TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technology
Department of Informatics
Chair of Information Systems

Suggesting The Best Information Security Management System For Palestinian e-Government

Master's Thesis

Student:	Mohammed A. M. Shahwan
Student Code:	132086
Supervisor:	Prof. Katrin Nyman-Metcalf

Tallinn

2015

Author's declaration

I confirm that I have constructed this Master's thesis individually and that the current paper has not been presented by anyone before. All resources, viewpoints, citations, and other materials from other authors that have been used in this thesis have been referred to.

-- --

(*date*) (*signature*)

Annotation

The goal of this thesis is to assess the need for implementing information security management system for e-government solutions in Palestine. In addition this thesis look for what would be the best information management system to be implementd.

This thesis mainly handles the comparison between a group of information security management systems, including a review of each one independantly.

Moreover this thesis aims to disscuss what would be a suitable criteria for conducting the comparison bettwen the different systems. In addition to relating this work to the case of e-government in palestine.

This thesis resulted in the suggestion of following the same approach as in the Estonian case which is to build a national information security management system based on IT-Grundschutz. And for the ease of understanding and use of such system, it was suggested that the newly developed system would be in Arabic language which is the official language in Palestine.

Moreover it should be supported with legislations and regulations. In addition implementing information security management system is not enough, other aspects should be considered such as educating personnel and system users, and founding CERT team.

The thesis is written in English language and contains 73 pages of text, 5 chapters, 6 figures, graphs and diagrams, and 1 table.

Acknowledgment

To my family (especially Mom and Dad), friends, my supervisor, and everyone who supported me through my work on this thesis.

Abbreviations and concepts:

- **[PA]** *[Palestinian Authority]*
- **[PCBS]** *[*Palestinian Central Bureau of Statistics*]*
- **[ISMS]** *[*Information security management system*]*
- **[MTIT]** *[*Ministry of Telecommunications and Information Technology*]*
- **[OECD]** *[*Organisation for Economic Co-operation and Development*]*
- **[PLC]** *[*Palestinian Legislative Council*]*
- **[Dos]** *[*Denial of Service*]*
- **[CIA, CIA triad, CIA security model]** Confidentiality, Integrity, and Availability*]*
- **[ISO]** *[*International Organization for Standardization*]*
- **[IEC]** *[*International Electrotechnical Commission*]*
- **[ICT]** *[*Information and communications technology*]*
- **[BSI]** *[*Bundesamt für Sicherheit in der Informationstechnik*]*
- **[COBIT]** *[*Control Objectives for Information and related Technology*]*
- **[ISACA]** *[*Information Systems Audit and Control Association*]*
- **[ITGI]** *[*IT Governance Institute*]*
- **[ITIL]** *[*Information Technology Infrastructure Library*]*
- **[ITAF]** *[*Information Technology Assurance Framework*]*

List of tables

List of figures

Contents

1. Introduction

Computers and personal computers started to be more involved with human life and there daily activities, and with the fast development of the smart devices. It wasn't a surprise that those kind of electronic devices have been seen as a tools to facilitate daily activities and a way to save time, effort, and even cost or money.

As a natural evolve to this dependability relation between human and computers, it was not a surprise that computers took a part in government daily routines. Computers have a very powerful ability to store huge amount of data and it saves a lot of effort. With the fast growing and spread of the internet it becomes more common to hear some new terms such as e-governance and e-government.

With the increased use of the computer and the internet, cyber security threats were also evolving with different types and different results. Such types of cyber security are: stealing personal and financial information, physically damaging and affecting computer hardware, or even affecting a whole country such as what happened in Estonia back in 2007 Tikk et al (2010).

This can be a result to underestimate the cyber security threats, or a result of not having the right procedures and planning to handle such situations. Those procedures aims to prevent, mitigate, or reduce the damage as much as possible and keep delivering the same functionality without a serious affect.

Within the constant search and induce of the PA (Palestinian Authority) to improve and enhance the quality of the services that it provides for the citizen and the business. It was a great move to adopt and implement the e-government concept to follow up the modernization and the quest to facilitate its services. This would help to overcome some of the imposed issues due to the Israeli occupation, and the fact that the two main parts of the jurisdictions (the West Bank and Gaza strip) are geographically separated.

With the help of the Estonian government throughout Estonian e-Governance Academy in (2010) the PA started the implementation of the e-government services. This was done by adopting some of the technologies that are running in Estonia such as the X-Road, but the cyber security side has not been taken into consideration.

1.2 Scope

It's been already proven that cyber security is one of the main and major key elements for trust worthy and reliable e-government. Without a proper cyber security planning and implementation to secure the main resources and infrastructure of the e-government, it will be in a certain danger to affect or take down the whole government.

In addition to risks with citizens and business data and information, and maybe in some cases it will affect all or part of the critical infrastructure of the country.

The main work for this thesis will be based on the integration of good and proper cyber security policies and plans, for mitigating and reduce the potential damage that would be caused by cyber-attacks. With more specialization about choosing and implementing the right Information Security Management System (ISMS) for the e-government project in the state of Palestine as an example and a case study.

1.3 Research Questions

During the work on this thesis the following question will be raised:

- How to choose the most suitable information security management system (ISMS)?

By answering this question the final result of the thesis should be achieved.

- What are the criteria for evaluating and comparing different ISMSs to choose amongst them?

This question is related to the first question, and by stating the criteria that will be used for the comparison the final result of the thesis should be achieved.

- Why it's important for the Palestinian state to adopt ISMS?

In order to get an answer for this question some facts should be reviewed and a couple of sub question should be answered what are the reasons for the Palestinian state to adopt ISMS? Is it a necessary to implement ISMS? And what are the other options or solution that might work as a replacement for and ISMS.

1.4 Research method

In order to achieve the goal of the thesis and answering the proposed research questions for the topic of the thesis, the literature that are related and discussing the topic of the thesis should be analyzed to get general understanding of the issue in addition to a deeper understanding of the issue which eventually will be form the general picture of the situation and will give a clue and general guidelines on how to solve the issues that the thesis discussing.

The result of this analysis should be a group of criteria that would be used to evaluate and compare between the different proposed solutions to choose the best and most suitable solution among them regarding the discussed issue.

One way to achieve the goal of the thesis and get to these answers for the proposed research questions, the main resources that will be used is in the form of documentations and interviews, the interviews would be in different forms such as Unstructured, Semi structured, and Structured; and in order to analyze the interviews qualitative research method would be used, as interviews are one form of collecting information for the qualitative research, and also the fact that qualitative research can be used to reach non predetermined results which is the case of this thesis this will for some levels guarantee that the final results of this thesis are not subjected to the author own thought and that those results are neutral.

And in order to evaluate the final results of the thesis action research can be used, as action research is better to be used for real life situation rather than experimental studies, and the case of this thesis is more practical and try to solve a real life problem.

Action research can be also used to analyze interviews which are already analyzed by qualitative research, this would result in more and deeper understanding of the issues as the interviews would be analyzed with two different research methods, which can also result in increasing the credibility of the final result as it will be based on the analysis of the two methods.

Another resource of data and information for action research would be the case studies, as in some part of the thesis there would be a use of some case studies about how the same issue that being discussed within the thesis how it was handled by different actors who already faced such problem or even similar problem.

So as a conclusion of the research method(s) that will be used for analyzing the data related to the topic’s issue a combination of both qualitative and action research will be used in order to get to a deep understanding of the issue which will help to provide the most suitable solution and answers to the proposed research question.

1.5 Structure

This thesis will be composed of (5) chapters which are as the following:

Chapter 2: titled “The Palestinian e-government”. This chapter will address the current situation of e-government in Palestine and will review the current policies and measures for cyber security.

Chapter 3: titled “Selection of ISMSs”. Within this chapter a number of ISMSs will be reviewed and classified. Those selected ISMSs will be evaluated later in the following chapter to choose the most suitable system amongst them to be adopted and implemented for the Palestinian e-government.

Chapter 4: titled “Comparison criteria and evaluation”. Within this chapter the criteria that will be used for the comparison and the evaluation will be stated. And then the evaluation will be conducted in order to get to the final result of this thesis.

Chapter 5: titled “Conclusion”. This chapter will conclude the work on the thesis and will state the final result of the thesis. The result will be the suggested ISMS to be implemented for the Palestinian e-government.

2. E-government in Palestine

2.1 The need for e-Governance

A quick review about Palestine: the geographical location of Palestine is in Western Asia where the Mediterranean Sea located to the west of Palestine, Lebanon, and Syria from north, Jordan, and also Syria from east, and Egypt and the Red Sea from south, with the total area of 27,000 Km².

In 1967 the United Nations (UN) has recognized Israel as a state on the Palestinian lands, which is about 22,072 Km² out of the total area of Palestine. This left around 4000 Km² that are geographically divided into two main parts which are the West Bank and Gaza strip, those two parts are governed by the PA (PLO, (2011)).

PA provides services for about 11.6 million Palestinian as stated by the Palestinian Central Bureau of Statistics (PCBS (2013)), this number is distributed into three main parts, and two of those parts are the main areas where the PA practices its authority (West Bank and Gaza Strip).

The third part is the different refugee camps in some of the neighboring countries (Lebanon, Syria, Jordan). The estimated distribution would be as the following: 2.79 million in West Bank, 1.76 million in Gaza Strip, and the rest are distributed on different refugee camps.

It can be seen from the previous situation, and the fact that freedom of mobility is limited between the different parts where the PA provides its services. It is a necessity for the PA to provide e-government services which will help to achieve some business outcomes as stated in the e-government strategic plan (2005).

Those outcomes can be divided into three main categorize as the following:

- **Government benefits:**

  By applying e-government it will help to increase the transparency and accountability. It will also enable the citizens to participate in government. The government will also benefit from connecting different data sources within different ministries and different governmental bodies (the e-government strategic plan (2005)).

- **Citizen benefits:**

  E-government will enable the citizens to access to high value citizen-centric services. Moreover it would help the citizens to reach different e-services throughout multiple and different channels. Plus citizens will have the chance to benefit from the new advantages of the health services (the e-government strategic plan (2005)).

- **Economic benefits:**

  For economic e-government is seen as an opportunity to provide new job opportunities. Also it will help to promote Palestine as a promising place for conducting business (the e-government strategic plan (2005)).

2.2 Planning for e-Government

Back to 2005, the ministerial committee for e-government was assigned by the Palestinian president Mahmoud Abbas.

The committee has made the first e-government strategic plan, which defined the road map to establish the e-government project, states the benefits, and the main out comes of the project as stated previously.

As part of the commitment to the plans and strategies to implement e-government, the Palestinian authority managed to establish a cooperation project with Estonia throughout the Estonian e-Governance Academy in (2010).

The Estonian cooperation project aims to help the PA to implement the Estonian X-Road which is an interoperability frame work. X-Road works as a backbone for the e-government and help to connect different data sources such as ministries, governmental bodies, and even private sector (e-Governance Academy (2010)).

Beside the e-government strategic plan, and the Estonian cooperation project, there were also some projects about capacity building and providing training and preparation of professional staffs that would work on building and implementing e-government projects and e-services.

An example of such project is the Palestinian e-Government Academy. The project was established in October 2010. The academy was held at Sina Institute - Birzeit University – Palestine, partnering with some local universities and ministries, and some international universities all from Europe. There were also some training projects with the cooperation with the Estonian e-Governance Academy.

Another project was conducted with the cooperation with Estonian e-Governance Academy with the support of the ministry of Foreign Affairs of Estonia.

The project was about “Supporting the development of ICTs in education”. The main goals of the project were “analyses, consultancy and training on using Information and communications technology (ICTs) in secondary education management and teaching/learning process in Palestinian Authority” (e-Governance Academy (2010)).

As can be seen from the previous examples, e-government is a high priority for the PA and it has been suggested for long time (e-Government Strategy Plan goes back to 2005). The PA is not saving an effort in order to achieve the goal of full implementation of fully functioning e-government framework that achieves the planned and suggested goals.

2.3 Implementation of e-Government

Recently in (26 February 2015) Ministry of Telecommunications and Information Technology (MTIT) has established and announced a working implementation of the X-Road as result of the Estonian cooperation project.

Dr. Allam Mousa the Palestinian minister of Telecommunications and Information Technology with the presence of Mr. Hannes Astok and Arvo Ott from the Estonian e-Governance Academy has announced the establishment of the Palestinian X-Road system (MA’AN NEWS AGENCY, (2015)).

The Palestinian X-Road system works as the interoperability layer for the e-government in Palestine and that it will be used to connect the different ministries and governmental bodies.

Alongside the X-Road system Dr. Mousa also announced a number of 12 e-services as the first implementation of the e-government.

The collection of the services diverse between citizen’s records such as birth, death, and business registration records, some services for the governmental employees, and some services for citizens who are benefiting from the ministry of Social Affairs (MA’AN NEWS AGENCY, (2015)).

2.4 Evaluating e-Government in Palestine

As part of the constant work of the PA, to implement e-government and meet the goals that was outlined in the e-Government Strategic Plan. PA had another collaboration project with the Organisation for Economic Co-operation and Development (OECD).

As a result of this collaboration OECD has published a report titled as “Modernizing the Public Administration: The Case of E-Government in the Palestinian Authority”. The main goal of the report is to “to present an evaluation of the Palestinian Authority’s (PA) e-government policies and their implementation” (OECD (2011)).

The report provided a wide analysis of the current situation of the e-government when the project started (2010). The analysis included the general situation, ICT infrastructure, policies and laws, in addition to adoptive version of the OECD E-Government Survey.

According to the report and based on the MTIT National Strategy for ICT and Post in Palestine, the Palestinian legal framework is currently lack of those main provisions:

- The E-Signature Law
- The Electronic Transactions law
- The Law of Protection of Individual and Personal Data
- The Intellectual Property Protection law
- The Electronic Commercial Transactions, and Internet and IT Laws
- The Law of Freedom and Confidentiality of Information in Electronic Communications
- The Cyber Crimes Law

It can be noticed that the legal framework needs to be modified and adopt new laws.

Currently there is an ongoing process to adopt and approve the Electronic Transaction Law. The law is currently in the second phase of revision within the Palestine cabinet, to be approved to the next level which is the approval from the Palestinian president (MTIT (2010)).

Among the main outcomes of the report, it was stated that conflict with Israel has a huge impact on the development of the e-government in Palestine. This is due to the fact that the imported equipment or services should pass through the Israeli borders, and Israel is making it difficult to issue the entry permits. Also it is difficult to issue the custom clearance for such equipment which makes it almost impossible to import some equipment from abroad (OECD (2011)).

Moreover, the armed conflict aspect with Israel is another key factor that affects the development and implementation of e-government in Palestine. As sometimes the infrastructure had been affected or damaged due to the armed conflict and in some cases some of the ministries had to be relocated (OECD (2011)).

With announce of the X-Road Center by the minister of MTIT. It is clear that PA has overcome some of those issues, but still there are a number of issues to be overcome in the future for achieving the goals that PA set in order to have a fully implemented e-government in Palestine.

2.5 Cyber security, data protection, and privacy

With the review of most of the reports which are about analyzing the e-government in Palestine, in addition to the e-governance strategic plan. Plus the previously mentioned issues related to legal framework in Palestine regarding the implementation of e-government. It is clear that there is no clear mention for a framework that handles the cyber security, data protection, and privacy in details.

The above mentioned aspects are a key factor for e-government. As the government will eventually moves its activities and services to the cyber world, it should guarantee that everything will function in a proper way or at least deliver some main and vital services in the case of cyberattacks.

Also data protection would be related directly to the case of providing e-services and the fact that data would be in electronic form, there should be means to protect citizen's and business's data. Plus what are the means to keep and preserve the data from lose or damage.

Lastly the private data that will be preserved by the government, there should be roles about how to handle this data, classification of the data, determine who has the right to check this data and under what circumstances. Plus in the case of the shared data sources between different governmental bodies, what data should be shared or accessed from the different parts other than the owner of the data.

Regarding the current state of the Palestinian legal framework as mentioned before that it lacks some of the basic laws which needed to exist in order to have a proper functioning e-government.

It is clear from the previously mentioned analysis, there still some work for developing and adopting new laws and acts that would be suitable solution or implementation for the lacked acts.

There have been a number of initiatives to overcome this lacking of acts, such as the "memorandum on a proposal for a draft law on Access to Information of Palestine" by (ARTICLE 19 (2005)).

Also there is an ongoing process to approve an under reviewing draft for "e-Transaction law" (MTIT, (2010)). The process for approving and activating new law is a time consuming process, because the fact that the Palestinian Legislative Council (PLC) is not functioning, so the Palestinian president should approve the new laws according to the Article 43 of the Palestinian Basic Law (palestinianbasiclaw.org (2007)).

It is obvious that PA is aware of the lack of some key legislations and acts that would facilitate the work of e-government if exist. PA is working to adopt such legislations and acts although the process is time consuming. For this reason the PA should be more active with adopting new legislations at almost the same time, not whenever there is a need for such legislations.

2.6 The need for Information Security Management System

As mentioned previously there is no clear mention for any specific framework to handle the cyber security aspect, although the topic of cyber security and information security is covered in the e-government strategic plan.

Moreover in other reports and studies, this aspect was handled in a general way with less detail. Mostly the cyber security issues were seen to be solved or avoided by using some basic methods or technology without stating how it should be used or how to be implemented and integrated to the e-government framework or infrastructure.

Such solutions mentioned in the e-Transaction Law[1] would be:

- Using Public Key Encryption.
- Using Firewalls.
- Using Antiviruses.
- Backups.
- Some services to prevent DoS Attacks.

Although the e-government strategic plan share some of the above mentioned methods, it has also some more technical and detailed techniques and methods regarding the security of information, systems, data centers, and the network.

Some of those methods would be[2]:

- For the Data Center:
  - Load balancing and Content Caching.
  - Quality of Service (QoS).

[1] As the law has no English translation yet, the methods were translated by the author.

[2] For full list of methods and specification review the Technical Discussion in the e-government strategic plan.

    - Provide application and middleware level message forwarding.
    - Security:
        - Virtual Firewall Service.
        - Intrusion Detection / Preventions Services.
- For the network (Wireless Edge Network which is suggested be used by end users) :
    - Radio/Access Point (AP) Authentication.
    - An open and standards based connectivity protocol.
    - Provide AES & TKIP encryption/de-encryption.

As can be seen there is no integration between the different security methods and how to manage them all together as a security framework even though some of those methods were stated with some details regarding its use.

During a meeting with Mr. Tarmo Oja (2015), an expert in cybersecurity from Estonia who is working on the Estonian Palestinian cooperation project (he was in Palestine several times with a duty to deal with the security aspect).

Mr. Oja provided an overview of the most common and main issues regarding the implementation of the e-government in Palestine.

The X-Road center and the connected ministries are all connected through the governmental network which is a private network that connects different ministries municipalities together (Oja, (2015)).

According to (Oja, (2015)) some of the issues are:

- The infrastructure of the network and internal networks within the ministries needs maintenance.
- There should be a unified structure for each internal network within the ministries (each ministry build the internal network in different way).
- Lack of monitoring.
- Some sub-networks are connected to the governmental network that should be connected.

It is clear that a proper planning for cybersecurity and related issues do not exist. In addition some issues regarding the implementation and the infrastructure are already exists.

With the proper planning most of those issues would be eliminated and would results in robust implementation for e-government.

This thesis will analyze some of the already existed frameworks, solutions, and ISMSs. The final result would be the best and most suitable solution for the Palestinian e-government which would mitigate some of the currently existed issues and would be suitable to mitigate / prevent other security issues/threats in the future.

3. Selection of ISMSs

3.1 Introduction

Information security management systems are crucial component for maintaining the information security for e-government. It can provide a well-documented and explained guidance for some topics related to information security. Those topics mainly handle the processes of managing information security including planning, implementation, and auditing information security practices.

In addition ISMS aims to achieve the right balance for the CIA security model (Confidentiality, Integrity, and Availability); CIA trilogy is the core goals of security.

In this chapter a collection of security frameworks and ISMSs will be viewed in some details. Those frameworks are the most widely used for information security in different areas starting with organizations and enterprises up to governmental level. In addition the list of frameworks will be used to conduct the comparison for choosing the suitable ISMS to be applied for the Palestinian e-government.

3.2 ISO/IEC 27000 series

The ISO/IEC 27000 series is considered as the most widely used and adopted ISMS. ISO 27000 series was a result of a joint work of both ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) with the final result of a combined information security standard by both organizations (Greene, (2014)).

The ISO 2700 family in general consists of approximately twenty standards (plus some others are under development). Those standards try to characterize and modularize the main substantial components for ISMS (Harris and Kumar, (2013)). So those standards would highlights what are the main requirements and/or components for implementing ISMS within an organization.

The ISO 27000 series is following the PDCA cycle (Plan – Do – Check – Act) to ensure that the implementation of the ISMS is in a proper way. Figure 1 shows how the PDCA cycle is applied to ISO/IEC 27000.

As for the **Plan** part it deals with planning and setting goals and objectives. While the **Do** part is dealing with the implementation of the plans. The **Check** part is handling the measurement of the results of the implementation to insure that the main goals and objectives were fulfilled. The last component of the cycle which is **Act** is dealing with providing directions and instructions on how to improves and adjust the plans to achieve the goals (Harris and Kumar, (2013)).

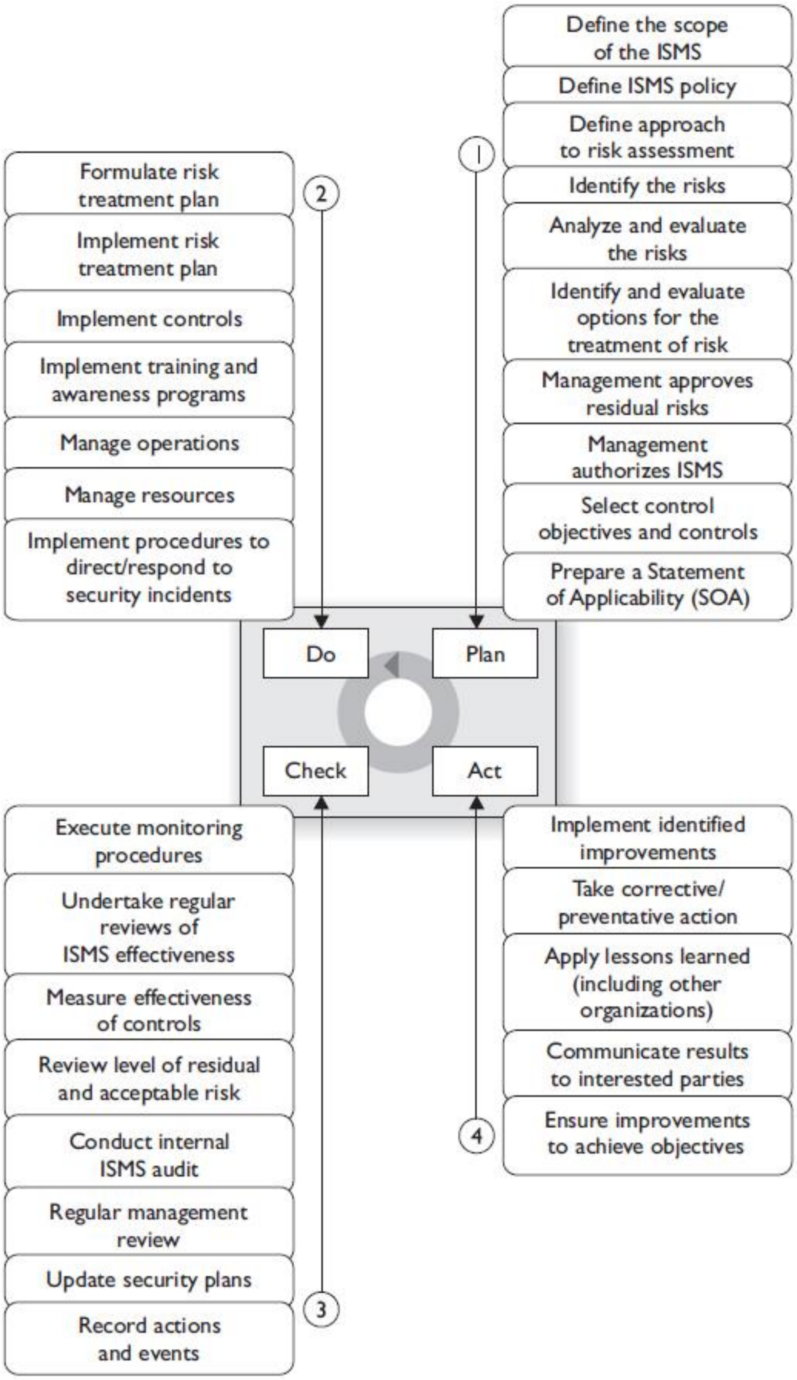

Define the scope of the ISMS
Define ISMS policy
Define approach to risk assessment
Identify the risks
Analyze and evaluate the risks
Identify and evaluate options for the treatment of risk
Management approves residual risks
Management authorizes ISMS
Select control objectives and controls
Prepare a Statement of Applicability (SOA)
1
2
Formulate risk treatment plan
Implement risk treatment plan
Implement controls
Implement training and awareness programs
Manage operations
Manage resources
Implement procedures to direct/respond to security incidents
Do
Plan
Check
Act
Execute monitoring procedures
Undertake regular reviews of ISMS effectiveness
Measure effectiveness of controls
Review level of residual and acceptable risk
Conduct internal ISMS audit
Regular management review
Update security plans
Record actions and events
3
Implement identified improvements
Take corrective/ preventative action
Apply lessons learned (including other organizations)
Communicate results to interested parties
Ensure improvements to achieve objectives
4

Figure 1 PDCA Cycle in ISO/IEC 27000 (Harris and Kumar, (2013))

As mentioned before the ISO 27000 series consist of approximately twenty standards, those standards provide detailed information about the requirements for ISMS implementation. The most important standards to be considered when starting to implement the ISMS are the first six standards/ documents (Greene, (2014)).

Those documents provide recommendations that help to go through the 4 components of the PDCA cycle to implement the ISMS. In the following parts those documents will be discussed with some details about each. Before start reviewing those six documents, a quick review of the first document of the series which is the ISO 27000 will be next step.

3.2.1 ISO/IEC 27000

The main title for this document is “ISMS Overview and Vocabulary”, as can be seen this document provides an overview about ISMS and a list of ISMS family of standards (ISO/IEC 27000, (2014)).

In addition it provides some vocabularies and terms will be used for the review of different standards and used in others standards of ISO/IEC 27000 series. It is clearly stated in other standards/documents that ISO/IEC 27000 is the reference for terms and definitions.

3.2.2 ISO/IEC 27001

The first document of the standard family titled as “ISMS Requirements”. This document is talking about the requirements for set up, maintain, and constantly enhance the ISMS. It also helps to assess organization’s ability to meet their information security requirements.

ISO/IEC 27001 document explain in details the requirements for ISMS implementation and insuring ISMS continuity. In order to understand those requirements a quick overview will be provided next (ISO/IEC 27001, (2013)).

3.2.2.1 Context of the Organization

General understanding of the organization and its context, and what are the needs and expectations of stakeholders in addition to the scope of the ISMS.

This includes stakeholder identification, understanding of issues which would affect achieving ISMS’s goal and defining ISMS’s scope (ISO/IEC 27001, (2013)).

3.2.2.2 Leadership

This is to consider the responsibilities and authorities of the management towards the ISMS.

This includes commitment of the management to the ISMS. And ensure that information security policy and objectives are compatible with the organization’s strategic plans, and availability of ISMS’s resources (ISO/IEC 27001, (2013)).

Moreover the management should insure that the ISMS meet the planned goals also support continuity and constant improvements of the ISMS.

3.2.2.3 Planning

Provide some guidelines for defining risks, information security objectives and how to fulfill those goals.

Organization should have proper risk assessment where risks and the actions to mitigate those risks are identified, and also evaluation for effectiveness of those actions (ISO/IEC 27001, (2013)).

As for the risk assessment, the whole process is "aligns with the principles and generic guidelines provided in ISO 31000" (ISO/IEC 27001, (2013)).

3.2.2.4 Support

It handles how to support the ISMS within the organization including:

- Personnel competence: at what level it would affect the performance of information security (ISO/IEC 27001, (2013)).
- Personnel awareness: information security policies (ISO/IEC 27001, (2013)).
- Communication: the need of consistence internal and external communication (ISO/IEC 27001, (2013)).

Documentation: appropriate identification and description, format, review and approval of information required for ISMS effectiveness (ISO/IEC 27001, (2013)).

3.2.2.5 Operation

Ensuring that requirements are implemented and each should produce documented information about the results of implementation.

3.2.2.6 Performance evaluation

Evaluate ISMS performance to insure that it has met the intended goals, and it continues to function in proper way. This can be done through monitoring and evaluation, internal audit, and management review of ISMS's performance (ISO/IEC 27001, (2013)).

3.2.2.7 Improvement

Dealing with nonconformities and how to handle it when occurred to make sure it would not recur again.

3.2.3 ISO/IEC 27002

Second document of ISO/IEC 27000 series; Titled as “Code of practice for information security controls”. It can be used as reference for selecting controls for ISMS implementation based on ISO/IEC 27001, while taking into consideration information security risks. In addition to controls selection this document help organizations to develop their own controls and guidelines.

The document contains fourteen security control clauses which divided into categories which contain the security controls that will be generalized and reviewed next.

3.2.3.1 Information security policies

This section is about information security polices management. It discusses defining and approving a set of information security polices, and reviewing those polices based on planned intervals (ISO/IEC 27002, (2013)).

It handles the information security policies in two levels. The highest level which is related to organization’s management states the main characteristics of the policy which are mainly handling requirements for different aspects such as business strategy, regulations and legislations, and information security threats.

The second level is the lower level which is related to employees and topic-specific policies. The main goal is to help implementing security controls such as access control, information classification, and physical security. Beside other controls regarding securing work stations and insuring that the work flow won’t be a source of security vulnerability.

3.2.3.2 Organization of information security

This handles the organization of information security regarding internal organization and mobile devices and teleworking.

As for the internal organization it is about setting up a framework for starting and running information security within the organization. This includes defining and allocating information security responsibilities, segregation of duties, contacting with authorities, and information security in project management (ISO/IEC 27002, (2013)).

It is possible to appoint information security manager to handle the overall responsibility for information security and support to identify controls. In addition the organization should maintain a proper contact with relevant authorities and with some special groups such as professional associations or specialized security forums

While mobile devices and teleworking is about mobile devices, which handles managing risks opposes from mobile devices usage. This includes the use of private mobile devices for work, and wireless devices.

And for teleworking, which handles the protecting information accessed, processed, or stored at teleworking sites (ISO/IEC 27002, (2013)).

Additionally the organization should take care of remote access to organization’s information systems, network security, and malware protection and firewall requirements.

3.2.3.3 Human resource security

As for this part, it mainly deals with employment aspects (prior employment, during the employment and the cases of termination and change of employment). The prior employment goal is to ensure that employees and contractors are suitable for their roles.

This includes background verification and checking for candidate employees, ensuring the acquisition of required skills for candidate employees, awareness of security responsibilities, and definition of valid duties after employment termination (ISO/IEC 27002, (2013)).

For during the employment part, the goal is to insure that employees and contractors are aware of their security responsibilities. This includes ensuring that employees and contractors apply information security policies and procedures. Plus awareness, educating, and updating employees and contractors regarding the organization’s security policies and procedures that are relevant to their duties (ISO/IEC 27002, (2013)).

And finally, the organization should have disciplinary process that shows what actions to be taken for employees who committed security breach.

Last part is about termination and change of employment. The goal is to protect the organization’s interests in the cases of changing or termination of employment responsibilities. This can be achieved through defining the responsibilities and duties that remain valid after termination or change of employment including ongoing information security requirements and legal responsibilities (ISO/IEC 27002, (2013)).

3.2.3.4 Asset management

Aim to identify organization’s assets and appropriate protection for those assets, through responsibility for assets, information classification, and media handling.

For responsibility for assets the organization should identify assets of information and information processing, assets ownership, acceptable use of assets, and return of assets (in the case of contract termination) (ISO/IEC 27002, (2013)).

This can be achieved by drawing up inventory for identified assets of information and information processing, and identifying rules for acceptable use of information and assets.

As for information classification, it aims to ensure that information would be protected with a proper level according to its importance to the organization (ISO/IEC 27002, (2013)).

Organization should ensure that information should be classified based on several aspects including legal requirements, value and sensitivity to unauthorized modification, and group assets and information with similar security requirements. Plus ensure that suitable procedures for labeling information should be implemented in accordance with the classification scheme (ISO/IEC 27002, (2013)).

Media handling is to ensure protection for information stored on media, through management of removable media, media disposal, and physical media transfer (ISO/IEC 27002, (2013)).

To ensure this, the organization should implement procedures for managing removable media regarding the classification scheme, and using formal procedures for securely dispose of media when it is no longer needed. In addition media should be protected during transportation.

3.2.3.5 Access control

To ensure the security of information processing facilities and systems by preventing unauthorized access (ISO/IEC 27002, (2013)). This can be achieved through a group of controls which are:

- Business requirements of access control: which include access control policy, and access to networks and network services.

  Organization should ensure that establishing, documenting, and reviewing access control policy should be on the bases of information security requirements.

  Also only access to specifically authorized network and services to be used should be granted to users (ISO/IEC 27002, (2013)).
- User access management: including user registration and de-registration, user access provisioning, management of privileged access rights, management of secret authentication

information of users, review of user access rights, removal or adjustment of access rights (ISO/IEC 27002, (2013)).

The organization should ensure implementation of formal process to handle user registration and deregistration which enables access rights assessment. Plus the organization should use formal authorization process to manage privileged access rights (ISO/IEC 27002, (2013)).

- User responsibilities through the use of secret authentication information.
- System and application access control: through information access restriction, secure log-on procedures, password management system, is use of privileged utility programs, and access control to program source code (ISO/IEC 27002, (2013)).

  Moreover access to information and systems should be based on access control policy and controlled by using secure log-on procedures.

3.2.3.6 Cryptography

This states that using a proper and effective cryptography to ensure protection of CIA model. This can be achieved with policy on the use of cryptographic controls taking into consideration regulations and restrictions for using cryptographic techniques.

In addition to the policy on using of cryptographic controls, a policy for key management should be considered which should handle the use, protection, and lifetime of cryptographic keys (ISO/IEC 27002, (2013)).

It should be brings to attention that ISO/IEC 11770 should be considered for further information about key management.

3.2.3.7 Physical and environmental security

Handle the physical security of assets and information processing facilities with two approaches.

First approach is **secure areas,** which is about physical security of sensitive information and information processing facilities. Including physical security perimeter, physical entry controls, securing offices, rooms and facilities, and protecting against external and environmental threats (ISO/IEC 27002, (2013)).

More practically, areas with sensitive information and information processing facilities should be protected by predefined security perimeters. And secure area should be protected by entry control to ensure only authorized persons can access (ISO/IEC 27002, (2013)).

Moreover the organization should seek expert's advice for protection against accidents such as fire, flood, and earthquakes.

Second approach is **equipment**, which handle the protection of assets. This include equipment siting and protection, removal of assets, security of equipment and assets off-premises, secure disposal or re-use of equipment, unattended user equipment, and clear desk and clear screen policy (ISO/IEC 27002, (2013)).

This includes equipment should be protected to reduce environmental threats, and ensure protection of equipment from power failure and other disruptions from supporting utilities.

Additionally equipment should be maintained properly to ensure its availability and integrity, and information, software, and equipment should not be removed without proper authorization (ISO/IEC 27002, (2013)).

For disposable or re-use of equipment, the organization should ensures that any sensitive data and licensed software being removed or overwritten before the disposal of items and equipment with storage media (ISO/IEC 27002, (2013)).

Finally users should ensure protection of unattended equipment.

3.2.3.8 Operations security

Ensure security and protection of information and information processing facilities (27002, (2013)), which include:

- Operational procedures and responsibilities including documented operating procedures, change management, capacity management, and separation of development).

  With more details about this section, changes to the organization, business processing, and systems should be controlled, and resource monitoring to ensure that future capacity requirement will meet desired system performance (ISO/IEC 27002, (2013)).
- Protection from malware.

  To ensure this, protection against malware, detection, prevention, and recovery controls should be implemented (ISO/IEC 27002, (2013)).
- Backup (Information backup).

  Policy should be implemented to handle regular backup and testing of backup for information, software, and systems (ISO/IEC 27002, (2013)).

- Logging and monitoring which include event logging, protection of log information, administrator and operator logs, and clock synchronization.

  This can be done by ensure keeping, producing, and regular reviewing of event log which includes recorded user activities, faults, and security events, and protecting log information and logging facilities from modifications and unauthorized access (ISO/IEC 27002, (2013)).
- Control of operational software (installation of software on operational systems).

  The organization should implement procedures to control installation on operational systems.
- Technical vulnerability management including management of technical vulnerabilities, restrictions on software installation.

  To manage technical vulnerability, information of technical vulnerabilities of information systems should be gained and appropriate measures to address risks related to the exposure to such vulnerabilities should be taken. Additionally the organization should implement rules for controlling installation of software by users (ISO/IEC 27002, (2013)).
- Information system audit consideration.

  In order to minimize interruption to business processes, audit requirements and activities should be planned carefully (ISO/IEC 27002, (2013)).

3.2.3.9 Communications security

Ensure the security of the organization’s network facilities and the information being transmitted through the network within the organization or with external parties.

This control handles network security management which includes network controls, security of network services, and segregation in networks. And information transfer, taking into consideration information transfer policies and procedures, agreements on information transfer, electronic messaging, and confidentiality or non-disclosure agreements (ISO/IEC 27002, (2013)).

For the security of the network services, network service agreement should include security mechanisms and service levels for all network services, in addition to specify whether the services provided in house or outsourced (ISO/IEC 27002, (2013)).

And for the segregation in networks, groups of services, systems, and users should be segregated on networks.

For information transfer, procedures, controls, and policies for formal transfer should be implemented within the organization to ensure the security of transferred information through all types of communication. Moreover secure transfer of business information with external parties should be handled by agreements (ISO/IEC 27002, (2013)).

3.2.3.10 System acquisition, development and maintenance

To ensure that information security is part of the systems during the whole lifecycle of the systems. And it has been implemented during the system development. Additionally to ensure the protection of the data that had been used for testing (ISO/IEC 27002, (2013)). The control consists of three parts which are:

- Security requirements of information systems including information security requirements analysis and specification, securing application services on public networks, and protecting application services transactions.
- Security in development and support processes which includes secure development policy, system change control procedures, technical review of applications after operating platform changes, restrictions on changes to software packages, secure system engineering principles, secure development environment, outsourced development, system security testing, and system acceptance testing.
- Test data, which ensure the protection of data used for testing.

3.2.3.11 Supplier relationships

This section is divided into two; the first part is information security in supplier relationships and consists of three controls.

The first control is information security policy for supplier relationships and it states that the organization should agree with the suppliers who have access to assets within the organization, both should agree on security requirements to avoid risks based on this access (ISO/IEC 27002, (2013)).

The control goal is to ensure that the organization had identified information security procedures and processes to be implemented by the organization and by those which are required for the suppliers to implement in order to connect to the organization’s information, and systems (ISO/IEC 27002, (2013)).

A group of procedures and processes are stated by the control an example of those procedures would be: categorizing the suppliers who would be allowed to access information, monitoring and controlling the access of the supplier and define the type of information based on the suppliers categories, managing suppliers relationship based on standardized process, and when to state information security requirements to be stated in agreement signed by the suppliers and the organization (ISO/IEC 27002, (2013)).

Next control for this part is addressing security within supplier agreements; the control states that proper information security requirements should be established and agreed with suppliers who will engage with IT infrastructure of the organization (ISO/IEC 27002, (2013)).

This means that the organization should establish supplier agreement to ensure there is no misunderstanding about both sides obligation to accomplish information security requirements.

The control states a group of statements that should be considered to be stated in the agreement, some of those statements are classification of information regarding the organization classification scheme, legal requirements and regulations, guidelines for acceptable use of information, and the organization right to audit supplier's controls regarding the agreement (ISO/IEC 27002, (2013)).

Last control for this part would be information and communication technology supply chain; this control states that requirements for identifying information security risks regarding ICT products supply chain should be agreed with suppliers (ISO/IEC 27002, (2013)).

The agreement should include some topics, a part of those topics would be: monitoring and validating delivered ICT products and services are comply with security requirements, assuring that critical components can be traced through the supply chain, and defining rules for information sharing regarding supply chain (ISO/IEC 27002, (2013)).

The second part in this section is supplier service delivery management; consisting of two controls to ensure agreed security and service delivery in line with supplier agreement.

The first control is monitoring and review of supplier services; the control states that the organization should monitor, review, and audit service delivery by supplier in a regular base, this ensures that the security terms and conditions of the agreement have been followed by the supplier, and to ensure proper management for security issues (ISO/IEC 27002, (2013)).

A service management relationship can be involved in this situation, and this relationship is to verify some aspects, some of those aspects are: monitoring of the service performance to ensure its constancy with the agreement, auditing suppliers and compare the results with reports from independent auditors and discuss identified problems, and resolve identified problems.

The last control for this part and the whole section is managing changes to supplier services; the control goal is to ensure that changes to the delivery of services by suppliers should be managed taking into consideration the critical nature of business information involved in the risks reassessment (ISO/IEC 27002, (2013)).

The control states three main aspects and some detailed information for some of those aspects to be taken into consideration, those aspects mainly handles the changes of the supplier agreement, some changes by the organization, and implementation for changes in supplier services (ISO/IEC 27002, (2013)).

3.2.3.12 Information security incident management

This section consists of a group of controls; all of the controls are under the management of information security incidents and improvements, with the goal of ensuring an effective information security incidents management (ISO/IEC 27002, (2013)).

The first control within this section is responsibilities and procedures; this control states that the organization should form procedures and responsibilities for the management to ensure quick and effective response to information security incidence.

Considering a group of aspects regarding establishing, reporting the procedures and responsibilities, and what the procedures should ensure, some of those aspects are: planning for incident response, logging incident management activities, competent staff to handle security issues, procedures to be triggered in case of security event, and feedback of results to personnel who reported security issues after dealing with the issue (ISO/IEC 27002, (2013)).

In addition this control states that ISO/IEC 27035 contains more detailed information about information security incident management.

Next control is reporting information security events; aiming to ensure quick and appropriate reporting of information security event, the control states a group of situations which require a quick reporting, a part of those situations is: access violation, human errors, breach of physical security, and violation to the CIA of information (ISO/IEC 27002, (2013)).

The following control is reporting information security weaknesses; the control states that all users of the organization’s information systems and services are required to report any security weaknesses.

The goal of the control is to ensure an easy, and quick reporting of information security weaknesses through a point of contact to avoid security incidents (ISO/IEC 27002, (2013)).

The next control is assessment of and decision on information security events; the control states that security events should be assessed to check if they can be classified as incidents.

The assessment should be done by the point of contact and based on agreed incident classification; the classification can help to identify the impact of the incident. In some cases the assessment can be assigned to information security incident response team in case that the organization already has such team (ISO/IEC 27002, (2013)).

Next control is response to information security incidents; the control states that the response to information security incidents should be according to the documented procedures previously mentioned.

The control states a group of action that should be included in the response; some of those actions are: start information security forensics analysis, proper logging of response activities to be analyzed later, and post incident analyses should be implemented to identify the source of the incident (ISO/IEC 27002, (2013)).

Next control is learning from information security incidents; the control states that the knowledge gained form resolving security incidents should be analyzed to reduce the likelihood of future incidents. The aim of the control is to ensure that there are mechanisms to quantify and monitor type, volume, and costs of security incidents and the results should be used to identify high impact incidents (ISO/IEC 27002, (2013)).

The last control for this section is collection of evidence; the control states that the organization should apply procedures for collect and preserve information that can be used as evidence.

The control states some cases to be taken into account by the procedures, a part of those cases is: evidence safety, documentation, and briefing. The control also refers to ISO/IEC 27037 for more information regarding handling digital evidence (ISO/IEC 27002, (2013)).

3.2.3.13 Information security aspects of business continuity management

This section is divided into two parts; the first part is information security continuity consisting of three controls goal is to ensure that the information security continuity is embedded to the business continuity system for the organization (ISO/IEC 27002, (2013)).

The first control within this part is planning information security continuity; the control is to ensure that the organization determined its information security requirements and continuity in adverse situations.

The organization should plan for information security continuity during crisis, and to decide if the continuity is fulfilled during the business continuity process or during the recovery from disasters (ISO/IEC 27002, (2013)).

This control also relates to other standards by ISO to handle business continuity management, those standards are: ISO/IEC 27031, ISO 22313, and ISO 22301.

Next control for this part is implementing information security continuity; this control states that the organization should ensure the level of information security continuity in the cases of adverse situation.

The control also ensure that the organization have a proper planning and management for information security continuity by planning for incidents response by nominating employees and staff with proper experience to ensure information security continuity during disasters (ISO/IEC 27002, (2013)).

The organization should also plan for procedures to respond and recover from disruptive events ensuring the functioning of information security to a predefined level by the management.

Last control for this part is verify, review and evaluate information security continuity; this control states that in order to make sure that the controls for information security continuity are valid for adverse situations, those controls should be regularly reviewed and verified (ISO/IEC 27002, (2013)).

The organization should test and verify the functionality, knowledge, and effectiveness of information security continuity procedures to ensure its consistency with continuity objectives and to ensure its validity during disasters (ISO/IEC 27002, (2013)).

The other part of this section is redundancies; this part has only one control which is availability of information processing facilities which is also the main goal of this part.

The control is to ensure that information processing facilities are implemented with sufficient redundancy to ensure availability requirements (ISO/IEC 27002, (2013)).

The organization should ensure the availability of information system by identifying business requirements or by using redundant components (ISO/IEC 27002, (2013)).

One note to be taken into consideration when planning for using redundant components which is that using redundant components can integrity and confidentiality of information systems.

3.2.3.14 Compliance

This is the last section of this standard; consisting of two main parts, the goal of this section is to ensure that information security is implemented according to the policies and procedures, and also to avoid breaches of legal obligations regarding information security and its requirements (ISO/IEC 27002, (2013)).

Starting with the first part of this section which is compliance with legal and contractual requirements, this part consists of five controls; first control is Identification of applicable legislation and contractual requirements.

The goal of this control is to ensure that all relevant legislative and contractual requirements and how the organization will meet those requirements should be explicitly identified and kept up to date for each information system (ISO/IEC 27002, (2013)).

Also the control ensures that if the organization is working with other countries, the manager should ensure compliance with different legislations in different countries.

Next control is intellectual property rights; the control states that procedures should be implemented to ensure compliance with legislatives requirements for intellectual property and the use of proprietary software (ISO/IEC 27002, (2013)).

The control stated a group of guidelines to be considered for intellectual property, some of those guidelines are: using software only through known sources, saving proof of ownership of licenses, and provide policy for software disposal (ISO/IEC 27002, (2013)).

Moving to the next control within this part which is protection of records; aiming to protect records, the control states a couple of protection aspects for controls and it should be in accordance with legislation and business requirements.

For the purpose of protecting records, organization should consider classifying the records based on the classification scheme within the organization. Also the organization should consider categorizing the records considering retention period, storage media, and encryption keys which enable decrypting the records when needed (ISO/IEC 27002, (2013)).

The control also point to the cases of possibility of storage media malfunction, and states that storage and handling the records should be done in accordance to manufacturer's recommendations, and for the cases of electronic media (ISO/IEC 27002, (2013)).

The control states that the organization should ensure the accessibility of the records stored on electronic media, and protect it from future changes in technology (ISO/IEC 27002, (2013)).

Also the system draws attention to the case of using data storage systems, using such systems should ensure the identification and retention period of the records taken into consideration national or regional legislations.

In addition the control states that such systems should consider the process of destroying the records if no longer needed by the organization (ISO/IEC 27002, (2013)).

The control also refers to ISO 15489-1 for additional information about managing organizational records.

Next control would be privacy and protection of personally identifiable information, according the control this should be ensured as required in related legislations and regulations.

To ensure the privacy and protection of personally identifiable information the control suggests that the organization should implement a policy for such purpose, and it goes further suggesting that for the best benefit organizations usually appoint privacy officer or any employee (ISO/IEC 27002, (2013)).

The main duty of privacy officer is to educate managers and employees how to handle such data, and to ensure that employees and managers are following the policy and related regulation and legislations (ISO/IEC 27002, (2013)).

Also the control relates to ISO/IEC 29100 for high level framework for the protection of personally identifiable information in ICT systems.

Last control within this part is regulation of cryptographic controls; stating that security control should be done in a way consenting to relevant regulations and agreements.

The control states some items to be considered such as: restrictions on computer hardware that can perform encryption or encryption functionality can be added to it, restriction on using encryption, and restrictions on authority's access to confidential content (ISO/IEC 27002, (2013)).

Moving to the other part of this section which is information security reviews; consisting of three controls this part is aiming to ensure that implementation of information security is in accordance with organization's policies and procedures (ISO/IEC 27002, (2013)).

First control is independent review of information security; stating that independent review for information security management and implementation should be carried out based on planned intervals or in the cases of serious changes.

Among the goals of the review is to assess the possibilities of improving and changes to security approach, also in the cases of inappropriate implementation of information security the management should consider some corrective actions (ISO/IEC 27002, (2013)).

The control refers to ISO/IEC 27007 for detailed information about ISMS auditing and ISO/IEC TR 27008 for auditors on information security controls.

Next control is compliance with security policies and standards; the control states that managers should review compliance of information processing with appropriate security requirements.

The managers should ensure the mechanism and reporting of the review, also in the cases of non-compliance managers should consider some actions including: identifying the causes, evaluate actions to achieve compliance, corrective actions implementation, and reviewing the corrective actions (ISO/IEC 27002, (2013)).

The last control for this part and the whole document is technical compliance review; this control is for ensuring that a regular review should be done for information system to check its compliance with security policies within the organization (ISO/IEC 27002, (2013)).

The review should be carried out by authorized person under supervision, in addition in the cases of using penetration testing the organization should be caution as such kind of assessment tools can lead to security compromises also it should be planned and documented (ISO/IEC 27002, (2013)).

The control also refers to ISO/IEC TR 27008 for additional information on technical compliance reviews.

Finally it should be mentioned that ISO/IEC 27002 refers to a group of other ISO standards, those are (ISO/IEC 11770, ISO/IEC 27005, ISO/IEC 27007, ISO/IEC TR 27008, ISO/IEC 27031, ISO/IEC 27033, ISO/IEC 27035, ISO/IEC 27036, ISO/IEC 27037, ISO/IEC 29100, ISO 31000, ISO 22313, ISO 22301, and ISO 15489-1).

3.2.4 ISO/IEC 27005

This is concerned with risk management, titled as "Information Technology - Security Techniques - Information Security Risk Management". Generally it does not provide any particular methodology for information security risk management, but leave this for the organization to specify which methodology to use (ISO/IEC 27005, (2011)).

It also refers to ISO 31000 for high level view and detailed information about risk management process.

The standard views information security risk management as an iterative process; for each iteration this can increase depth and details of the assessment. And can balance between time and effort minimization, and appropriate assessment of high risks (ISO/IEC 27005, (2011)).

The activities of information security risk management process are:

3.2.4.1 Context establishment

Providing all information about the organization, that relates to information security risk management context establishment. This action can provide basic criteria specification, scope and boundaries, and organization of risk management process.

Context establishment also provide detailed information about the basic criteria. It provides four criteria which are: risk management approach, risk evaluation criteria, impact criteria, and risk acceptance criteria. In addition it provides detailed information about both scope and boundaries, and organization of risk management process.

3.2.4.2 Risk assessment

Consisting of risk identification, risk analyses, and risk evaluation. It provides prioritized assessed risks list based on evaluation criteria. More over processes of risk assessment are discussed in details as the following:

- Risk identification

Consists of a group of activities which are: (identification of assets, identification of threats, identification of existing controls, identification of vulnerabilities, and identification of consequences)

- Risk analyses

  Also consists of a group of activities which are: (assessment of consequences, assessment of incident likelihood, and level of risk determination).

- Risk evaluation

  Compare risk's level against risk acceptance and evaluation criteria, to produce prioritized risks list, based on evaluation criteria.

3.2.4.3 Risk treatment

This process provides risk treatment plan and residual risks which got decision of acceptance from the manager of the organization.

It also provides some details about the sub activities of this process, those sub activities are:

- **Risk modification**

  This action enables selecting justified and suitable controls to meet requirements from risk assessment and treatment. Moreover it provides some constraints that should be taken into consideration such as time, technical, operational, and environmental constraints.

- **Risk retention**

  It enables making decision of retaining risk without further action should be based on risk evaluation. If risk's level met risk acceptance criteria, no need for additional controls implementation.

- **Risk avoidance**

  To avoid conditions or activities that rise particular risk. Avoidance decision can be made in the case of highly cost implementation of risk treatment option.

- **Risk sharing**

  Share risks with other party that can manage risk most effectively based on risk evaluation. When sharing risk it should be taken into accounts that it is possible to share risk management responsibility, but sharing liability of an impact is not normally possible.

3.2.4.4 Risk acceptance

This action produces list of accepted risks including justification for risks that do not meet normal risk acceptance criteria. Assessed risks in the risk treatment plan should be described how to meet risk acceptance criteria

3.2.4.5 Risk communication and consultation

It provides continues understanding of the results and process of information security risk management for the organization. The stakeholders may judge risk acceptance based on their perception, in order to provide stake holders with appropriate information about risks it should develop risk communication plan that ensure effective communication and provide clear information about risks to support choosing suitable decisions.

3.2.4.6 Risk monitoring and review

Provide continuous adjustment of risks management, business objectives, and risk acceptance criteria. And continuously relate risk management process to business objectives, or updating the process.

Consistent monitoring is required for detection of changes in threats, likelihood, and consequences. This can be supported with external services which provide information about new threats and vulnerabilities.

In addition continuous monitoring and review is important to ensure that management plans, and risk assessment and treatment all are remain relevant to the situation.

PDCA cycle of implementation for ISO/IEC 27000 series can be mapped with the risk management activities as can be seen in the following table (ISO/IEC 27005, (2011)):

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

Table 1 Maping Risk Management activities in ISO/IEC 27005 to PDCA

3.2.5 ISO/IEC 27006

This standard was established to provides "for bodies providing audit and certification of information security management systems" which is also the title for this standard.

This standard mainly provide some additional information regarding auditing information security, as ISO/IEC 17021 provides information for auditing, the ISO/IEC 27006 uses the same information in ISO/IEC 17021 but with additional information to make it suitable for information security auditing (ISO/IEC 27006, (2007)).

The document also refers to ISO 9000 for the definition of "management system" which is used in the document. In addition the document also refers to ISO/IEC 19011, and ISO/IEC 27001.

After the introduction and some definitions the document started with principles and states that it is the same as in ISO/IEC 17021.

Then the document moves to the next section which is "management of impartiality" this section also uses the same requirements as in ISO/IEC 17021, with an addition to some requirements and guidance related to ISMS (ISO/IEC 27006, (2007)).

This section is about "conflict of interest" the requirements and guidance the document added can be done by the certification bodies without causing any possible conflict of interest (ISO/IEC 27006, (2007)).

Some of those requirements are: participating in training related to information security management or auditing (in this case certification bodies should provide general information that is publicly available and avoid providing information or examples related to the organization, publishing or providing on request information about how certification body explain certification requirements and auditing standards, and adding value within its visits for surveillance and certification audits) (ISO/IEC 27006, (2007))..

The next section is “structural requirements” this section has no additional information all information and requirements are applied form ISO/IEC 17021.

Then the document continue with the next section which is “resource requirements” this section consists of five parts, the first part is “competence of management and personnel” this part refers to the same part in ISO/IEC 17021, plus it adds some requirements and guidance related to ISMS (ISO/IEC 27006, (2007)).

Within this part it is mentioned that personnel with skills and common competence should be selected and managed to insure they are convenient to the activities and information security issues which will be audited.

The certification body shall prove conducting of competence analyses before contract review, then contract review can be done based on competence analyses (ISO/IEC 27006, (2007)).

The next part is “resources” which is aiming to ensure that the certification body’s management has required resources and processes to ensure competency of individual auditors to perform required tasks (ISO/IEC 27006, (2007)).

Then moving to the next part which is “personnel involved in the certification activities”, which is also applies the same requirements from ISO/IEC 17021 in addition to some extra requirements related to ISMS such as “competence of certification body personnel” to ensure that they have required skills to check the skills of ISMS auditors, lead ISMS auditors, and handle complaints process (ISO/IEC 27006, (2007)).

Also certification body shall have criteria for audit teams training which ensure some requirements including information security understanding, understanding of risk assessment and management, and understanding of audit’s principle based on ISO 19011 (ISO/IEC 27006, (2007)).

Then this part states a group of criteria for each auditor, a part of those criteria is: at least four year of full time practical experience in information technology (with at least two years of role regarding information security, successfully passed five days training regarding ISMS auditing, and continuously develop their skills and knowledge to be up to date (ISO/IEC 27006, (2007)).

Next part is "use of individual external auditors and external technical experts" which also applies the same requirements from ISO/IEC 17021 with additional requirements related to ISMS.

The requirements mainly to ensure that external auditors or external technical experts are qualified enough to be among the auditing team and that they do not have any direct involvement with the organization, moreover external expert shall be supervised by auditors (ISO/IEC 27006, (2007)).

The last two parts within this section are "personnel records" and "outsourcing", both implemented as shown in ISO/IEC 17021 (ISO/IEC 27006, (2007)).

Next section is "information requirements", and starting with "publicly accessible information" as the first part of this section, the additional information regarding ISMS is about certification management including granting, suspending, and withdrawing certification (ISO/IEC 27006, (2007)).

The organization should have documented information about ISMS which comply with ISO/IEC 27001, while the certification body should have documented information about initial certification audit, and surveillance audit for organization's ISMS complying with both ISO 19011 and ISO/IEC 17021 (ISO/IEC 27006, (2007)).

Next part is "certification documents" in addition to applying requirements from ISO/IEC 17021; some requirements regarding ISMS can be applied, and mainly those requirements to ensure that certification body should provide client organization with signed document of certification (ISO/IEC 27006, (2007)).

Next part is "directory of certified clients" which has no additional requirements other than the requirements from ISO/IEC 17021 (ISO/IEC 27006, (2007)).

Next part is "reference to certification and use of marks", it also applies the same requirements from ISO/IEC 17021 with additional requirements related to ISMS. Mainly those requirements are to ensure the organization control over the certification marks and that organization is using only the stated mark (ISO/IEC 27006, (2007)).

The next part is “confidentiality” it also states some requirements related to ISMS in addition to the requirement from ISO/IEC 17021.

Such requirements are to handle the access to confidential record, if the organization cannot grant access to records with confidential information, certification body should decide whether it is possible to audit ISMS without such documents or not, and in the case of impossibility to conduct the audit, certification body shall mention to the organization that audit cannot take a place without proper access to information (ISO/IEC 27006, (2007)).

The last part of this section is “information exchange between a certification body and its clients” this part has no additional requirements other than the requirements from ISO/IEC 17021.

Next section is “process requirements” this section also consists of a group of parts, starting with the first part which is “general requirements” which is also applies the same requirements from ISO/IEC 17021 with some additional requirements related to ISMS (ISO/IEC 27006, (2007)).

The additional general requirements related to ISMS provides additional information about different aspect of auditing process such as audit criteria, policies and procedures for certification process implementation, and audit team.

In addition to audit time which to ensure that audit team have adequate time to perform audit process taken into consideration a group of factors, auditing organizations with multiple sites, audit methodology, and certification audit report. (ISO/IEC 27006, (2007)).

Moving to the next part which is “initial audit and certifications” this part also has a group of requirements related to ISMS in addition to the requirements from ISO/IEC 17021.

An example of those requirements is “audit team competence” which to ensure that the audit team applies some requirements including that at least one member of the audit team should meet criteria to take team responsibility.

An example of such criteria is: team management, knowledge of implementation and controls of ISMS, and knowledge of information security related regulations and legislations (ISO/IEC 27006, (2007)).

The next requirements are to handle the “initial certification audit” which consists of two stages and some additional information and requirements.

First stage is “stage 1 audit”, the goal if this audit is to provides understanding of the ISMS regarding policy and objectives, this understanding is a preparation for stage 2 audit, and based on the results of stage 1 audit the certification body can choose auditing team members (ISO/IEC 27006, (2007)).

Moving next to “stage 2 audit” which to ensure that organization is following its own policies and procedures, and to verify that ISMS is meeting the requirements from ISO/IEC 27001 (ISO/IEC 27006, (2007)).

Next part within this section is “surveillance activities” which also applies additional requirements related to ISMS in addition to requirements from ISO/IEC 17021 (ISO/IEC 27006, (2007)).

Mainly the requirements are about “surveillance audits” which handles the verification for approved ISMS continue implementation.

The document also states a group of topics to be covered by surveillance program, an example of such topics is documented system changes, elements of the system maintenance that are part of ISMS audit, and areas affected of changes (ISO/IEC 27006, (2007)).

Next part is “recertification” which applies the same requirements from ISO/IEC 17021 and some ISMS related requirements which handle the “recertification audits” (ISO/IEC 27006, (2007)).

Recertification audits are to ensure that if nonconformities arise it should be corrected within a specific period of time; otherwise certification can be suspended or withdrawn.

Moving to the next part which is “special audits” which also applies the same requirements from ISO/IEC 17021 in addition to requirements related to ISMS which are “special cases” (ISO/IEC 27006, (2007)).

The special cases are when certified organization applies major changes to its system which affects the certification bases.

Next two parts are “suspending, withdrawing or reducing scope of certification”, and “appeals” which just applies the same requirements from ISO/IEC 17021 (ISO/IEC 27006, (2007)).

Next part is “complaints” which applies the same requirements from ISO/IEC 17021 in addition to some ISMS related requirements.

The certification body should ensure that client organization is using sufficient investigations to develop corrective actions; this includes some measurements such as conformity restoration, recurrence prevention, and assessment of effectiveness of the applied corrective measures (ISO/IEC 27006, (2007)).

Last part for this section is “records of applicants and clients” which has no additional requirements other than those from ISO/IEC 17021.

Last section is “management system requirements for certification bodies”. All parts of this section are implementing the same requirements as in ISO/IEC 17021 except for the third part which is “general management system requirements” which recommends certification bodies to implement an ISMS according to ISO/IEC 27001. (ISO/IEC 27006, (2007)).

3.2.6 Notes and examples

A remarkable note about ISO/IEC 27000 series is that different countries have different versions based on the original version but with translation to local languages (Roebuck, (2012)) such as:

- NEN-ISO/IEC 27002:2005, Netherlands
- DS/ISO27002:2014 (DK), Denmark
- JIS Q 27002, Japan
- UNE 71501, Spain
- SS-ISO/IEC 27002:2014, Sweden
- SANS 27002:2008/ISO/IEC 27002:2005, South Africa

Another case of implementing ISO/IEC 27000 series for e-government solutions is the case of Azerbaijan. During an interview with Mr. Nail T. Mardanov who is director of e-government portal at the ministry of Communication and High Technologies of the republic of Azerbaijan, he stated that ISO/IEC 27000 family of standards is used for information security management.

When asked about the bases of choosing ISO/IEC 27000 family of standards he replied that it was based on suggestions from different stakeholders and international partners (Mardanov, (2015)).

Later on he replied for the question about legislations and regulations that in 2010 the "State Committee for Standardization, Metrology and Patent of the Republic of Azerbaijan" had approved a protocol for developing a national standard based on different standards from ISO/IEC 2700 series and other ISO/IEC standards (Mardanov, (2015)), ((Azstand.gov.az, (2015))).

3.3 IT-Grundschutz

IT-Grundschutz or BSI (Bundesamt für Sicherheit in der Informationstechnik) standards is a group of methods, approaches, processes, procedures and measures for information security recommended by the Federal Office for Information security in Germany.

Although IT-Grundschutz provide organizations with guidelines for information security and protection, and share the same goal of any ISMS which is insuring the effectiveness of the CIA model for information (BSI-Standard 100-1, (2008)).

Still there are two ways to implement this standard: the first one is using it as standalone ISMS (an example of this case is ISKE in Estonia: which is a security guidelines built on the bases of IT-Grundschutz. (www.ria.ee, (2015))). While the second option is that IT-Grundschutz guidelines are fully compatible with ISO/IEC 27001 and those guidelines can be implemented in order to get the ISO/IEC 27001 certification (BSI-Standard 100-1, (2008)).

One big different between IT-Grundschutz and ISO/IEC 2700 is that IT-Grundschutz provides more details and actions for information security requirements showing the most suitable solution for different requirements.

In 2005 a restructuring for what was known as IT-Grundschutz Manual resulted in separating the manual into two parts (BSI-Standard 100-1, (2008)) which are:

The BSI standards of Information security, which consists of four standards that are "Information Security Management Systems (ISMS)", "IT-Grundschutz Methodology", "Risk Analysis based on IT-Grundschutz", and "Business Continuity Management" (BSI-Standard 100-1, (2008)); later on all of those standards will be discussed with more details.

The second part is: IT-Grundschutz Catalogues, which consists of multiple documents in modular structure. Those documents provide additional information about different security threats and the recommended measures. Additionally those documents get regular updates taking into consideration latest development in technology (BSI-Standard 100-1, (2008)).

3.3.1 Information Security Management Systems (ISMS)

This is the first document from the BSI series of standards for information security. It provides the general requirements for ISMS, and as mentioned before those requirements are fully compatible with ISO/IEC 27001.

The standard additionally provides some general understanding about information security. Including the rule of the management, resources of information technology security, and how to develop, implement, and improve information technology security concept (BSI-Standard 100-1, (2008)).

Later on the standards will explain briefly about risk assessment and development of security concept in accordance with IT-Grundschutz. Although the risk analyses process is discussed in details in the third standard of the BSI series which is (BSI- 1003: Risk Analysis based on IT-Grundschutz).

3.3.2 IT-Grundschutz Methodology

This is the second standard of the BSI series. It provides practical step-by-step and detailed information about ISMS implementation and what to be taken into consideration when developing information security policies (BSI-Standard 100-2, (2008)).

Moreover, this standard provides detailed information that can help in the process of maintaining and improving ISMS during its operational lifetime (BSI-Standard 100-2, (2008)).

According to what was previously mentioned about IT-Grundschutz methodology, it can be seen that IT-Grundschutz follows the same PDCA concept as ISO do. Moreover it is noticed that IT-Grundschutz methodology handle almost the same approaches as ISO/IEC 27002 do.

3.3.3 Risk Analysis based on IT-Grundschutz

BSI-3 or BSI- 1003 is the third standard of the BSI standard series. The standard handles the risk analyses based on IT-Grundschutz. And for this reason it is best to use it in the cases of adding additional security analyses with less effort (BSI-Standard 100-3, (2008)).

The analyses start with preliminary work. This is to ensure that some parts and aspects have been handled in the way it is described in IT-Grundschutz methodology. This includes initiating information security process, defining scope of security concept, and modeling process (BSI-Standard 100-3, (2008)).

Moving next to preparing the threat summary, the goal of this step is to summarize threats related to the target objects which are under review and listed in the IT-Grundschutz catalogues. This section also provides a group of steps to be followed in order to reduce the information domain for the target objects to be reviewed (BSI-Standard 100-3, (2008)).

Next step in the risk analyses is the determination of additional threats. This aims to include and take into consideration additional threats for the target objects that were not included in the IT-Grundschutz model. It also provides some description about the nature of such threats and how to identify such threats (BSI-Standard 100-3, (2008)).

The following step in the risk analyses is threat assessment. This step provides some criteria to be used for testing the effectiveness of the security measures from IT-Grundschutz catalogues which are related to the target objects.

The final result of the assessment is OK (Y/N) for each measure. Where OK=Y means that security measures provides adequate protection. And OK=N means that security measures do not provide adequate protection (BSI-Standard 100-3, (2008)).

Next step is handling risks. It consist of two parts, the first part is Alternative methods for handling risks. It also shows how to handle risks that are not adequately halted by measures from IT-Grundschutz catalogues. In addition this part also provides a group of alternatives to handle threats that were marked as OK=N in the threat summary (BSI-Standard 100-3, (2008)).

The other part within this step is risks under examination. This is concerned with risks that can be marked as acceptable for the current situation but in the future it can be marked as unacceptable. For such situation a supplementary security safeguards should be created in advance (BSI-Standard 100-3, (2008)).

Moving to next step, which is consolidation of the security concept. This step provides some criteria for checking security measures for targeted objects and then consolidates the security concept (BSI-Standard 100-3, (2008)).

Last step for the risks analyses is feedback to the security process. This step is performed at the end of the risks analyses aiming to provide the consolidated security concept as a base for a group of steps from IT-Grundschutz methodology (BSI-Standard 100-3, (2008)).

One note to be mentioned here is that for all of the previously mentioned steps, the document provides some examples for each step except the last step.

3.3.4 Business Continuity Management

The fourth standard of the BSI series (other standards referred to this standard as BSI-4 or BSI – 1004) provides some guidelines and methods for setting up business continuity management system. Those methods were built up based on the methods and procedures in BSI-2 (IT-Grundschutz Methodology) (BSI-Standard 100-4, (2009)).

The goal of the business continuity management is to implement safeguards against critical risks that would endanger the continuity of the organization. Thus the main aim is to ensure that business processes are temporarily interrupted or not interrupted at all in any situation even critical situations (BSI-Standard 100-4, (2009)).

It should be mentioned here that business continuity management is handled as part of ISO/IEC 27002 with a group of controls. But it is handled with more details as a separate document in IT-Grundschutz.

3.3.5 Notes and examples

As an example of implementing IT-Grundschutz as ISMS, Estonia has built its ISMS based on IT-Grundschutz and now it is called ISKE (www.ria.ee, (2015)).

A group of Information Technology standards were available and under discussion at the time when Estonia started to think about adopting and implementing ISMS (Reintam, (2012)). Some of those standards are:

- ISO 13335
- ISO 17799
- BSI- IT Baseline Protection Manual
- US Department of Energy Security Manuals

Estonians were mostly interested in information technology security standard that has the following characteristics (low cost or free of charge, regularly updated, big granularity, and have appropriate security goals and levels) (Reintam, (2012)).

Among the different security standards that were under discussion in Estonia IT-Grundschutz (BSI-IT Baseline Protection Manual) has met the specified criteria in addition it provides less time consuming risk assessment.

3.4 COBIT

Control Objectives for Information and related Technology (COBIT), was developed by Information Systems Audit and Control Association (ISACA) and IT Governance Institute (ITGI). It is a framework that defines goals for IT management controls.

The final version of COBIT is COBIT 5. It consists of a group of principles (five principles) that allows building effective governance and management framework. This is based on a group of enablers (seven enablers) for information and technology investment optimization (COBIT 5 for Information Security Introduction, (2012)) that can be useful for all kind of enterprises. In general COBIT provides a “checklist approach to IT governance” (Harris and Kumar, (2013)).

The following figures illustrate the COBIT 5 principles and enablers:

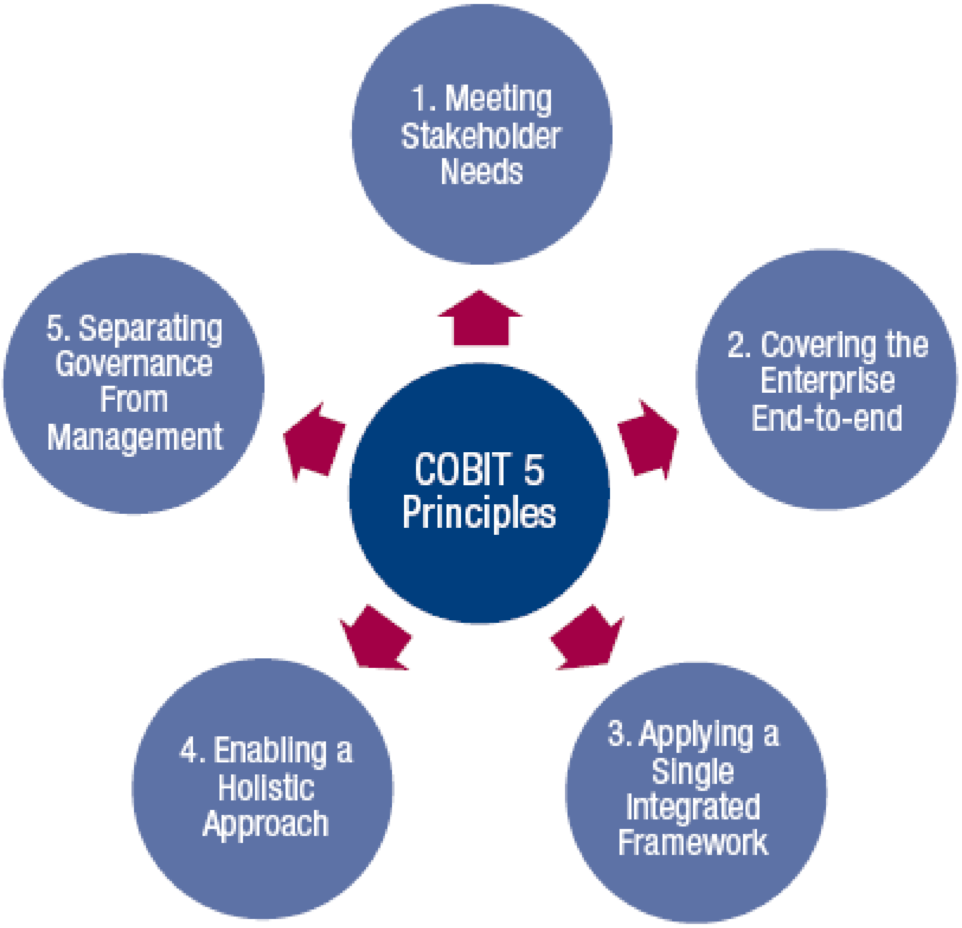

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Figure 2 COBIT 5 Principles, (COBIT 5 for Information Security Introduction, (2012))

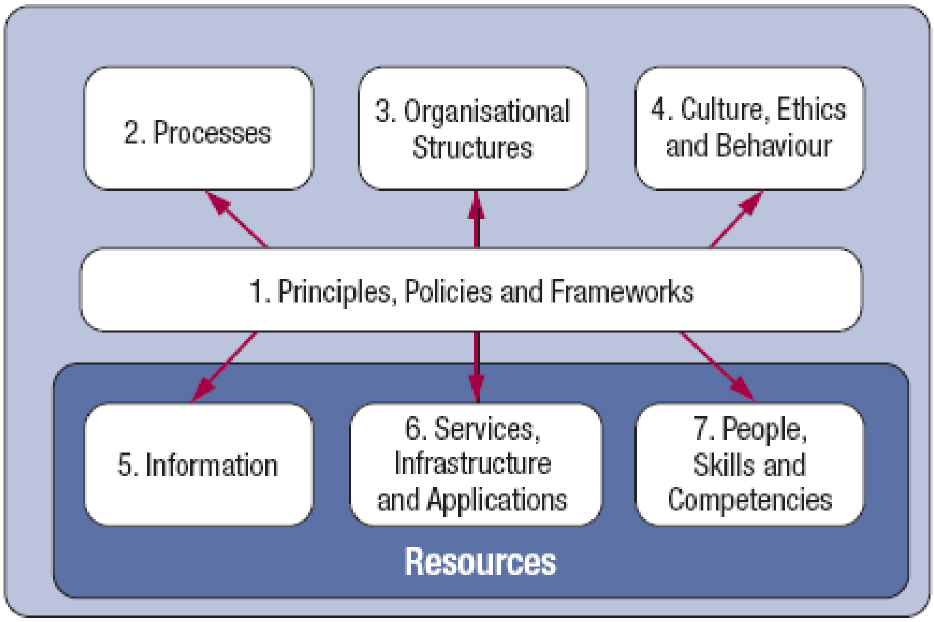

2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Figure 3 COBIT 5 Enablers, (COBIT 5 for Information Security Introduction (2012))

Although COBIT 5 manages IT governance it provides different tools and guidance that handle different topics which are:

- Audit and Assurance
- Risk Management
- Information Security
- Regulatory and Compliance
- Governance of Enterprise

COBIT 5 for information security deals with the ubiquity of information security within the enterprise and provides overall framework of enablers.

In addition COBIT 5 does not ignore other security frameworks and standards such as ISO/IEC 27000, and it aims to act as connecting framework that connects different frameworks (COBIT 5 for Information Security Introduction, (2012)).

According to (COBIT 5 for Information Security Introduction, (2012)), it is obvious that COBIT 5 follows the same approach as some other standards and frameworks (i.e. ISO/IEC 2700) as can be noticed COBIT 5 aims to manage information security, handle risks, define information security, manage information security policies,… etc.

A remarkable note to be mentioned here is that according to Harris and Kumar (2013) COBIT provides implementation objectives to take a place, this can be seen as a similar approach as IT-Grundschutz.

Finally; a point of advantage for COBIT is that COBIT's control objectives considered as industry best practices (Harris and Kumar (2013)) it would be preferable for information security auditors as the current security auditing practices are based on COBIT.

3.5 ITIL

ITIL stands for (Information Technology Infrastructure Library), although it has a component for information security, ITIL is more focused on internal service level agreement (Harris and Kumar (2013)). In addition, ITIL is considered as the world's best practices for IT service management ((Harris and Kumar (2013)), (Meziani and Saleh, 2010)).

Generally ITIL is a group of books that provided in online format. And acting as a customizable framework, ITIL goal is to provide a common language for communication and understanding between business people and IT people. This is due to the lack of such common language causes a fusion between business objectives and IT functions for organizations (Harris and Kumar (2013)).

Moreover ITIL can be implemented in addition to other ISMS and frameworks such as ISO/IEC 27000 series and COBIT (Arraj, 2013).

Latest version of ITIL is 2011 editions which enhances the five core publication (V3 of ITIL was consisting of five core publications) where it introduces some additions and improve clarity in those core publications (TSO, 2012).

The following figure illustrates the main components of the ITIL:

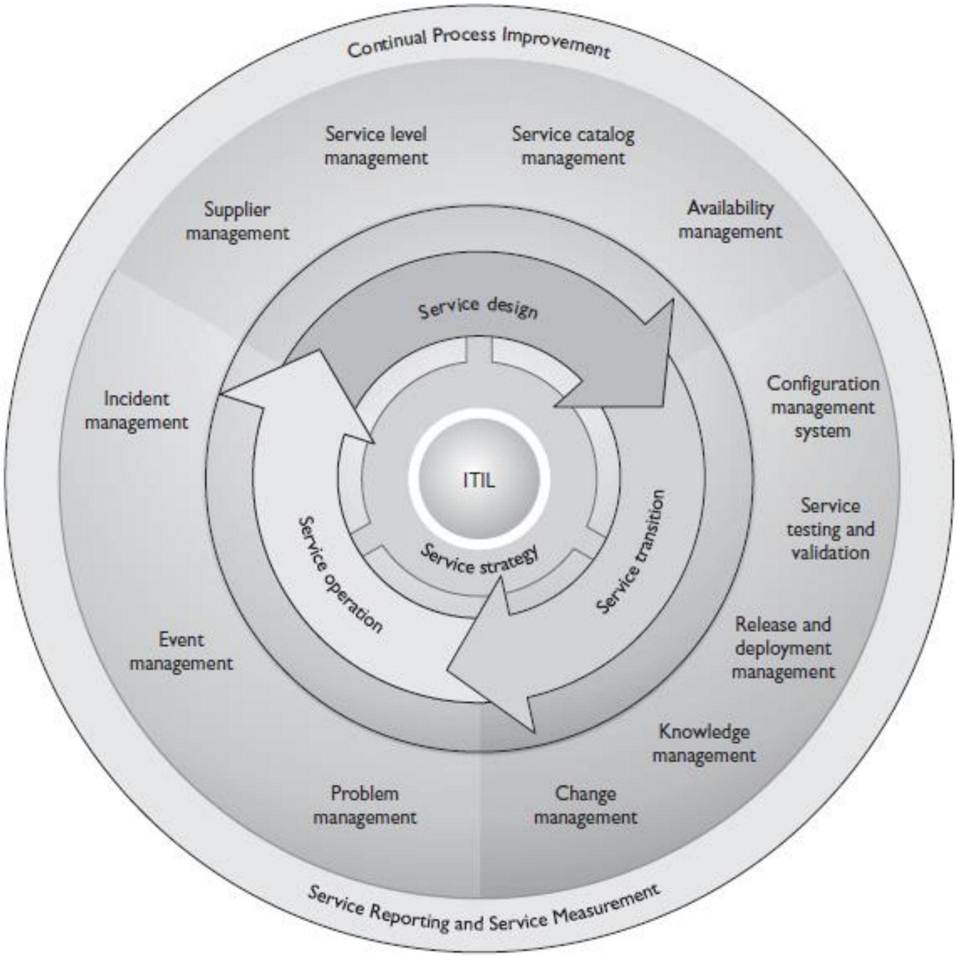


Figure 4 ITIL Components (Harris and Kumar (2013))

4 Comparing Information security management systems

Within this chapter the comparison criteria will be stated and discussed regarding the reason for using such criteria and its relevance to the situation of e-government in Palestine.

Each criterion for comparison will consist of information about each ISMS or framework that was mentioned in previous chapter. The source of the information is the information mentioned in the previous chapter, in addition to some new resources whenever needed.

4.1 Implementation cost, and licensing cost

This is one of main criterion to be considered, as the Palestinian authority does not have much resources and the fact that a big part of the projects conducted by PA depends on international aids (knowing that the sources of around 50% of the state budget are external and international fund (Al-Monitor, (2013))).

For such reasons it is important that the ISMS to be implemented would be cost efficient regarding the implementation cost (i.e. cost of implementing, adopting security controls and counter measures) and licensing cost (i.e. cost of license to use the ISMS).

For the purpose of the thesis implementation cost will not be taken into much consideration as it require deep analysis for the already implemented solutions and the suggested solution by each ISMS. The focus will be on licensing cost for each ISMS.

4.1.1 ISO/IEC 27000 series

As been reviewed previously, the most important part for implementing ISO/IEC 27000 series is the first six documents of the series (Greene (2014)), the estimated price for this group of documents would be around a couple of thousands of euros.

In addition, taking into consideration the fees of information security audit process to ensure the right implementation of the ISMS and eventually will result on granting the certificate of the ISO/IEC 27001.

Moreover, as previously mentioned that some of the series parts refers to other ISO standards which my results in implementing additional standards for achieving the recommended solutions by ISO/IEC 27001.

One last thing to be mentioned here is that in the case of the centralized implementation, that one part will be responsible for the implementation of all other parts (ministries and e-services providers) then the cost will be calculated once.

In the case of decentralization, each part is responsible for its own implementation; the cost will be multiplied based on the number of e-services providers.

4.1.2 IT-Grundschutz

Moving to the next framework which is IT-Grundschutz, beside the implementation cost the information security auditing cost can be considered. As for the licensing or documents cost IT-Grundschutz would be the most effective among the other ISMS / frameworks discussed here, because as mentioned before those documents are free and available online.

Knowing that IT-Grundschutz is fully compatible with ISO/IEC 27001 and it is possible to use IT-Grundschutz to get the ISO/IEC 27001 certificate.

The information security audit that mentioned here is about to check the implementation of ISMS in order to get the ISO/IEC 27001 certificate.

4.1.3 COBIT

Next framework to be discussed here is COBIT; it provides some documents that can be purchased online each document will cost couples of tens of euros.

In addition, ISACA provides different types of licenses for COBIT; in this case the most suitable license would be “Unlimited commercial use license” which costs about US $50,000 annually (Isaca.org, (2015)).

It was mentioned in the previous chapter the COBIT can be implemented beside ISO/IEC 27001, which means additional cost beside the license cost and the cost of ISO/IEC 27001 certificate.

4.1.4 ITIL

Last framework to be discussed is ITIL; this framework also provides licensed products with different types of licenses.

As previously mentioned that ITIL consists of five core components each component consists of a group of documents (around three documents or more). Each document have different price and mostly do not exceed a hundred and twenty euros.

Also ITIL can be implemented in addition to ISO/IEC 27001 or other frameworks and ISMSs, which means additional cost depending on the other framework.

4.1.5 Results

As a conclusion for this part, it is obvious that each ISMS/ framework have different approach for licensing and in some cases additional cost for implementing more than one framework.

Based on the information stated in this criterion IT-Grundschutz can be considered the most effective ISMS to be implemented as it is free of charge, and provides the ability to implement other ISMS (ISO/IEC 27001) based on implementation guidance provided by IT-Grundschutz.

4.2 The need for adoption of regulations, legislations, and policies

The importance of regulations or legislations is crucial. It aims to insure that all stakeholders of the e-government in addition to e-service providers who are part of the e-government will commit to the implementation of the ISMS.

Palestine still evolving when it comes to IT related legislations and regulations. This can be seen through the ongoing process of developing and adopting of electronic transaction law draft. The draft law aims to govern and legalize electronic transaction which is one main part of e-government functionality.

The electronic transaction law also provides some definitions for main components of electronic transactions such as digital signature, electronic records, encryption, electronic data, and data exchange (Electronic Transaction Law Draft, (2010)).

Legislations are needed to ensure that all e-services providers and all related parties regarding the implementation of the e-government will apply and implement the suggested ISMS.

This will ensure that all e-service providers will apply the same information security tools and policies that are stated by the ISMS, which will reflect to the whole security of the e-government as a whole body.

This means that each service provider that does not implement the information security policies would be a potential vulnerability to the whole e-government.

As a result of this it is important that the government adopt appropriate legislations and regulations regardless to which ISMS will be implemented, this will insure that each service provider would implement the minimum required information security level.

Each one of the suggested ISMSs deals with information security policies in different ways, ISO/IEC 27000 and IT-Grundschutz provides more details about information security policies, but the advantage would be in the side of ISO/IEC 27000 series.

It is mentioned in ISO/IEC 27002 beside the characteristics of an information security policy and how it should looks like, that information security policy “should be supported by topic-specific policies“(ISO/IEC 27002, (2013)).

4.2.1 Results

As a conclusion for this part, regardless the implemented ISMS, regulations and legislations are needed. When it comes for information security policies, ISO/IEC 27000 would be better solution as it provides more details regarding information security policies.

4.3 ISMS’s updates frequency

With the fast growing development of technologies, it is important that any ISMS to keep up with the technology developments.

Outdated ISMS may endanger the whole system instead of delivering the desired functionality which is information security.

The goal of the updates is to keep the ISMS in a level that manages potential threats from different technologies especially new technologies. So when an organization adopt or implement new technologies it would mostly managed and covered by the implemented ISMS to avoid any potential threats.

Following each of the ISMS which are subjected to the thesis research will be discussed with proved update history:

4.3.1 ISO/IEC 27000 series

The origin of ISO/IEC 27000 goes back to PD 0003 which was developed in 1989 by the National Computing Centre (NCC) in UK (Gammassl.co.uk, (2015)).

This standard later updated and developed to BS7799:1995 and BS7799-2:1998, which kept developed until it was published as ISO/IEC 17799:2000 (Gammassl.co.uk, (2015)).

It was until the year of 2005; the BS 7799-2 was adopted by the ISO organization and changed to ISO/IEC 27001:2005 and after a couple of years ISO/IEC 17799 was changed to ISO/IEC 27002:2005.

The current version of ISO/IEC 27001 and ISO/IEC 27002 are 2013. It is clear that the update pace of the ISO/IEC 27000 series is not quite fast; still it provides stable versions with some additional parts.

4.3.2 IT-Grundschutz

IT-Grundschutz is quite newer standard than ISO/IEC 27000 series, all of the four standard's documents are back to 2005 except for the risk analysis which goes back to 2004 and the current versions back to 2008.

Although the standards have not got many versions, the most important part is the IT-Grundschutz catalogues. As previously mentioned, the catalogues provide recommended countermeasures for information security threats.

The catalogues were previously known as IT-Grundschutz manual and the first version back to 1992 (BSI-002, (2008)), while the latest version of the IT-Grundschutz back 2013 which is version no 13th (IT-Grundschutz-Catalogues, (2013)).

4.3.3 COBIT

The first version of COBIT was published in 1996 which was mainly targeting auditing, while the last version was published in 2012 which introduced the concept of IT Governance or Governance of Enterprise IT (COBIT 5 for Information Security Introduction, (2012)).

In general COBIT has five versions (although version 4 has two versions which are 4.0 and 4.1) the following figure shows the evolution of COBIT:

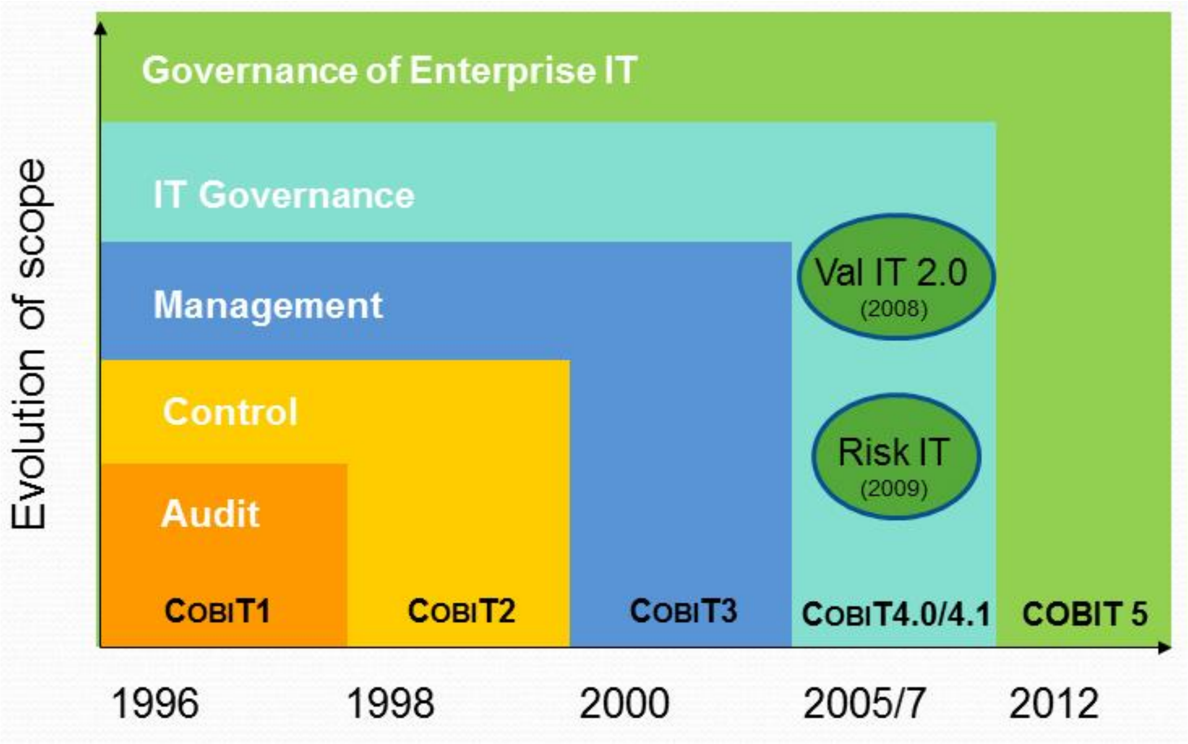


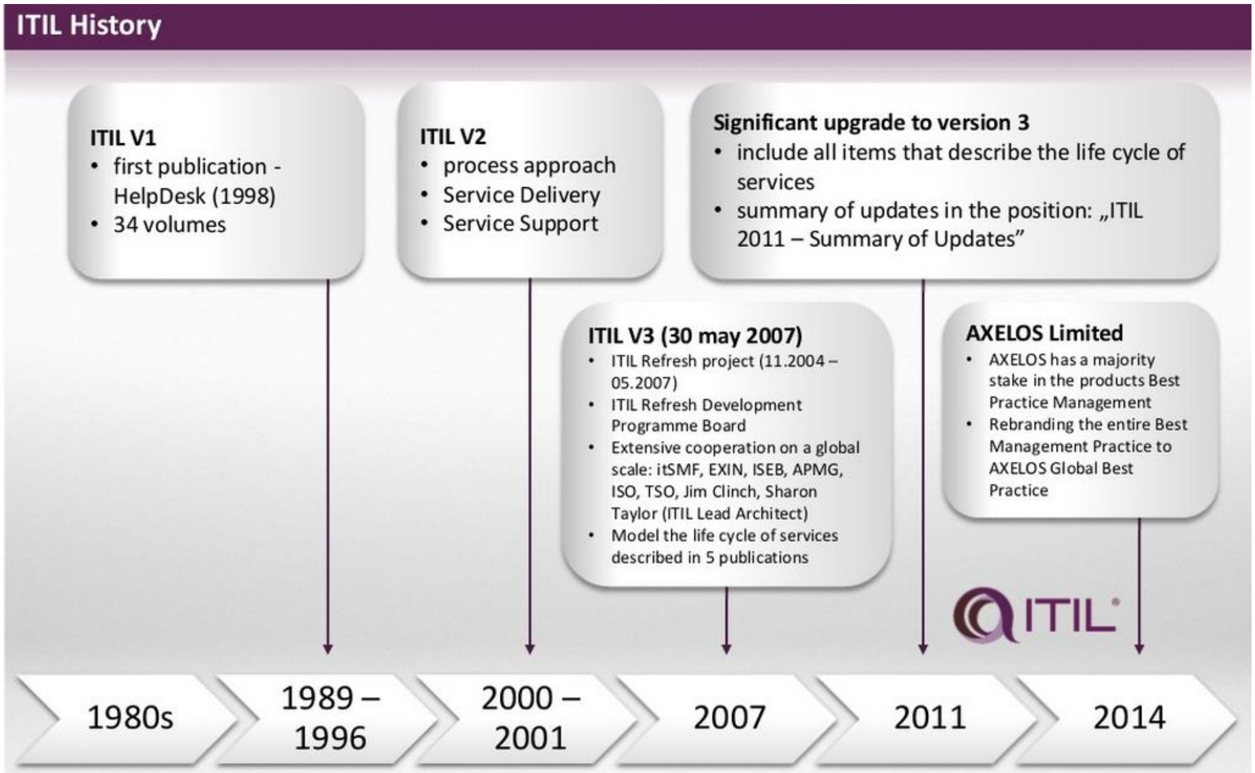
Figure 5 COBIT Evolution (COBIT 5 for Information Security Introduction, (2012))

It is clear that each version of the COBIT framework provided additional scopes beside what was included in the previous versions.

4.3.4 ITIL

Last framework for this part is ITIL; the first version of ITIL was published in 1989, while the latest version was published in 2011 which is an upgrade to version 3.

It is clear that ITIL haven't got much updates during its lifecycle, the following figure shows the history of ITIL versions including basic information about each:



ITIL History

ITIL V1
- first publication - HelpDesk (1998)
- 34 volumes

ITIL V2
- process approach
- Service Delivery
- Service Support

Significant upgrade to version 3
- include all items that describe the life cycle of services
- summary of updates in the position: „ITIL 2011 – Summary of Updates"

ITIL V3 (30 may 2007)
- ITIL Refresh project (11.2004 – 05.2007)
- ITIL Refresh Development Programme Board
- Extensive cooperation on a global scale: itSMF, EXIN, ISEB, APMG, ISO, TSO, Jim Clinch, Sharon Taylor (ITIL Lead Architect)
- Model the life cycle of services described in 5 publications

AXELOS Limited
- AXELOS has a majority stake in the products Best Practice Management
- Rebranding the entire Best Management Practice to AXELOS Global Best Practice

Figure 6 ITIL History (Dabrowski, (2015))

4.3.5 Results

Based on the previously mentioned information about the history of each of the ISMSs/ Frameworks, it is clear that IT-Grundschutz Catalogues are the most updated framework among the others.

It is crucial for the IT-Grundschutz to be regularly updated, as it provides solutions for the proposed information security threats, so it should be catching with latest technology and eliminates or reducing the gap between the proposed solution and the latest technologies.

To conclude this part, the advantage is in the side of IT-Grundschutz for the reasons discussed before.

4.4 Information security auditing approach

Information security auditing is an important process for the implementation of ISMS and for monitoring process after the implementation. Some of the previously discussed frameworks (i.e. ISO/IEC 27000) also benefit of the auditing process for certifying the ISMS, and later for recertification, withdrawal, and termination of certification.

The importance of auditing process for the case of this thesis (e-government in Palestine) is derived from the emphasis on accountability and transparency in the e-government strategic plan.

4.4.1 ISO/IEC 27000 series

ISO/IEC 27006 is the part of the ISO/IEC 27000 series that handles the auditing process. It handles the different aspect of the audit process including general requirements, the use of external auditors and technical experts (ISO/IEC 27006, (2007)).

In addition, it also handles access to confidential records, and how the auditing organization should act in the cases of impossibility to access confidential records.

It should be mentioned here that ISO/IEC 27006 mainly focus on the audit process to ensure that the implementation of the ISMS has met the ISO/IEC 27001.

Another note to be taken into consideration is that ISO/IEC 27006 provides some additional information about ISMS while mainly it applies the same as ISO/IEC 17021.

4.4.2 IT-Grundschutz

IT-Grundschutz provides more details about information security auditing than ISO/IEC 27006 provides. It also shares a couple of activities with ISO/IEC 26006 such as auditing team, and the use of external auditors (Information security audit (IS audit) - A guideline for IS audits based on IT-Grundschutz, (2008)).

In addition, IT-Grundschutz provides information about auditing techniques, evaluation scheme, and a group of six steps. Starting with the preparation for the audit, ending with audit report, and it also provides estimated amount of time each step would consume from the overall auditing time (Information security audit (IS audit) - A guideline for IS audits based on IT-Grundschutz, (2008)).

Moreover, IT-Grundschutz states that auditing process is a cyclic process, and it states that the audit should be performed every three years based on the federal implementation plan.

4.4.3 COBIT

When it comes to COBIT for information security auditing, it is without any doubts the most favorable framework for information security auditors to deal with (Harris and Kumar (2013)). According to the same resource COBIT is the base of current security auditing practices, moreover, it was clear in figure 5 that auditing was the goal of the first version of COBIT.

Information Technology Assurance Framework (ITAF) is a standard published by ISACA. It provides detailed information about auditing process, and consists of three main parts which are: auditing and assurance standards, audit and assurance guidelines, and Audit and Assurance Tools and Techniques (ITAF™: A Professional Practices Framework for IS Audit/ Assurance, (2014)).

ITAF provides detailed information about criteria, performance and supervision, and follow-up activities of the auditing and assurance standards and guidelines.

4.4.4 ITIL

As previously mentioned, ITIL focuses more on internal service level agreement; it does not provide an explicit approach for information security audit. Thus ITIL will fail to score any points in this part of comparison with other ISMS/ frameworks.

4.4.5 Results

As a conclusion for this part, it is clear that COBIT would be the one with the highest recommendations when it comes to information security audit. Although IT-Grundschutz can be also taken into consideration as it provides detailed information about auditing process.

Based on the results of the comparison between the suggested ISMSs/ frameworks, it is obvious that IT-Grundschutz would be the most suitable framework to be taken into consideration for implementation.

Conclusion

It is clear that the Palestinian authority needs to adopt an approach towards cyber security in general and information security management in specific.

The current situation might looks like that there is no need for information security management, but in the future it is a matter of time until there is a real need for it.

Among the different ISMSs and information security frameworks that discussed within this thesis; IT-Grundschutz was the most suitable ISMS to be implemented for the Palestinian e-government. Based on the results of the comparison IT-Grundschutz offered better solutions for two of the comparison criteria, and can also be considered in another criterion.

As for the implementation and adoption of IT-Grundschutz as ISMS in Palestine, it would be more practical to follow the Estonian approach. This means that the Palestinian authority should implement its own ISMS based on IT-Grundschutz, with the use of Arabic language as a formal language for such ISMS.

This means a better understanding for the personnel, who are going to work on the implementation, and for interested researchers. In addition, this will also add a value for the ISMS as other frameworks also provides Arabic translation for all necessary documentation.

Implementing ISMS is not enough to ensure security; the government should work also on educating personnel who are involved with the e-services, and also educating citizens about basic security aspect such as data privacy and personal data.

In addition, Implementation and adoption of ISMS should be backed up with proper legislations and regulation that ensure all of the involved parties will follow the same approach and have the minimum level of security.

Moreover, the governments should work on creating national cyber security agenda as it currently not available, this will ensure definition of vital services and what are the plans for handling cyber security especially on the national level approach.

Finally, beside the ISMS and the national cyber security plan, there should be a CERT team (Computer Emergency Response Team) to handle the security incidents.

Bibliography

- Al-Monitor, (2013). Palestinian Authority’s 2013 Budget Passed Despite Political Rift - Al-Monitor: the Pulse of the Middle East. [online] Available at: http://www.al-monitor.com/pulse/originals/2013/04/palestinian-authority-budget-2013.html [Accessed 1 May 2015].

- Arraj, V. (2013). ITIL: the basics.

- ARTICLE 19 (2005) “memorandum on a proposal for a draft law on Access to Information of Palestine”. London.

- Azstand.gov.az, (2015). AZSTAND. [online] Available at: http://www.azstand.gov.az/index.php?id=178&lang=3 [Accessed 13 May 2015].

- BSI-Standard 100-1: Information Security Management Systems (ISMS). (2008). Bundesamt für Sicherheit in der Informationstechnik (BSI): Bonn, Germany.

- BSI Standard 100-2 IT-Grundschutz Methodology. (2008). 2nd ed. Bundesamt für Sicherheit in der Informationstechnik (BSI): Bonn, Germany.

- BSI-Standard 100-3: Risk analysis based on IT-Grundschutz. (2008). 2nd ed. Bundesamt für Sicherheit in der Informationstechnik (BSI): Bonn, Germany.

- BSI-Standard 100-4: Business Continuity Management. (2009). Bundesamt für Sicherheit in der Informationstechnik (BSI): Bonn, Germany.

- COBIT 5 for Information Security Introduction. (2012).

- Dabrowski, M. (2015). AXELOS - ITIL® Foundation.

- e-Governance Academy (2010) “The President of Estonia, Toomas Hendrik Ilves opened Estonian-Palestina x-Road cooperation project implemented by e-Governance Academy” Estonian e-Governance Academy (2010) website 30 June 2010. Available at: http://www.ega.ee/node/627 [Accessed 1 March 2015].

- e-Governance Academy (2010) “Palestinian Authority ICT in education project started!” Estonian e-Governance Academy (2010) website 2 October 2010. Available at: http://www.ega.ee/node/727 [Accessed 1 March 2015].

- Electronic Transaction Law Draft. (2010). Ramallah: Ministry of Telecommunication and Information Technology.

- Gammassl.co.uk, (2015). History of ISO/IEC 27001. [online] Available at: http://www.gammassl.co.uk/27001/history.php [Accessed 15 May 2015].

- Greene, S. (2014). Security program and policies. Indianapolis, Ind.: Pearson.

- Harris, S. and Kumar, P. (2013). CISSP all-in-one exam guide, sixth edition. New York: McGraw-Hill.

- Information security audit (IS audit) - A guideline for IS audits based on IT-Grundschutz. (2008). Bonn: German Federal Office for Information Security.

- ISO/IEC 27000 "Information technology — Security techniques — Information security management systems — Overview and vocabulary". (2014). 3rd ed. Switzerland: ISO copyright office.

- ISO/IEC 27001 “Information technology — Security techniques — Information security management systems — Requirements”. (2013). 2nd ed. Geneva, Switzerland: ISO copyright office.

- ISO/IEC 27002 “Information technology — Security techniques — Code of practice for information security controls”. (2013). 2nd ed. Geneva, Switzerland: ISO copyright office.

- ISO/IEC 27005 “Information technology — Security techniques — Information security risk management”. (2011). 2nd ed. Geneva, Switzerland: ISO copyright office.

- ISO/IEC 27006 “Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems”. (2007). Geneva, Switzerland: ISO copyright office.

- Isaca.org, (2015). COBIT 5 Licensing. [online] Available at: http://www.isaca.org/About-ISACA/Licensing-and-Promotion/Pages/Information-on-COBIT-5-Licensing.aspx [Accessed 14 May 2015].

- ITAF™: A Professional Practices Framework for IS Audit/ Assurance. (2014). 3rd ed. Rolling Meadows: ISACA.

- IT-Grundschutz-Catalogues. (2013). 13th ed. Bonn: Federal Office for Information Security.

- MA'AN NEWS AGENCY, (2015). الاتصالات تطلق نظام ناقل البيانات الحكومي X-Road. [online] Available at: http://www.maannews.net/Content.aspx?id=763612 [Accessed 12 Mar. 2015].

- Mardanov, Nail Interviewed by Shahwan, Mohammed. Personal interview (13th May 2015).

- Meziani, R. and Saleh, I. (2010). e-government: ITIL-based service management case study. In: The 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010). New York, NY, USA: ACM, pp.509-516.

- MTIT (2010) "e-Transaction Law". Ramallah - Palestine.

- OECD (2011) "Modernising the Public Administration: The Case of E-Government in the Palestinian Authority".

- Oja, Tarmo Interviewed by Shahwan, Mohammed. Personal interview (11th February 2015).

- Palestinian Central Bureau of Statistics (2013) "Special Statistical Bulletin on the 65th Anniversary of the Palestinian Nakba" Palestinian Central Bureau of Statistics (PCBS) website, 14 May 2013. Available at: http://www.pcbs.gov.ps/site/512/default.aspx?tabID=512&lang=en&ItemID=788&mid=3171&wversion=Staging [Accessed 1 March 2015].

- Palestinian National Authority - Ministerial Committee for e-Government (2005) "e-Government Strategic Plan".

- palestinianbasiclaw.org (2007) "2003 Amended Basic Law". Available at: http://www.palestinianbasiclaw.org/basic-law/2003-amended-basic-law [Accessed 4 March 2015].

- PLO: Palestinian Liberation Organization, (2011). Frequently Asked Questions: THE GREEN LINE IS A RED LINE: THE 1967 BORDER AND THE TWO-STATE SOLUTION. PLO NEGOTIATIONS OFFICE.

- Reintam, A. (2012). Estonian Security System Overview.

- Tikk et al (2010). Eneken Tikk, Kadri Kaska, Liis Vihul. "International cyber incidents: Legal considerations". Tallinn: CCD COE Publications.

- TSO (2012). An Introductory Overview of ITIL® 2011. Norwich: TSO (The Stationery Office).

- www.ria.ee, (2015). IT Baseline Security System ISKE. [online] Available at: https://www.ria.ee/iske-en [Accessed 21 Apr. 2015].

Appendices

Appendix A (Transcript of interview with Mr. Tarmo Oja)

Shahwan: As a security expert who had worked on the Estonian - Palestinian project for implementing e-government. Do you know if there is any implemented ISMS, or any plans to implement ISMS?

Oja: No, there is no ISMS implemented, and there is not any ISMS taken into consideration to be implemented.

Shahwan: what were the problems and issues that you had encountered during your work which may affect the information security or the implementation of ISMS?

Oja: The main issue was about the infrastructure, it is missed up, and even if any controls are implemented it will not work out effectively.

Shahwan: are there any other issues?

Oja: mainly, lack of monitoring, human resources, coordination, and polices.

Shahwan: what about the lack of human resources?

Oja: only one employee is responsible about almost everything regarding information security and technical aspect.

Shahwan: and what about coordination? What are the issues you had encountered regarding coordination?

Oja: there is no enough coordination between different ministries and other parties. I can give you an example about this to get to the point.

One day while we were working, the power went off the whole building and the backup generator was off due to some issues. After checking for the source of this problem it turned out that the power supplier (Power Company) have a scheduled maintenance for the building. And later we knew that the electrician who was working to solve the problem have access to the room where all power supplies and equipment where located, he just get in and switched off the power and start the maintenance.

There was not a communication during that day between the power company and the Governmental Computer Center (GCC) to inform about the exact time of maintenance, the result was we had to wait until the maintenance is done, and wasted a couple of hours from training time.

Shahwan: what about policies?

Oja: the project is conducted with different ministries, each has their own policies, and it would be great if there is a single source of polices. It would also avoid the issues related to services in silos.

Shahwan: any suggestions for the infrastructure issues?

Oja: first the infrastructure should be subjected to maintenance, and then there should be a clear methodology to build the networks. Each ministry builds their own networks in different ways, which would affect the whole infrastructure.

Also another issue is that there are some networks should not be connected to the main network, during one of the training sessions, we managed to access so easily to the main network which is supposed to be secure, and we are not supposed to connect to this network.

Shahwan: do you have any information about how IT-Grundschutz was selected to be implemented in Estonia?

Oja: currently I do not have enough information about this topic, but I can say that some of the reasons are: IT-Grundschutz documents are clear and easy to understand, and the documents do not link or refer to other documents or standards like the case of ISO/IEC 27000.

Shahwan: are there any other suggestions to be considered for the Palestinian case?

Oja: mostly how the legislations and regulations are provided to the ministries for implementation, and there should be a single body to monitor and supervise the implementation process.

Appendix B (Transcript of interview with Mr. Nail T. Mardanov)

This was not an official interview; it was conducted during Tallinn e-Governance Conference 2015. Mr. Mardanov was part of the delegation of Azerbaijan, and due to his busy schedule the interview consists of a couple of questions.

Shahwan: as a director for the e-government portal for the republic of Azerbaijan, can I ask you how do information security management handled? Is there any ISMS implemented.

Mardanov: yes we have implemented ISMS, which is ISO/IEC 27000.

Shahwan: why did you (the state portal) decide to implement ISO/IEC 27000? And what are the bases to choose ISO/IEC 27000 although there are different ISMSs.

Mardanov: when the ministry of communication and high technologies started to work on the implementation of the e-government portal, we had the chance to work with many different international partners; our partners have suggested that we implement ISO/IEC 27000 for information security management.

Shahwan: so ISO/IEC 27000 was adopted directly based on the suggestions from your partners, and there was not any process for choosing which ISMS to be implemented.

Mardanov: yes.

Shahwan: one last question, does the implementation of ISO/IEC 27000 supported by legislations or regulations?

Mardanov: yes, you can check the website of the “State Committee for Standardization, Metrology and Patent of the Republic of Azerbaijan” and there you can find more information about this topic.

Appendix C (Translation for the used part of the Palestinian e-transaction law draft)

Original text in Arabic:

الفصل السابع: طرق حماية المعاملات الإلكترونية:

مادة (38)

يجب استخدام الطرق الاتيه لحماية نظم المعلومات:

- التشفير بطريق المفتاح العام
- الجدران النارية
- مرشحات المعلومات
- وسائل منع الإنكار
- إجراءات حماية نسخ الحفظ الإحطياطية
- البرامج المضادة للفيروسات
- اية طريقة اخرى تجيزها الهيئة

Translated text in English:

Chapter seven: methods of protecting electronic transactions:

Article (38)

The following methods should be used for protecting information systems:

- Public Key Encryption.
- Firewalls
- Information filters
- Some services to prevent DoS Attacks
- Backups
- Antiviruses
- Any other methods approved by the organization