An Analysis of Major Information Security Management System Standards

Arpana Bharani*
Rupesh R. Shukla**

Abstract

In the era of globalization information is an important asset for any organization. Due to rapid growth in the use of electronic devices and networking, protecting the information and providing its security is an important task for any organization. However, in spite of tremendous growth in information security management system there is scarcity of a standard which can guarantee total information security to any organization. This paper tries to introduce different information security management system standards. It also presents an analysis of pros and cons of major information security standards, like ISO27001, PA DSS, PCIDSS, ITIL and COBIT. The study will provide various features, compatibility and usability of major information security standards. It will also imbibe the profile and methodology of each standard under study.

Introduction

The use of internet and networking technology has increased the operational efficiency but it has also increased the risk to protect the important information available with in the organization. Access to high-class, absolute, precise and up-to date information is very important for managerial decision making process that leads to correct decisions. Thus, securing information system resources must be the prime concern in any organization.

Every organization has its own management information system which generates the report of business deals, project progress status and employee information. Any interruption in the value, measure, significance and delivery of **information systems** can put any organization at risk. This is due to the fact that information is exposed to a growing number and a wider variety of threats and vulnerabilities.

Major losses due to incidents like hacking, changing and misuse of information, online fraud is the important concerns for management and consumers. Thus the critical information of any organization must be properly managed to protect confidentiality, maintain integrity and ensure availability of those information assets to employee, clients, consumers, shareholders, authorities and also to society.

Information security is not just about anti-virus software, implementing the latest firewall or locking down your laptops or web servers. The overall approach to information security should be strategic as well as operational, and different security initiatives should be prioritized, integrated and cross-referenced to ensure overall effectiveness. An Information Security Management System is a systematic approach to manage confidential and significant information of an organization so that it remains secure. It includes people, processes and IT systems. An Information Security Management System (ISMS) helps you coordinate all your security efforts – both electronic and physical – coherently, consistently and cost-effectively.

Since information security has a very important role in supporting the activities of the organization, we need a standard or benchmark which regulates governance over information security. Several private and government organizations developed Information Security Management System standards bodies whose function is to setup benchmarks, standards and, legal regulations on information security to ensure that an adequate level of security is preserved, to ensure resources used in the right way, and to ensure the best security practices adopted in an organization. There are several standards for IT Governance which leads to information security such as PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL and COBIT.

However, some of these standards are not well adopted by the organizations, with a variety of reasons. In this paper we will discuss the major four ISMS standards that are widely used Standards for information security. The standards are ISO27001, PCIDSS, ITIL

*Assistant Professor, Shri Cloth Market Kanya Vanijya Mahavidyalaya, Indore
**Assistant Professor, Shri Cloth Market Kanya Vanijya Mahavidyalaya, Indore

and COBIT. This comparative study conducted to determine their respective strengths, focus, main components and their adoption based on ISMS.

ISO 27001: The full name of ISO 27001 is ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements* which is an information security management system (ISMS) standard. It was published in October 2005 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). ISO27001 can be included in all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations).Keeping in view the organization's overall business risks, this standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System. This standard provides a complete knowledge of information security and the information which needs protection, ranging from digital information, paper documents, and physical assets (computers and networks) to the knowledge of individual employees.

THE PDCA CYCLE: The ISO 27001 follows the “Plan-Do-Check-Act” (**PDCA**) **process model** that is applied to all the processes of ISMS.

PLAN (establishing the ISMS)

- Identify Business Objectives
- Obtain management support
- Select proper scope of implementation
- Define risk assessment
- Prepare inventory of information assets and
- rank assets according to risk classification based on risk assessment

DO (implementing and workings of the ISMS)

- Manage the risk and create risk treatment plan
- Set up policies and procedures to control risks
- Allocate resources and train the staff.

CHECK (monitoring and reviewing of the ISMS)

- Monitor implementation of ISMS
- Prepare for the certification Audit.

ACT (updating and improving the ISMS)

Conduct periodic assessment audit for

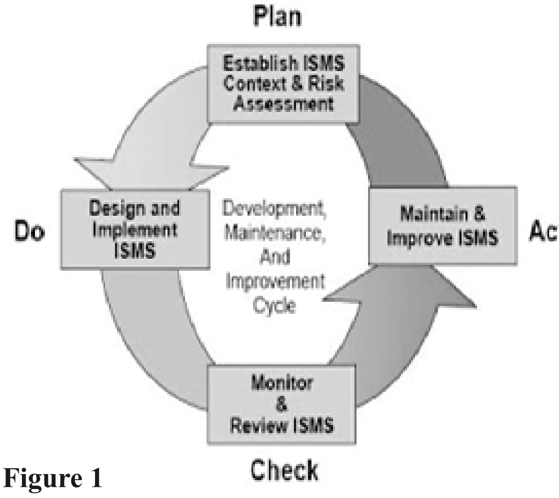

Plan
Establish ISMS Context & Risk Assessment
Do
Design and Implement ISMS
Development, Maintenance, And Improvement Cycle
Maintain & Improve ISMS
Act
Monitor & Review ISMS
Check

Figure 1

- Continual improvement
- Corrective action
- Preventive action

ISO 27001 follows the plan-do-check-act (PDCA) cycle, as shown in **figure 1**.

The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines (2002) governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

PA-DSS: The applications which stores, processes, or transmits cardholder data comes under the scope of the Payment Card Industry Data Security Standards (PCI DSS).

If this application is sold to 3rd parties it comes under the compliance program known as Payment Application Data Security Standard or PA-DSS which was formally known as Visa's Payment Application Best Practices PABP.

The objective of PA-DSS standard is to help software vendors and others develop secure payment applications that do not store prohibited data, (like full magnetic stripe, CVV2 or PIN data), and to ensure their payment applications support compliance with the PCI DSS.

The Standard makes sure that the payment software is compliant with 14 specific requirements (similar to PCI DSS). The headline requirements are:

1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVV2), or PIN block data
2. Protect stored cardholder data.
3. Provide secure authentication features.
4. Produce an audit log of user access.
5. Payment applications must be designed in line with PCI DSS.
6. Wireless transmissions must be implemented in line with PCI DSS.
7. Software vendors must establish a process to test payment applications to address vulnerabilities
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to the Internet.
10. Facilitate secure remote software updates.
11. Facilitate secure remote access to payment application.
12. Encrypt sensitive traffic over public networks.
13. Encrypt all non-console administrative access.
14. Maintain instructional documentation/training programs for customers, resellers, and integrators.

ITIL

The **Information Technology Infrastructure Library** (**ITIL**) is a set of practices for IT service management (ITSM) that focuses on IT security in the view to the needs of business. The **IT Infrastructure Library** originated as a collection of books, each covering a specific practice within IT service management. The current form of ITIL are ITILv3 and ITIL 2011 edition. In these forms, ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage. It mainly consists of 8 main components, they are: Service Support, Service Delivery, ICT Infrastructure Management, Security Management, Application Management, Software Asset Management, Planning to Implement Service Management, Small-Scale Implementation.

ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

COBIT

COBIT (Control Objectives for Information and Related Technology) is a standard which is designed by ISACA for information technology (IT) management and IT governance. COBIT provides good practices for managing the IT processes in a manageable and logical structure by meeting the multiple needs of enterprise management also by bridging the gaps between business risks, technical issues, control needs and performance measurement requirements.

COBIT is designed to be used by three distinct audiences.

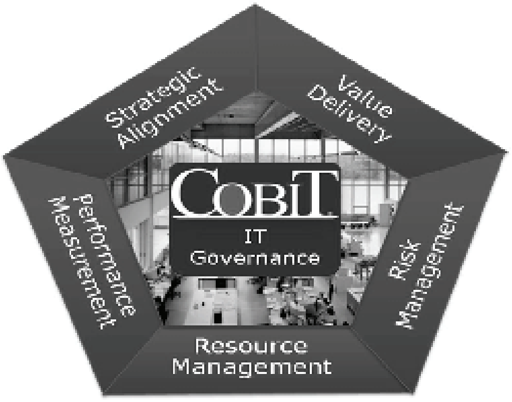
Management: to help them balance risk and control investment in an often unpredictable IT environment.

Users: to obtain assurance on the security and controls of IT services provided by internal or third parties.

Auditors: to substantiate their opinions and/or provide advice to management on internal controls.

COBIT standard is

- accepted globally as a set of tools that ensures IT is working effectively
- functions as an overarching framework
- provides common language to communicate goals, objectives and expected results to all stakeholders
- based on, and integrates, industry standards and good practices in:
  - Strategic alignment of IT with business goals
  - Value delivery of services and new projects
  - Risk management
  - Resource management
  - Performance measurement



According to Alfantookh2009, there are some essential features that should be implemented by an organization, which are defined as11 essential control, called as *11EC*. As a benchmark almost all ISMS standards must cover some or all of these features.

1. ***Information Security Policy:*** how an organization secure information
2. ***Communications & Operations Management:*** define policy in reducing security risk and ensuring correct operational and computing procedures.
3. ***Access Control*****:** is a system which enables an authority to control access to computer-based information system.
4. ***Information System Acquisition, Development and Maintenance*****:** is an integrated process that defines boundaries for the maintenance of information systems.
5. ***Organization of Information Security:*** is a structure to implement information security, consists of management commitment to information security, information security co-ordination.
6. ***Asset Management*****:** is based on the idea that it is important to identify, track, classify, and assign ownership for the important assets to ensure they are adequately protected.
7. ***Information Security Incident Management:*** is a program that prepares for incidents. It prepares to prevent from the future incidents.
8. ***Business Continuity Management:*** provide means to ensure continuity of operations under abnormal conditions.
9. ***Human Resources Security:*** to ensure that all employees are qualified and understand their responsibilities.
10. ***Physical and Environmental Security:*** includes measures taken to protect systems, buildings, and related supporting infrastructure that contain information and information technology systems.
11. ***Compliance:*** is divided into two parts. First part includes compliance with the innumerable laws, regulations and or even contractual requirements of the organization. The second part is compliance with information security policies, standards and processes.

S.No.	Feature	ISO27001	PCIDSS	COBIT	ITIL
1.	*Information Security Policy*	✓	✓	✓	✓
2.	*Communications and Operations Management*	✓	✓	•	✓
3.	*Access Control*	✓	✓	✓	✓
4.	*Information Systems Acquisition, Deve. and Maintenance*	✓	✓	•	✓
5.	*Organization of Information Security*	✓	✓	✓	✓
6.	*Asset Management*	✓	✓	✓	✓
7.	*Information Security Incident Management*	✓	✓	✓	✓
8.	*Business Continuity Management*	✓	✓	✓	✓
9.	*Human Resources Security*	✓	✓	•	✓
10.	*Physical and Environmental Security*	✓	✓	•	✓
11.	*Compliance*	✓	✓	✓	✓

Comparison of four major ISMS Standards

	ISO 27001	PCIDSS	ITIL	COBIT
Profile of standard	ISO is a **nongovernmental organization** that forms a bridge between the public and private sectors.	Is defined by the Payment Card Industry Security Standards Council. The standard was created to help organizations that process card payments to prevent credit card fraud.	The main focus of IT Infrastructure Library, the development was on mutual best practices for all British government data centers to ensure comparable services.	Is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
Initiated By	Delegates from 25 countries	**VisaCard**, **MasterCard**, **American Express**, **Discover Information** and Compliance, and the **JCB**Data Security Program	The Central Computer and Tele-communications Agency (CCTA), now called the Office of Government Commerce (OGC) UK	Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) USA
Launched on	February 23, 1947 996	15 December 2004	1980s	1996
Standards and Components	**18,500 International Standards**	**6 main components on standard**	**8 main components + 5 components version 3**	**6 main components on standard**
Certificate name	Certificate of ISO 27000 Series Information Security Information Security	Certificate of PCI-DSS Compliance	Certificate of ITIL Compliance	Certified Information Systems Auditor™ (**CISA**®) Certified Information Security Manager® (**CISM**®) Certified in the Governance of Enterprise IT® (**CGEIT**®) Certified in Risk and Information Systems Control TM (**CRISCTM**)
Scope	Information Security	Information and Data Transaction Security on debit, credit, prepaid, e-purse, ATM, and POS	Service Management	IT Governance
Usability	163 national members out of the 203 total countries in the world	125 countries out of the 203 total countries in the world.	50 international chapters	160 countries

Table 1 below we showed up head to head comparisons on the four ISMS standards deal with 11EC of information security.

Conclusion

Each standard plays its own role and has its own position in implementing ISMS, several standards such as ISO 27001 and BS 7799 focuses on information security management system as main domain and their focus on, while PCIDSS focus on information security relating to business transactions and smartcard, then ITIL and COBIT focuses on information security and its relation with the Project management and IT Governance.

Refers to is the usability, ISO (27001) leading than other three standards. It can be describe as the standard which can be easily implemented and well recognized by top management, staff, suppliers, customers/ clients, regulators. We can also describe ISO (27001) like a global language in standards and benchmarking on ISMS

References

1. Abdulkader Alfantookh. An Approach for the Assessment of the Application of ISO 27001, Essential Information Security Controls; Computer Sciences, King Saud University 2009
2. http://www.dqsindia.com/iso-certifications/iso-27001-isms-information-security-management-system.php
3. http://standards.narod.ru/COBIT/ag.pdf
4. www.ijens.org/vol_11_i_05/113505-6969-ijecs-ijens.pdf
5. en.wikipedia.org/.../Information Technology Infrastructure Library