis in order to effectively identify IT problems and provide resolution.	Effective

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Communications and Operations Management	IT problems should be prioritized and subject to summary reports to management.	The registration commission priotorizes the problems. The results are kept in hard copy format.	No risks identified.	N/A	Effective
Communications and Operations Management	Issues which have been resolved should be documented for future reference	The resolved issues are also documented in the issue files.	No risks identified.	N/A	Effective
Communications and Operations Management	Back-up of essential business information such as production server, critical network components, configuration backup etc., should be taken regularly. Example: Mon-Thu: Incremental Backup and Fri: Full Backup.	The data in the system is backed up dailiy on CD's. They are cycled when the capacity of the CD's are full. Application backups are not taken regularly but they are taken twice in a year on average	No risks identified.	N/A	Effective
Communications and Operations Management	The backup media along with the procedure to restore the backup should be stored securely and well away from the actual site.	The backup CD's are kept on site in a file cabinet	Offsite storage of backup tapes protects system data against disaster affecting the local offices of Registration Office. Therefore, only onsite storage of backup tapes is in place, the risks related to business interruption in case of a disaster affecting Registration Office and inability to recover the	At least one copy of backup tapes should be kept at an offsite location.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
			systems using the backup dates increases.		
Communications and Operations Management	Backup tapes should be properly labeled and organized to facilitate recovery	The backup CD's are properly labeled.	No risks identified.	N/A	Effective
Communications and Operations Management	The backup media should be regularly tested to ensure that they could be restored within the time frame allotted in the operational procedure for recovery.	The backup CD's are not tested.	Unless the backup tapes are tested regularly, the required recovery times may be misestimated. Another possible risk is that, any defects in backup tapes affecting the ability of recovering them may go undetected and tapes may be not functioning with the equipment set utilized for the recovery.	Backup tapes should be tested regularly in order to review recovery procedures performed, required recovery times and to observe whether the hardware equipment is compatible for the recovery of the backup tapes.	Deficiency
Communications and Operations Management	The security Policy should identify any Operating procedures such as Back-up, Equipment maintenance etc.,	Since there is no formal documented security policy in place, operating procedures are not identified.	Absence of such procedures may lead to problems in communicating the security-related operational steps to be performed and gaps between what is done to perform the job and what is done. Therefore such procedures are required in order to	Operating procedures should be completed as soon as possible to provide guidance on the operational jobs performed and responsibilities of personnel for these jobs.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
			minimize the grey areas between responsibilities of the related employees and steps to be performed.		
Communications and Operations Management	All programs running on production systems should be subject to strict change control i.e., any change to be made to those production programs need to go through the change control authorisation.	All of the changes applied to the programs on production system is handled by the third party. The registration office interferes only at the testing phase.	In absence of a formally established change management process, the risk related to intended/unintended migration of unauthorized and/or erroneous program changes to production environment increases. Thus, applications may function other than expected, erroneously and/or inefficiently.	A formal change management process should be in place, defining change initiation, development and testing of changes, migration steps and the required approvals taken at several milestones of change management process. Changes, their approvals and related information should be centrally registered in order to provide a traceable past data on the changes performed in systems.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Communications and Operations Management	There should a control against malicious software usage. The security policy should address software licensing issues such as prohibiting usage of unauthorised software.	There is no control in place for malicious software. Since there is no formal and documented security policy in place, software licensing issues are not properly addressed.	Lack of controls over malicious software and unauthorized software may result in expose of critical information to unauthorized individuals.	Necessary security practices must be implemented to control malicious software usage(i.e. Anti-malware software). Information Security policy must address the software licencing isssues including usage of unauthorized software. Periodic controls must be in place to prevent usage of unauthorized software.	Deficiency
Communications and Operations Management	There should be a policy in place for the acceptable use of electronic mail or does security policy does address the issues with regards to use of electronic mail.	There is no policy in place for the acceptable use of electronic mail.	Usage of e-mail without having enough awareness of the possible dangers may result in expose of critical data to unauthorized individuals and lloss of information resources.	There should be a seperate policy in place and published to all of the users regarding the acceptable use of e-mail. This policy could refer to main information security policy for broader comprehension of the information security dangers.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Access Control	Firewall, Internet Connection and E-Mail service should work fast, secure and should be reliable	Firewall is managed by the Registration Office and the Internet Connection is fast and secure. E-mail service is provided by the Information Systems Office of the university.	No risks identified.	N/A	Effective
Access Control	Anti-virus software should be implemented and regularly updated for all users	There is no central anti-virus solution in place. Anti virus application is installed on some of the computers.	Todays sophisticated viruses could harm system resources in short periods of times. Viruses that go unnoticed could manipulate or delete critical data or even let unauthorized individuals gain access to these resources.	A central anti-virus solution should be implemented. The maintenance of this software and update of the definitions must be controlled by documented procedures and practices. Whole systems resources including individual computers must be scanned for viruses periodically (min. weekly)	Gap
Access Control	Penetration testing should be considered	The third party performs penetration testing. The results are not presented to the Registration Office.	Third parties may not pay attention on all of the security vulnerabilities in the systems or may not share this information with Registration Office. That could lead to unauthorized access to critical information and damaging of the system resources.	Penetration testing must be performed periodically by an authorized third party with a contact in which necessary requirements and obligations are addressed. The results	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
				of the testing must be evaluated and necessary actions must be taken.	
Access Control	There should be a formal user registration and deregistration procedure for granting access to multi-user information systems and services.	There is a formal rule for providing Registration ID to the students. The ID and the password is provided to the student with a sticked paper on their file.	In absence of a formal user registration and deregistration process, unauthorized people may gain access to system resources. This in return leads to the risk of intended malicious transactions in the system performed by unauthorized people. Data integrity and confidentialy may be compromised in absence of this process as well.	A formal user registration and deregistration process should be established. In addition to this, compliance to these procedures should be regularly assessed and results should be provided to the high level administration.	Gap
Access Control	The allocation and reallocation of passwords should be controlled through a formal management process.	There is no formal and documented procedure for allocating and reallocating the passwords.	Printing passwords on papers in the allocation process may lead to the risk that unauthorized people may obtain other people's passwords.	Allocation of e-mail account passwords should be performed on the basis of personal application of the users, as in the reallocation process.	Deficiency
Access Control	There should be guidelines in place to guide users in selecting and maintaining secure passwords.	On the 'Change Password' option in the registration menu, password guideline is provided to the user to guide	No risks identified.	N/A	Effective

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
		in selecting secure passwords.			
Access Control	There should be authentication mechanisms for challenging external connections. Examples: Cryptography based technique, hardware tokens, software tokens, challenge/ response protocol etc.,	There is no authentication mechanism in place except for User ID and password.	Although external connections are secured with firewalls and HTTPS protocol, not utilizing tokens increases the risk of exposure to security vulnerabilities.	Tokens should be utilized for remote connection to the systems.	Gap
Access Control	The network (where business partner's and/ or third parties need access to information system) should be segregated using perimeter security mechanisms such as firewalls.	The third party can access to the applications of the Registration Office at any time.	Lack of nesessary security mechanism in order to protect network of Registration Office could lead to unauthorized access to the system resources. Even though third party is allowed to access to system resources, insuffficient access rules may increase the risk of accesing these resources without authorization of Registration Office.	Firewalls must be in place and access rules must be configured appropriately so that third party access is monitored and unauthorized attempts of accesses are blocked.	Deficiency
Access Control	There should be network connection controls for shared networks that extend beyond the organisational boundaries. Example: electronic mail, web access, file transfers, etc.,	The firewall in place controls the network connection for web access, file transfers, etc.	No risks identified.	N/A	Effective

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Access Control	There should be a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form,	The only password controls in place are not using specific characters in the password which are provided at the web site and not using passwords with more than 10 characters. There is no password management system in place.	If a formal password management system is not in place, security vulnerabilities related to sharing of passwords and acquisition of passwords by unauthorized people increases. Therefore, unauthorized people may gain access to systems.	A formal password management process should be established. Users should be forced to select strong passwords by the system. Minimum and maximum password ages should be forced as well.	Gap
Access Control	The audit logs recording exceptions and other security relevant events are should be produced and kept for an agreed period to assist in future investigations and access control monitoring.	The third party is maintaining the logs of the systems in place. There is no control of the Registration Office on the log system.	If exception logs are not reviewed periodically, several exceptions and security related events may remain unrecognized.	The exception logs should be reviewed periodically in order to identify any suspicious exceptions and log review results should be reported to management.	Gap
System Development and Maintenance	Systems developments should be undertaken in a structured way, using systems development lifecycle: - Project planning, feasibility study - Systems analysis, requirements definition - Systems design - Implementation - Integration and testing	All system development is maintained by the third party.	In absence of a formal system development life cycle, needs of the university units may not be met within the allocated time frame in an efficient and cost effective manner and the required outputs at the required quality level may not be produced.	A formal and documented system development methodology should be adopted in Registration Office. The required approvals in 'Analysis', 'Development' 'Testing' and 'Migration' phases should be clearly communicated and obtained.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
	- Acceptance, installation, deployment			Documentation related to these phases should be retained in order to serve as a future reference.	
System Development and Maintenance	Digital signatures should be used to protect the authenticity and integrity of electronic documents.	Digital signatures are not used.	Digital signatures are utilized for authenticity and integrity of electronic documents. Without digital signatures, the source of the electronic document can not be verified and possible impairments made in the electronic document may be unrecognized.	Digital signatures should be utilized in order to obtain assurance on the authenticity and integrity of the electronic documents and compliance with current regulations.	Deficiency
System Development and Maintenance	Strict controls should be in place over access to program source libraries. This is to reduce the potential for corruption of computer programs.	There is no strict controls in place over access to program source libraries.	Lack of strict controls over access to program source libraries could lead to unauthorized access to the source libraries which could lead to potential corruption of programs used. A malicious user could alter the program source in order to gain benefit from the program.	Access to the program source libraries must be restricted to the individuals who could only migrate developed codes from test or development environment to production environment.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
System Development and Maintenance	There should be strict control procedures in place over implementation of changes to the information system. This is to minimise the corruption of information system.	All system development is maintained by the third party.	In absence of formal control procedures over implementation of changes, the risk related to intendedly/unintendedly performed changes in information system increases. Thus, applications and systems may function other than expected, erroneously and/or inefficiently.	Implementation of changes should be performed only if required testing of changes is performed and approvals are obtained for the implementation. Testing results and obtained approvals should be retained. The changes performed should be reported to management reporting or communicated to the relevant users of the IT systems.	Deficiency
Business Continuity Management	There should be a managed process in place for developing and maintaining business continuity throughout the organisation. This might include Organisation wide Business continuity plan, regular testing and updating of the plan, formulating and documenting a business continuity strategy etc.,	There is no specific Business Continuity Plan in place for the computer systems at the Registration Office. The office is subject to the general building directives in case of a disaster.	In absence of a business continuity plan, the university may not be able to react properly in case of an emergency. This could result in partial or total loss of the information systems as well as the critical system room.	There should be a process in place for developing and maintaining the business continuinty. The process should include defining a Business Continutiy Plan, reviewing and testing of the plan and applying necessary updates on the plan.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Business Continuity Management	Systems should be prioritized and scheduled for recovery in accordance with work impact	Systems are not priotized.	If the systems are not priotized and scheduled for recovery in accordance with work impact, less critical systems which have less affect on the healt of the information systems are recovered while critical systems may remain damaged.	Information systems should be priotized according to the their impact on the university operations. Based on the prioritized systems, a recovery strategy should be constituted.	Deficiency
Business Continuity Management	Contingency plans should be tested on a regular basis to ensure they work.	There is no formal contingency plan in place	If the continuity plans are not tested, they might include insufficient information about the updated/changes systems in place which could result in inappropriate/improper methods for providing continuity to the university operations.	The contingency plans should be tested at least annually in order to reflect the current status of the information systems in place. The test should also applied in order to see if the plans are applicable and sufficient for the systems.	Deficiency
Business Continuity Management	Events that could cause interruptions to business process should be identified example: equipment failure, flood and fire. A risk assessment should be conducted to determine impact of such interruptions. A strategy plan should be developed based on the risk assessment results to	The evacuation plan of the university facilities includes general information about the possible disasters and common emergency plans against them. However these possible disasters and their impact on the information systems are not identified.	In absence of identifying possible disasters that could cause interruptions to the university operations may result in insufficient response to these disasters. In absence of a strategy plan based on the risk assessment results could lead to total or partial loss of the information systems during times of disasters.	In order to define and implement Disaster Recovery Plans, risk assesment must be performed. Durign risk assessment phase, possible causes of business interruptions must be defined. The results of the risk assesment should be	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
	determine an overall approach to business continuity.			used to direct or update the overall business continuity plans in place.	
Business Continuity Management	Plans should be developed to restore business operations within the required time frame following an interruption or failure to business process. The plan should be regularly tested and updated.	There is no BCP in place	The lack of defining a time frame for recovery of the information systems may result in significant disruptions in the university operations and may even result in unauthorized access to the critical systems. Recovery plans might include insufficient information about the updated/changes systems in place which could result in inappropriate/improper methods for recovery.	Within the disaster recovery plans, time frames should be defined for the systems' recovery durations. This time frames should be based on the priotization of these systems related to their criticality level. The DRP's should also be tested at least annually and updated if necessary.	Deficiency
Business Continuity Management	Copies of the contingency/ disaster recovery plan and restart/recovery procedures should be stored off-site.	There is no BCP in place	In case of a disaster, the location where the information systems reside may partially or totally damaged and may become unreachable. In absence of the BCP and DRP storage off-site, on-site plans may not be reached and applied.	The BCP's and DRP's should be stored off-site and the location of these plans should be included in the plans.	Deficiency

Table 2 – Questionnaire Results of Computer Center

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Security Policy	There should be an Information security policy, which is approved by the management, published and communicated as appropriate to all employees. It should state the management commitment and set out the organisational approach to managing information security.	There is a policy published at the web site of Computer Center. The policy includes information about the usage of several parts of information systems. Although the policy contains adeqauate information about the usage of the information technology systems, it does not state the management commitment and set out organizational approach to managing information security.	The lack of management commitment and setting of organizational approach may cause the policy to stay un-updated for a long period. That could result in unexpected exposure of the information systems due to non-protection againts latest security threats.	The information security policy should include management statement of commitment, approach on information security and responsibilities for reviewing and approving the policy.	Gap
Security Policy	University strategy should address IT strategy	Mission and vision of Computer Center is announced on the web site of the organization. The mision of Computer Center is stated as: "To closely follow up developing information technologies and provide them to the University in the fastest and most dynamical manner; and help University units by developing and providing the applications which are needed by the units." The vision of Computer Center is stated as: "Computer Center; · Will be more actively involved in	No risks identified.	N/A	Effective

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
		trainings and provide all students the media and additional facilities in which they can develop themselves in information technology. · will enhance the organizational structure, render global point of view continous by documenting and continuously updating all business processes			
Organizational Security	Risks from third party access should be identified and appropriate security controls implemented. The types of accesses should be identified, classified and reasons for access are justified.	The organization acquires services from third parties. The access of third party service providers to the resources of Computer Center is restricted at the firewall level. Recenlty, security software is been purchased for securing access to the information systems. However there is no formally documentation of the types and classification of accesses.	Not classifying the possible types and reasons of accesses may result in unidentified acccess to critical data and security breaches that could not be identified at the firewall level.	The types of access related to the third parties should be identified, justified and classified. According to every type of access, necessary security controls should be designed and implemented. At least one officer should be responsible for the access of the third parties.	Gap
Organizational Security	Remote access by vendors should be initiated by the University not the vendor	Since restriction to the University resources are managed at the firewall level, initiation of the remote access is performed by Computer Center employees.	No risks identified.	N/A	Effective

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Organizational Security	Vendor accounts should be disabled when not in use	Vendor accounts are not disabled when not in use but the access is restricted at the firewall.	Although the firewall is configured not to allow unauthorized access, enabled accounts could be compromised internally to access to critical systems files.	Vendor accounts should be disabled during inactivity. The activities performed by the vendor account should also be logged and reviewed as an additional control.	Gap
Organizational Security	Vendor password should be regularly changed	Vender passwords are not regularly changed	Unchanged vendor passwords increases the risk of unauthorized use of the vendor accounts for accessing critical system files.	Vendor passwords should be changed after each usage and they should be change by Computer Center.	Deficiency
Organizational Security	Information Security Officer should report to a senior level	There is no information security officer function in place. Employees are responsible for ensuring the security of their responsibility areas.	Not having a seperate information security officer in place decreases the attention given to the security of the information systems. That could result in unauthorized exposure of the critical data, manipulation and even deletion of the critical data.	There should be information security officer in place seperate from the IT department. IS officer should directly report to the management about the security strategy, security operations and security actions planned to be taken.	Deficiency
Organizational Security	The function should be appropriately separated from the information systems department.	N/A	same as above	The information security officer funtion should be seperated from IT department. The responsbilities of the function should be defined on the corporate level.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Organizational Security	The Information Security Officer should monitor compliance with the policy and report breaches	N/A	same as above	Information security officer should define the security policies as well as monitor the compliance of the operations with those policies. IS officer should report and non-compliance issues and security breaches to the management.	Deficiency
Asset Classification and control	Management should define and implement security levels related to the sensitivity of specific information.	There is no formally documented data classification scheme in the organization. The data stored in systems is not classified as public, secret, confidential, etc. Instead, access to sensitive sources, like servers, is protected and restricted with firewall settings.	Not defining the security levels to the specific information may result in unauthorized access to the sensitive data. That could even result in not recognizing this kind of security breach.	Management should first consitute an information repository regarding the university information systems and data related to the university operations. Then the security levels of the information shoule be defined. Finally necessary procedures should be designed to sustain the security of critical information.	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Asset Classification and control	Data owners should be assigned for all systems	There is no formal data ownership structure in the organization.	Not assigning data owners may result unexpected exposure of the critical and sensitive data to unauthorized users.	After defining the system inventory and related security levels to be preserve, data owners should be assigned for these systems. The data owners should be provided the roles and responsibilites related to the systems they are responsible of based on the criticality of the systems and measures that are defined to preserve the security.	Deficiency
Asset Classification and control	There should be a central log of IT equipment and this should be reconciled to physical assets on a periodic basis	The IT equipment log is kept with the physical asset list of university properties. A manual list is also kept by the Computer Center. There is no process of periodic reconciliation of physical assets to the log.	IT equipments could be stolen or damaged and they cannot be noticed until there is a necessity. Further more there may be a risk in place that the equipment is somehow logged mistakenly and this would go unnoticed for a long time.	A central log for the IT equipment should be designed. There should be a perodic reconciliation of the log with the physical asset for the integrity of the log.	Gap
Asset Classification and control	All movements of IT equipment should be logged	All movements of IT equipment is logged manually.	No risks identified.	N/A	Effective
Asset Classification and control	Disposal of IT equipment must be authorized by management.	Disposal of IT equipment is authorized by the management of Computer Center	No risks identified.	N/A	Effective

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Asset Classification and control	There should be an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.	There is no information classification scheme or guideline in place.	In absence of information classification scheme or guideline, the sensitive data may be compromised without knowledge of the IT personnel. IT personnel may lack awareness of handling method of the sensitivie information.	A formal information classification scheme should be in place, defining levels of data and data handling procedures related to these levels. Access to the data in the systems should be restricted in line with the levels defined in the scheme.	Deficiency
Personnel Security	Job description should detail scope of role and accountabilities	The roles and responsibilities are defined at the division level. Specific job descriptions are not defined.	Undefined role and responsbilities may result in lack of appropriate skills and knowledge identifying and handling security incidents.	Specific job descriptions for personnel should be in place, covering responsibilities and accountabilities of personnel. Personnel should be provided with a clear description of accountability areas.	Gap
Personnel Security	Staff should have sufficient experience and training for role	When a group of IT personnel attends a course provided by a third party, they give the same training to the other IT personnel. However there is no formally documented plan of the training and experience necessary for the IT personnel.	Lack of adequate training of the IT personnel may result in inproper planning of the security systems and inadequate handling of the security incidents.	IT personnel should be provided with regular trainings on IT systems and IT security. The trainings should be provided in line with a training program accepted by the management. IT personnel should be provided by the means to	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
				increase their level of experience in IT systems.	
Personnel Security	Employees should be asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment. This agreement should cover the security of the information processing facility and organisation assets.	No seperate confidentiality aggreement is signed by the personnel apart from the general officer aggrement signed by every employee in the university.	Not signing a confidentiality aggreement may result in lack of awareness about the usage of information systems. That could increase the risk of unintended misuse of the systems in place.	Personnel with access to critical data sources should sign a confidentiality aggreement with the university.	Deficiency
Personnel Security	Terms and conditions of the employment should cover the employee's responsibility for information security. Where appropriate, these responsibilities might continue for a defined period after the end of the employment.	N/A	If the responsibilities of the personnel for information systems is not properly delivered to the personnel, the risk of unintended systems disruptions/misuse may increase.	The responsibilities of personnel for IT security should be clearly communicated. Terms and conditions of employment may obtain security related responsibilities. Personnel may be required to sign a declaration indicating being acknowledged on security related responsibilities.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Physical and Environment Security	Access to sensitive IT areas should be restricted to IT staff by keypad or other security mechanism.	The access to the system room is restricted to the IT staff by a card reader mechanism.	No risks identified.	N/A	Effective
Physical and Environment Security	Physical access into the computer room should be limited to those individuals whose primary functions require them to have access	The card reader mechanism is configured to permit access to the authorized IT personnel. There is a list in place of the authorized personnel.	No risks identified.	N/A	Effective
Physical and Environment Security	A record should be kept of visitors to the data room	No record is kept for the card reader mechanism. On the other hand the system room is monitored by the cameras inside the system room.	Logging of access to the system room enables proper tracking of access to the room. In absence of access logs, unauthorized access and/or abnormal access to the system room may go unrecognized and responsible people in case of an unauthorized access may remain unidentified.	Logging of card reader mechanism should be enabled and logs should be retained for a period specified by the management. The logs should be reviewed periodically in order to identify any abnormal accesses made to the system room.	Deficiency
Physical and Environment Security	Unauthorized individuals should be escorted by an authorized individual during visit.	Unauthorized individuals are escorted by an authorized individual during visit to the system room. No visitor log is kept.	Although the visitors are escorted by the authorized individuals, absence of a visitor log decreases the traceability of access to the system room.	System room access of the visitors, who are not among the responsible personnel of Computer Center, should be registered in a visitor log. The visitors should sign in a visitor book in order to enhance tracking of the visitors accepted in the	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
				system room.	
Physical and Environment Security	Fire suppression equipment should be installed Temperature and humidity controllers should be in place Water and drainage pipes should be routed away from IT systems Uninterruptible power supply (UPS) Emergency Power System (EPS) (e.g., generators, transformers)	There is a smoke detector and manual fire extinguishers in place. There are motion sensors and an alarm system in place. Air conditioning is in place. The servers has a heat alarm mechanism that sends e-mail and sms when the heat exceeds a level. UPS is in place. Power generators are shared by the other facilities of the university.	The heat alarm mechanism in place informs the responsible personnel by e-mail. In case of a situation where the responsible personnel are unable to access their e-mails, the delivered heat alarm e-mails may not reach their targets. The sharing of power generators with the other facilities of the university may result in power shortage for the critical servers in the system room in case of a long power failure.	The heat alarm should deliver the alert messages via SMS. It is planned in Computer Center to switch to SMS-messaging as well. There should be a power generator allocated only for the critical servers in Computer Center in order to decrease university operations interruption risk due to power failures.	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Physical and Environment Security	Periodic preventative maintenance of computer components	There is no preventative maintenance of computer components.	Preventive maintenance held for the critical equipment decreases the risks of unexpected hardware failures and interruption of the university operations resulting from hardware failures. Hence, in absence of preventive maintenance, the risk related to unexpected failures and/or major defects resulting from minor failures in hardware increases.	Preventive maintenance should be performed periodically to cover the critical hardware equipment of Computer Center. For the equipment for which technical knowledge of the personnel is not adequate, third party services should be provided. For the services provided by third parties, the service levels and responsibilities of sides should be clearly stated in SLAs that are signed by both parties.	Deficiency
Physical and Environment Security	The rooms, which have the Information processing service, should be locked or should have lockable cabinets or safes.	The servers are kept in the locked cabinets.	No risks identified.	N/A	Effective
Physical and Environment Security	The power and telecommunications cable carrying data or supporting information services should be protected from interception or damage.	The system room has a raised floor and cables are stored in the raised floor.	No risks identified.	N/A	Effective

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Communications and Operations Management	Management should review systems capacity on a regular basis to ensure that there are sufficient resources for demand increases	A periodical review of the current systems capacity is not preformed. Instead, a review of the system capacity is performed in cases of new acquisitions.	Not reviewing the systems capacity might result in not meeting the required level of resourced on sudden or regular demand increases. This could not only decrease the satisfaction level of the users but could also result in unexpected systems problems and event security breaches.	Management should request montly and yearly capacity analyssis of the information systems and should review them. The review results and possible actions to be taken should be communicated to the related personnel and be formally documented for further use.	Deficiency
Communications and Operations Management	Incident Management procedure should exist to handle security incidents.	There is no formally documented Incident Management procedure in place.	Creating effective responses to security incidents confronted requires a definition of security incidents, incident escalation procedures and incident handling management procedures. In absence of an Incident Management procedures, problems may be encountered in identifying security incidents, the required analysis steps and resolution means. Hence, the action steps taken may be insufficient to minimize the business effects of possible security incidents.	Formal incident management procedures should be in place in order to identify and manage any security incidents that may be confronted. The procedures should be periodically reviewed in order to keep up to date with the university operations requirements.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Communications and Operations Management	IT problems should be logged and tracked for resolution.	Security related IT problems are kept in the logs of the servers.	No risks identified.	The logs related to IT security should be reviewed on a periodical basis in order to effectively identify IT problems and provide resolution.	Effective
Communications and Operations Management	IT problems should be prioritized and subject to summary reports to management.	There is a system in use by the university by which IT users may convey their IT requests to Computer Center. But, this system is not utilized for central registration of the IT problems encountered. IT problems are neither prioritized nor reported to the management.	In absence of a formal prioritization of the IT problems, limited IT resources may be allocated to resolve the problems with lower priorities or less severe university operations impact. Hence, business priorities may be unmatched and the IT satisfaction provided may decrease. Management reporting increases management awareness of the IT problems. If management reporting of the encountered IT problems is not in place, awareness of the IT problems (both repeated and first-time problems) may be insufficient and delays in identifying potential solutions for the IT	Prioritization conditions should be clearly stated in a formally documented prioritization procedure. Management approval might be sought in prioritization process. IT problems should be reported to management periodically in order to increase awareness of the IT problems.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
			problems may be confronted.		
Communications and Operations Management	Issues which have been resolved should be documented for future reference	The issues resolved are not documented.	Creating a repository of the past issues increases the ability to identify the confronted IT issues and represents a reference for the resolution steps. If documentation of the resolved issues is not in place, several delays and/or erroneous actions may be encountered in the identification of the problems encountered and definition of the resolution steps to be followed. Absence of documentation	The definition, analysis and resolution steps and results of IT issues should be registered in a central repository to serve as a future reference.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
			of issues also contribute to difficulties in identifying trends of the problems.		
Communications and Operations Management	Back-up of essential business information such as production server, critical network components, configuration backup etc., should be taken regularly. Example: Mon-Thu: Incremental Backup and Fri: Full Backup.	The daily backup of the critical systems (Web server, mail server, DNS server, firewall) is taken incremental and weekly backup is taken full. Apart from these full monthly backups are taken.	No risks identified.	N/A	Effective
Communications and Operations Management	The backup media along with the procedure to restore the backup should be stored securely and well away from the actual site.	The backup tapes are kept at the cabinets inside the system room.	Offsite storage of backup tapes protects system data against disaster affecting the local offices of Computer Center. Therefore, only onsite storage of backup tapes is in place, the risks related to business interruption in case of a disaster affecting Computer	At least one copy of backup tapes should be kept at an offsite location.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
			Center and inability to recover the systems using the backup dates increases.		
Communications and Operations Management	Backup tapes should be properly labeled and organized to facilitate recovery	The backup tapes are labeled properly.	No risks identified.	N/A	Effective
Communications and Operations Management	The backup media should be regularly tested to ensure that they could be restored within the time frame allotted in the operational procedure for recovery.	The backup tapes are tested but testing does not take place regularly.	Unless the backup tapes are tested regularly, the required recovery times may be misestimated. Another possible risk is that, any defects in backup tapes affecting the ability of recovering them may go undetected and tapes may be not functioning with the equipment set utilized for the recovery.	Backup tapes should be tested regularly in order to review recovery procedures performed, required recovery times and to observe whether the hardware equipment is compatible for the recovery of the backup tapes.	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Communications and Operations Management	The security Policy should identify any Operating procedures such as Back-up, Equipment maintenance etc.,	There is no formally documented Operating procedures in place but they are planned to be established.	Absence of such procedures may lead to problems in communicating the security-related operational steps to be performed and gaps between what is done to perform the job and what is done. Therefore such procedures are required in order to minimize the grey areas between responsibilities of the related employees and steps to be performed.	Operating procedures should be completed as soon as possible to provide guidance on the operational jobs performed and responsibilities of personnel for these jobs.	Deficiency
Communications and Operations Management	All programs running on production systems should be subject to strict change control i.e., any change to be made to those production programs need to go through the change control authorisation.	There is no change management in place.	In absence of a formally established change management process, the risk related to intended/unintended migration of unauthorized and/or erroneous program changes to production environment increases. Thus, applications may function other than expected, erroneously and/or inefficiently.	A formal change management process should be in place, defining change initiation, development and testing of changes, migration steps and the required approvals taken at several milestones of change management process. Changes, their approvals and related information should be centrally registered in order to provide a traceable past data on the changes	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
				performed in systems.	
Communications and Operations Management	There should a control against malicious software usage. The security policy should address software licensing issues such as prohibiting usage of unauthorised software.	There is an antivirus software and firewall software installed on the workstations. Also there is a hardware firewall in place.	No risks identified.	N/A	Effective
Communications and Operations Management	There should be a policy in place for the acceptable use of electronic mail or does security policy does address the issues with regards to use of electronic mail.	The policy in the web site of Computer Center describes the acceptable usage of e-mail.	No risks identified.	N/A	Effective

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Access Control	Firewall, Internet Connection and E-Mail service should work fast, secure and should be reliable	Firewall, Internet Connection and e-mail service is working fast and secure.	No risks identified.	N/A	Effective
Access Control	Anti-virus software should be implemented and regularly updated for all users	The antivirus software is updated regularly.	No risks identified.	N/A	Effective
Access Control	Penetration testing should be considered	There is an Intrusion Prevention System purchased recently. Before the purchase, penetration testing is performed. But the test is not regularly performed during normal times.	Unless penetration tests are not regularly performed, the potential vulnerabilities of network and systems may remain undetected.	Penetration tests should be performed regularly at an interval that is specified by the management.	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Access Control	There should be a formal user registration and deregistration procedure for granting access to multi-user information systems and services.	There is a contact page on the web site of Computer Center. Users can request for new passwords or user accounts by using the form on the page.	No risks identified.	N/A	Effective
Access Control	The allocation and reallocation of passwords should be controlled through a formal management process.	There is no formal management proces for allocation and reallocation of e-mail passwords. During the allocation process, the passwords are delivered to the users on a printed page during the registration. For reallocation, users are asked to apply to Computer Center personally in order to obtain a new password.	Printing passwords on papers in the allocation process may lead to the risk that unauthorized people may obtain other people's passwords.	Allocation of e-mail account passwords should be performed on the basis of personal application of the users, as in the reallocation process.	Gap
Access Control	There should be guidelines in place to guide users in selecting and maintaining secure passwords.	E-mail usage' part in the usage policy provides a guideline for users in selecting and maintaining secure passwords.	No risks identified.	N/A	Effective
Access Control	There should be authentication mechanisms for challenging external connections. Examples: Cryptography based technique, hardware tokens, software tokens, challenge/ response protocol etc.,	Secure connection is used for web page. (HTTPS protocol is used.) There is no token usage in place.	Although external connections are secured with firewalls and HTTPS protocol, not utilizing tokens increases the risk of exposure to security vulnerabilities.	Tokens should be utilized for remote connection to the systems.	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Access Control	The network (where business partner's and/ or third parties need access to information system) should be segregated using perimeter security mechanisms such as firewalls.	Network is segregated using firewall.	No risks identified.	N/A	Effective
Access Control	There should be network connection controls for shared networks that extend beyond the organisational boundaries. Example: electronic mail, web access, file transfers, etc.,	Firewall controls access to e-mail, web access and file transfers.	No risks identified.	N/A	Effective
Access Control	There should be a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form,	There is no formal password management system.	If a formal password management system is not in place, security vulnerabilities related to sharing of passwords and acquisition of passwords by unauthorized people increases. Therefore, unauthorized people may gain access to systems.	A formal password management process should be established. Users should be forced to select strong passwords by the system. Minimum and maximum password ages should be forced as well.	Deficiency
Access Control	The audit logs recording exceptions and other security relevant events are should be produced and kept for an agreed period to assist	The audit logs are kept for security exceptions. The logs are, though not regularly, reviewed .	If exception logs are not reviewed periodically, several exceptions and security related events may remain unrecognized.	The exception logs should be reviewed periodically in order to identify any suspicious exceptions and log review results should	Gap

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
	in future investigations and access control monitoring.			be reported to management.	
System Development and Maintenance	Systems developments should be undertaken in a structured way, using systems development lifecycle: - Project planning, feasibility study - Systems analysis, requirements definition - Systems design - Implementation - Integration and testing - Acceptance, installation, deployment	There is no formally documented system development methodology in place. But 'Analysis', 'Development' 'Testing' and 'Migrating' phases are performed.	In absence of a formal system development life cycle, needs of the university units may not be met within the allocated time frame in an efficient and cost effective manner and the required outputs at the required quality level may not be produced.	A formal and documented system development methodology should be adopted in Computer Center. The required approvals in 'Analysis', 'Development' 'Testing' and 'Migration' phases should be clearly communicated and obtained. Documentation related to these phases should be retained in order to serve as a future reference.	Gap
System Development and Maintenance	Digital signatures should be used to protect the authenticity and integrity of electronic documents.	Digital signatures are not used to protect the authenticity and integrity of electronic documents.	Digital signatures are utilized for authenticity and integrity of electronic documents. Without digital signatures, the source of the electronic document can not be verified and possible impairments made in the electronic document may be unrecognized.	Digital signatures should be utilized in order to obtain assurance on the authenticity and integrity of the electronic documents and compliance with current regulations.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
System Development and Maintenance	Strict controls should be in place over access to program source libraries. This is to reduce the potential for corruption of computer programs.	The access to the program source libraries are controlled via access rules defined on the firewall.	No risks identified.	N/A	Effective
System Development and Maintenance	There should be strict control procedures in place over implementation of changes to the information system. This is to minimise the corruption of information system.	There is no formal strict control procedures in place over implementation of changes to the information system.	In absence of formal control procedures over implementation of changes, the risk related to intendedly/unintendedly performed changes in information system increases. Thus, applications and systems may function other than expected, erroneously and/or inefficiently.	Implementation of changes should be performed only if required testing of changes is performed and approvals are obtained for the implementation. Testing results and obtained approvals should be retained. The changes performed should be reported to management reporting or communicated to the relevant users of the IT systems.	Deficiency
Business Continuity Management	There should be a managed process in place for developing and maintaining business continuity throughout the organisation. This might include Organisation wide Business continuity plan, regular testing and updating of the plan, formulating and	The roles and responsibilities in case of a business discontinuity are known by the Computer Center employees. But, there is no formally documented business continuity plan in the organization; testing of the plan is not applicable as well.	In absence of a business continuity plan, the university may not be able to react properly in case of an emergency. This could result in partial or total loss of the information systems as well as the critical system room.	There should be a process in place for developing and maintaining the business continuinty. The process should include defining a Business Continutiy Plan, reviewing and testing of the plan and applying necessary updates on the plan.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
	documenting a business continuity strategy etc.,				
Business Continuity Management	Systems should be prioritized and scheduled for recovery in accordance with work impact	N/A	If the systems are not priotized and scheduled for recovery in accordance with work impact, less critical systems which have less affect on the healt of the information systems are recovered while critical systems may remain damaged.	Information systems should be priotized according to the their impact on the university operations. Based on the prioritized systems, a recovery strategy should be constituted.	Deficiency
Business Continuity Management	Contingency plans should be tested on a regular basis to ensure they work.	N/A	If the continuity plans are not tested, they might include insufficient information about the updated/changes systems in place which could result in inappropriate/improper methods for providing continuity to the university operations.	The contingency plans should be tested at least annually in order to reflect the current status of the information systems in place. The test should also applied in order to see if the plans are applicable and sufficient for the systems.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Business Continuity Management	Events that could cause interruptions to business process should be identified example: equipment failure, flood and fire. A risk assessment should be conducted to determine impact of such interruptions. A strategy plan should be developed based on the risk assessment results to determine an overall approach to business continuity.	The evacuation plan of the university facilities includes general information about the possible disasters and common emergency plans against them. However these possible disasters and their impact on the information systems are not identified.	In absence of identifying possible disasters that could cause interruptions to the university operations may result in insufficient response to these disasters. In absence of a strategy plan based on the risk assessment results could lead to total or partial loss of the information systems during times of disasters.	In order to define and implement Disaster Recovery Plans, risk assesment must be performed. Durign risk assessment phase, possible causes of business interruptions must be defined. The results of the risk assesment should be used to direct or update the overall business continuity plans in place.	Deficiency
Business Continuity Management	Plans should be developed to restore business operations within the required time frame following an interruption or failure to business process. The plan should be regularly tested and updated.	N/A	The lack of defining a time frame for recovery of the information systems may result in significant disruptions in the university operations and may even result in unauthorized access to the critical systems. Recovery plans might include insufficient information about the updated/changes systems in place which could result in inappropriate/improper methods for recovery.	Within the disaster recovery plans, time frames should be defined for the systems' recovery durations. This time frames should be based on the priotization of these systems related to their criticality level. The DRP's should also be tested at least annually and updated if necessary.	Deficiency

Process Areas	Controls	Findings	Risks	Recommendations	Type of Result
Business Continuity Management	Copies of the contingency/ disaster recovery plan and restart/recovery procedures should be stored off-site.	N/A	In case of a disaster, the location where the information systems reside may partially or totally damaged and may become unreachable. In absence of the BCP and DRP storage off-site, on-site plans may not be reached and applied.	The BCP's and DRP's should be stored off-site and the location of these plans should be included in the plans.	Deficiency

TABLE 3 - Comparison of Registration Office and Computer Center

Process Areas	Controls	Type of Result	
		Registration Office	Computer Center
Security Policy	Information security policy	Deficiency	Gap
Security Policy	IT strategy	Deficiency	Effective
Organizational Security	Risks from third party access	Deficiency	Gap
Organizational Security	Remote access by vendors	Deficiency	Effective
Organizational Security	Vendor accounts	Deficiency	Gap
Organizational Security	Vendor passwords	Deficiency	Deficiency
Organizational Security	Information Security Officer	Deficiency	Deficiency
Organizational Security	Information Security function	Deficiency	Deficiency
Organizational Security	Monitor compliance	Deficiency	Deficiency
Asset Classification and control	Security levels related to the sensitivity of specific information.	Deficiency	Gap
Asset Classification and control	Data owners	Deficiency	Deficiency
Asset Classification and control	Central log of IT equipment	Gap	Gap
Asset Classification and control	Movements of IT equipment	Effective	Effective
Asset Classification and control	Disposal of IT equipment	Effective	Effective
Asset Classification and control	Information classification scheme	Deficiency	Deficiency
Personnel Security	Job descriptions	Gap	Gap
Personnel Security	Staff experience and training	Gap	Gap
Personnel Security	Confidentiality or non-disclosure agreement	Deficiency	Deficiency
Personnel Security	Terms and conditions for information security	Deficiency	Deficiency
Physical and Environment Security	Access mechanism to sensitive IT areas	Deficiency	Effective

Process Areas	Controls	Type of Result	
		Registration Office	Computer Center
Physical and Environment Security	Authorized access to Physical access	Gap	Effective
Physical and Environment Security	Data room visiting log	Deficiency	Deficiency
Physical and Environment Security	Unauthorized individuals	Gap	Gap
Physical and Environment Security	System Room Conditions	Gap	Gap
Physical and Environment Security	Periodic preventative maintenance	Deficiency	Deficiency
Physical and Environment Security	The rooms that have the Information processing service	Effective	Effective
Physical and Environment Security	The power and telecommunications cables	Effective	Effective
Communications and Operations Management	Review systems capacity	Gap	Deficiency
Communications and Operations Management	Incident Management procedure	Deficiency	Deficiency
Communications and Operations Management	Logging IT problems	Effective	Effective
Communications and Operations Management	Prioritization of IT problems	Effective	Deficiency
Communications and Operations Management	Documentation of the resolved issues	Effective	Deficiency
Communications and Operations Management	Back-up of essential business information	Effective	Effective
Communications and Operations Management	Secure storage of the backup mediaand the procedure	Deficiency	Deficiency
Communications and Operations Management	Backup tapes	Effective	Effective
Communications and Operations Management	Testing of the backup media	Deficiency	Gap
Communications and Operations Management	Operating procedures such as Back-up, Equipment maintenance etc.,	Deficiency	Deficiency
Communications and Operations Management	Change controls	Deficiency	Deficiency
Communications and Operations Management	Malicious software usage	Deficiency	Effective
Communications and Operations Management	Acceptable use of electronic mail policy	Deficiency	Effective
Access Control	Firewall, Internet Connection and E-Mail service	Effective	Effective

Process Areas	Controls	Type of Result	
		Registration Office	Computer Center
Access Control	Anti-virus software	Gap	Effective
Access Control	Penetration testing	Gap	Gap
Access Control	Formal user registration and deregistration procedure	Gap	Effective
Access Control	The allocation and reallocation of passwords	Deficiency	Gap
Access Control	Guidelines in selecting and maintaining secure passwords.	Effective	Effective
Access Control	Authentication mechanisms for external connections.	Gap	Gap
Access Control	The network security using perimeter security mechanisms	Deficiency	Effective
Access Control	Network connection controls	Effective	Effective
Access Control	Password management system	Gap	Deficiency
Access Control	The audit logs	Gap	Gap
System Development and Maintenance	Systems development lifecycle	Deficiency	Gap
System Development and Maintenance	Digital signatures	Deficiency	Deficiency
System Development and Maintenance	Access to program source libraries	Deficiency	Effective
System Development and Maintenance	Implementation of changes to the information system	Deficiency	Deficiency
Business Continuity Management	Managed processfor developing and maintaining business continuity	Deficiency	Deficiency
Business Continuity Management	Systems prioritization and scheduling for recovery	Deficiency	Deficiency
Business Continuity Management	Testing contingency plans	Deficiency	Deficiency
Business Continuity Management	Identification of the events that could cause interruptions to business process	Deficiency	Deficiency
Business Continuity Management	Plans to be developed to restore business operations	Deficiency	Deficiency

Process Areas	Controls	Type of Result	
		Registration Office	Computer Center
Business Continuity Management	Copies of the contingency/ disaster recovery plan and restart/recovery procedures	Deficiency	Deficiency

BIBLIOGRAPHY

Anderson, J.M. (2003). Why we need a new definition of information security. *Computers & Security, 22,* 308-313.

Banking Regulation and Supervision Agency (BRSA). (May 2006). *Regulation on information systems audit to be made in banks by independent audit institutions*. Retrieved August 5, 2007, from http://www.bddk.org.tr/english/Legislation/1881BSDY_eng.pdf.

Barnard, L. & von Solms, R. (2000). A formalized approach to information security controls. *Computers & Security, 19,* 185-194.

Bodnar, G.H. (2006). What's new in CobiT 4.0. *Internal Auditing, 21,* 37-44.

Brown, W. & Nasuti, F. (2005). Sarbanes-Oxley and enterprise security: IT governance - What it takes to get the job done. *Information Systems Security, 14,* 15-28.

Cerullo, V. & Cerullo, M.J. (2003). Impact of SAS No. 94 on computer audit techniques. In *Information Systems Control Journal*, *1*. Retrieved on July 19, 2007, from http://www.isaca.org/Template.cfm?Section=Article_Index1&CONTENTID=16201&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Chang, S.E. & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security. *Management Industrial Management & Data Systems, 106,* 345-361.

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management, 22,* 77-85.

Deloitte Touche Tohmatsu. (2006). *Deloitte's the 2006 global security survey.* Retrieved August 9, 2007, from www.deloitte.com/dtt/cda/doc/content/us_fsi_150606globalsecuritysurvey(1).pdf.

Dhillon, G. & Mishra, S. (2006). The impact of Sarbanes Oxley Act on information security governance. In Warkentin, M. & Vaughn R.B. (Ed), *Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues* (pp. 62-79). US: Idea Group Publishing.

Eloff, J.H.P. & Eloff, M.M. (2005). Information security architecture. *Computer Fraud & Security, 2005*, 10-16.

Eloff, M.M. & von Solms, S.H. (2000). Information security management: An approach to combine process certification and product evaluation. *Computers & Security, 19*, 698-709.

Ezingeard, J.N., McFadzean, E. & Birchall, D. (2005). A model of information assurance benefits. *Information Systems Management, 22,* 2-29.

Goins, B.A. (2005). Sarbanes-Oxley compliance: A technology practitioner's guide. *EDPACS, 33,* 1-12.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy, 25*, 503–530.

Haber Vitrini. (2003). *İmar bankası'nda durum... Bddk ikinci başkanı yanıtlıyor.* Retrieved August 5, 2007, from http://www.habervitrini.com/haber.asp?id=109466.

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report II*, 55 – 61.

Hawkins, K.W., Alhajjaj, S. & Kelley, S.S. (2003). Using CobiT to secure information assets. *The Journal of Government Financial Management, 52*, 22-32.

Hong, K.S., Chi, Y.P., Chao, L.R.. & Tang, J.H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11,* 243-248.

Howarth, D.A. & Pietron, L.R. (2006). Sarbanes Oxley: Achieving compliance by starting with ISO 17799. *Information Systems Management, 23,* 73-87.

ISACA. (2007). *COBIT overview.* Retrieved August 15, 2007, from http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981.

ISO/IEC. (2000). *Information technology – Code of practice for information security management.* ISO/IEC 17799- 2000.

ISO/IEC. (2004). *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.* ISO/IEC 13335-1:2004.

IT Governance Institute. (2005). *Aligning COBIT®, ITIL® and ISO 17799 for business benefit*. Retrieved August 15, 2007, from http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/AligningCOBIT,ITIL.pdf.

IT Governance Institute. (2007). *Control Objectives for Information and Related Technology.* COBIT 4.1. United States of America: IT Governance Institute.

Kenning, M.J. (2001). Security management standard -- ISO 17799/BS 7799. *BT Technology Journal, 19,* 132-136.

Landwehr, C.E. (2001). Computer security. *International Journal of Information Security, 1,* 3-13.

Le Roux, Y. (2005). Using ISO 17799, COBIT & ITIL for solving Compliance Issue. In S. Paulus, N. Pohlmann, H. Reimer (Ed), *Securing Electronic Business Processes* (pp. 313-323). Vieweg: Computer Associates Int.

Lichtenstein, S. (1997). A review of information security principles. *Computer Audit Update, 1997,* 9-22.

Little, A. & Best, P.J. (2003). A framework for separation of duties in an SAP R/3 environment. *Managerial Auditing Journal, 18,* 419-430.

Lobel, Mark (2006). *PWC's global state of the information security 2006.* Retrieved August 9, 2007, from http://www.pwc.com/extweb/pwcpublications.nsf/docid/3929AC0E90BDB001852571ED0071630B.

Logan, P.Y. (2002). Crafting an undergraduate information security emphasis within information Technology. *Journal of Information Systems Education, 13,* 177-182.

Lonsdale, D., Clark, W. & Udvadia, B. (2006). ITIL in a complex world: Focusing on success in a multisourced environment. *Information Systems Control Journal, 1*. Retrieved on July 19, 2007, from http://www.isaca.org/Template.cfm?Section=Archives&CONTENTID=30706&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Luthy, D. & Forcht,K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security, 14*, 155-166.

Marquis,H. (2006). ITIL: What it is And what it isn't. *Business Communications Review, 36,* 49-52.

Miller, C. (2005). Security in the age of compliance. *iSeries News, Dec 2005,* 18-24.

Moulton, R. & Coles, R.S. (2003). Applying information security governance. *Computers & Security, 22,* 580-584.

Nyanchama, M. (2005). Enterprise vulnerability management and its role in information security management. *Information Systems Security, 14,* 29-56.

Poole, V. (2006). Why information security governance is critical to wider corporate governance demands. *Information Systems Control Journal*, *1*. Retrieved on July 19, 2007, from http://www.isaca.org/Template.cfm?Section=Archives&CONTENTID=30681&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Poore, R.S. (2005). Information security governance. *EDPACS, 33,* 1-8.

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

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39,* 4.

Schlarman, S. (2007). Selecting an IT control framework. *EDPACS, 35,* 2.

Schneider, G.P. & Bruton, C.M. (2006). Information technology professionals meet Sarbanes-Oxley. *Journal of Legal, Ethical and Regulatory Issues, 9,* 89-94.

Sweren, S.H. (2006). ISO 17799: Then, now and in the future. *Information Systems Control Journal*, *1*. Retrieved on July 19, 2007, from http://www.isaca.org/Template.cfm?Section=Article_Index1&CONTENTID=30704&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Şenyüz, H. (2003). *İmar'dan ders alındı*. Retrieved August 5, 2007, from http://www.radikal.com.tr/haber.php?haberno=93791.

Thiagarajan, V. (2003). *BS 7799 audit checklist*. Retrieved May 31, 2007, from http://www.sans.org/score/checklists/ISO_17799_checklist.pdf.

Thorp, C. (2006). Implementing ISO17799: Pleasure or pain*? Information Systems Control Journal, 4*. Retrieved on July 19, 2007, from http://www.isaca.org/Template.cfm?Section=Article_Index1&CONTENTID=21319&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Tryfonas, T., Kiountouzis, E. & Poulymenakou, A. (2001). Embedding security practices in contemporary information systems development approaches. *Information Management & Computer Security, 9,* 183-197.

Violino, B. (2005). Best-practices library gains fans. *InformationWeek*, 1049, 57-59.

Volonino, L., Gessner, G.H. & Kermis, G.F. (2004). Sarbanes-Oxley links IT to corporate compliance. In *Proceedings of the Tenth Americas Conference on Information Systems, August 2004.* New York, USA.

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

Von Solms, B. & von Solms, R. (2005). From information security to business security. *Computers & Security, 24,* 271-273.

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security, 20,* 215-218.

Von Solms, B. (2000). Information security — The third wave? *Computers & Security, 19,* 615-620.

Von Solms, B. (2005). Information security governance: COBIT or ISO 17799 or both?. *Computers & Security, 24,* 99-104.

Von Solms, R. (1999). Information security management: Why standards are important. *Information Management & Computer Security, 7,* 50-57.

Whitman, M.E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24,* 43–57.

Williams, P. (2001). Information security governance. *Information Security Technical Report, 6,* 60-70.

Worthen, B. (2005). ITIL Power; Why the IT Infrastructure Library is becoming the most popular process framework for running IT in America, and what it can do for you. *CIO, 18,* 1-7.