International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special Issue 11 (Nov-Dec 2014), PP. 22-24

EVALUATION AND COMPARISON OF COBIT, ITIL AND ISO27K1/2 STANDARDS WITHIN THE FRAMEWORK OF INFORMATION SECURITY

Yavuz Ozdemir, Huseyin Basligil, Pelin Alcan, Bahadir Murat Kandemirli
Industrial Engineering Dept.,
Yildiz Technical University,
Istanbul, Turkey
ozdemiry@yildiz.edu.tr, basligil@yildiz.edu.tr, palcan@yildiz.edu.tr, muratkandemirli@gmail.com

Abstract— **Information, like other economic assets, is a precious asset for an enterprise so it must be properly protected. The basic solution to protect is to provide "information security". To understand information technology security, it is fundamental to understand the importance of IT management and governance concepts. In this study, the most widely practised and popular information technology security, management and governance standards, ISO 27001 standard, COBIT (Control Objectives for Information Technology) and ITIL (Information Technologies Infrastructure Library), will be investigated and compared.**

Index Terms— **Information Security Management System (ISMS), Information Technologies Management Systems (ITMS), ISO/IEC 27001, ISO/IEC 27002, CobIT, ITIL.**

I. Introduction and Literature Review

Although some computer security problems are caused unintentionally by users, some of them are caused by malicious people who wish to cause damage to the system. With the spread of the internet, the number and variety of attacks on computer communications have increased [1]. On the other hand, these attacks drove the development of security solutions such as authentication, authorization and antivirus programs.

In the internet environment, the first substantial damage to information systems was caused by the internet worm developed by Robert Morris. This computer worm emerged in 1988 and caused damage worth $200–5300 to each computer affected. As a result, it abused the trust placed on the internet and had negative impacts on internet users and those considering using it [1, 2, 3]. As a consequence of the substantial damage caused by this computer worm, the Computer Emergency Response Team (CERT) was established in order to intercept such computer attacks and to raise user awareness of attacks and their effects [4]. Despite such mechanisms aimed at protection and prompt intervention, attackers still cause serious damage to information systems.

Many research and development projects have been developed and are still being developed by a great number of institutions and countries in order to take proactive measures against harmful software and attacks and to maintain security in information systems. Antivirus software, firewalls, VPN software/hardware, attack detection and protection systems, content controllers and central management software have all been developed in these projects. Besides these technical solutions, researchers also strive to develop standards and frameworks to ensure safe and secure design and management of information systems [3, 5, 6]. The European Union has allocated 32% of its total budget, amounting to 32,365 million euro, to support research and development projects in the fields of security and information and communication technologies within 7th Framework programmes during 2007–2013 [7].

Management strategies of information technology systems should be determined prior to information security concepts so that an Information Security Management System (ISMS) can be implemented. The objectives of such standards as COBIT (Control Objectives for Information Technology), referred to as Information Technologies Management Systems (ITMS), ISO 20000-1,2 / ITIL (Information Technologies Infrastructure Library) and COSO (Committee of Sponsoring Organizations of the Treadway Commission) include rendering the information technology services accessible to customers at the desired level and maintaining the surveillance, observability, scalability, functionality, efficiency, reliability and continuity of information technology systems. When all the concepts which the standards concerning the information system refer to are taken into consideration, seven basic concepts stand out. These are efficacy, efficiency, confidentiality, integrity, accessibility, compatibility and reliability. Standards provide information about these concepts at different levels. Today, managements generally assist their IT professionals in using and managing the technology during IT processes. ITIL is the most common process in service management applications.

The aforementioned COBIT, ITIL and ISO 27001 standards are the most widely accepted and most frequently used standards throughout the world. However, they may not always be compatible with the structures of all organizations for a variety of reasons. In this paper, ISO 27001, COBIT and ITIL standards will be addressed in terms of their strong aspects, basic focal points and compatibility with ISMS.

The remainder of the paper is organized as follows: Information security and ISMS standards are introduced in Section 2. Section 3 describes information security management systems. Section 4 focuses on information security criteria. Some concluding remarks are made in Section 5.

II. Information Security and ISMS Standards

Information security is defined as protecting the confidentiality, integrity and accessibility of the information. It is impossible to ensure information security during business activities only through technological measures (virus protection, firewall systems and encoding, etc.). Information security should be integrated into processes, and thus it needs to be addressed as a business matter as well as a management and cultural problem.

III. Information Security Management Systems

The objectives of this section are to provide general information concerning ISO 27001, ITIL and COBIT, including structural characteristics of these standards and approaches and their application methodologies, and to explain these concepts in the light of this information.

A. ISO 27001

Figure 1 shows inputs and outputs of the ISO process and the content of this process. This system, called a Plan-Do-Check-Act (PDCA) cycle, also forms the basis of ISO 27001 ISMS standard [8].

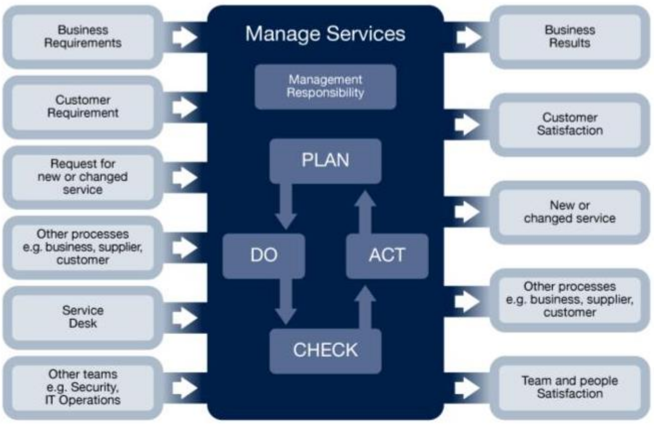
Business Requirements
Customer Requirement
Request for new or changed service
Other processes e.g. business, supplier, customer
Service Desk
Other teams e.g. Security, IT Operations
Manage Services
Management Responsibility
PLAN
DO
ACT
CHECK
Business Results
Customer Satisfaction
New or changed service
Other processes e.g. business, supplier, customer
Team and people Satisfaction

Fig. 1. **PDCA cycle used to revise the processes of ISO 20000 series**

ISO 27000 series security standards constitute a fundamental reference guide in raising the awareness of users, reducing the security risks and determining the measures to be taken when security gaps are encountered.

ISO 27000 is a standard explaining the concepts related to the ISO 27000 family of standards and including basic information concerning information security management. While a majority of ISO 27000 standards are known, some of them are in the press.

B. ITIL

ITIL provides a detailed and structural series of best practice examples in managing information technologies services. ITIL allows for a sound communication between client, supplier, IT department and users owing to its process approach. ITIL is a process and method library where IT infrastructure and service processes are explained and standards are defined considering the available best practice examples. ITIL puts forward appropriate processes and methods in order to provide IT services as a whole at maximum quality, order and continuity, to ensure maximum harmonization between IT services and business targets of institutions and to meet customer expectations at the highest level possible. We can list the reasons for worldwide acceptance of ITIL as a standard as follows (OGC, 2001) [9, 10]:

- It is available for public use
- It consists of best practices
- It is a de facto standard
- It presents a quality approach

Information security management is a process or function that raises awareness and takes into consideration the information security risks in the background for each step of a successful IT service management system within ITIL [10].

While ISO standards investigate the supporting guidelines, procedures, processes, improvements and requirements necessary for effective and successful ISMS in depth with all headings, ITIL does not address most of these headings in depth.

C. COBIT

COBIT is a framework for information technologies risk management created by the Information Systems Audit and Control Association & Foundation (ISACA) and the IT Governance Institute (ITGI). COBIT provides generally-accepted information technologies control target sets in order to increase the benefits of using information technologies as well as developing and controlling appropriate governance for information technologies for information technologies managers, auditors and users. COBIT is composed of four main domains:

- Planning and Organization
- Acquisition and Implementation
- Delivery and Support
- Monitoring and Evaluation

COBIT associates with 34 information technologies processes with the following information criteria and sources:

- Information criteria: Efficacy, efficiency, confidentiality, integrity, continuity, compatibility, and reliability.
- Information sources: Human resources, implementation systems, technology, physical environment, and data.

While the objective of ISO 20000 is to ensure the provision of information technologies services at a certain service level, continuity, quality, pace and cost, COBIT places the business requirements and the nature of the business to the forefront and prefers shaping the information technologies needs accordingly. ISO 20000 standards are based on best information technologies practices. However, COBIT demonstrates how information technologies will be used for business targets. COBIT is generally preferred by institutions that have transferred all of their processes into an information technologies environment and whose business lives are dependent on the protection of their information.

IV. Information Security Criteria

As stated in ISMS, information mass created within the scope of confidentiality, integrity and accessibility, information security criteria necessary for ensuring that information security can be listed as security policy, organization security, classification/audit of assets, personnel security, physical/environmental security, communication management, access control, system development, business continuity management, information security event management and compatibility [11].

Figure 2 displays the standard structuring of these domains. Each domain includes information concerning the managerial, technical and physical measures. In other words, they include activities from managerial level to executive level [12].

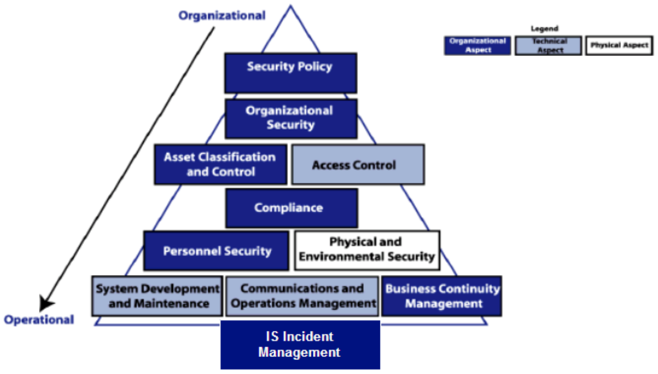

Fig. 2. **ISMS control schema (ISO/ISE 27K)**

V. Conclusions

Within the scope of this study, COBIT, ITIL, 27001/2 standards and frameworks which guided the installation of

ISMS as regards to COBIT, ISO 20000 and ITIL Information Technologies Service Management Systems or supported ISMS installation from various aspects (information security, IT service continuity, IT governance, etc.) were examined from the aspects of risk management and ISMS by addressing the applications of ITMS.

ISO ISO27001 / ISO27002 standards are substantially different from COBIT and ITIL standards. While ISO27001 / ISO27002 standards address information security in-depth from a narrow point of view, COBIT and ITIL standards address many information technologies processes, including information security, from a broad perspective but they are not as comprehensive as the ISO 27001 standard in terms of information security. Thus it is difficult to compare these standards.

A question of this study is "Which one of the abovementioned standards should be applied to ensure information security?" This is a difficult question to answer and it does not have an obvious answer. Its answer differs according to the strategies, requirements and policies of the company. Even though there are a lot of points distinguishing these standards from one another, they have much in common, especially in the field of information security.

Other factors affecting the selection are budget and authorities. COBIT practices are usually implemented with funds received from the auditing budget, while ITIL and ISO27001 / ISO27002 practices generally use the IT budget. Therefore, management policy will determine the standard to be given priority.

Another question concerning these standards is in relation to which standard can be implemented more easily than the others. Implementation of ITIL practices is much easier than COBIT and ISO ISO27001 / ISO27002 processes, as ITIL practices can be easily implemented separately at different times, while partial implementations of COBIT and ISO standards are difficult.

This study is part of a more comprehensive thesis study of information technologies management systems, information security management systems and the importance of risk management and its effects on information security, which also contains a case study where an ISMS application is performed. Based on the basic points emphasized in the study, three important points need to be taken into consideration during the implementation of an ISMS system.

- Risk analysis must be as accurate as possible: a proper risk analysis allows an understanding of the system and its relationships with the surrounding assets. When a complete list of assets is analyzed in accordance with the risk analysis methodologies, risk and effect estimates of possible problems will largely turn out to be correct and risk measures will be sufficient to overcome high risks.
- System and business continuity must be ensured: an organization develops together with its surroundings and thus systems and processes need to be updated to adapt to these changes. Skipping the continuous improvement approach will result in old and ineffective security control processes.
- An ISMS can never provide constant and 100% security: today, it is impossible to ensure 100% security in computer systems. The complexity of these systems and the high number of possibilities that ISMS should handle make system security impossible in the long term. The cost of such complete security will be high; it can even exceed the cost of the system.

Despite these facts, information security is an appropriate field to invest in. Information assets are of crucial importance and measures are necessary for them. Information security can be executed successfully in a balanced and well-organised company if it is appropriate in terms of budget and planning.

In conclusion, it should be noted that information security is not a technological problem but a matter of business management. Organizations need to protect their information assets, ensure and guarantee their business continuity and spread these at the institutional level with a management system approach to survive in today's competitive global economy. Thus they are obliged to adopt, establish, use and spread an ISMS in line with their strategic decisions.

References

[1] L. DeNardis, "A History of internet security," in The History of Information Security: A coprehensive handbook, Elsevier, 2007.

[2] B. P. Kehoe, "Zen and Art of the Internet", CERT Advisory CA-90:01, 1990.

[3] M. Kara, H. Basci, "Bilgi sistemleri güvenliği araştırmalarının yönü," TUBITAK UEKAE, http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.htm, 2010

[4] M. B. Salem, S. S. Hershkop, S. J. Stolfo, "A Survey of Insider Attack Detection Research," Advances in Information Security, vol. 39, pp. 69-90, 2008.

[5] "ISO/IEC 27001, Information Technology - Security techniques -Information security management systems Requirements," 2005.

[6] "System Security Engineering Capability Maturity Model V 3.0," http://www.sse-cmm.org/docs/ssecmmv3final.pdf, 2011.

[7] T. Skordas, "Next Generation Networks: Evolution and Policy considerations," OECD Foresight Forum, Budapest, 2006.

[8] B. Alpay, "Implementation of ITIL (Information Technology Infrastructure Library) security management processes in middle/big companies," MSc Thesis, Halic University, Istanbul, 2008.

[9] "ISO/IEC 20000-1," 2005.

[10] H. Esener, "Service Management System," MSc Thesis, Yildiz Technical University, Istanbul, 2005.

[11] "TSE Information Technology, Practice Principles for Information Security Management," November, 2002.

[12] B. Jacquelin, R.Saint-Germain, "The BS 7799 / ISO 17799 Standard," https://www.callio.com/files/wp_iso_en.pdf, 2006.