An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls

Razieh Sheikhpour[1] and Nasser Modiri[2]

[1]*Department of Computer Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran*
[2]*Department of Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran*
[1]*r_sheikhpour@yahoo.com*, [2]*nassermodiri@yahoo.com*

Abstract

Information is a fundamental asset within any organization and the protection of this asset, through a process of information security is of equal importance. COBIT and ISO27001 are as reference frameworks for information security management to help organizations assess their security risks and implement appropriate security controls. One of the most important sections of IT within the COBIT framework is information security management that cover confidentiality, integrity and availability of resources. Since the issues raised in the information security management of COBIT, are the area covered by the ISO/IEC27001 standard, the best option to meet the information security management in COBIT infrastructure, is using of ISO/IEC27001 standard. For coexistence of and complementary use of COBIT and ISO27001, mapping of COBIT processes to ISO/IEC 27001 controls is beneficial. This paper explores the role of information security within COBIT and describes mapping approach of COBIT processes to ISO/IEC27001 controls for information security management.

Keywords: *Information security management, Mapping, Organization, COBIT, ISO/IEC 27001, PDCA cycle*

1. Introduction

All organizations are dependent on their information technology resources, not only for their survival but also for their growth and expansion in today's highly competitive global markets [1]. However, the use of information technology brings significant risks to information systems and particularly to the critical resources, due to its own nature [2]. Therefore, the security of information needs to be managed and controlled properly [3].

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities [4]. For effective management of information security in organization, Information Security Management Systems (ISMSs) are developed. ISMS manages and operates continuously information security system, in terms of technology, management, and hardware, for the aim of the information security that is to achieve confidentiality, integrity, and availability. The implementation of the ISMS follows the concept of the Plan-Do-Check-Act (PDCA) cycle [5].

Some of the best practices such as COBIT and ISO/IEC 27001 can be used as a foundation for the development of a sound information security process [6]. ISO/IEC27001 standard specifies requirements for the design and implementation of an appropriate information security management system in an organization, ensuring that adequate and proportionate

controls are selected to protect information assets and to give confidence to interested parties [4].

COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks [7]. The main focus of COBIT is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organizations [8]. Since the issues raised in the information security management of COBIT like confidentiality, integrity and availability, are the area covered by the ISO/IEC 27001 standard, The best option to meet the information security management in COBIT infrastructure, is using of ISO/IEC 27001 standard.

In this paper, we describe a mapping between COBIT processes to ISO/IEC 27001 controls to investigate the coexistence of and complementary use of COBIT and ISO/IEC 27001 for information security management. The mapping describes relationship between subjects and control parameters of both standards.

Rest of the paper is organized as follows: Section 2 presents an overview of COBIT framework. Section 3 describes ISO/IEC 27001 standard. In Section 4, we describe a mapping of COBIT processes with ISO/IEC 27001 controls for information security management. Finally, In section 5, conclusion of the paper is presented.

2. COBIT Framework

The Control Objectives for Information and related Technology (COBIT) is a set of best practices for information technology governance created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) [7, 9].

COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company. The COBIT mission is to research, develop, publicize and promote an authoritative, up-to date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors. Managers, auditors, and users benefit from the development of COBIT because it helps them understand their IT systems and decide the level of security and control that is necessary to protect their companies' assets through the development of an IT governance model [7, 9].

COBIT can be widely applied to various purposes. COBIT covers security in addition to all the other risks that can occur with the use of IT.

2.1. Description of the Guidance and Content of the COBIT

Enterprise governance (the system by which organizations are governed and controlled) and IT governance (the system by which the organization's IT is governed and controlled) are, from a COBIT point of view, highly related. Enterprise governance is inadequate without IT governance and vice versa. IT can extend and influence the performance of the organization, but it has to be subject to adequate governance. On the other hand, business processes require information from the IT processes, and this interrelationship has to be governed as well [10].

In this subject matter, PDCA cycle becomes evident. The concept of the PDCA cycle is usually used in structured problem-solving and continuous improvement processes. Both the information need (enterprise governance) and the information offer (IT governance) have to be planned with measurable and constructive indicators (plan). The information and, possibly, information systems have to be implemented, delivered and used (do). The outcome of the

information delivered and used is measured against the indicators defined in the planning phase (check). Deviation is investigated and corrective action is taken (act).

Considering these interdependencies, it is apparent that the IT processes are not an end in themselves. They are a means to an end that is highly integrated with the management of business processes. The following definition is from ITGI:

IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives [10].

2.2. Characteristics of the COBIT Framework

COBIT framework was created with the following main characteristics of being [7]:

2.2.1. Business-focused: Business orientation is the main theme of COBIT. It is designed not only to be employed by IT service providers, users and auditors, but also, and more importantly, to provide comprehensive guidance for management and business process owners. The COBIT framework is based on the principle to provide the information that the enterprise requires to achieve its objectives, the enterprise needs to invest in and to manage and control IT resources using a structured set of processes to provide the services that deliver the required enterprise information. Managing and controlling information are at the heart of the COBIT framework and help ensure alignment to business requirements.

Information Criteria

Information delivered to the core business processes has to fulfill certain criteria, which are summarily characterized as follows:

• **Quality Requirements:**

– **Effectiveness**: Deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

– **Efficiency**: Concerns the provision of information through the optimal (most productive and economical) use of resources.

• **Security Requirements:**

– **Confidentiality**: Concerns the protection of sensitive information from unauthorized disclosure.

– **Integrity**: Relates to the accuracy and completeness of information, as well as to its validity in accordance with business values and expectations.

– **Availability**: Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

• **Fiduciary Requirements:**

– **Compliance**: Deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria, as well as internal policies.

– **Reliability**: Relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

2.2.2. Process-Oriented: COBIT divides information technology governance into 34 processes grouped into four domains, and provides a high level control objective for each of these 34 processes. These domains are:

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

The domains map to IT's traditional responsibility areas of plan, build, run and monitor. The COBIT framework provides a reference process model and common language for everyone in an enterprise to view and manage IT activities. Incorporating an operational model and a common language for all parts of the business involved in IT is one of the most important and initial steps toward good governance. It also provides a framework for measuring and monitoring IT performance, communicating with service providers and integrating best management practices. A process model encourages process ownership, enabling responsibilities and accountability to be defined.

2.2.3. Controls-based: COBIT defines control objectives for all 34 processes, as well as overarching process and application controls. Control is defined as the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

2.2.4. Measurement-driven: A basic need for every enterprise is to understand the status of its own IT systems and to decide what level of management and control the enterprise should provide. To decide on the right level, management should ask itself: How far should we go and is the cost justified by the benefit? Enterprises need to measure where they are and where improvement is required, and implement a management tool kit to monitor this improvement.

These COBIT characteristics emphasise the basic principle of the COBIT framework which is that IT resources are managed by IT processes to achieve IT goals that respond to business requirements.

2.3. COBIT Framework Model

The purpose of COBIT framework is to provide the management with an IT governance model that helps them control and manage the information and related technology. The Framework explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The Framework identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which of the IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objectives [11].

IT Governance Institute has identified four domains as the building blocks of the COBIT framework, as illustrated in Figure 1: [11]

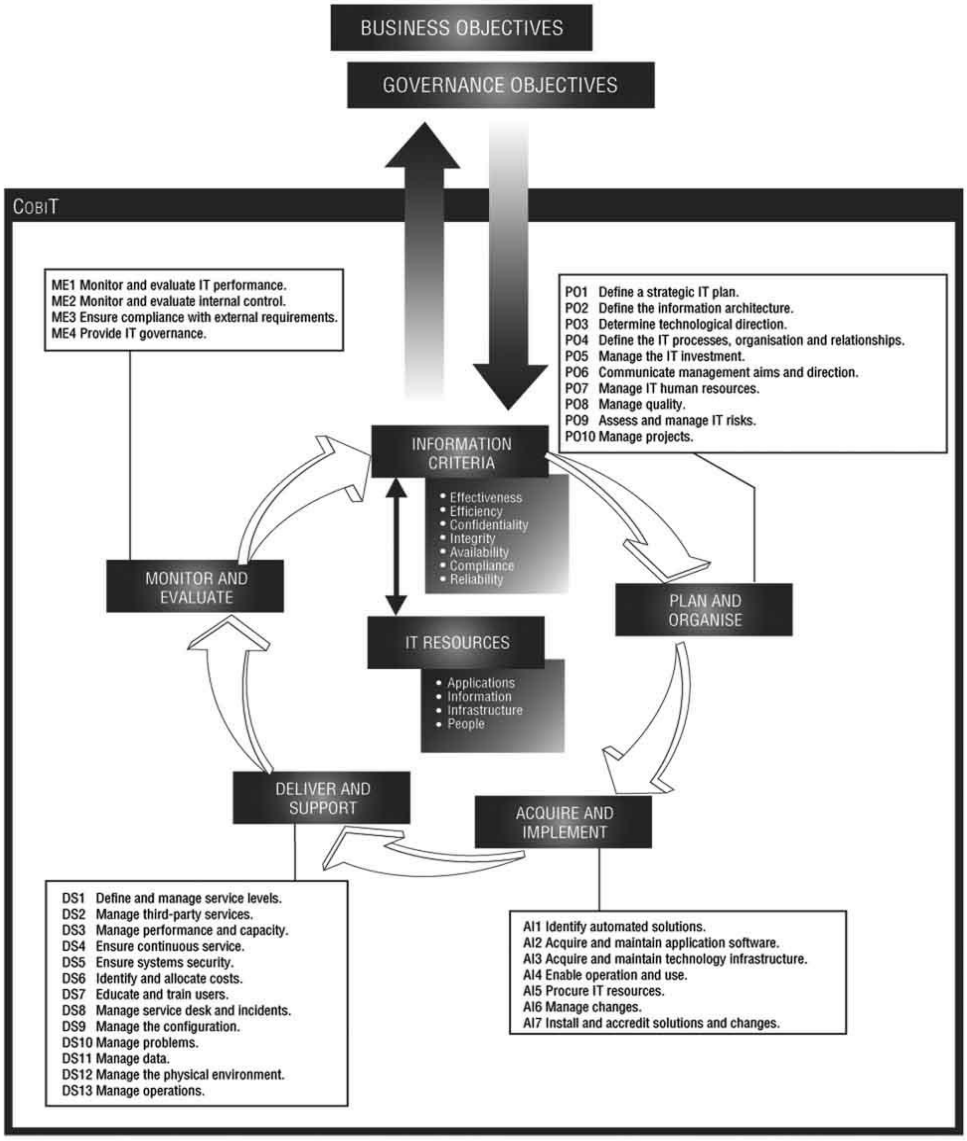

Figure 1. COBIT IT Processes Defined within the Four Domains [10]

This structure is based on PDCA cycle.

2.4. COBIT as a Foundation for Information Security Management

Effective information security requires a comprehensive, integrated set of security, management and governance processes to plan, organize and counter the organization's information security risks. COBIT provides an integrated governance, management and process framework to implement and execute information security.

COBIT describes sound processes, practices, and control objectives for managing and operating IT systems, including their security state. Organizations using the framework report an increased ability to deliver high quality service to their customers, which includes being able to measure and satisfy confidentiality, availability, and integrity requirements.

COBIT supports security needs to be addressed as a part of every business function. While only one COBIT process (DS5) is specifically devoted to security, control objectives that

address security are scattered throughout the various processes in each domain. The COBIT security baseline document [12] highlights the high-level COBIT control objectives related to information security within the four domains in the COBIT framework.

The DS5 Delivery and Support, Ensure systems security process, looks as though it contains the requirements of ISO/IEC 27001. It maps to some of the controls and management system requirement of ISO/IEC 27001. DS5 includes 21 control objectives:

- **DS5.1** Manage Security Measures
- **DS5.2** Identification, Authentication and Access
- **DS5.3** Security of Online Access to Data
- **DS5.4** User Account Management :
- **DS5.5** Management Review of User Accounts
- **DS5.6** User Control of User Accounts
- **DS5.7** Security Surveillance
- **DS5.8** Data Classification
- **DS5.9** Central identification and Access Rights Management
- **DS5.10** Violation and Security Activity
- **DS5.11** Incident Handling
- **DS5.12** Re-accreditation
- **DS5.13** Counterparty Trust
- **DS5.14** Transaction Authorization
- **DS5.15** Non-repudiation
- **DS5.16** Trusted Path
- **DS5.17** Protection of Security Functions
- **DS5.18** Cryptographic Key Management
- **DS5.19** Malicious Software Preventions, Detection and Correction
- **DS5.20** Firewall Architectures and Connections With Public Networks
- **DS5.21** Protection of Electronic Value

3- ISO/IEC 27001 Standard

ISO/IEC 27001 has its origins from a code of good practice published by the UK department of Trade and Industry in 1989, which slowly evolved into BS7799 [13]. ISO/IEC 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organization's overall business risks. ISO/IEC 27001 specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and

give confidence to interested parties. The proposed requirements are structured in a classification of 11 clauses that include 39 objectives aimed by 133 controls [4,14,15].

ISO/IEC 27001 sets out how a company should address the requirements of **confidentiality**, **integrity** and **availability** of its information assets and incorporate this into an Information Security Management System (ISMS) [3, 5]. This standard is used throughout the world by organizations, both commercial and government, as the basis for the management of the organization's policy and implementation of information security. It is being used by small, medium and large organizations across a diverse range of business sectors. In fact the standard is designed to be flexible enough to be used by all types of organization. The standard has become the de facto ''common-language'' for information security management [14,15].

The standard introduces a cyclic model known as the "Plan-Do-Check-Act" (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS. The PDCA cycle has these four phases: [4,6, 7]

The PDCA cycle has these four phases:

a) "Plan" phase – establishing the ISMS: Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

b) "Do" phase – implementing and operating the ISMS: Implement and operate the ISMS policy, controls, processes and procedures.

c) "Check" phase – monitoring and reviewing the ISMS: Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

d) "Act" phase – maintaining and improving the ISMS: Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS [4].

Figure 2 shows PDCA model applied to ISMS processes.

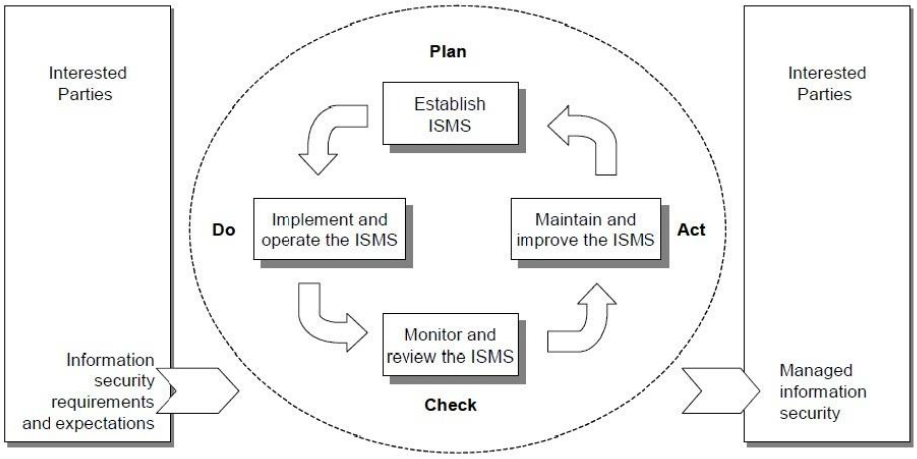

Figure 2. PDCA Model Applied to ISMS Processes [4]

One of the standards that support the implementation of ISO/IEC 27001 is the code of practice ISO/IEC 27002. This code of practice provides implementation guidance for the

information security controls defined in ISO/IEC 27001 (Annex A) [15]. The control areas covered by both these standards are : [4,10]

Security Policy: Management commitment and support for information security policy is addressed in this domain.

Organizational information security: The coordination and management of the overall organizational information security efforts is detailed in this domain. Also, information security responsibility is defined in this domain.

Asset management: All critical and/or sensitive assets are defined in this domain.

Human resources security: This domain addresses user awareness and training. User awareness and training can reduce the risk of theft, fraud, and error.

Physical and Environmental Security: This domain restricts access to facilities to authorized personnel. Additionally, this domain addresses limiting the amount of damage caused to the physical plant and the organizations information.

Communications and Operations Management: This domain addresses the risk of failure and the resulting consequences. This is achieved by ensuring the proper and secure use of information processing facilities.

Access Control: This domain ensures the access to respective systems and information is restricted to authorized personnel. The detection of unauthorized activities is also addressed in this domain.

Information security incident management: Security events and weaknesses should be reported. This domain addresses definition of the responsibilities and procedures for managing security incidents and improvement, and collects evidence for security incidents.

Information systems acquisition, development and maintenance: This domain addresses the loss and misuse of information in applications used in the enterprise.

Business Continuity Management: This domain addresses the ability of the organization to rapidly respond to any interruption of business critical systems. The interruption of these systems may be caused by hardware failures, incidents, and natural disasters.

Compliance: This domain addresses legal compliance by the business. Additionally, this domain ensures that the objectives established by top level management are being followed and met.

These areas of controls provide a comprehensive coverage of organizational requirements for managing risk across the business involving people, information, processes, services, IT and physical assets.

There are 39 control objectives according to the 11 security controls of ISO/IEC 27001, which are listed in Table 1. These control objectives encompass the functional requirements' specification for an organization's information security management architecture [4].

Table 1. ISO/IEC 27001 (Annex A) Control Objectives

Controls	Control Objectives
A.5 Security policy	A.5.1 Information security policy
A.6 Organizational information security	A.6.1 Internal organization A.6.2 External parties

A.7 Asset Management	A.7.1 Responsibility for assets A.7.2 Information classification
A.8 Human resources security	A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment
A.9 Physical and environmental security	A.9.1 Secure areas A.9.2 Equipment security
A.10 Communications and operations management	A.10.1 Operational procedures and responsibilities A.10.2 Third party service delivery management A.10.3 System planning and acceptance A.10.4 Protection against malicious and mobile code A.10.5 Back-up A.10.6 Network security management A.10.7 Medical handling A.10.8 Exchange of information A.10.9 Electronic commerce services A.10.10 Monitoring
A.11 Access control	A.11.1 Business requirement for access control A.11.2 User access management A.11.3 User responsibilities A.11.4 Network access control A.11.5 Operating system access control A.11.6 Application and information access control A.11.7 Mobile computing and teleworking
A.12 Information systems acquisition, development and maintenance	A.12.1 Security requirements of information systems A.12.2 Correct processing and application A.12.3 Cryptographic controls A.12.4 Security of system files A.12.5 Security in development and support processes A.12.6 Technical vulnerability management
A.13 Information security incident management	A.13.1 Reporting information security events and weaknesses A.13.2 Management of information security incidents and improvement
A.14 Business continuity management	A.14.1 Information security aspects of business continuity management
A.15 Compliance	A.15.1 Compliance with legal requirements A.15.2 Compliance with security policies and standards and technical compliance A.15.3 Information system audit considerations

4. Mapping of COBIT Processes to ISO/IEC27001 Controls

The basic difference between COBIT and ISO27001 is that ISO 27001 is only focused on information security, whereas COBIT is focused on more general information technology controls. Thus, COBIT has a broader coverage of general information technology topics, but does not have as many detailed information security requirements as ISO 27001. If an organization addresses all of the security controls within ISO 27001, then they will be covering a large part of COBIT in the process - especially the section DS5 Ensure Systems Security. However, COBIT covers a much larger set of issues related to information technology governance, and is typically used as part of an overall corporate governance framework.

One of the most important sections of information technology within the COBIT framework, is information security management that cover confidentiality, integrity and availability of resources. Since the issues raised, are the area covered by the standard ISO/IEC 27001 standard, and the standard has also considered a PDCA cycle as infrastructure, the best

option to meet the information security management in COBIT infrastructure, is using of ISO/IEC 27001 standard. For coexistence of and complementary use of COBIT and ISO/IEC 27001, a mapping between COBIT and ISO/IEC27001 is beneficial.

The purpose of the mapping is providing an integrated way for complementary use of COBIT and ISO/IEC 27001 for information security management. Mapping of ISO/IEC 27001 into COBIT processes enables the organization to lower the overall cost of maintaining acceptable security levels, effectively manage risks and reduce overall risk levels.

For mapping of these frameworks, every COBIT process is investigated, and the corresponding, ISO 27001 Annex A control objectives are indicated. According to the ISO/IEC 27001:2005 domains and COBIT processes, the relationship between subjects and control parameters of both standards are given in Table 2.

Table 2. Mapping of COBIT 4.0 Processes to ISO/IEC 27001:2005 Control Objectives

COBIT Processes	ISO/IEC 27001 Control Objectives
Plan and Organize	
PO1:Define a strategic IT plan	No control objective of ISO/IEC 27001:2005 was mapped to PO1
PO2:Define the information architecture	A.7.1 Responsibility for assets A.7.2 Information classification A.10.7 Medical handling A.10.8 Exchange of information A.11.1 Business requirement for access control
PO3:Determine technological direction	A.5.1 Information security policy A.6.1 Internal organization A.10.3 System planning and acceptance A.10.8 Exchange of information A.11.7 Mobile computing and teleworking A.14.1 Information security aspects of business continuity management
PO4:Define the IT processes, organization and relationships	A.6.1 Internal organization A.6.2 External parties A.7.1 Responsibility for assets A.8.1 Prior to employment A.8.2 During employment A.9.1 Secure areas A.9.2 Equipment security A.10.1 Operational procedures and responsibilities A.10.6 Network security management A.15.1 Compliance with legal requirements A.15.2 Compliance with security policies and standards and technical compliance
PO5:Manage the IT investment	A.5.1 Information security policy A.13.2 Management of information security incidents and improvement
PO6: Communicate management aims and direction.	A.5.1 Information security policy 6.1 Internal organization A.6.1 Internal organization A.6.2 External parties A.7.1 Responsibility for assets A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment A.9.1 Secure areas A.9.2 Equipment security A.10.7 Medical handling

	A.10.8 Exchange of information A.10.9 Electronic commerce services A.11.1 Business requirement for access control A.11.3 User responsibilities A.11.7 Mobile computing and teleworking A.12.3 Cryptographic controls A.13.2 Management of information security incidents and improvement A.15.1 Compliance with legal requirements A.15.2 Compliance with security policies and standards and technical compliance
PO7:Manage IT human resources	A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment
PO8:Manage quality	A.6.1 Internal organization A.6.2 External parties A.12.5 Security in development and support processes
PO9: Assess and manage IT risks	A.5.1 Information security policy A.13.1 Reporting information security events and weaknesses A.14.1 Information security aspects of business continuity management
PO10:Manage projects	No objective of ISO/IEC 27001:2005 was mapped to this process
Acquire and Implement	
AI1:Identify automated solutions	A.6.1 Internal organization A.8.2 During employment A.10.1 Operational procedures and responsibilities A.10.3 System planning and acceptance A.11.6 Application and information access control A.12.1 Security requirements of information systems
AI2:Acquire and maintain application software	A.6.1 Internal organization A.7.2 Information classification A.10.3 System planning and acceptance A.10.10 Monitoring A.11.6 Application and information access control A.12.1 Security requirements of information systems A.12.2 Correct processing and application A.12.3 Cryptographic controls A.12.4 Security of system files A.12.5 Security in development and support processes A.13.2 Management of information security incidents and improvement A.15.3 Information system audit considerations
AI3:Acquire and maintain technology infrastructure	A.9.1 Secure areas A.9.2 Equipment security A.10.1 Operational procedures and responsibilities A.12.1 Security requirements of information systems A.12.4 Security of system files A.12.5 Security in development and support processes A.12.6 Technical vulnerability management
AI4:Enable operation and use	A.10.1 Operational procedures and responsibilities A.10.3 System planning and acceptance A.10.7 Medical handling A.13.2 Management of information security incidents and improvement
AI5:Procure IT resources	A.6.1 Internal organization A.6.2 External parties A.10.8 Exchange of information

	A.12.5 Security in development and support processes
AI6:Manage changes	A.10.1 Operational procedures and responsibilities A.11.5 Operating system access control A.12.5 Security in development and support processes A.12.6 Technical vulnerability management
AI7:Install and accredit solutions and changes	A.6.1 Internal organization A.8.2 During employment A.9.1 Secure areas A.10.1 Operational procedures and responsibilities A.10.3 System planning and acceptance A.12.4 Security of system files A.12.5 Security in development and support processes
Deliver and Support	
DS1:Define and manage service levels	A.10.2 Third party service delivery management
DS2:Manage third-party services	A.6.2 External parties A.8.1 Prior to employment A.10.2 Third party service delivery management A.10.8 Exchange of information A.12.4 Security of system files A.12.5 Security in development and support processes A.15.1 Compliance with legal requirements
DS3:Manage performance and capacity	A.10.3 System planning and acceptance
DS4:Ensure continuous service	A.6.1 Internal organization A.10.5 Back-up A.14.1 Information security aspects of business continuity management
DS5:Ensure systems security	A.5.1 Information security policy A.6.1 Internal organization A.6.2 External parties A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment A.9.1 Secure areas A.9.2 Equipment security A.10.1 Operational procedures and responsibilities A.10.4 Protection against malicious and mobile code A.10.6 Network security management A.10.7 Medical handling A.10.8 Exchange of information A.10.9 Electronic commerce services A.10.10 Monitoring A.11.1 Business requirement for access control A.11.2 User access management A.11.3 User responsibilities A.11.4 Network access control A.11.5 Operating system access control A.11.6 Application and information access control A.11.7 Mobile computing and teleworking A.12.2 Correct processing and application A.12.3 Cryptographic controls A.12.4 Security of system files A.12.6 Technical vulnerability management A.13.1 Reporting information security events and weaknesses A.13.2 Management of information security incidents and improvement A.15.1 Compliance with legal requirements A.15.2 Compliance with security policies and standards and technical compliance

	A.15.3 Information system audit considerations
DS6:Identify and allocate costs	No control objective of ISO/IEC 27001:2005 was mapped to this process.
DS7:Educate and train users	A.8.2 During employment
DS8:Manage service desk and incidents	A.13.1 Reporting information security events and weaknesses A.13.2 Management of information security incidents and improvement A.14.1 Information security aspects of business continuity management
DS9:Manage the configuration	A.7.1 Responsibility for assets A.7.2 Information classification A.10.7 Medical handling A.11.4 Network access control A.12.4 Security of system files A.12.5 Security in development and support processes A.12.6 Technical vulnerability management A.15.1 Compliance with legal requirements
DS10:Manage problems	A.13.2 Management of information security incidents and improvement
DS11:Manage data	A.9.2 Equipment security A.10.5 Back-up A.10.7 Medical handling A.10.8 Exchange of information A.12.4 Security of system files A.15.1 Compliance with legal requirements
DS12:Manage the physical environment	A.6.2 External parties A.9.1 Secure areas A.9.2 Equipment security
DS13:Manage operations	A.9.2 Equipment security A.10.1 Operational procedures and responsibilities A.10.7 Medical handling
Monitor and Evaluate	
M1:Monitor and evaluate IT performance	A.10.10 Monitoring

ME2:Monitor and evaluate internal control	A.5.1 Information security policy A.6.1 Internal organization A.6.2 External parties A.10.2 Third party service delivery management A.10.10 Monitoring A.15.2 Compliance with security policies and standards and technical compliance A.15.3 Information system audit considerations
ME3:Ensure regulatory compliance	A.6.1 Internal organization A.15.1 Compliance with legal requirements A.15.2 Compliance with security policies and standards and technical compliance
ME4:Provide IT governance	A.5.1 Information security policy A.6.1 Internal organization A.10.10 Monitoring

Here, a number of scenarios where mapping of COBIT and ISO/IEC 27001 can be very beneficial are discussed.

4.1 Scenario 1

Suppose a company have been implemented an IT governance framework based on COBIT and the information security department had subsequently also based on the some COBIT processes. The information security department now decides to use ISO/IEC 27001. Using the mapping approach, the information security department can work easily with other department like risk management department and audit department. The benefit of the mapping approach is that the information security department does not have to change anything and can easily determine which of the ISO/IEC 27001 objectives have been implemented through the use of COBIT, and which must still be given attention.

4.2 Scenario 2

Suppose the information security department of a company uses ISO 27001 as information security management guideline and the audit department decides to use COBIT as an IT governance framework. Since information security department has addressed security controls within ISO 27001, therefore a large part of COBIT processes have been covered. Using the mapping approach, the information security department does not have to expend additional cost and can easily determine which processes from COBIT have been implemented through ISO 27001.

4.3 Scenario 3

If a company implement an IT governance framework based on COBIT because of its wide coverage of information technology topics and an information security management guideline based on ISO/IEC 27001 because of its more detailed information security requirements, the company can better meet IT governance and information security management. Using the mapping, company will able to implement both frameworks without no additional cost and time and also information security department can work easily with other department like risk management department and audit department.

5. Conclusion and Future Work

Information security plays an important role in protecting the assets of an organization. As no single formula can guarantee 100% security, there is a need for a set of benchmarks or standards to help ensure an adequate level of security is attained, resources are used efficiently, and the best security practices are adopted. Systems such as COBIT and ISO/IEC 27001 can be used together as a foundation for the development of a sound information security process. For coexistence of and complementary use of COBIT and ISO/IEC 27001 as reference frameworks for information security management, mapping of COBIT processes to control objectives of ISO/IEC 27001 can be used. In this paper we described the mapping between COBIT and ISO/IEC 27001. Mapping of ISO/IEC 27001 into COBIT processes enables the organization to lower the overall cost of maintaining acceptable security levels, effectively manage risks and reduce overall risk levels. Moreover, the use of the mapping will also reduce confusion and deviations that exist between IT and Audit. For future work, we plan to design a comprehensive and cost effective framework for organizations usage for balancing establishment of ISO/IEC 27001 and COBIT processes.

References

[1] M. M. Eloff and S. H. von Solms, "Information Security Management: A Hierarchical Framework for Various Approaches", J Computers & Security, Vol. 19, **(2000)**, pp.243-256.

[2] T. Pereira and H. Santos, "A Security Audit Framework to Manage Information System Security. Communications in Computer and Information Science", Vol. 92, **(2010)**, pp. 9-18.

[3] K. L.,Thomson and R. von Solms, "Information security obedience: a definition", J Computers & Security, Vol. 24, **(2005)**, pp. 69-75.

[4] ISO/IEC 27001: 2005, "Information technology- Security techniques - Information security management systems- requirements," ISO Office, Published in Switzerland **(2005)**.

[5] J. Heasuk, K. Seungjo and W. Dongho, "A Study on Comparative Analysis of the Information Security Management Systems", Lecture Notes in Computer Science, Vol. 6019, **(2010)**, pp. 510-519.

[6] A. Nakrem, "Managing Information Security in Organizations, A Case Study", Master thesis in information systems, **(2007)**, Institute of information science, department of economy and social studies HIA.

[7] N. Deysel, "A model for information security control audit for amall to mid-sized organizations", Masters thesis in Business Information Systems in the Faculty of Engineering, the Built Environment and Information Technology at the Nelson Mandela Metropolitan University, **(2009)** January.

[8] IT Governance Institute (ITGI), "COBIT in Academia", **(2004)**, United States of America.

[9] Sh. Sahibudin, M. Sharifi and M. Ayat, "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations", Proceeding of Second Asia International Conference on Modelling & Simulation (AICSM 08), IEEE, **(2008)**, pp. 749 – 753.

[10] IT Governance Institute (ITGI), "COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT", 2 nd Edition, Printed in the United States of America ,United States of America, **(2000)**.

[11] S. J. Hussain and M. S. Siddiqui, "Quantified Model of COBIT for Corporate IT Governance", Proceeding of First International Conference on Information and Communication Technologies, **(2005)**. ICICT 2005, pp. 158 – 163.

[12] IT Governance Institute (ITGI), "COBIT Security Baseline. An Information Security Survival Kit", Rolling Meadows: Author. Retrieved **(2008)** June 30, from http://www.isaca.org.

[13] W. Boehmer, "Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001", Proceeding of Second International Conference on Emerging Security Information, Systems and Technologies, **(2008)**, pp. 224-31.

[14] A. Tsohou, S. Kokolakis, C. Lambrinoudakis and S. Gritzalis, "Information Systems Security Management: A Review and a Classification of the ISO Standards", Next Generation Society, Vol.26, Technological and Legal Issues, Part 6, **(2010)**, pp. 220-235.

[15] E. Humphreys, "Information security management standards: Compliance, governance and risk management", J Information Security Technical Report, Vol.13, No. 4, **(2008)**, pp. 247-55.

Authors

Razieh Sheikhpour received the B.Sc degree in computer engineering from department of computer engineering , Islamic Azad University of Iran in 2007. She is now M.Sc student in computer engineering at Islamic Azad University of Iran. Her research interests include Information Security, IT Governance and Wireless Sensor Networks.

Nasser Modiri received his M.S. Degree from the University Of Southampton, U.K., and Ph. D. degree from the University of Sussex, U.K. in 1986 and 1989, respectively. In 1988 he joined The Networking Centre of Hemel Hempstead, and in 1989 he worked as a Principal Engineer at System Telephone Company (STC) Telecommunications Systems, U.K. Currently, Dr. Modiri is the president of Ayandehgan Rayaneh Co. developing web-based software and designer and implementer of information technologies services for Intranet networks while teaching actively MSc courses in network designing, software engineering and undertaking many MSc projects. He is currently developing applications for Virtual Universities, Virtual Parliaments, Virtual Organizations, ERP, GPS+GSM, GPRS, RFID, ISO/IEC 27000, ISO/IEC 15408 technologies.