World Academy of Science, Engineering and Technology
International Journal of Industrial and Manufacturing Engineering
Vol:2, No:1, 2008

Combination of Information Security Standards to Cover National Requirements

Sh. Ladan, A. Yari, and H. Khodabandeh

***Abstract*—**The need for Information Security in organizations, regardless of their type and size, is being addressed by emerging standards and recommended best practices. The various standards and practices which evolved in recent years and are still being developed and constantly revised, address the issue of Information Security from different angles. This paper attempts to provide an overview of Information Security Standards and Practices by briefly discussing some of the most popular ones. Through a comparative study of their similarities and differences, some insight can be obtained on how their combination may lead to an increased level of Information Security.

***Keywords*—**Information security management, information security standard, BS7799, ISO 17799, COBIT.

I. Introduction

SUCCESSFUL management of the Information Security process requires adequate control over a variety of documentation. Efficiency managing this documentation is not easy and usually requires an organized approach.

Organizations are therefore encouraged to design and implement a structured documentation to set an early stage. It is necessary to say that the issue of Information Security within an organization is a broad subject and is not limited to IT security. At present, there is an ongoing effort towards the standardization of practices and processes in order to ensure a high level of security with respect to all forms of information handled within an organization's scope of operation. In this document, an attempt will be made to introduce a brief comparative study of various security standards which are used in Information Security process [1].

The remainder of this paper is structured as follows: Section 2 tells the importance of Information Security in all aspects of our systems and products, followed by brief discussion in this section; we have a short overview of BS7799, ISO17799 and COBIT in section 3. Section 4 contains the comparison between the different standards and practices, followed by a conclusion.

II. What are Information Security and the Importance of Information–Security?

Current Information is an asset, which has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films or spoken in conversation. What ever form the information takes, or means by which it is shared or stored, it should always be suitably protected. Information security management enables information to be shared, whilst ensuring the protection of information and computing assets. It has three key components to provide assurances:

- Confidentiality – ensuring that information is accessible only to those authorized to have access.
- Integrity – safeguarding the accuracy and completeness of information and processing methods.
- Availability – ensuring that authorized users have access to information and associated assets when required.

There are many reasons Information Security is a big deal today. A few of most important are:

- Public companies are required to use security and control of financial information.
- There is considerable evidence of the risks and associated cost of Information Security threats and attacks.
- Computer systems and processes that have been built and implemented over the years have not been designed with the proper safeguard in place. Hence, there is a big security gap.
- The critical infrastructure of most organization is run by computers and is exposed to disruption and misuse of sensitive information.
- The growth of internet has connected people and opened opportunities but also has increased the risks and potential for security threats.

Complicating the problem is a number of associated issues. First, computer systems and information that support an organization's critical infrastructure are complex and widely distributed. Systems are interconnected and information is shared and communicated in a tangled web both inside and outside of the company. Second, security risks are not well understood and as a result investment in security has been lower than required. Third, traditional technology oriented solutions are necessary but not sufficient to solve the problem. As a result, security standards are not met and information and systems are exposed [2].

III. Security–Information Standards

If we want to have a good Security–Information, it is necessary to consider some factors such as:

Scalability: The cost-effectiveness of applying a particular set of security criteria depends on the relationship between the effort and costs involved in applying the criteria and the size or complexity of the object under investigation. If it is possible to control this effort, for example through different levels of detail, then it may be possible to contain the effort within bounds that are appropriate to the particular requirements.

Updateability: Rapid changes to the technical environment mean that sets of security criteria can quickly become outmoded. Their usefulness therefore depends also on whether their present version reflects the latest technology or not. This gives rise to the question of what procedures are in place for ensuring regular updates

Completeness / security level: The number of possible application fields for a particular set of security criteria depends on whether the criteria contained constitute a closed, exhaustive catalogue for the focal point concerned or whether only selected aspects are handled. The security level for which the relevant catalogue of criteria is suitable must be noted here.

Applicability to common enterprise structures: The possible applications of a particular set of security criteria in a specific environment frequently depend on how well it can be applied to common enterprise structures or whether the criteria are largely independent of specific enterprise structures as regards their possible applications thanks to a general, organization-wide approach.

Effort and costs of implementation: Whether a particular set of IT security criteria can be used at all depends not just on its applicability but not least also on the effort and costs associated with its use. These can in specific cases be very different, but standard values can be helpful for assessment in typical scenarios.

There are many standards in the Security–Information area, but we limit our discussion and only explain these standards: BS7799, ISO17799 and COBIT.

A. BS7799 [7]

BS7799 was originally published in 1995 to give guidance on implementing Security–Information Management and was substantially revised in April 1999 to take account of development in the application of information processing technology, particularly in the area of networks and communications. It also gave greater emphasize to business involvement in the responsibility for information technology. It is an international security standard allows an organization to understand and measure the threats, vulnerabilities and impacts that face its information security assets and to ensure that controls are in place to manage any subsequent risk.

BS 7799 is issued in two parts:

1. Part 1: It consists of code of practice for information security management.
2. Part 2: It consists of specification for information security management systems (ISMS).

Part I - ISO/IEC 17799:2000

It is a standard code of practice and serves as a comprehensive catalogue of good security practices. It defines 127 security controls structured under 10 major headings that enable readers to identify the particular safeguards that are appropriate to their particular business or specific area of responsibility. These security controls contain further detailed controls and thus, in total comprise more than 5,000 controls and elements of best practices in it.

Part II - BS 7799-2:2002

It was formally released on September 5, 2002. This latest edition harmonizes with other management system standards like ISO 9001:2000 and ISO 14001:1996. It introduced a Plan-Do-Check-Act (PDCA) model as part of a management system approach to developing, implementing and improving the effectiveness of the organization's information security management system. BS 7799- 2: 2002 standard is a comprehensive security framework covering 10 clauses, 36 objectives and 127 controls.

BS 7799 identifies 10 controls:

1. Security policy
2. Organization of assets and resources
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

B. ISO17799 [3]

ISO17799 resulted from BS7799. Part 1 of BS7799 become ISO standard 17799 in 2000 after being adopted by Joint Technical Committee ISO/IEC JTC1-Information Technology.

ISO17799, contrary to other security standards or proposed practices for IT systems, does not only cover IT security. It attempts to identify vulnerabilities and suggest controls for the security of information, irrespective of the form, method of handling and level of this information within an organization. ISO17799 forms an invaluable tool in identifying possible areas of vulnerabilities throughout any corporate structure. It does so by providing guidelines for the establishment of security requirements, the assessment of security risks and the selection of controls for identified vulnerabilities. However, ISO17799 can definitely not function as a technology guideline because it does not provide practical solutions to security-related problems of a technical nature.

ISO17799 attempts to be as broad as possible. This is probably the result of a strategy to guarantee ISO17799's wide acceptance. In this sense, small and medium enterprises may decide to deal with a subset of controls instead of considering

the full list. It is interesting to note the number of commercial packages emerging which are presumed compatible to ISO17799 and claim to provide for and support all security issues addressed in ISO17799. This trend also verifies the degree of acceptance of the standard.

ISO17799 is self-described as "a starting point for developing organization specific guidance". This signifies the fact that ISO17799 is not self-sufficient in providing for a total security solution. Consequently, the need for additional guidance in the form of a technical standard is highlighted.

If we want to consider above indicators in these standards, we should say that, in the point of view of scalability, BS7799 and ISO17799 are explicitly intended for institutions of any size and also for separately identifiable subsystems. They are also deal in principle with organizations of any size. Anyhow the measures are primarily oriented towards larger institutions. Much of the standards are relatively independent of the size of the institution under consideration, so that the effort is proportionally greater for a smaller institution. Only in the framework of risk analysis do the classical size-effort ratios apply, but the amount of effort required can be reduced by grouping objects. When a system is broken down into subsystems, there is then the problem of joining together the subsystems, as aggregation is not immediately possible.

About being up to date, we should know that the latest version of BS7799 is version 2 (1999), while ISO/IEC 17799 is still in version 1 (2000). It is planned that regular updates should occur – in accordance with the general approach for modification of ISO/IEC standards – but there are no fixed, organized, mandatory cycles.

If we want to discuss about Completeness and security level of these standards it should be said BS7799 and ISO17799 standards are heavily oriented to the top-down approach and primarily contain generic standard security measures. These measures cover all the areas of relevance. The standard does not contain any product-oriented measures and only heavily aggregated technology-oriented measures, as generally the measures contain only a moderate amount of detail. Generally these standards are not restricted to one specific security level, but the recommended measures are rather oriented to the baseline security approach and are only suitable for high to maximum security levels after modifications. When a somewhat low security level is claimed, these standards permit recommendations to be declined with justification, and modification to suit smaller enterprises.

The applicability of BS7799 and ISO17799 are largely independent of the institutional structure, although it is better suited to large institutions than to smaller ones, and it is possible to consider institutions and organizational areas with very high security requirements by making additions. On the basis of the management-oriented approach, restriction of applicability to particular technical systems and system types cannot be assumed.

About effort and costs of implementation of these standards it is necessary to say that the strong emphasis on organizational measures makes the effort required for implementation heavily dependent on the general organizational quality of an institution. Institutions which are not well organized require significantly more effort than ones that are advanced organized. The baseline security approach generally makes it possible – without additional costs to use existing measures in the enterprise to increase the security level in optimal fashion. The effort required to perform the analysis is largely determined by the scope of the risk analysis. The choice of risk analysis type has a major effect on the amount of effort required.

C. COBIT

COBIT issued by the IT Governance Institute, is a generally applicable and internationally accepted standard for good Information Technology (IT) security and control practices. It provides a reference framework for management, users, and Information Security (IS) audit, control and security practitioners also provides guidance that enables an enterprise to implement effective governance over IT. [5,6]

COBIT is designed to be the breakthrough IT governance tool that helps in understanding and managing the risks and benefits associated with information and related IT. It is a tool that allows managers to bridge the gap with respect to control requirements, technical issues and business risks and communicate that level of control to stakeholders.

In the point of view of scalability, COBIT's matrix structure is made for the user to consider only individual domains or processes and/or to select a subset from the seven business requirements.

About being up to date it should be mentioned that COBIT was issued by the Information System Audit and Control Foundation (ISAFC) in 1996. In 1998 the second edition was published with additional control objective and implementation tool set. The third edition currently available was issued by the IT Governance Institute in 2000.

About completeness of security level of COBIT, it is necessary to say that, COBIT offers a method for recording IT-oriented and accompanying processes. The associated control objectives are defined independently of technology and can be used for different system environments. However, to create security concepts it is necessary to add extra system-specific measures. COBIT is oriented to the security interests of a typical enterprise. Preservation of fundamental company interests (integrity and confidentiality of internal information and processes) and also adherence to statutory regulations (data privacy protection, financial reporting) are considered. There is no fixed security level, orientation is to enterprise objectives.

In the point of view of being applicable, COBIT can be used as a process-oriented method independently of the internal structure or legal form of an enterprise.

About effort and costs of implementation of COBIT it should be mentioned that complete analysis of all control objectives within a medium-sized enterprise with COBIT should take no longer than one working month.

COBIT structure includes:

1. Implementation Tool Set

It provides lesson learned from those organizations that have successfully applied COBIT in their work environment. In order to help an organization in analyzing its control environment, the tool set has two useful tools:

1. Management Awareness Diagnostic
2. IT Control Diagnostic

2. Framework

The COBIT framework provides IT governance guidance.

3. Management Guidelines

The Management Guidelines enhance and enable enterprise management to deal more effectively with the needs and requirements of IT governance. It provides:

1. Maturity Models for control over IT processes
2. Critical Success Factors that define the most important management–oriented implementation guidelines.
3. Key Goal Indicators that define the process goal or a target to achieve and also is a measurable indicator of the process achieving its goals.
4. Key performance Indicator, which are the indicators that define measures of how well the IT process is performing in enabling to meet goals.

4. Control Objectives

COBIT also provides and focuses on high level controls for each IT processes. These Control Objectives are directed to the management and staff of the IT, control and audit functions and especially to the owners of the business. It contains statement of the desired results by implementing specific control procedures within an IT activity and thus, provides a clear policy and good practice for IT control throughout the industry.

These controls include a set of 34 high–level control objectives, one for each of the IT processes, grouped into four domains:

1. Planning and organization
2. Acquisition and implementation
3. Delivery and support
4. Monitoring

IV. Combination of Information Technology Security Standards

Studying of the standards which have been introduced in the previous section shows that each of theses security standards has its own weak points and strong points. For example BS7799 and ISO17799 are very powerful in establishing an Information Security Management System (ISMS) but COBIT has very strong control objectives that help in understanding and managing the risks and benefits associated with information and related IT. If we compare theses standards, it results from the indicators that are introduced in past section, BS7799 and ISO17799 have a complete level of security that covers all aspects of security information but it should be mentioned these standards only cover the information security of a system and don't contain any product–oriented measures. In order to have security in our products it is recommended to use another standard such as ISO15000. COBIT just offers a method for recording IT–oriented and accompanying processes. Therefore for having a complete measurement in aspect of information security, it is necessary to add some extra system–specific measures in order to have a complete measurement it is also important to consider that COBIT does not have any specific level of security, and it changes from one system to another system. In fact ISO17799 and COBIT have many common in points and in some cases they complete each other, so combination of them can be resulted in a very comprehensive standard. In the other word by combining some of complementary information security standards, we can provide a complete standard with powerful control objectives, strong guidance for establishing Information Security Management System, and IT Service Management services and businesses.

As a result of the above discussion, since we are in IT era, it is too important to have security in our information systems. To achieve such a complete Information Security and for covering national requirements it is necessary to have a powerful control objectives, strong guidance for establishing Information Security Management System, and IT Service Management services and businesses. Therefore it is recommended to specify our requirements and consider all the aspects of Information Security and combine different sets of standards to arrive at complete security information at both system and product levels [4].

V. Conclusion

This comparative study has shown that each of the examined documents approach the issue of security from different angles. ISO 17799 and BS7799-2 attempt to provide a total solution for Information Security, reaching a practical level of implementation in the form of controls. COBIT is designed to be the breakthrough IT governance tool that helps in understanding and managing the risks and benefits associated with information and related IT. In the section 4 we have suggested that in order to achieve better Security Information in our systems and products it is recommended to combine different security standards.

For an Information Security Management System implementation should be truly effective, one should be able to objectively measure its compliance to the directives and principles by which it is designed. The issue of security compliance and measuring still remains open and a great amount of research effort is expected to be directed in this area.

Acknowledgment

The authors would like to thank Iran Telecommunication Research Centre (ITRC) for its financial and scientific support.

REFERENCES

[1] Executive Brief: Managing Security Risk–Value of a Security Program Approach February 2004.
[2] Evangeles D. Frangopoulos, Mariki M. Eloff, "A Comparative Study of Standards and Practices Related to Information Security Management" Cairo, Egypt, 2004.
[3] Tom Carlson, "Understanding ISO17799", Principal Consultant - Information Protection & Assurance HotSkills, Inc.
[4] Information Security Forum, "The Standard of Good Practice for Information Security," Version 4, March 2003..
[5] Information Systems Security Association (ISSA), "The Generally Accepted Information Security Principles (GAISP)", in preparation.
[6] Information Technology Governance Institute, "Information Security Governance: Guidance for Boards of Directors and Executive Management," 2001.
[7] WWW.bsi–global.com