Master Thesis

University of Piraeus

Department of Digital Systems
Digital System Security

<< Information Security Management System Toolkit >>

Author: Karamanlis Manos

Supervisor: Katsikas Sokratis

Acknowledgements

I would like to thank my family members for their support and encouragement.

I would also like to thank all professors to this postgraduate program for their valuable contribution to my studies.

Table of Content

Table of Content

1 Introduction 1

1.1 What is information? 2

1.2 What is information management? 3

1.3 The information security and its necessity 4

2 Information Security Management Systems (ISMS) 7

2.1 Why ISMS is needed? 8

2.2 Information Security Management System Frameworks and Standards 9

3 ISO 27000 Standard Family 12

3.1 ISO/IEC 27001:2013 Standard 20

3.1.1 ISO 27001:2013 structure 21

3.1.2 Comparison of ISO 27001:2005 and ISO 27001:2013 22

4 The need of ISMS toolkit 24

4.1 Building an ISMS and finding supporting tools 24

4.2 Previous related researches 26

4.3 Creation of an ISMS toolkit 28

4.4 Criteria of an effective ISMS toolkit 28

4.4.1 Documents and Records Management tools 29

4.4.2 Risk Analysis Methodology tools 30

4.4.3 Asset Inventory tools 32

4.5 Difficulties and future work 32

4.6 Conclusion 33

Summary

Secure management of information is becoming critical for any organization because information is one of the most valuable assets in organization's business operations. An Information security management system (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. Consequently, it is difficult to do all tasks in ISMS without any support tools. In this thesis we will try to present an appropriate toolkit identifying software supportable tasks in ISMS life cycle process. This toolkit will become the basis for organizations who wants to implement and maintain their ISMSs.

Chapter 1

1 Introduction

In the present day, information becomes one of the most valuable assets and extremely important in an organization's business operations. Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations). Unsecured management of information may lead to the loss of business, the business's reputation, and also put the organizations' future existence in a dangerous state. Security breaches can be catastrophic for business in every way. Therefore, secure management of information is becoming critical for any organization. For this reason, many organizations have adopted information security management systems (ISMSs) to help them manage their information securely as a mean to protect their business operations. However, due to the complexity is difficult for organizations to have effective ISMSs. ISMSs require involvement of wide range of participants to perform a number of tasks as well as a number of documents. The standards are inadequate to cover every aspect in ISMSs because the standards do not cover all managerial aspects or activities that are need for information security management in the business of organizations. The standards also do not pay enough attention to the cultural differences among organizations. Consequently, implementing and maintaining ISMSs can be quite difficult and burdensome activities without any support tools. These tools have been designed to help organizations keep its information assets secure. All these available tools can create a toolkit which will guide organizations through all elements of the standard, protecting the intellectual property, customer records, financial information, employee details and, mostly importantly of all, the business reputation. For all of the above there is an essential need for organizations to have in their disposal an efficient and useful toolkit which will reduce their effort to create and manage an ISMS.

1.1 What is information?

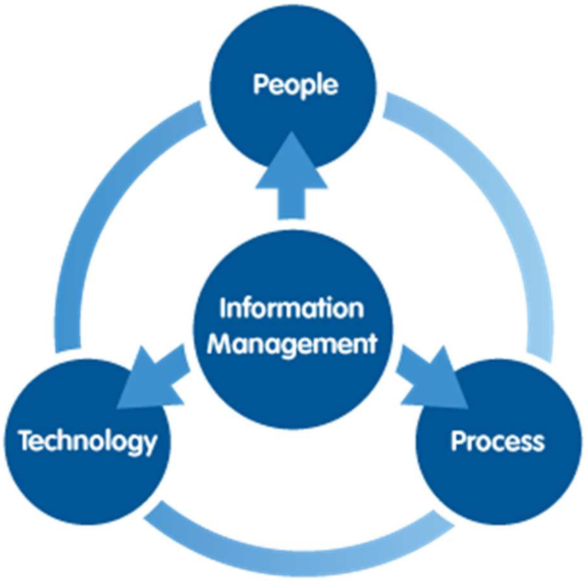
The ancient Greek word for information is πληροφορία, which transliterates (plērophoria) from πλήρης (plērēs) "fully" and φέρω (phorein) frequentative of (pherein) to carry-through. It literally means "fully bears" or "conveys fully". In modern Greek language the word Πληροφορία is still in daily use and has the same meaning as the word information in English. Unfortunately biblical scholars have translated (plērophoria) into "full assurance" creating a connotative meaning of the word. In addition to its primary meaning, the word Πληροφορία as a symbol has deep roots in Aristotle's semiotic triangle. In this regard it can be interpreted to communicate information to the one decoding that specific type of sign. This is something that occurs frequently with the etymology of many words in ancient and modern Greek language where there is a very strong denotative relationship between the signifier, e.g. the word symbol that conveys a specific encoded interpretation, and the signified, e.g. a concept whose meaning the interpretant attempts to decode.

Organizations of all types and sizes (including public and private sector, commercial and non-profit) store, collect, process, and transmit information in many forms including physical, electronic and verbal. The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization’s business and consequently deserve or require protection against various hazards.

Information is a key resource for all organizations, and from the time that information is created to the moment that it is destroyed, technology plays a significant role. Information technology is increasingly advanced and has become pervasive in enterprises and in social, public and business environments. As a result, organizations and their executives strive to maintain high-quality information to support business decisions and embrace the management of information like any other significant part of doing business.

1.2 What is information management?

According to Wikipedia, Information management (IM) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences. This sometimes involves those who have a stake in, or a right to that information. Management means the organization of and control over the structure, processing and delivery of information. Information Management can have many different meanings. Good definitions emphasize that people have information requirements in order to steer processes by using information technology. Information Management is centered around People, Processes and IT.



Sometimes and mostly in information technology field, Information management is closely related to, and overlaps, the management of data. Data is an important resource in an organization. When employees cannot dispose of business data, or when data get lost, these events will seriously disturb business processes. To mitigate damages there should be an integrated approach to data management, consisting of the following elements:

- Compliance
- Control of data and metadata
- Storage
- Back-up & Archiving
- Recovery & Retrieval

Information, as we know it today, includes both electronic and physical information. The organizational structure must be capable of managing this information throughout the information lifecycle regardless of source or format (data, paper documents, electronic documents, audio, social business, video, etc.) for delivery through multiple channels that may include cell phones and web interfaces. Given these criteria, we can then say that the focus of IM is the ability of organizations to capture, manage, preserve, store and deliver the right information to the right people at the right time.

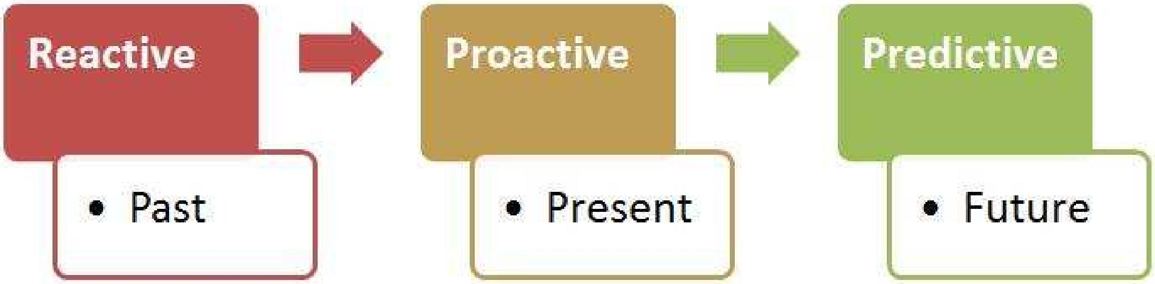
Information management is a corporate responsibility that needs to be addressed and followed from the upper most senior levels of management to the front line worker. Organizations must be held and must hold its employees accountable to capture, manage, store, share, preserve and deliver information appropriately and responsibly. Part of that responsibility lies in training the organization to become familiar with the policies, processes, technologies and best practices in IM.

1.3 The information security and its necessity

Information security includes three main dimensions: confidentiality, availability and integrity. Information security involves the application and management of appropriate security measures that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing impacts of information security incidents. Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets. These controls need to be specified, implemented, monitored, reviewed and improved where necessary, to ensure that the specific information security and business objectives of the organization are met. Relevant information security controls are expected to be seamlessly integrated with an organization’s business processes.

There are three possible approaches to information security: reactive, proactive, and predictive.

Reactive Information Security – approach which is primarily based on post incident detection, analysis, notification, containment, eradication, and remediation. In other words, a system responds to events that have already happened, such as incidents and accidents. Alerts occur at failure, e.g. a customer calls or alerts on application, server, node or when other components are down or don't work properly. It can be noticed by users, monitoring or security tools. In this case reaction is oriented toward past events that already inflicted their effect.



Proactive Information Security – this approach is oriented toward avoiding or opposing threats against computers and networks through understanding the situation, assessing potential impacts, and implementing deterrence based on defensive methodologies. Information security based on this method actively seeks the identification of risky conditions through analysis of organization's processes, systems, networks, applications etc. Alerts occur before failure e.g. some parts of system are in danger of threat or attack. For example, an alert that new virus has been found somewhere in the wild and you need to update definitions on your antivirus software before it reaches your system. One more example would be that a new type of attack is recognized and you need to update your intrusion prevention system with new signatures, or one disk in RAID crashed and you need to replace it, active analyzing of network traffic and host activity to detect early signs of intrusion and cut off or stop suspicious connections or activities before they harm your system, etc. In this case reaction is oriented toward present events that are happening or there is likelihood that it will happen very soon.

Predictive Information Security – is an approach in which you use anticipating and predicting future threats and vulnerabilities based on strategic analysis, threat intelligence, and correlation of disparate datasets to protect the confidentiality, integrity, and availability of data and IT infrastructure. On basic level it analyzes system processes and environment to identify potential future problems. It also alerts that trend on a possible failure. One more step is to design and develop systems which are, at some degree, immune on attacks, intrusions by architecture and design, etc. Furthermore, it can mean implementing self-learning systems which can learn about threats and attacks and protect themselves. In this case reaction is oriented toward anticipated events that could happen in future.

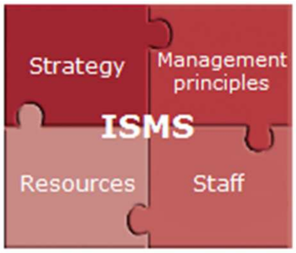
Everyone needs to have a security program because it helps to maintain and focus on IT security. It helps to identify and stay in compliance with the regulations that affect how to manage the data. It keeps organizations on the right footing with their clients and their customers so that they meet both their legal and contractual obligations. Its life cycle process ensures that security is continuously adapting to the organization and the ever-changing IT environment we live in. And, of course, it’s the right thing to do because protecting the data’s security is the same as protecting your most important asset.

Chapter 2

2 Information Security Management Systems (ISMS)

An information security management system (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security program to achieve business objectives. It is based upon risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analyzing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS:

a. Awareness of the need for information security.
b. Assignment of responsibility for information security.
c. Incorporating management commitment and the interests of stakeholders.
d. Enhancing societal values.
e. Risk assessments determining appropriate controls to reach acceptable levels of risk.
f. Security incorporated as an essential element of information networks and systems.
g. Active prevention and detection of information security incidents.
h. Ensuring a comprehensive approach to information security management and
i. Continual reassessment of information security and making of modifications as appropriate.



2.1 Why ISMS is needed?

Risks associated with an organization's information asset need to be addressed. Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the organization. The adoption of an ISMS is expected to be strategic decisions for an organization and it is necessary that this decision is seamlessly integrated, scaled and updated in accordance with the needs of the organization. The design and implementation of an organization's ISMS is influenced by the need and objectives of the organizations, security requirements, the business processes employed and the size and structures of the organization. The design and operation of an ISMS needs to reflect the interests and information security requirement of all of the organization's stakeholders including customers, suppliers, business partners, shareholders and other relevant third parties.

In an interconnected world, information and related processes, systems, and networks constitute critical business assets. Organizations and their information systems and networks face security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire and flood. Damage to information systems and networks caused by malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated. The interconnection of public and private networks and the sharing of information assets increases the difficulty of controlling access to and handling of information. When organizations adopt the ISMS family of standards the ability to apply consistent and mutually-recognizable information security principles can be demonstrated to business partners and other interested parties.

In summary we can say that the successful adoption of an ISMS is important to protect information assets allowing an organization to achieve greater assurance that its information assets are adequately protected against threats on a continual basis and also to maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness. Finally a successful ISMS can help an organization to continually improve its control environment and effectively achieve legal and regulatory compliance.

2.2 Information Security Management System Frameworks and Standards

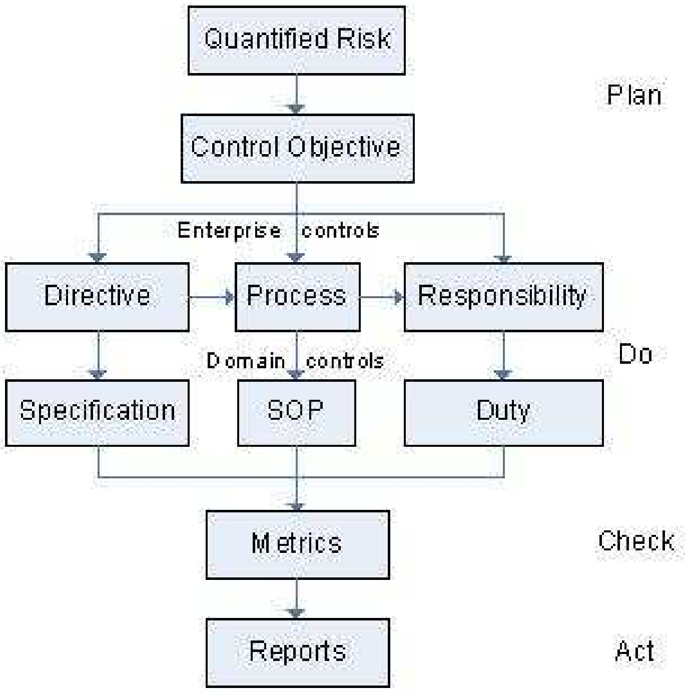
As with all management processes, an ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment. Rapid technological development raises new security concerns for organizations. The existing security measures and requirements become obsolete as new vulnerabilities arise with the development in technology. To overcome this issue, the ISMS should organize and manage dynamically changing requirements and keep the system up-to-date.

Several professional associations focused on IT Governance have tried to design and create frameworks in which organizations can be consulted in order to define their information management system. Most of those associations are dedicated to investigating, clarifying and resolving key issues in information security, and developing best practice methodologies, processes and solutions that meet the business needs of its members. In this section we will present some ISMS standards concluding to the most completely which can be adjusted more easily and efficiently not only in small and medium organizations but also in big ones. Bellow we will present the most known frameworks/standards with a brief description.

The widely known and for the majority of the participants in information technology community the best standard, is the family of ISO 27000 and especially the ISO/IEC 27001 which is the best-known standard in the family providing requirements for an information security management system (ISMS). ISO/IEC 27001 is a risk-based information security standard, which means that organizations need to have a risk management process in place. The risk management process fits into the PDCA model but in latest years there is the flexibility to use and other management process approaches, like Six Sigma’s DMAIC

As we already said, an ISMS is typically risk based, and process oriented. There may be multiple layers of abstraction to accommodate the distinct audiences whose concerns must be addressed. The Plan-Do-Check-Act (PDCA) process-based approach defined as:

- **Plan**: Establish the ISMS
    - Understand the environment
    - Assess enterprise risk
    - Charter information security program
    - Assess program risk
- **Do**: Implement and operate the ISMS
    - Create enterprise information security baseline
    - Create domain specific implementations
- **Check**: Monitor and review the ISMS
    - Assess operational risk
- **Act**: Maintain and improve the ISMS
    - Measure and monitor

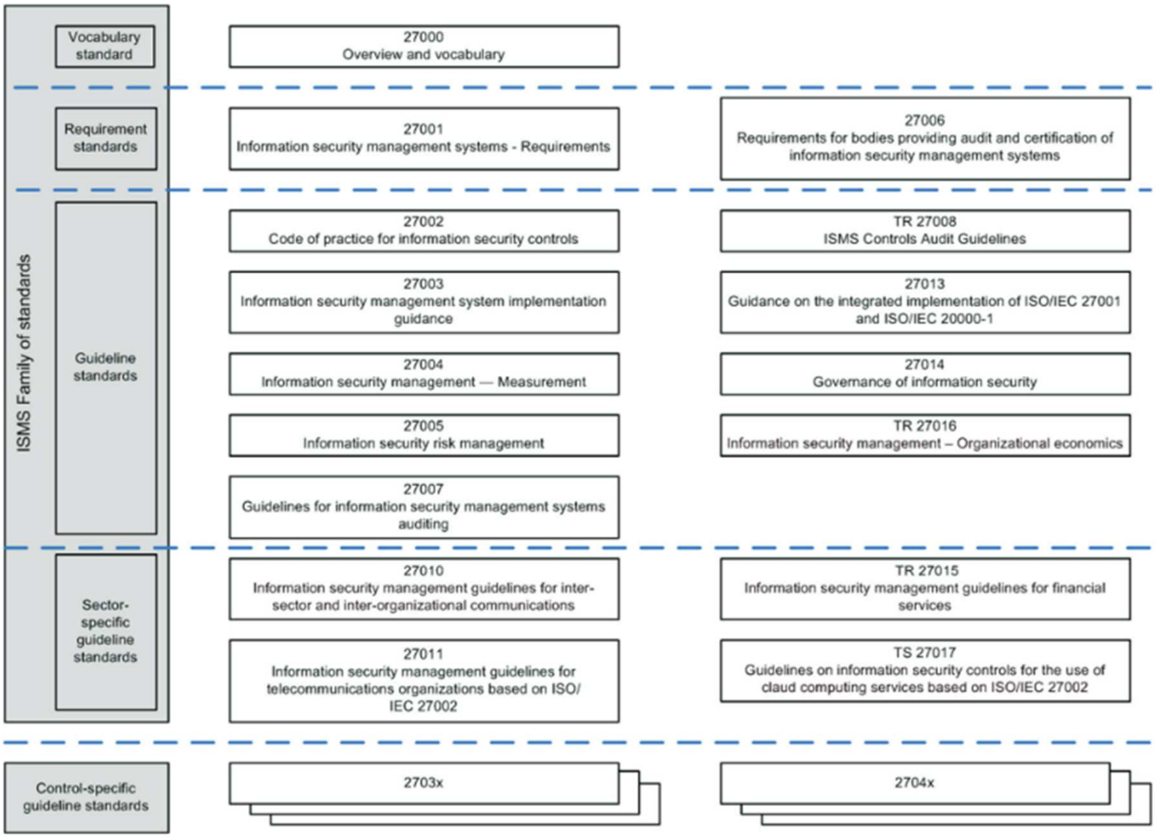


Another competing ISMS is Information Security Forum's **Standard of Good Practice (SOGP)**. It is a best practice-based as it comes from ISF's industry experiences. Some best-known ISMSs for computer security certification are the **Common Criteria (CC) international standard** and its predecessors **Information Technology Security Evaluation Criteria (ITSEC)** and **Trusted Computer System Evaluation Criteria (TCSEC)**. Some nations publish and use their own ISMS standards, e.g. the **Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP)** of USA, the **Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)** of USA, the **German IT baseline protection**, **ISMS of Japan**, **ISMS of Korea**, **Information Security Check Service (ISCS)** of Korea. Other frameworks such as **COBIT** and **ITIL** touch on security issues, but are mainly geared toward creating a governance framework for information and IT more generally. COBIT has a companion framework Risk IT dedicated to Information security.

Chapter 3

3 ISO 27000 Standard Family

The ISMS family of standards consists of inter-related standards, already published or under development, and contains a number of significant structural components. These components are focused upon normative standards describing ISMS requirements (ISO/IEC 27001) and certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001. Other standards provide guidance for various aspects of an ISMS implementation, addressing a generic process, control-related guidelines as well as sector-specific guidance. Relationships between the ISMS family of standards are the following


ISMS Family of standards
Vocabulary standard
27000 Overview and vocabulary
Requirement standards
27001 Information security management systems - Requirements
27006 Requirements for bodies providing audit and certification of information security management systems
Guideline standards
27002 Code of practice for information security controls
TR 27008 ISMS Controls Audit Guidelines
27003 Information security management system implementation guidance
27013 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
27004 Information security management — Measurement
27014 Governance of information security
27005 Information security risk management
TR 27016 Information security management – Organizational economics
27007 Guidelines for information security management systems auditing
Sector-specific guideline standards
27010 Information security management guidelines for inter-sector and inter-organizational communications
TR 27015 Information security management guidelines for financial services
27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
TS 27017 Guidelines on information security controls for the use of claud computing services based on ISO/IEC 27002
Control-specific guideline standards
2703x
2704x

As we can see on the above table, the applicable clauses are:

1. Standards describing an overview and terminology
2. Standards specifying requirements
3. Standards describing general guidelines
4. Standards describing sector-specific guidelines

All kind of organizations has identified and admitted that Information Security can improve the profitability of the company. Management teams have been convinced that the implementation of an ISMS is an integral part of their business plan. So the most important benefits of ISO 27000 are:

Compliance: It might seem odd to list this as the first benefit, but it often shows the quickest "return on investment" – if an organization must comply to various regulations regarding data protection, privacy and IT governance (particularly if it is a financial, health or government organization), then ISO 27000 series can bring in the methodology which enables to do it in the most efficient way.

Marketing Edge: In a market which is more and more competitive, it is sometimes very difficult to find something that will differentiate you in the eyes of your customers. ISO 27000 series could be indeed a unique selling point, especially if you handle clients' sensitive information.

Lowering the expenses: Information security is usually considered as a cost with no obvious financial gain. However, there is financial gain if you lower your expenses caused by incidents. You probably do have interruption in service, or occasional data leakage, or disgruntled employees.

Organizing the business processes: This one is probably the most underrated – if you are a company which has been growing sharply for the last few years, you might experience problems like – who has to decide what, who is responsible for certain information assets, who has to authorize access to information systems etc. ISO 27000 series is particularly good in sorting these things out – it will force you to define very precisely both the responsibilities and duties, and therefore strengthen your internal organization.

The following ISO/IEC 27000-series information security standards are either published or currently being developed:

Standard	Published	Title	Notes
ISO/IEC 27000	2014	Information security management systems - Overview and vocabulary	Overview/introduction to the ISO27k standards as a whole plus the specialist vocabulary; FREE!
ISO/IEC 27001	2013	Information security management systems — Requirements	Formally specifies an ISMS against which thousands of organizations have been certified compliant
ISO/IEC 27002	2013	Code of practice for information security controls	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls
ISO/IEC 27003	2010	Information security management system implementation guidance	Basic advice on implementing ISO27k
ISO/IEC 27004	2009	Information security management — Measurement	Basic (and frankly rather poor) advice on information security metrics
ISO/IEC 27005	2011	Information security risk management	Discusses risk management principles; does not specify particular methods for risk analysis etc.
ISO/IEC 27006	2011	Requirements for bodies providing audit and certification of information security management	Formal guidance for the certification bodies

Standard	Published	Title	Notes
		systems	
ISO/IEC 27007	2011	Guidelines for information security management systems auditing	Auditing the management system elements of the ISMS
ISO/IEC TR 27008	2011	Guidelines for auditors on information security management systems controls	Auditing the information security elements of the ISMS
ISO/IEC 27009	DRAFT	Application of ISO/IEC 27001 - requirements	Sector- or service-specific certifications (possibly)
ISO/IEC 27010	2012	Information security management for inter-sector and inter-organisational communications	Sharing information on information security between industry sectors and/or nations, particularly those affecting “critical infrastructure”
ISO/IEC 27011	2008	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Information security controls for the telecoms industry; also called “ITU-T Recommendation x.1051”
ISO/IEC 27013	2012	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Combining ISO27k/ISMS with IT Service Management/ITIL
ISO/IEC 27014	2013	Governance of information security	Governance in the context of information security; will also be called “ITU-T Recommendation

Standard	Published	Title	Notes
			X.1054”
ISO/IEC 27015	2012	Information security management guidelines for financial services	Applying ISO27k in the finance industry
ISO/IEC TR 27016	2014	Information security management – Organizational economics	Economics applied to information security
ISO/IEC 27017	DRAFT	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	Information security controls for cloud computing
ISO/IEC 27018	DRAFT	Code of practice for controls to protect personally identifiable information processed in public cloud computing services	Privacy controls for cloud computing
ISO/IEC TR 27019	2013	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry	Information security for ICS/SCADA/embedded systems (not just used in the energy industry!)
ISO/IEC 27031	2011	Guidelines for information and communications technology readiness for business continuity	Continuity (i.e. resilience, incident management and disaster recovery) for ICT, supporting general business continuity

Standard	Published	Title	Notes
ISO/IEC 27032	2012	Guidelines for cybersecurity	Despite the curious title, it is actually about Internet security
ISO/IEC 27033	-1 2009	Network security overview and concepts	Various aspects of network security; gradually updating and replacing ISO/IEC 18028
	-2 2012	Guidelines for the design and implementation of network security	
	-3 2010	Reference networking scenarios - threats, design techniques and control issues	
	-4 2014	Securing communications between networks using security gateways	
	-5 2013	Securing communications across networks using Virtual Private Networks (VPNs)	
	-6 DRAFT	Securing IP network access using wireless	
ISO/IEC 27034	-1 2011	Application security — Overview and concepts	Multi-part application security standard
	-2 DRAFT	Organization normative framework	
	-3 DRAFT	Application security management process	

Standard	Published	Title	Notes
	-4 DRAFT	Application security validation	
	-5 DRAFT	Protocols and application security control data structure	
	-6 DRAFT	Security guidance for specific applications	
	-7 DRAFT	Application security control attribute predictability	
	-8 DRAFT	Protocols and application security controls data structure – XML schemas	
ISO/IEC 27035	2011	Information security incident management	Replaced ISO TR 18044; now being split into three parts
ISO/IEC 27036	-1 DRAFT	Information security for supplier relationships – Overview and concepts	Information security aspects of ICT outsourcing and services
	-2 DRAFT	Information security for supplier relationships – Common requirements	
	-3 2013	Information security for supplier relationships – Guidelines for ICT supply chain security	
	-4 DRAFT	Information security for supplier relationships –	

Standard	Published	Title	Notes
		Guidelines for security of cloud services	
ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition, and preservation of digital evidence	First of several IT forensics standards
ISO/IEC 27038	2014	Specification for digital redaction	Redaction of digital documents
ISO/IEC 27039	DRAFT	Selection, deployment and operations of Intrusion Detection [and Prevention] Systems (IDPS)	IDS/IPS
ISO/IEC 27040	DRAFT	Storage security	IT security for stored data
ISO/IEC 27041	DRAFT	Guidelines for assurance for digital evidence investigation methods	Assurance is critically important for all forms of forensics: the courts demand it
ISO/IEC 27042	DRAFT	Guidelines for the analysis and interpretation of digital evidence	IT forensics analytical methods
ISO/IEC 27043	DRAFT	Digital evidence investigation principles and processes	The basic principles of IT forensics investigations
ISO/IEC 27044	DRAFT	Guidelines for security information and event management (SIEM)	SIEM

Standard	Published	Title	Notes
ISO 27799	2008	Health informatics — Information security management in health using ISO/IEC 27002	Developed by a different committee; tailored advice for the healthcare industry

3.1 ISO/IEC 27001:2013 Standard

ISO 27001:2013 is an information security standard that was published on the 25th September 2013. It supersedes ISO/IEC 27001:2005, and is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27. It is a specification for an information security management system (ISMS). ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature. This international standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirement.

ISO/IEC 27001 is designed to be used for certification purposes. Once organizations have established an ISMS that meets ISO's requirements and deals with organization's unique risks, they can ask a registrar (certification body) to audit the system. If pass the audit, the registrar will issue an official certificate that states that the ISMS meets the ISO/IEC 27001:2013 requirements. While ISO IEC 27001:2013 is specifically designed to be used for certification purposes, organizations don't have to become certified. They can be in compliance without being formally registered by an accredited certification body.

3.1.1 ISO 27001:2013 structure

ISO/IEC 27001:2013 is an information security management standard which defines a set of information security management requirements. These requirements can be found in the following seven sections:

- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

This structure mirrors the structure of other new management standards such as ISO 22301 (business continuity management). This helps organizations who aim to comply with multiple standards, to improve their IT from different perspectives.

As we have seen and According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system". ISO 27001 uses a topdown, risk-based approach and is technology-neutral. The specification defines a six-part planning process:

I. Define a security policy.
II. Define the scope of the ISMS.
III. Conduct a risk assessment.
IV. Manage identified risks.
V. Select control objectives and controls to be implemented.
VI. Prepare a statement of applicability.

In the 2013 version of ISO 27001, the changes to which it was subjected, project not only the integration with others standards for the implementation of several managements systems to speak the same structural languages, but also provides for the adoption to new technology trends, allowing the implementation of guidelines and requirements in line with reality technology and business. This new structure of ISO 27001, involves challenges, changes and variations in how the Organizations should address it, because companies that are certified under the 2005 version, have a period of time (usually two years) to upgrade to the new version (2013), where the impact can be reduced because you can see the development of internal audits to detect respective differences and changes, to establish and develop actions aimed at achieving the requirements defined in the new version of the standard.

3.1.2 Comparison of ISO 27001:2005 and ISO 27001:2013

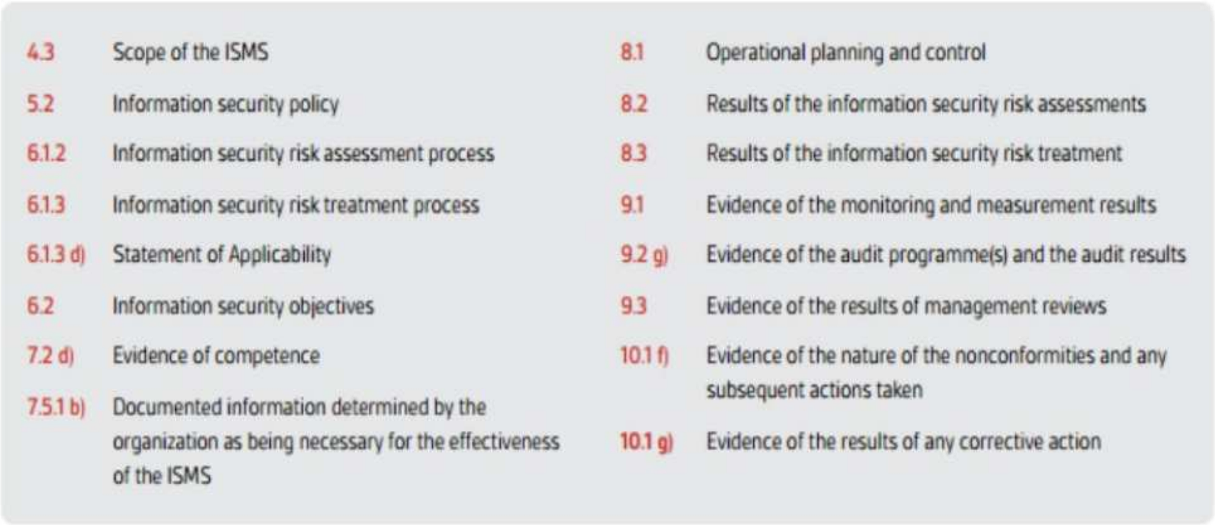
As we have noticed in previous sections, due to the huge changes to the ecosystem which organizations are developed, generated the need of a revision of the old ISO/IEC 27001:2005 to the new ISO/IEC 27001:2013. The generic changes are that the new standard puts more emphasis on measuring and evaluating how well an organization's ISMS is performing. It does not emphasize to Plan-Do-Check-Act cycle and has been added a new section of outsourcing, a process which was absent in previous years. More attention is paid to the organizational context of information security and also there are some changes at Risk assessment process. Finally it is designed to fit better alongside other management standards such as ISO 9000 and ISO 20000, and share many common features with them.

Annexes B and C of 27001:2005 have been removed and the following controls have been added Annex A

- A.6.1.5 Information security in project management
- A.12.6.2 Restrictions on software installation
- A.14.2.1 Secure development policy
- A.14.2.5 Secure system engineering principles
- A.14.2.6 Secure development environment
- A.14.2.8 System security testing
- A.15.1.1 Information security policy for supplier relationships

- A.15.1.3 Information and communication technology supply chain
- A.17.1.3 Verify, review and evaluate information security
- A.17.2.1 Availability of information processing facilities

In the next table we can see in which clauses we need documented information



4.3	Scope of the ISMS	8.1	Operational planning and control
5.2	Information security policy	8.2	Results of the information security risk assessments
6.1.2	Information security risk assessment process	8.3	Results of the information security risk treatment
6.1.3	Information security risk treatment process	9.1	Evidence of the monitoring and measurement results
6.1.3 d)	Statement of Applicability	9.2 g)	Evidence of the audit programme(s) and the audit results
6.2	Information security objectives	9.3	Evidence of the results of management reviews
7.2 d)	Evidence of competence	10.1 f)	Evidence of the nature of the nonconformities and any subsequent actions taken
7.5.1 b)	Documented information determined by the organization as being necessary for the effectiveness of the ISMS	10.1 g)	Evidence of the results of any corrective action

Chapter 4

4 The need of ISMS toolkit

Often, information protection decisions are made in an ad hoc manner, based on the IT department's prior experience with vulnerabilities and the threats that they currently know about. Thus, risks tend not to be systematically managed or are managed by the wrong people. Most current approaches to information-security risk management tend to be incomplete, expert-driven, or both. Most approaches fail to include all the components of information security risk (assets, threats, and vulnerabilities). In these cases, the organization has insufficient data to fully match a protection strategy to its security risks. Many organizations outsource information security risk assessments because they do not have in-house capability to perform this vital service. They hire experts to perform risk assessments, and the resulting assessment is only as good as the experts who perform it. Often the consumers of such services have no way to understand if the risk assessment performed for them is adequate for their enterprise. This led to the attempt to create a toolkit, identifying some of the most useful tools that could cover the majority of main and not only task, in order to implement an efficient ISMS.

4.1 Building an ISMS and finding supporting tools

The first step is to design an ISMS. In this step we have to select the framework within which the ISMS will function (e.g. iso 27001). The framework will depend on the type of industry or the need to go for certification. Building an ISMS involves also many steps. While performing each step, inputs from all the stakeholders should be included and results discussed to reach an agreed upon path. A security manual serves as the central repository for ISMS. This manual will be maintained by the Chief security officer and usually considered a confidential document.

In this section we have divided the building process in to six high level steps. With this method will be easier for someone to find the appropriate tool for each step. These steps are:

1. **Risk Assessment**: The goal is to identify assets, threats, vulnerabilities and controls to mitigate risks. Some risks will be accepted and management approval should be attained on this.
2. **Top down approach**: Security is a management issue and not just an IT issue. Hence it is critical that top management plays an important role in building an ISMS. Management should have the overall ownership of ISMS. Management should encourage a culture within the enterprise to follow security principles.
3. **Functional Roles**: Once management's approval is attained, functional roles will have to be identified. Depending on the type and size of the enterprise, the roles can vary in type and number. A chief information security officer should be identified who solely owns the ISMS. Other functional roles could include Data stewards, Security awareness trainers etc.
4. **Write the policy**: The security policy is a document that states the enterprise's information security strategy at a high level. The language in the policy is derived from the risk assessment. Details should be avoided in a policy. In order to make the policy acceptable to all stakeholders, the wording in the policy should be at a high level and align nicely with the enterprise's business priorities and goals.
5. **Write the standards**: Standards are definite requirements that an enterprise should put forth for everybody to follow. The standards should support the security policy and be measurable. It is good practice to document what the penalties are when standards are not met.
6. **Write the guidelines and procedures:** Guidelines are recommended ideas for an enterprise. They can also be termed as 'nice to haves'. It should be noted that the effectiveness of an enterprise's security management will not be measured by the guidelines present. There, usually, are no penalties for not following the guidelines. However, there can be some incentives if the enterprise follows the guidelines.

   Procedures are step by step description on how to meet the standards or guidelines so that the policy is supported. Procedures are usually targeted at the system level people who actually implement the control.

4.2 Previous related researches

The first thing that we have already noticed from the initial of this thesis, is the difficulty to collect all the factors in order to have an effective ISMS. ISMS is a complex management system that requires involvement of wide range of participants to perform a number of tasks as well as a number of documents. Thus many researchers have tried to approach this aspect analyzing as much as possible every factor in order to create a useful methodology for any to be concerned to perform appropriate actions for an ISMS.

One of these works that it's worth to be noticed, is a publication from Saitama University with the title << AN ANALYSIS OF SOFTWARE SUPPORTABLE TASKS IN INFORMATION SECURITY MANAGEMENT SYSTEM LIFE CYCLE PROCESSES >>. In this publication the authors have tried to make an analysis identifying the participants and generally all the task related with ISMS and can be supported by software tools. Some other similar works do not cover all tasks in ISMS life cycle process in detail and do not consider participants who are important to perform the tasks.

ISMS requires special focus and participation from all levels of participants. The involvement of participants in ISMSs are based on different responsibilities. The authors have been identified 10 kinds of participants with their responsibilities. These are:

- Management
- Information Security Committee
- Chief Information Security Officer (CISO)
- Project Management Office
- Information Security Managers
- Security training team
- Information Asset Owners
- Internal Auditors
- Employees
- Certification body

One other main task in ISMS life cycle processes are the documents. The documents sets out how the ISMS should works and which records the evidence that it has worked and achieved its goals. According to the publications ISMS documents can be classified into 4 classes: policies, standards, procedures and records. Based on the PDCA model, they elaborated ISMS life cycle processes into 7 phases: preparation, establishment, implementation and operation, monitor and review, improvement and optimization, certification, and abolishment. On each phase, there are a number of processes that organizations have to perform. Each process in ISMS consists of a set of various tasks. The final conclusion of the research showed that there are 10 kinds of participants, 20 documents, 7 phases, 41 processes, and 111 tasks. 77 from 111 tasks in ISMS life cycle processes can be supported by software tools. The software supportable tasks can be summarized as follows:

- Documentation of ISMS policy, information security policies, and procedures.
- Memorization of risk assessment method, assets classification, threats and vulnerabilities identification, and controls selection tasks.
- Calculation to estimate risk level.
- Documentation of security controls objectives and controls, SoA, and RTP.
- Visualization of implemented controls, operations, and available resources.
- Documentation of procedures to manage operation and resource.
- Documentation of procedures to take action in security incident.
- Documentation of reports and logs of security incidents.
- Documentation of monitoring procedures.
- Calculation to measure effectiveness of controls.
- Documentation of audit procedure and records.
- Documentation of records of management review.
- Documentation of corrective and preventive procedures and records.
- Visualization of ISMS certification status.

4.3 Creation of an ISMS toolkit

On this thesis we do not try to present which of the available tools is better. In my opinion this very difficult without knowing more about the organization in terms of its maturity in risk analysis and information security management, its size and complexity, industry, ISMS status and so forth. The way in which we can choose the appropriate tools for each case is an objective of another research. The answer in questions “What do you expect the method or tool to achieve for you? Which factors and/or features are most important?” and so on, is the beginning of a new research. To this point it will be useful the usage of ISO 27005 standard.

4.4 Criteria of an effective ISMS toolkit

On this work we will present some tools and we will compose a toolkit which will be available to any organization for use in order to design their ISMS. After investigation of the whole process of ISMS and having into consideration the summarized results of the aforementioned publication on 4.2 chapter we concluded that in a higher level the tools which will compose the integrated toolkit will be divided in two categories. These are:

- Documents and Records Management
- Risk Assessment Methodology

The risk assessment methodology now can be divided in also two subcategory tools which can be used supportive to the whole Risk assessment process. The penetration testing and vulnerability assessment is the first supportive subcategory and asset inventory is the second one. Both of them are necessary in order to have an accurate Risk assessment.

According to the above criteria and categorization we will elaborate the tools that we believe are suitable for an effective ISMS toolkit. The way that we conducted the selection of the tools was done based on some common parameters. First and most significant was the used tools will be open source. Our vision is the utilization of open source tools at least at the main core, where everyone who is interested to develop and extend the existing tool can have the ability to do it.

One other criteria we set as prerequisite was the tools will be supported and updated. It’s very important for the users who in the majority are not security experts, to have the support of the community and from related user guide documents. Regarding the update is also important for them to know that the tool they use is compliant with the latest version of international and other standards.

The adjustment to any kind of organization, independently of the size and the operation, is one more thing that we considered during the assessment of the tools we selected.

Last but not least is the usability and the features that provided from the tool. All organizations are willing to use software that are compatible with their existing infrastructure. It is very important to have a tool that can be communicate with the organization’s infrastructure and retrieve data from them. A nice example on this is some tools is the ability to communicate with the ldap data base and grant permissions directly from them. With this way, the organization deplete from extra effort.

4.4.1 Documents and Records Management tools

The most available toolkits existing in the market and used from the majority of the organizations, usually are referred as Documentation Toolkits. The reason is why in the most known standards, is mandatory to have documented the ISMS in order to be certified. These toolkits provide templates for every required document. Some of those are templates for Procedure for Control of Documents, Information Security Policy, ISMS Scope Document, Risk Assessment Methodology, Risk Assessment Matrix, Security Risk Assessment template, Risk Treatment Plan, Statement of Applicability, Incident Management Policy, Business Impact Analysis Questionnaire, Business Continuity Plan template, Incident Response Plan, Acceptable Use Policy template, Network Security Policy template, Access Control Policy template, Backup Policy, and many others.

There are several commercial and open source documentation toolkits. For academic purposes and after investigation we concluded to the **Eramba.** Eramba is an open-source enterprise class IT Governance, Risk & Compliance application. Some of the features of Eramba are:

Simplify & Centralize Governance, Compliance Management, Risk Management, Exception Management, Business reports & Dashboards, Audit Management, Project management, Role based awareness, Security control catalogues, Business continuity management, Workflows, ISO 27001, Security policies, Incident Management.

In other words this tool gives the opportunity to create and manage any kind of needed document for an ISMS. Regarding to Controls and Audits, it helps to document all your controls, their costs, policies, etc. It define an audit schedule for each control and get notified when audits are about to come. Also it helps to record improvement projects.

Now regarding the policy management, Eramba helps to document all the policies. Link policies to controls, risks and compliance items and send notifications when policy reviews are required. Finally it publish policies on an automated access controlled portal to be available to any concerned user.

For more info you can visit the website http://www.eramba.org/

4.4.2 Risk Analysis Methodology tools

At the same mode with the previous paragraph, we will try to expose the most known risk analysis and assessment methodologies which are supported by software tools. International Standards do not specify any specific method, giving you the flexibility to select a method, or more likely several methods and/or tools, that suit your organization’s requirements. Bellow we will list two open source tools but have in mind that there also many valuable commercial products.

The tools that we decided to present after an extensive investigation of their attributes and features are:

OCTAVE: The OCTAVE method is an approach used to assess an organization's information security needs. OCTAVE methods are self-directed, flexible, and evolved. Using OCTAVE, small teams across business units and IT work together to address the security needs of the organization. The method can be tailored to the organization's unique risk environment, security and resilience objectives, and skill level. OCTAVE Allegro focuses on information assets. An organization's important assets are identified and assessed based on the information assets to which they are connected. This process eliminates potential confusion about scope and reduces the possibility that extensive data gathering and analysis are performed for assets that are poorly defined, outside of the scope of the assessment, or in need of further decomposition. It is well suited for those who want to perform risk assessment without extensive organizational involvement, expertise, or input.

VERINICE: Verinice is a tool for managing information security. The software comes without license or subscription costs and is provided under the GPLv3 license. Organizations can use it for establishing, maintaining and improving an ISMS based on ISO 27001. Verinice lets the organization to execute a full risk analysis of its information assets and derive further actions from the results. Add threats and vulnerabilities from various existing sources such as a vulnerability scanner or penetration test. Use the results in the risk analysis and automatically perform a risk assessment for all assets. Also Verinice can be used for auditing, document management and report generation. Finally, one of the biggest advantage of this tool is that it gives the possibility to maintain the processes and information assets. An asset register within the meaning of the ISO 27001 (Inventory of Assets) can be exported at the push of a button.

If the organization has decided that will be moved according to the ISO 27001 in order to construct its ISMS, Verinice is the tailor made tool. If the requirements of the organization are in normal state, Verinice we can say that from its own can be an integrated toolkit. It covers with high accuracy the above criteria of an effective ISMS toolkit. Risk assessment, asset register and documentation management are some of the embedded functions of this tool. Despite the fact that it can use its own functions, Verinice has also the ability to receive data like results from penetration testing and vulnerability scanner tools in compatible formats and import them to its functions, exporting the respective reports and charts. The tool is published as open source software, uses open standards and provides numerous interfaces itself. Additionally the user friendly environment with the simple attributes, makes Verinice easy enough for individuals and experts who are interested in creating an ISMS.

Finally Verinice can execute a risk treatment process mapping to the controls of ISO 27001 and ISO 27002 and connect these controls with other inputs.

4.4.3 Asset Inventory tools

Apart from the tools that can have the asset inventory process as an embedded feature like Verinice we have already seen, there are also dedicated tools for the inventory of the assets. The results of these tools can be exported in compatible format, in order to be used by other tools during the risk assessment process. This action shall be conducted in prior of the execution of risk assessment and analysis. At the same line with the previous presentations we also list some open source tools.

Open-AudIT: Open-AudIT intelligently scans an organization’s network and stores the configurations of the discovered devices. A powerful reporting framework enables information such as software licensing, configuration changes, non-authorized devices, capacity utilization and hardware warranty status to be extracted and explored.

SpiceWorks: Get a full and accurate scan of all network devices including Windows, Mac, and Linux machines. It can also discover routers and switches, printers, even VoIP devices. Spiceworks virtualization management software makes it easy to discover hardware and VM hypervisors, view hardware configs, get detailed info, and find virtual machines through your network inventory. Automatically retrieve up-to-date information from a single device to your entire network. Create your own attributes for anything you choose and get troubleshooting tools to compare what’s working and what isn’t.

4.5 Difficulties and future work

The difficulties that we faced during the construction of ISMS toolkit was several and distributed in different areas. Firstly the requirement for open source products made our work more difficult. The open source tools that the reliable organizations can use and worth to be referred are limited.

The most under certification standards are commercial products targeting organizations that are willing to pay. For this reason the most of the tools are available under licensing.

One other main issue is the difficulty to create an integrated toolkit collecting different tools for each process. Most of the tools, utilize features where sometimes overlap the attributes and features from each other. For example some risk assessment methodologies can execute also asset inventory and documentation management but also there are standalone tools for the same scope. On the other hand is risky for us to propose the combination and comparison of the different tools because there is the danger to conclude in big deviations on the results. In this case there may be major troubles. This could be happen due to the methodologies have been designed based on the subjectivity and many times it doesn't reflect to the strict parameters of mathematics and probabilistic models. Thus the human factor is another one issue we have to overcome.

At the end, we must repeat that on account of the diversity of the organizations on size and culture, is difficult to distinct and define responsibilities of each participant; a process which is mandatory during the creation of an Information Security Management System.

To sum up, as a future work it will be good the development of a software tool which will include the most common and qualified tools for the processes of Risk assessment, Documentation management, asset inventory, penetration testing and vulnerability scanning and based on some arguments will result to the appropriate tools. A well designed algorithm will take into account the arguments like size and business scope additionally with the desire of the user for a commercial or an open source tool and will suggest the most suitable tool composing a toolkit.

4.6 Conclusion

Summarizing and for the purpose of this work we recognized that is not fair to conclude in a fix toolkit where organizations can build their ISMS. For the aforementioned tools we could say with prejudice that Verinice could cover the majority of ISMS task. Complementary with the ability to import data from other tools, it strengthens our valuation to say that this is the most completely and decent tool to create an ISMS.

In conclusion we have to say that the design and creation of an ISMS is not so easy in order to be supported from some tools. There is a whole industry behind the standardization and expert consultants with expertise in different areas, that certainly every organization have to consult before begin its own ISMS.

Bibliography

- International Organization for Standardization. (2014). ISO/IEC 27000: Information technology – Security Techniques – Information Security Management Systems – Overview and vocabulary.
- International Organization for Standardization. (2013). ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management Systems – Requirements.
- International Organization for Standardization. (2013). ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Management.
- International Organization for Standardization. (2011). ISO/IEC 27005: Information Technology – Security Techniques – Information security risk management.
- ISO 27001 Security. The FREE ISO27k toolkit. Retrieved from http://www.iso27001security.com
- Ahmad Iqbal Hakim Suhaimi, Yuichi Goto, and Jingde Cheng - AN ANALYSIS OF SOFTWARE SUPPORTABLE TASKS IN INFORMATION SECURITY MANAGEMENT SYSTEM LIFE CYCLE PROCESSES
- Verinice tool for managing information security. Retrieved from http://verinice.org/en/
- https://en.wikipedia.org/wiki/ISO/IEC_27000
- Eramba open-source enterprise class IT Governance, Risk & Compliance application. Retrieved from http://www.eramba.org/
- Octave Alegro Risk assessment methodology. Retrieved from www.cert.org
- Open Audit network inventory tool. Retrieved from http://www.open-audit.org/
- Spiceworks network inventory tool. Retrieved from http://www.spiceworks.com/