JJMIE

Volume 8 Number 2, April. 2014
ISSN 1995-6665
Pages 102 - 118

Jordan Journal of Mechanical and Industrial Engineering

Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study

Awni Itradat [*], Sari Sultan, Maram Al-Junaidi, Rawa'a Qaffaf, Feda'a Mashal, and Fatima Daas

Department of Computer Engineering, Hashemite University, Zarqa 13115, Jordan

Abstract

Information is becoming one of the most important assets for almost every organization. Information systems are essential for every organization to access its information. However, these systems need to be secure in terms of confidentiality, integrity, and availability of the information. Information security comes as a magical solution for these requirements where a security audit of the system is developed to define and prioritize the risks that face information asset of the information system. So, risk assessment is applied to identify the risks and their impact on the system. Risk assessment is developed based on the vulnerability assessment, targeting specific information assets. Securing the information systems is the concern of the Information Security Management System ISMS adopted by the organization. Universities information systems are critical systems due to the rapid growth demand of students enrolling in universities in different programs, which will pay a higher level of complexity of these information systems. In this paper, an evaluation of the information security level at the Jordanian universities has been developed by launching a case study targeting the Hashemite University (HU). The case study focuses on analyzing the risks that faces HU information systems from two different perspectives (organizational and technical risks) by applying vulnerabilities assessment and penetration testing, finally organized into a risk assessment plan. During the case study, an ISO/IEC 27001:2005 ISMS has been developed in order to eliminate the risks that face the HU information systems. The ISMS (Information Security Management System) provides the required policies and controls in order to minimize the identified risks and to facilitate examining and enhancing the information security experience of HU.

© 2014 Jordan Journal of Mechanical and Industrial Engineering. All rights reserved

Keywords: *Information Security Management System ISMS, Risk assessment, Vulnerability Assessment, ISO/IEC 27001.*

1. Introduction

Information is becoming one of the most important assets in the 21st century for almost every organization. Vulnerability assessment comes as a solution for identifying the security holes in (a) specific information system(s), by identifying the threats that pose a serious exposure to the organization's assets, which leads to identifying unattended threats and quantifying the reactive measures. A unique set of testing processes, tools, and techniques are followed to detect and identify vulnerabilities in information systems. The penetration testing goes beyond the level of identifying vulnerabilities and hooks into the process of exploitation, privilege escalation, and maintaining access to the information system, showing the real value of the threat and how it can affect the information system. Vulnerability assessment and penetration testing are not a good indemnity for a secure information system. Since most of the highest impact security breaches come from inside the organization, there should be a control mechanism for the information system users/implementer to protect the system from being compromised internally, this could extend also to insuring that the information system business continuity do not exclusively depend on a specific individual existence which could lead to a serious system halt/crash based on the availability of specific personnel. Information Security Management Systems (ISMS) provide a complete solution for a better information security experience by providing the needed policies, tools, and procedures for enhancing and maintaining a secured information system.

Recently, most of the Jordanian universities (for example, the Hashemite University (HU)), have been facing a rapid growth demand of students enrolling in its programs, both undergraduate and graduate. As the number of student's increases, the organization and maintainability of its information, which is one of the most important assets affecting the business continuity of the

[*] Corresponding author. e-mail: itradat@hu.edu.jo.

universities, are becoming more and more complicated due to huge amount of paper work to do as well as the hard copy that should be stored and retrieved regularly. Moreover, hard copies must be stored in a secure manner to avoid their sensitive content from being disclosed, tampered, modified, or disrupted, which could lead to the destruction of organization's reputation. This might lead to damaging the credibility of the organization concerning the protection of its own information properly or even to skepticism about the legitimacy of the organization's information as well as the validity of its graduate student's certificates.

The Hashemite University is one of the highly reputable universities in The Hashemite kingdom of Jordan (HKJ). The HU Information, Communication and E-learning Center (ICET) has been working closely with different HU departments since 1996 in order to computerize its operations such as (student's registration, student's exams, students/employees portals, mailing services, and financials). Computerizing manual operations and some of the paper work comes as a magical solution by using computer-based applications to complete complex, time-consuming, redundant operations in order to organize and maintain student's information efficiently time-wise and effort-wise. These computerized operations must insure information Confidentiality, Integrity, and Availability, unless they can be very easily disclosed, tampered, modified, or disrupted.

Computerized systems are usually built by adopting one of the common solutions such as Microsoft, Oracle, or others. Security holes in these solutions would make the computerized system weak and easy to penetrate. Moreover, lack of awareness about the usage and the configuration for a specific solution leads to more dangerous vulnerabilities in the resulting system. For example, allowing default login credentials on a specific solution allows unauthorized users to get authenticated to a specific system using default login credentials.

In this paper, an evaluation of the information security level at the Jordanian universities has been developed by launching a case study targeting HU. The case study focuses on analyzing the risks that face HU information systems from two different perspectives (organizational and technical risks) by applying vulnerabilities assessment and penetration testing, which is finally organized into a risk assessment plan. Furthermore, a risk mitigation plan is developed in order to eliminate these identified risks. During the case study, ISO/IEC 27001:2005 ISMS have been developed in order to eliminate the risks that face the HU information systems. The ISMS provides the required policies and controls in order to minimize the identified risks and minimize the likelihood of new vulnerabilities emersion. The provided ISMS should facilitate examining and enhancing the information security experience of HU-ICET.

ISO/IEC 27001:2005 ISMS is among the most strict information security standards that guarantee an ultimate secure environment for technology based organization. The ISMS takes care of almost every single side affecting the organization's security experience by applying the needed tools and procedures to insure confidentiality, integrity, and the availability of the information system. During the development of the ISMS, an information security policy must be development to standardize the procedures developed by ICET; this includes identifying the personnel's responsibilities from an information security perspective. Regular updates of the information security policy are applied and reviewed until every single transaction inside ICET is controlled by these policies. In this paper, we have introduced an information security policy, the ICET. Procedures should also be developed to insure a standardized communication mechanism inside ICET for different operations. ISMS also goes beyond the vulnerability assessment and penetration testing by applying a risk management [1] methodology, which is a continuing process of identifying the vulnerabilities mapped to their risk profile and of proposing a mitigation process.

Section 2 of this paper includes a brief background material on topics concerning vulnerability assessment, penetration testing, and ISMS. It starts with a brief overview of the vulnerability assessment and penetration testing and its importance for information systems; moreover, it addresses one of the methodologies used in penetration testing, which is the backtrack methodology. In addition, ISMS is discussed in details and reflected on ISO27001 ISMS, showing the importance of this standard as a complete solution for information security against the rapidly growing number of security breaches.

In Section 4, we introduce the steps of implementing ISO27001 ISMS; it starts with identifying the scope of implementation. After that, it addresses the proposed information security policy which is designed to meet the requirements of ICET. The policy contains controls that have two different perspectives: technical and organizational. An example of the technical perspective is the password policy which addresses the confidentiality techniques to be used, such as using SSL/TLS and the minimum number of char's to be used and their space (e.g. char's lower and upper as well as numbers). The physical security policy also identifies the technical control for protecting the assets from a physical perspective (e.g., logging control, door/looks). An example of the organizational policies is the strategy and planning policy which identifies the need for security administrator/officer position in the ICET. Access control policy addresses the appropriate personnel privileges. The risk management methodology is addressed, after which the risk assessment and risk mitigation plans are presented.

Section 5 will conclude the paper, showing that the final results of the paper proved to be better than the ones expected a year ago when the study was first launched. Moreover, it will present our future plans concerning this research.

The main contributions of this paper are the following:

- To enrich knowledge in the fields of Information Security (IS), Information Security Management Systems (ISMS), and Penetration Testing.
- To evaluate the information security level at The Hashemite Kingdom of Jordan Universities generally and the HU specifically by applying a case study on the HU, one of the leading university in Jordan.
- To define and prioritize the HU information assets affecting its business continuity.

- To define and prioritize vulnerabilities affecting the information assets of ICET at technical and organizational levels.
- To implement ISO/IEC 27001:2005 ISMS for the scope of ICET, including development of an information security policy in addition to risk assessment and risk mitigation plans to provide the solutions needed to eliminate the existing vulnerabilities.

2. Background

2.1. Vulnerability

Vulnerability is a weakness point of an asset or group of assets that can be exploited by one or more threats [2], and results can potentially compromise the confidentiality, integrity and/or the availability of services. Attacks are the processes of exploiting an existing vulnerability. Attacks are divided into two sub-categories based on their effect on the security requirements, namely, active, and passive attacks. They are called active when the attacks affect the services by compromising the integrity or availability, and passive when they affect the information confidentiality only. The attack itself is a threat for the information system, and every threat has a specific risk based on the vulnerabilities. Figure 1 illustrates the relationship between vulnerabilities, threats, and risk [3].

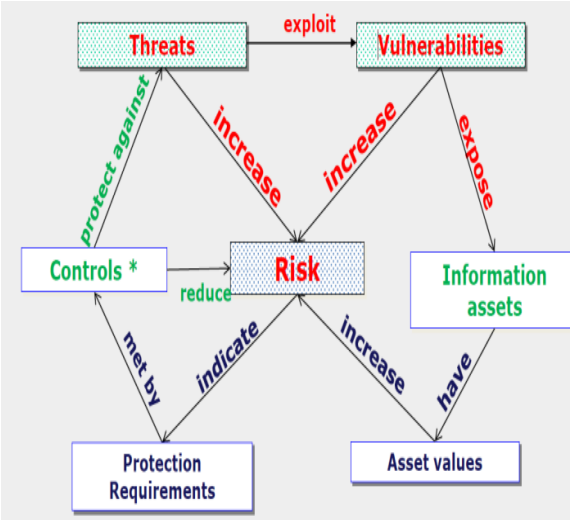

Figure 1. Relation between threat, vulnerabilities, and risk

Based on ISO27005:2008, vulnerabilities are classified according to the asset class they are related to. The following chart in Figure 2 illustrates this classification [2]:

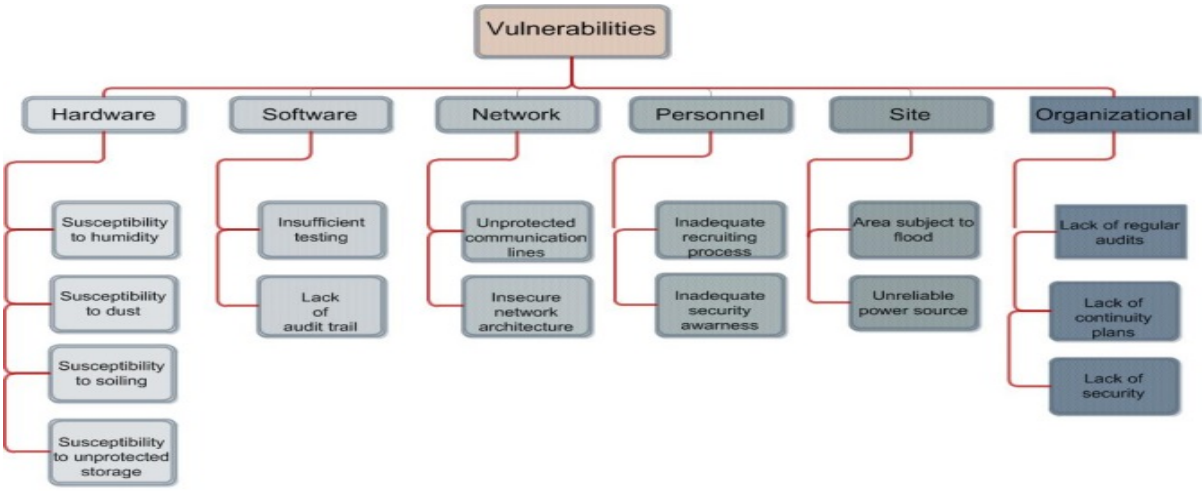

Figure 2. Vulnerabilities classification according to the relating asset class

According to the chart above, hardware components are affected by humidity, dust, and soiling, where the unprotected storage is another vulnerability that must be also taken into consideration. Hardware vulnerabilities are relatively easier to detect, but the damage can be huge and irreversible. We can control hardware security by hardware sighting and monitoring, with respect to equipment security. On the other hand, software is easier to exploit by attackers due to insufficient testing and lack of an audit trail. It is possible to handle these vulnerabilities by doing internal/external a vulnerability test where we can summarize a list of recommended fixes, or build a software trail from the beginning to keep track of the qualities of software, or audit the current software.

The most commonly exploited vulnerabilities by attackers are network vulnerabilities. Because all internal and external communications of any company are based on a network, unprotected communication lines and insures network architecture is serious risks. To reduce this vulnerability, it is important to build the network infrastructure securely and use suitable cabling methods in an appropriate way from the beginning. Using a firewall is a good idea, even though it has its own problems.

Personnel risks are more difficult to manage because they are abstract. The key risk indicators refer to the poorly recruited candidates, and the current employees who are not aware of the security process. In response to personnel vulnerability, audit employees access the IT systems, set access privileges for everyone, train employees to increase security awareness, including ethics and the use of policies, and separate employees duties by setting standards and guidelines for the system's development staff.

Unexpected external threats, such as flood and unreliable power source, are vulnerabilities depending on the site; a company should realize the occurrence of a risk,

put the necessary disaster planning steps, and use generators and power back-ups to present the data lost during power outage [4,5].

The lack of monitoring and auditing policies and procedures causes organizational vulnerabilities. To reduce them, the organization should build preventive IT controls. Tests to confirm and validate the correctness of data, auditing, and monitoring must be done.

2.2. Vulnerability Assessment and Penetration Testing

Under the enormous number of attacks that infect many organizations and companies caused by the existence of the information system vulnerabilities, Vulnerability Assessment and Penetration Testing came as tools to identify and quantify the system weakness points in order to improve the security controls and services that protect the information assets. They also give a better understanding about the weaknesses in the existing information system.

Vulnerability assessment is the evaluation of the information technology infrastructure of the organization; it tends to identify the weakness of these infrastructure components and how to control in order to protect from threats and attacks. Vulnerability assessment is an important activity to understand most of the various vulnerabilities in a system that might compromise its critical information assets. Penetration Testing is the process of exploiting the discovered weakness points by a malicious user. The tester needs to gather information, enumerate the vulnerabilities, and finally exploit the given vulnerabilities and gain access to the system [4].

There have been various methodologies introduced to address security assessment needs. The BackTrack testing methodology is one of the methodologies proposed for these purposes. BackTrack is a Linux-based platform aimed for the purpose of penetration testing and security auditing with advanced tools to identify, detect, and exploit any vulnerabilities uncovered in the target network environment. It is very commonly used for this purpose where studies show that as the end of July 19, 2010, BackTrack 4 has been downloaded by more than 1.5 million users. [6] This platform provides users with large collection of security related tools ranging from port scanners to password crackers, applying appropriate testing methodology with defined business objectives and a scheduled test plan will result in robust penetration testing of your network. BackTrack is the official operating system that is used in this study, in addition to windows OS. BackTrack testing methodology which is shown in Figure 3 is implemented in this study.

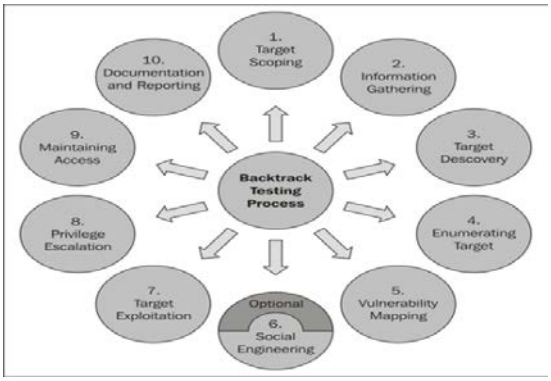

Figure 3. BackTrack testing methodology

1. Target scoping:

To make a successful penetration testing, we must take into consideration the technology under assessment and its basic functionality. An auditor must understand the given scope for the target network environment before starting the security assessment; this step will take him one step closer to the purpose.

2. Information gathering:

It is also called reconnaissance phase. During this phase, we should gain information using a number of publicly available resources; the more information we gather, the more chances for the success of penetration testing we gain. This information can be gathered using various methods.

3. Target discovery:

This phase deals with identifying the target status, operating system, and its network architecture. This process provides a full image of the technologies interconnected. By using tools available in Backtrack, it is possible to determine the live network hosts, and identify the operating systems running on these machines.

4. Enumerating target:

This phase is for finding the open ports on the target systems. Scanning may help in determining the port visibility with a number of port scanning techniques such as full open, half-open, and stealth; it sometimes works even if the host is behind a firewall or an Intrusion Detection System (IDS). These ports can be enumerated for the running services.

5. Vulnerability mapping:

This phase tends to identify the vulnerabilities based on the valuable information that has been gathered about the target network. This process can be done through using a number of automated network vulnerability assessment and Backtrack tools.

6. Social engineering:

When there is no other way available for an auditor to enter the target, the art of deception takes place. A successful penetration may require watching the human psychology before applying the suitable deception technique against the target.

7. Target exploitation:

After examining the revealed vulnerabilities, now it is possible to penetrate the target system. This phase may require modification on the existing exploit; backtrack tools are provided to accomplish this process.

8. Privilege escalation:

Once the target is acquired, the penetration is successfully done. Now we can escalate access privileges using any local exploit that matches the system environment; once they are executed, super-user access or system-level access privileges are attained. After this phase, it is possible to launch other attacks against the local network systems.

9. Maintaining access:

Sometimes maintaining access to the system without applying any noisy behavior is required for a specific period of time. Such activity can be used demonstrating illegal access to the system without applying the penetration testing process again, which saves time, cost, and resources being used. Using some secret tunneling methods, that make use of protocol or end-to-end connection strategy leads to establishing a backdoor access and maintains the auditor's presence in the target system as long as required.

10. Documentation and reporting:

Presenting Documentation and reports about the vulnerabilities found and exploited is the ethical and the final step in the penetration testing methodology. These documents are very important because the concerned technical team will check the method of penetration and will try to close any security loopholes that may exist.

2.3. Information Security Management System (ISMS)

Information Security Management System (ISMS) is a management plan which specifies the requirements for the implementation of security controls customized to the needs of organizations. The ISMS is designed to protect the information assets from any security breaches.

ISO27k is a series of international standards for Information security management. This standard covers all types of organizations (e.g., commercial enterprises, government agencies and non-profit organizations) and all sizes from micro-businesses to huge multinationals.

ISO/IEC 27001:2005 standard is a process of applying security management controls on organizations to obtain security services in order to minimize assets' risks and ensure business continuity. The main security services that present the C-I-A triad taken into consideration are [7]:

A. Information Confidentiality.
B. Information Integrity.
C. Services Availability.

This international standard adopts a model called Plan-Do-Check-Act (PDCA) model, which is applied to structure all ISMS processes. Figure 4 illustrates the PDCA model.

Figure 4. Plan Do-Check-Act model

1. Plan: Is the process of establishing the ISMS by applying the policies and objectives of the ISMS as well as developing the procedures concerning managing the risks.
2. Do: Is the process of implementing and operating the ISMS which was planned in the previous step.
3. Check: Is the process of monitoring and reviewing the ISMS by measuring the performance against the applied controls including policies, and, finally, exporting the results to management review.
4. Act: Based on management reviews, in the previous step, improvements of the applied ISMS is taking place.

Security experts say and statistics confirm that:

- Information technology security administrators should expect to devote approximately one-third of their time addressing technical aspects. The remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk, addressing contingency planning and promoting security awareness;
- security depends on people more than on technology;
- employees are a far greater threat to information security than outsiders;
- Security is like a chain. It is as strong as its weakest link;
- the degree of security depends on three factors: the risk you are willing to take, the functionality of the system and the costs you are prepared to pay;
- Security is not a status or a snapshot, but a running process.

These facts inevitably lead to the conclusion that security administration is a management issue, and not a purely technical issue [8,9].

We will be discussing the details of implementation steps in Section 3.

3. Proposed ISO27001 Based ISMS for HU ICET

3.1. Proposed Scheme

An introduction about ISMS is discussed in Section 2, which has the background material. In this section, we will be addressing the ISMS management framework in addition to the implementation steps of ISO/IEC 27001:2005. ISMS management framework describes the systematic and structural approach of managing information security at ICET. It defines the key elements of information security management and also the ways it is implemented and maintained. Figure 5 illustrates the implementation steps needed for the ISO27k. This will be discussed in details in the next subsections.

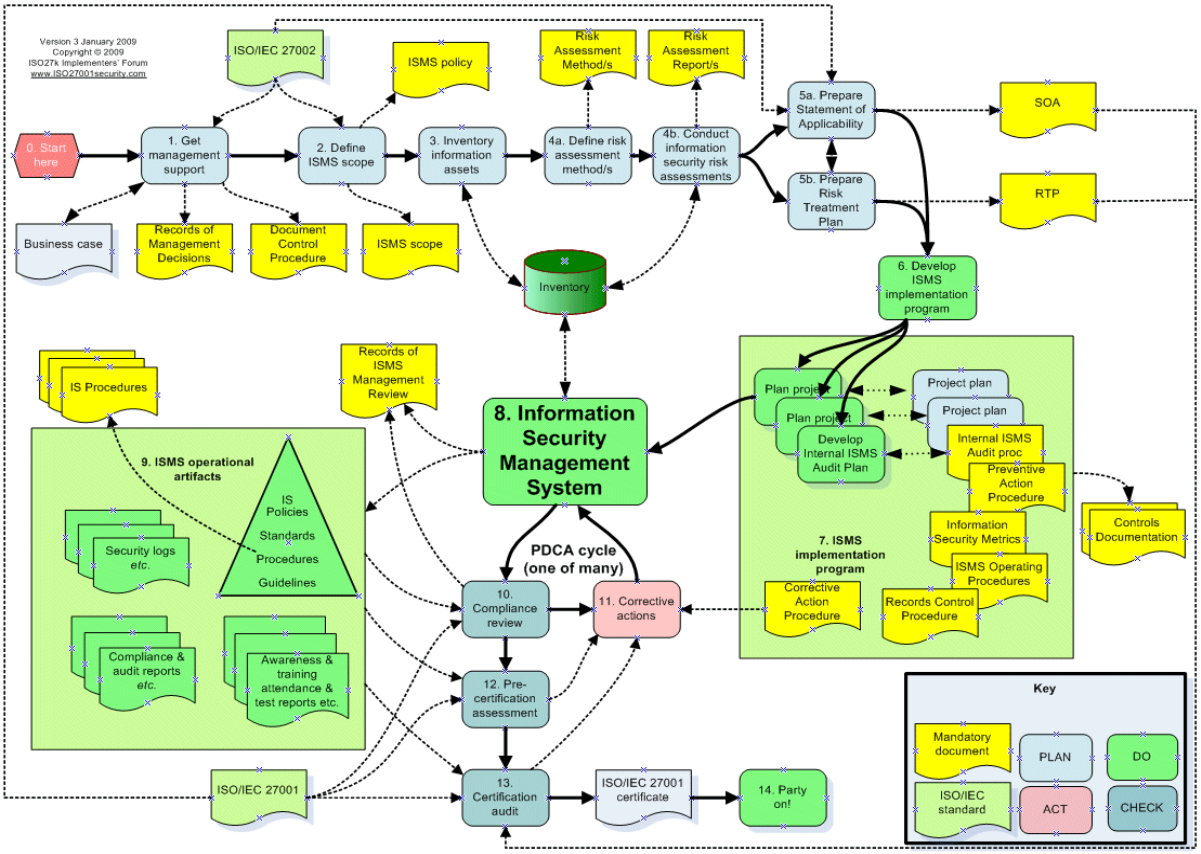

Figure 5. ISO27K implementation steps

In this paper, our work starts with step (0) of Figure 5, and ends with step (6) including the Statement of Applicability (SOA) and the Risk Treatment Plan (RTP). By finishing the previously mentioned steps, we will finish all the required planning requirements for the ISO2k standard. Planning is the process of establishing the ISMS by applying the policies and objectives of the ISMS as well as the developing of the procedures concerning managing the risks, in addition to finishing most of the required documented works which are the policies, scope, risk assessment methods, risk assessment plan, risk mitigation plan, and statement of applicability (SoA).

By this the ICET will be ready to start the DO (the green color in Figure 5) step which is the process of implementing and operating the ISMS, which was planned in the previous step.

After that, there will be some CHECKING (the dark blue color in Figure 5) which is the process of monitoring and reviewing the ISMS by measuring the performance against the applied controls including policies and finally exporting the results to management review. Checking steps are steps 10, 12, and 13 from Figure 5. The certificate audit (step 13) is done by a certified iso27001 lead auditor which will result in some **ACT** steps according to the management reviews and auditor recommendations. Based on the auditor report, the ICET will or will not receive the iso27001 certificate being the second organization in Jordan to get the iso27001. It is to be noted that the first organization who got the certificate was ZAIN Telecommunication Company [10]. The final implementation step (number 14), which is a DO step, implies that a party should take place after all the hard work established by ICET until the accreditation.

We defined the scope of our study to be the Hashemite University ICET Computer Center. The main problem we faced was in step (3) where we adopt a black-box methodology, which means that we should treat the ICET as a black box. We made our own assets inventory by identifying the most important assets in the center.

3.1.1. Establish the ISMS for ICET

A. Define the scope of the ISMS.
B. Define an ISMS policy.
C. Define a systematic approach to risk assessment.
D. Identify the risks.
E. Assess the risks.
F. Identify and evaluate options for the Mitigation of risks.
G. Select control objectives and controls for the Mitigation of risks.
H. Prepare a Statement of Applicability (SoA).
I. Obtain management approval of the proposed residual risks and authorization to implement and operate the ISMS.

- *Documentation Requirements*

ISMS Documentation shall contain:
A. Documented ISMS Policies.
B. Documented ISMS Procedures.

C. Documents needed by the organization to ensure planning, operation and control of the ISMS processes.
D. ISMS records depicting the proof of implementation and improvement.

- *ISMS Scope*

Information assets of Hashemite University ICET Center for which the computer center has the assigned authority of or responsibility for administrating and managing information assets.

- *Information Security Policy*

Information security management in ICET center should be taking the issue of security management very seriously. These information security policies are applied to all the employees.

- *Risk Assessment*

Risk assessment is a very important topic in our project.

- *Risk Mitigation*

A Risk Treatment Plan (RTP) which is a coordination document defining the actions to reduce unacceptable risks and to implement the required controls to protect information assets. For each identified risk, the Risk **Treatment Plan shows:**
A. The method selected for treating the risk.
B. What controls are in place.
C. What additional controls are proposed.
D. The time frame over which the proposed controls are to be implemented.

- *Controls to be applied*

The risk management process will have identified critical areas of risk, as well as areas of lesser risk. Some controls are not applicable to every environment and may be used selectively according to local circumstances. The needed ISO 27001 applicable controls should be decided.

- *Statement of Applicability*

The Statement of Applicability (referred to as SoA) is a document that describes which of the 133 controls of ISO 27001 are applicable to Hashemite University Computer Center. Figure 6 illustrates the security process of the establishment.

3.1.2. Risk Management Methodology

Risk management will be presented and designed to mitigate the Hashemite University network. By applying this step, the ICET will be able to operate, monitor, maintain and improve its Information Security Management System according to the requirements of ISO/IEC27001:2005. Table 1 shows the information security risk management activities according the four phases of the ISMS. process [1]:

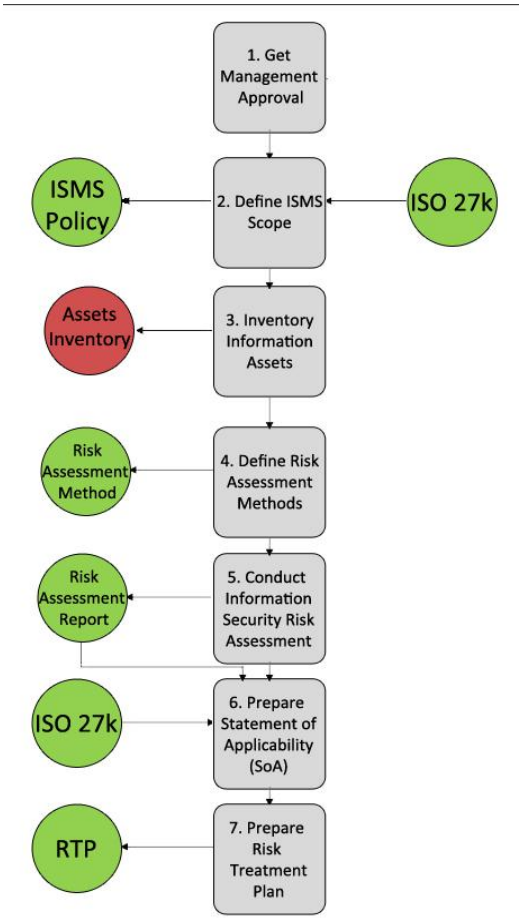

Figure 6. Security process

Table 1. Alignment of ISMS and information security risk management process

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

The Hashemite University, as any other organization, faces a struggle in keeping its network secure from inside and outside influences (threats), and in order to keep the business continuity, we need to draw a plan that defines these threats and their impact on the organization and propose a method of how to mitigate them before they pose a great risk on the institution. Plus to continue monitoring the risk management plan on the organization. The ISO 31000 standard is designed to and intended for implanting risk management codified by the Standardization; the purpose of these standards is to set some boundaries and guidelines regarding the risk assessment and management. Figure 7 illustrates the risk management process. Beneath it, we explain each step and show how we implemented it on the ICET.

 © 2014 Jordan Journal of Mechanical and Industrial Engineering. All rights reserved

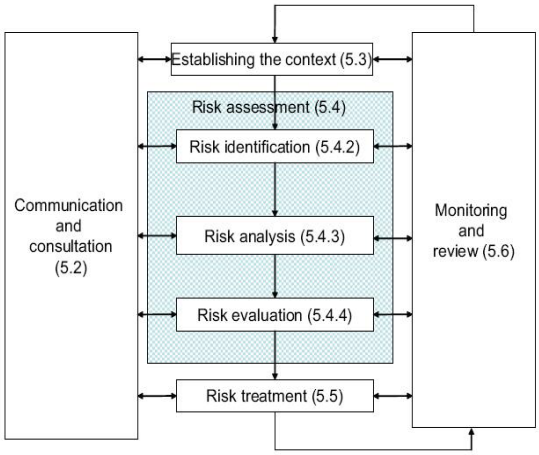

Figure 7. ISO 31000 risk management process

Risk management process consists of many stages according to the ISO 31000:

- *Communication and consultation*

All the risk information obtained from the risk management must be exchanged or shared between the decision-maker and the stakeholders based on an agreement. The communication is needed with the stakeholders in order to document their perception of the risks and their classifications of the assets values. In order to satisfy this procedure, we have distributed a survey to the employees of the computer center, asking questions regarding some ISMS policies. We did our best to keep the survey short and ask very obvious and short questions. Table 2 shows the result of these surveys:

Table 2. Survey results

The Assets		Assets value				
Site	OS	Very high	high	moderate	Low	Very low
Oracle application server	Sun Solaris 10	X				
Mail server "mail.hu"	Microsoft Windows Server 2003 SP2	X				
labsrv.labs.hu 10.238.0.18	Microsoft Windows Server 2003 SP2		X	X		
Hu-database-115	Sun Solaris 10	X				
Hu.edu.jo (87.236.232.218) 87.236.232.216	Sun open Solaris 2008.11	X				
Hu.edu.jo (87.236.232.220) 87.236.232.216	Microsoft Windows	X				
Hu.edu.jo (87.236.232.223) 87.236.232.216	Cisco 870 router or 2960 switch (IOS 12.2 -12.4)		X			
WEBREG 10.238.0.45	Server 2008 Enterprise Edition SP2		X			
EZPROXY 87.236.232.210 -87.236.232.15	Microsoft Windows Server 2003 SP2		X	X		
Juniper 87.236.232.194	NetScreen Screen OS	X				
Web portal	Microsoft Windows		X			
Juniper 87.236.232.195	Juniper Networks SSG 20 firewall	X				

The results of this survey helped us in preparing the risk treatment plan; we used the results to help us in the risk prioritization. Table 3 is about checking the applicability of ISMS policies on the organization:

Table 3: Statement of applicability

Question	Yes/No	ISO27001 Control
Is there a document describing the security policy related to information systems and in particular the organization, management and piloting of security (roles and responsibilities) as well as the fundamental principles underlying information security management?	NO	5.1.1
Is there a procedure for regularly updating organizational documents related to information systems security in line with changing organization structures?	NO	6.1.8
Are information systems covered by an insurance policy which accounts for material damage (fire damage, miscellaneous risks and accidents, damage to machines, all computing risks, "all risks except", named risks etc.)?	NO	
Are the information systems covered by an insurance policy which covers non material damage (malevolence, non authorized usage, and accidental loss of data or programs, denial of service)?		
Is the site completely enclosed by a perimeter fence which is difficult to cross or to scale? For a building on the public highway to be considered secure, all windows on the ground floor must be locked shut and all access points must have been taken into consideration (garages or underground car parks, roof etc.)	YES	9.1.1
Are the automatic access control systems under 24 hr surveillance enabling the detection of a failure, a system deactivation or the usage of emergency exits in real time?	YES	9.1.1
Is there an operational intrusion detection system to the site, linked to a 24 hr monitoring center?	YES	9.1.1
Has a thorough and systematic analysis of all the conceivable environmental risks for the site been conducted? Potential risks are : Avalanche, hurricane, storm, flooding, forest fire, land slide, earthquake, Volcano, broken dam or dike, torrential flood, falling rocks, collapse, gullies, drought	NO	9.1.4
Has a thorough and systematic analysis of all the conceivable industrial risks for the site been conducted? Potential risks are: high risk site nearby (Seveso like), dangerous internal installations, gas station, transport of dangerous materials...	NO	9.1.4
Is there a complementary video surveillance system, complete and coherent, for protected office areas, able to detect movement and abnormal behavior?	NO	
Is there a general control of movement of visitors and occasional service providers (time stamping at arrival and departure, signature of the person visited, etc.)?	NO	9.1.2
Are visitors and occasional service providers recorded in such a way as to enable a subsequent verification of the reason of their visit and has a procedure been put in place which enables the detection of dishonesty or abuse?	NO	
Is there an air conditioning system which regulates air quality (temperature, pressure, water content, dust) corresponding to the specifications of builders of installed equipment?	YES	9.2.2
Has there been a systematic and exhaustive analysis of all the possible points at which water might enter? For example: position of locations relative to natural overflows in the case of flood or violent storms, flooding from floors above, rupture of hidden or exposed pipes, usage of fire extinguisher systems, overflow of water evacuation conduits, untimely start of humidifier systems etc.	NO	9.1.4
Is there an automatic fire detection system for sensitive locations (raised floors and false ceilings if they exist)?	YES	9.1.4
Is there a possibility to declare sites or remote access points as sensitive and, as such, requiring an authentication of the entity accessed?	YES	
Is there a mechanism of authentication of the entity called before access to sensitive sites from the internal network?	YES	
Is access to the various parts of the information system (applications, data bases, systems, equipments, etc) defined in terms of job profiles which regroup roles or functions within the organization (profiles define access rights which are available to holders of the profile)? Note: in certain circumstances the notion of "profile" may be replaced by the notion of "group".	YES	11.2.2
Is there a regular audit at least once a year of all rights attributed to each profile and the profile management procedures?	YES	11.2.4
Are the archive storage locations under permanent video surveillance?	NO	
Does the procedure and mechanisms of storage, distribution and exchange of keys and more generally the management of the keys offer solid guarantees which merit confidence and are they approved by the Information Security Officer?	YES	12.3.2
When changes are made to the operating systems, is there a review and test of their impact on the applications?	YES	12.5.2
Are all change requests for an application subject to a formal review procedure (requestor, rationale, decision process)?	YES	12.5.1
Are the decisions to change or update users' software versions subject to a control procedure (registration, planning, formal approval, communication to all concerned individuals, etc.)?	YES	10.1.2; 10.3.1
Does the Hashemite University have a formalized risk-analysis process that includes the identification and prioritization of risks and the development of an action plan?	NO	
Does the Hashemite University have an advisory group that cuts across different departments to facilitate the risk management process?	NO	

The answers to this survey help in building the risk mitigation plan as well as defining the risks posed to the organization, though some answers were misleading. However, we used the answers in the risk treatment plan.

- *Establishing the context*

Defining the scope of our work is performed by discovering all the assets using many vulnerabilities scanners such as Nexpose, Metasploit Pro, Web-securify [11].

- *Risk assessment*

This is the step where we identify the information assets that are of value to the Hashemite University ICET Center, the threats and the vulnerabilities of information assets, the existing controls present to counter the identified threat and assess the probability and the impact of the threats on the Hashemite University Computer Center. Then risks are determined and prioritized. Finally, the control effectiveness of the implemented controls are measured. Figure 8 illustrates the stages of risk assessment:

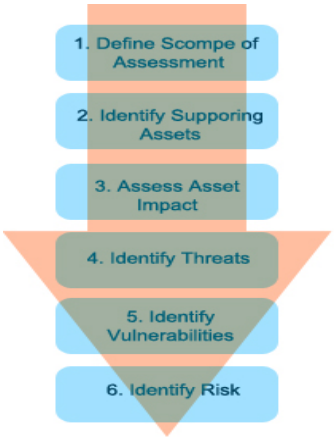

Figure 8. ISO 31000 Risk Management Process

- *Risk Identification*

Defining the scope of risk assessment includes the services provided by the assets listed in the Information Asset Inventory based on their importance to Hashemite University ICET Center, then we can specify the application of controls as required by ISO/IEC 27001:2005 and ICET Center Standards (if available). In this step we identify and list all the supporting assets that compliment and support supplying the information technology services provided. As in the information asset inventory, each identified supporting assets shall be mapped to relevant service offering covered under the scope of Risk Assessment, which is describes previously in Figures 5 and 6.

- *Risk Analysis*

After running vulnerability scan on the assets, and after defining the real vulnerabilities on each asset, the rule of risk analysis pups up. Risk analysis is the process to decide the nature of risk and to determine the level of the risk; it provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation; when estimating the level of the risk two factors should be taken into consideration:

a) The impact of the vulnerability:

The impact rating of each identified supporting asset shall be high, medium or low, taking into consideration the availability importance of services. The severity of each vulnerability is usually defined by global organizations such as CVE (common vulnerabilities and exposures), and CERT which is the United States computer emergency team [12].

b) The likelihood:

Likelihood is defined as the chance of something happening. In this context, it refers to the chance of occurrence of a specific threat based on the vulnerability, it can be determined objectively or subjectively, qualitatively or quantitatively. The ratings are identified as high, medium or low. In the calculation of risk assessment, the term “Probability” is the equivalent of the likelihood [13].

The following will provide the factors to be considered during the rating of an identified vulnerability:

High	In order to exploit the vulnerability, it would require minimal resources and have maximum probable opportunities.
Medium	In order to exploit the vulnerability, it would require minimal resources but have little opportunity or low probabilities. Or, to exploit the vulnerability, it would require a high degree of resources and have maximum probable opportunities.
Low	In order to exploit the vulnerability, it would require a high degree of resources and have minimal opportunity.

Risk is the outcome of an incident, when a threat successfully exploits t h e weakness present in an asset. Risk will have a negative impact on an entity or organization. Risk can be measured as the product of an asset impact and a probability that a weakness in an asset will successfully be exploited by a threat action. Risk Assessment Methodology:

- *Risk evaluation*

The purpose of this step is to assist in making decisions and, especially, in risk treatment and the priority for the treatment implementation based on the outcomes of risk analysis. The risk evaluation can lead to a decision not to treat the risk (risk acceptance). Figure 9 illustrates the risk determining matrix. Based on the determined risk, the risk should be rated from 1 to 6 as illustrated in Table 4. Risk rating helps in the prioritization of risk treatment which will be discussed in the next step, i.e., risk treatment.

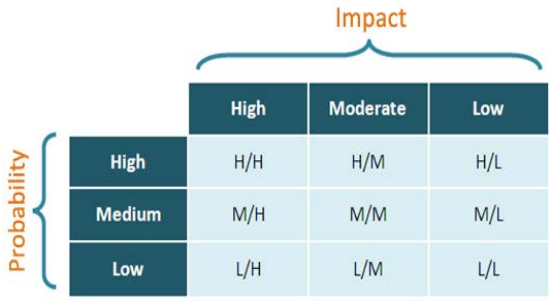

Figure 9: Risk Determining Matrix

- *Risk treatment*

This is the second phase of risk management and it is the process of applying adequate protection, based on a management decision to reduce, avoid, transfer and accept risk. An overall planning for the treatment of identified risks should be formulated based on the risk assessment report. All risks identified during risk assessment may not have the same level of impact on Hashemite ICET Center information assets and all recommended controls may not necessarily mitigate the identified risk in a cost effective manner. Risk treatment involves suggesting options for modifying risks, and implementing those options plus prioritizing risk treatment and offering risk mitigation techniques as well as defining the risk treatment option. Detailed planning and management approval sorting shall be done before treating the identified risks. A risk treatment plan is shown in Figure 10. For all the assets investigated, we offered the risk treatment option and added the required controls plus the ISO 27001 compliance for each vulnerability.

After analyzing all these risks and threats (Figure 10), we found out that most of the solutions to these vulnerabilities were:

1. Turning off some services or capabilities related to the vulnerability.
2. Adding access controls using firewalls or network borders.
3. Increasing monitoring to detect or prevent attacks (monitor the intrusion, prevention system) for 24 hours a day.
4. Raising the employees awareness about the vulnerability, giving them courses regarding these matters.
5. Testing and evaluating the patches, before installing, to ensure that they are effective and will not be any side effects.

3.2. Information Security Policies

3.2.1. Planning Policy

The objective of planning is to implement information security, and establish information security plans for the systems.

- *Information Security Planning Policy*

a) Information Security Officer must be established and filled by ICET that will be responsible for the leading and management of the ICET information security program.
b) The scope of each service must be defined in terms of its supporting assets, assets owners, and its technologies.
c) A risk profile must be created for each included service which should include identification of risks to the assets. Identification of risks must include threats to assets, vulnerabilities that may be exploited by the threats, and the possible impact that loss of CIA (confidentiality, Integrity, and Availability) on the assets.

3.2.2. Requirement Policy

The objective of policies and standards is to define the requirements and responsibilities that the users/employees must follow.

- *Information Security Policy*

An information security policy document must be established to manage the information security experience for the ICET. This document must set all applicable policies, security responsibilities and supporting information security procedures for the ICET. It must be reviewed and updated as necessary.

- *Statement Policy*

a) Security policy should have a clear statement which should include the vision measures for the ICET that should be protected.
b) Confidentiality, integrity, and availability of information should be met. Business continuity plan should be produced maintained and tested.
c) Defining the acceptable risk ranges, otherwise it will be considered for risk treatment.

3.2.3. Risk Management Policy

The objective of risk management is to manage threats and vulnerabilities facing ICET assets.

- *Risk Assessment Policy*

a) A risk assessment must be executed on all services at least once every three years or whenever major changes to the services occur.
b) Ongoing monitoring as well as mitigation of risks against different risks must be conducted.

*3.2.4. **Awareness** Policy*

The objective of awareness and training is to provide a formal technique for educating the employees of the ICET regarding their responsibilities with respect to information security.

a) The security officer must lead ICET wide security awareness campaign that delivers targeted information security awareness to all services users.
b) All employees of the ICET must receive appropriate training which must cover security requirements and legal responsibilities, as well as instruction in the correct use of information processing (e.g. logging to server remotely) before access to information or service is granted.

© 2014 Jordan Journal of Mechanical and Industrial Engineering. All rights reserved - Volume 8, Number 2 (ISSN 1995-6665)

OS	Supporting host asset	Risk vulnerability	Severity	Risk treatment option	Mitigation/acceptance	ISO 27001 Compliance
Microsoft Windows Server 2008 Enterprise Edition SP2	10.238.0.45/WEBREG	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (windows-hotfix-ms12-020)	High	Risk modification	Download and install Microsoft patch windows6.0-kb2621440-x64.cab (632043 bytes)	10.4.1,12.2.2
		SMB signing disabled (cifs-smb-signing-disabled).	Medium	Risk modification	Configure the system to enable or require SMB signing as appropriate. Note: ensure that SMB signing configuration is done for incoming connections (Server).	
		SMB signing not required (cifs-smb-signing-not-required)	Medium	Risk modification	Configure the system to enable or require SMB signing as appropriate. The method for doing this is system specific ,Note: ensure that SMB signing configuration is done for incoming connections (Server).	
		Database Open Access (database-open-access)	Medium	Risk modification	Configure the database server to only allow access to trusted systems	11.6.1/11.6.2
		ICMP timestamp response (generic-icmp-timestamp)	Low	Accepted	disable the service	11.4.1
		TCP timestamp response (generic-tcp-timestamp)	Low	Risk modification	Disable TCP timestamp responses on Windows Set the Tcp1323Opts value in the following key to 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters	11.4.1
	10.238.16.4/DNS	DNS server allows cache snooping (dns-allows-cache-snooping)	Medium	Risk modification	Restrict the processing of DNS queries to only systems that should be allowed to use this nameserve	10.6.1,
		Nameserver Processes Recursive Queries (dns-processes-recursive-queries)	Medium	Risk modification	Restrict the processing of recursive queries to only systems that should be allowed to use this nameserver.	11.6.2
		LDAP Anonymous Directory Access Permitted (ldap-anonymous-directory-access)	Medium	Risk modification	Disable anonymous access from the "Anonymous" tab of the LDAP protocol configuration in the Exchange Administrator.	11.4.4 ,11.4.6
		LDAP Anonymous Directory Access Permitted (ldap-anonymous-directory-access)	Medium	Risk modification	Disable anonymous access from the "Anonymous" tab of the LDAP protocol configuration in the Exchange Administrator.	11.4.4 ,11.4.6
		ICMP netmask response (generic-icmp-netmask)	Low	Risk modification	Disable ICMP timestamp responses on Windows Vista/2008 ICMP timestamp responses can be disabled via the netsh command line utility. Go to the Windows Control Panel.	11.4.1

Figure 10. Risk treatment plan

3.2.5. Performance Management Policy

The objective of performance management is to provide metrics to measure progress of the information security program.

a) ICET shall develop measurement procedures to measure the performance of the implemented information security management system, in-line with ISO27001:2005 standard.
b) The Security Officer shall monitor the effectiveness and efficiency of controls in-line with standard requirements.

3.2.6. Assets Management Policy

The objective of asset management is to maintain appropriate protection of assets by assigning assets owner(s) and the acceptable use of assets.

- *Inventory of Assets Policy*

a) An inventory of the important assets associated with each service must be produced. Each asset must be clearly identified along with its ownership.
b) Movement of physical IT assets shall be done only after approval from the IT manager; any changes in location of physical assets such as servers shall be updated in the asset inventory.
c) Software license inventory shall be maintained and updated on purchase of new license or on removal.
d) The loss, theft of assets shall be reported immediately to the IT manger/ Security officer.

- *Ownership Polic*

a) Each information asset shall have an owner who will be responsible for the assets that they own.
b) Asset owners will be responsible for ensuring that they have the correct skills and tools for protecting their assets to meet the security policies requirements.

- *Classification policy*

a) Information shall be classified considering the impact of loss of confidentiality, integrity, and availability.
b) Information assets available at the ICET shall be classified as Confidential, Internal and Public:

- Confidential: Information that is extremely sensitive and is intended for use only by named individuals within ICET.
- Internal – For Official Use Only: Non-sensitive information intended for distribution within ICET Only.
- Public: Non-sensitive pieces of information that are meant for release to general public

3.2.7. Physical Security Policy

The objective of physical security is to provide standards for the protection of personnel, hardware, software, and data from physical circumstances that could cause serious losses or damage to the ICET. This includes protection from fire, and natural disasters.

- *Physical Security Policy*

a) The security perimeter must be clearly documented.
b) The perimeter of the ICET building must be physically protected, i.e., there must be no gaps in the perimeter or areas where a break-in could easily occur. External walls of the site must be of solid construction and all external doors must be suitably protected against unauthorized access by appropriate control mechanisms (e.g. alarms).
c) Controlling physical access to the ICET building must be in place; access to ICET building is restricted to authorized personnel only.
d) Secured areas must be clarified and must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
e) Doors and windows must be locked when unattended, and external protection must be considered for windows particularly those at ground level.
f) Visitor log book shall be used to record all visitors entering and leaving a secure area such as the server's room. Visitors should register details, such as name, date, entrance-time, and exit-time.

- *Supporting Utilities and Equipment's Policy*

a) Equipment shall be protected from power failure.
b) All supporting utilities such as electricity, air conditioning must be adequate for the systems they are supporting.
c) All servers and network equipment's hosted in the data center shall be provided with uninterruptible power supply system (UPS) to facilitate orderly shutdown of the information system in the event of a primary power failure.
d) The UPS should ideally protect all the ICET information processing assets, within the data center.
e) The air conditioners shall be checked for effective functioning regularly.
f) The air conditioning system should be effective and the temperature in the data center should be monitored. The server room should have temperature monitoring devices and it should be ensured that the temperature should always be maintained in appropriate levels.
g) Air conditioning should be provided on a 24-hour basis.
h) It must be ensured that the UPS is not switched off and that the power cord is properly secured to the equipment. Checking the functionality of batteries is necessary as well.
i) It must be ensured that no unauthorized person tamper or change the switch settings on the UPS.

- *Cabling Security Policy*

a) Power and cabling into data centers will be underground or will provide the required protection from any interference or damage.
b) Cabling maps should be made available and updated regularly.
c) All cables should be labeled and tagged.

3.2.8. Operation Management Policy

The objective of operation management is to introduce procedures to manage the information processing and administer their management.

- *Operating Procedures Policy*

The ICET center must provide the operators with documents showing the tasks and responsibilities of employees involved in information systems operations.

- *Capacity Management Policy*

a) Capacity of all servers must be monitored regularly and reported to the security officer.
b) Hardware capacity monitoring must include:
- Disk Space Capacity.
- Processors Utilization.
- Main Memory.
- Network Interfaces Utilization.

- *System Acceptance Policy*

a) Acceptance criteria for a new information system, upgrades and new versions should be established after suitable tests of the system before acceptance, some controls that should be considered during acceptance testing includes:
- Security controls in place.
- Performance and system capacity requirements are defined.
- Error recovery, restart plans are established.
- Training for the users in the operation or use of the new system.

b) All in-house developed system shall have appropriate documentation and functional requirements, technical specification, testing acceptance, and user's manuals prior deploying the new system.
c) Risk evaluation related to the introduction of new information systems, upgrades must be established before acceptance, and risk mitigation of risks shall be initiated, before acceptance.

- *Backup Policy*

a) Valuable, critical information must be backed up periodically.
b) b) Daily backup must be applied for all very sensitive information.
c) ICET management must define which information and system are to be backed up, the frequency of backup, and methods.
d) Disaster recovery sites must be established in a separate location from the primary location, and have the appropriate infrastructure needed.
e) Standardized naming procedure must be produced.
f) Information must be retained for no longer than its necessity.

- *Removable Media Policy*

a) Removable media on which information is stored (e.g., CD, USB, DVD, printed papers) must be controlled and physically protected with their classification, to protect the information from unauthorized disclosure, modification or destruction.
b) USB ports shall be disabled on all user desktops and workstations, and only enabled based on business requirements. Approvals for enabling the USB and removable media shall be approved by the security officer.
c) Removable media containing ICET confidential data shall not be taken off-site unless prior agreement. Confidential data shall be encrypted (Oracle Database encryption research APPENDIX A)
d) Attempting to install applications from removable media onto any ICET computer assets is prohibited unless authorized by security officer.

- *Information Exchange Policy*

a) Information systems must provide non-repudiation capability to determine whether a given individual took a particular decision at specific time or not.
b) Sensitive information and classified documents must be excluded from systems which do not provide an appropriate level of protection.
c) The information system must protect the integrity of the transmitted information during information transaction.
d) The information system must terminate an open session at the end of session or after pre-defined time period of inactivity.

- *Patch Management Policy*

a) Checks for new security-related patches and updates that are published via vendor web sites must be made at least once every week (e.g., windows server 2008 patches).
b) Newly released patches, service packs, and hot fixes must be installed on the information systems.

- *Server Access Management Policy*

a) Access to server consoles and operating systems shall be limited to system administrators only. All server administrator accounts shall match with password requirements set by ICET password policy.
b) All non-essential, and defaults users, group, and service accounts must be removed (e.g., Scott/Tiger in oracle).
c) All non-essential services must be removed immediately during installation (e.g., netBios).
d) Administrators are prohibited to share their credentials with anyone.

- *Perimeter Security Controls*

Network shall be protected using a firewall and related technologies so as to enable blocking unwanted traffic:
- Hiding vulnerable systems from the external network.
- Providing logs of traffic to and from the private network.
- Hiding information like system names, network topology, network device types and user ID's from the external network.

- *Routers & Switches Security Policy*

a) All routers and switches shall be configured only by the authorized network administrator.
b) The routers and switches shall be configured in order to reduce the risk by allowing only necessary services.
c) Routers must be placed in temperature and humidity controlled environment.
d) Routers must be powered by an uninterrupted power supply (UPS).
e) ICET shall create individual usernames for all administrators with appropriate privilege levels to enable access to routers and switches.
f) Access Control List (ACL) shall be used to restrict the hosts that are not allowed to access the router.
g) All passwords used in the routers and switches should meet the requirements of the password policy.
h) All the routers must have logon banner stating that the unauthorized access to this network device is prohibited, and there should be explicit permission to access or configure the device.
i) Telnet may never be used across any network to manage a router (unless there is a secure tunnel protecting the communication), SSH is the preferred management protocol.

- *Desktop Security*

a) Users at ICET shall not be given local administration privileges.
b) The use of removable storage shall be prohibited as per Removable Media Policy.
c) All desktop should be running standard password-enabled screen saver.
d) All desktops should be running only ICET standard and licensed software's.

- *Wireless Network Controls*

a) Wireless Access Point (WAP) passwords should not be set to default.
b) SSID name should not be set to default.
c) WEP Encryption should not be used to grant access.
d) Wireless network gateways shall be configured so that they employ firewalls to filter communications with remote devices.
e) MAC filtering should not be used to grant access.
f) Ensure that WAP are secured properly.

- *E-mail Management Policy*

a) E-mail content scanning and spam control must be used to reduce the risk from denial of service attacks (DoS).
b) ICET retains the rights to access employee e-mail if it has reasonable grounds to do so. E-mail content will not be disclosed other than for security purposes.
c) To prevent computer viruses and spams employees are advised not open attachments that are from unknown sources.
d) ICET employees must treat e-mail messages and attachments as confidential information. E-mail must be handled as a confidential and direct communication between both entities sender and recipient.
e) All messages sent by employees by e-mail are the records of ICET. ICET reserves the right to examine emails, personal file directories, and other information stored on ICET computers and servers. E-mail messages may be monitored for many reasons such as supporting internal investigations for suspected criminal activity or fraud.
f) Offensive e-mails must be reported directly to the security officer.
g) Users should not use their official e-mail ID to subscribe to news groups that generate heavy amount of mail traffic.
h) E-mail signature for ICET shall be standardized.

3.2.9. Access Management Policy

The objective of access management is to ensure good management of users' identities, and granting access to these users.

- *User Access Management Policy*

a) All employees must sign the acceptable use statement before being granted system access.
b) Allocation of user privileges must be controlled.
c) User access rights must be reviewed regularly to very ICET access control policies.

- *Password Policy*

a) Users must not share passwords.
b) Passwords are a must requirement for all accounts.
c) Forgotten passwords must be managed in a secure manner.
d) Passwords provided through a procedure, that involved third party knowledge (e.g., doctors to student password delivery techniques), must require the password's owner to change it at first use.
e) Passwords must have a defined expiry period which depends on the sensitivity of the accounts.
f) Passwords must contain at least one numeric or special character.
g) Password must contain a mixture of at least one uppercase and at least one lowercase letter.
h) Passwords must not be displayed in clear text as they are being typed.
i) Authentication mechanism must be done in a secure manner to ends, end-user and authenticator.

- *Lockout Policy*

a) Inactive terminals, which serve high-risk services, must shutdown after a defined period of inactivity to prevent access by unauthorized person.
b) The time-out procedure must clear the terminal screen and close both the application and network sessions after pre-defined period of inactivity.
c) Restrictions on connection times must be considered to provide additional security for applications. (E.g. brute force attacks).

- *Network Security Policy*

a) Users must only have access to the services that they have been authorized to.

b) All methods of remote access to the information system must be documented, monitored, including remote access for privileged functions.
c) Users are prohibited from attaching modems directly to their computers.
d) Access to all external networks must pass through and access control point (e.g. firewall) before reaching and intended hosts.
e) All information must be transmitted in an encrypted format. Including wireless local area networks (LANs), all protocols must be encrypted (e.g. HTTPS).
f) Only authorized and approved network devices may be connected to the network.
g) Use of unencrypted passwords to access network devices internally or externally is prohibited.
h) Network monitoring mechanisms must be active to detect, record, and prevent network hacking attempts and denial of service attack (DoS).
i) All network management passwords must be changed based on password policy.

- *Encryption Policy*

a) Encryption must be considered for the protection of information processing which is categorized as moderate or high classification.
b) An appropriate cryptography technique/algorithm must be implemented taking into consideration the needed protection, implementation and key management.
c) Care must be taken to protect confidentiality of the private key, which must be kept secret.
d) Protecting the public key is mandatory by using public key certificate.
e) Non-repudiation services must be used where it is necessary to resolve any misunderstanding about event occurrences.
f) To reduce the risks of compromise of cryptographic keys, a management system must be in place to support the ICET use of two cryptographic techniques:

- Private Key technique, where two or more entities share the same key for encryption and decryption. This key must be secret since anyone have access to it would be able to decrypt information uses encrypted by this key. This technique could be used for encryption of Database columns for access control needs.
- Public Key techniques, where each user has pair of keys. A public which is revealed to everyone and private which is secret. Private keys must be protected from any unauthorized disclosure.

3.2.10. Business Continuity Management Policy

The purpose of business continuity management is to create a practiced plan for how the ICET will recover within a specific time period after a disaster or disruption.

a) Business continuity plans must be established.
b) Each business continuity plan must clearly specify the conditions for its activation.
c) Each plan must have a specific owner.
d) Emergency procedures must take place in every plan and must be within the responsibility of the owner of the plan.
e) Business continuity plans may fail upon being tested, usually due to incorrect assumptions or change in equipment's or employees. They must therefore be tested regularly to ensure that they are up-to-date and effective. Such tests must ensure that all members of the recovery team and all ICET staff are aware of the plan.
f) Test schedule must be established, which ensures that the plan(s) will operate in real life.

3.2.11. Acceptable Use Policy

ICET must specify the acceptable use of every information system assets, in which all asset end users must be documented.

3.2.12. Risk Assessment and Risk Mitigation Plan

An excel sheets for the plan have been developed and submitted to the ICET center. It should be noted that due to the size (many pages) of the excel sheets; we have excluded them from this paper. However, they are available upon request.

4. Summary and Conclusions

Security breaches have been addressed as a major threat for organizations around the world. Organizations and governments spend millions of dollars annually to recover from attacks' negative impact on their information assets. Many statistics have stated that most of the security breaches caused by an internal organization problem or can be prevented by eliminating an internal problem. Hence, information security management systems are being adopted by many organizations in order to have appropriate controls to eliminate possible internal organizational problems that may introduce some serious security breach. In this paper, we have taken HU as a case study (most of Jordanian universities have similar IT setup) and it is concluded that Jordanian universities information systems are facing real possible dangerous security breaches due to the presence of a huge number of different kinds of vulnerabilities in their information systems. The vulnerabilities can be categorized as:

- Inadequate information security awareness for the organization personnel.
- Organizations do not adopt an information security management system to control the security process of the information systems.

We have presented a full package solution for different kinds of vulnerabilities whether technical or organizational by implementing ISO27001 information security management system ISMS, which should eliminate all the vulnerabilities identified during vulnerabilities assessment phase. The main focus was to identify the risks in Jordanian universities' information systems as well as planning for implementing ISO27001 by developing the needed controls. Hence, it enables Hashemite University to start the stages of eliminating the identified risks. With the introduction of these procedures and documents, the Hashemite University

will be ready to start the **Do stage,** which is applying the ISMS on the ICET toward getting an ISO accreditation.

References

[1] Jacobs, S., Security Management of Next Generation Telecommunications Networks and Services, Wiley-IEEE Press, 2014

[2] ISO/IEC, "Information technology-Security techniques-Information security risk management", ISO/IEC 27005:2011, 2011.

[3] Tipton, Harold F. and Micki K., Information Security Management Handbook, 4th Edition. New York: Auerbach Publications, 2000.

[4] Donald Waters. Supply Chain Risk Management: Vulnerability and Resilience in Logistics, 2nd Edition. London, UK, Kogan page, 2011.

[5] G. N. Ericsson, "Cyber security and power system communication—Essential parts of a smart grid infrastructure", *in* IEEE Transaction. Power Del., vol. 25, no. 3, pp.1501 -1507, 2010

[6] Shakeel Ali, Heriyanto Tedi, ”Master the art of penetration testing with BackTrack”, BackTrack 4: Assuring Security by Penetration Testing, 2011.

[7] British standards (BS) ISO/IEC 27001:2005, British standards (BS) ISO/IEC 27002:2005.

[8] C. Alberts and A. Dorofee, "Managing information security risks: The OCTAVE SM approach". Boston: Addison-Wesley Anderson, 2002.

[9] Moyo, M. ; Abdullah, H. ; Nienaber, R.C., "Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems" *in Proc*. of Information Security for South Africa, pp. 1-6, 2013

[10] Zain-jordan sustainability report 2010, http://www.zain.com/media/social_responsibility/zain-sustainability-report-english_1.pdf, (accessed Feb 2013)

[11] R. Munir, A. Alhomoud, J. P. Disso, and I. Awan, "On the Performance Evaluation of Intrusion Detection Systems," *in Proc*. of Advances in Security Information Management: Perceptions and Outcomes, pp. 117-138, 2013.

[12] Vogt, M., Hertweck, D. Hales, K. Strategic ICT Alignment in Uncertain Environments: An Empirical Study in Emergency Management Organizations, *in Proc.* 44th Hawaii International conference on System Sciences (HICSS), pp. 1-11, 2011.

[13] H. Kumamoto, and E. J. Henley Probabilistic Risk Assessment and Management for Engineers and Scientists, Wiley-IEEE Press, 2000.