On the Inter-dependence of Security Controls of ISO/IEC 27002:2005

Anil K. Kaushik*
Anirban Sengupta**
Chandan Mazumdar**
P. Banerjee***

Abstract

An enterprise is viewed as a collection of assets and their interrelationships. These assets contain vulnerabilities, which may be exploited by threats to breach information security aspects of enterprises. In order to prevent this, security controls need to be implemented. ISO/IEC 27002:2005 is a widely accepted security standard that contains details of enterprise security controls. These controls are inter-dependent. The present study proposes a model of control-dependence for ISO/IEC 27002.

Keywords: Enterprise Information Security, Security controls, Control dependence, Risk Management, ISO/IEC 27002

1. Introduction

An "enterprise" [1] can be viewed as a collection of assets, including Information Assets, Software Assets, Hardware Assets and People [2, 3]. Different assets and their interrelationships may contain inherent weaknesses, or vulnerabilities [3], which can be exploited by threats [3], resulting in the disruption of business functions of the enterprise. Risk analysis [4] is performed to determine the impact and likelihood of harm that may occur in case of such security incidents. Based on the results of risk analysis, a set of information security controls [3] are identified, and implemented, in order to mitigate the identified risks.

Security controls are safeguards, or countermeasures, for managing risks to enterprise assets. They may include policies, procedures, guidelines, practices or organizational structures. A security policy [5] consists of sets of high-level statements of enterprise beliefs, goals, and objectives, and the general means for their attainment, in order to secure an enterprise. A security procedure [5] details the steps needed to implement a security policy. Usually, each security policy has a corresponding procedure. A guideline [3] is a description that clarifies what should be done, and how, to achieve the objectives set out in security policies. There are several information security

*Dept. of Information Technology, 6, CGO Complex, New Delhi, India.
**Dept. of Comp. Sc. & Engg., Jadavpur University, Kolkata, India.
***National Institute of Science Technology and Development Studies, New Delhi, India.

standards containing details of security controls that may be followed by enterprises in order to manage risks. Some of them are ISO/IEC 27002:2005 [3], COBIT [6], NIST SP 800-53 [7], and IT Baseline Protection Manual [2]. But, owing to its generic nature and flexibility, ISO/IEC 27002 is the most widely accepted security standard today.

While some security controls of ISO/IEC 27002 are independent, several others are inter-dependent. It is extremely important to consider the inter-dependence of controls while implementing them in an enterprise. But, owing to lack of proper research and guidance, this aspect is often overlooked during control implementation, resulting in an incomplete risk management exercise. It may further lead to the advent of newer risks in an enterprise. This paper addresses this research problem by presenting an analytical study of the inter-dependence of security controls of ISO/IEC 27002. It will enable an enterprise to formulate and implement a proper control implementation programme, which will help in mitigating all identified information security risks without opening up newer ones.

Rest of this paper is organized as follows. Section 2 presents a survey of related work. Section 3 details the structure of ISO/IEC 27002 and classifies its controls. Our control dependency model is described in Section 4, while its utility is discussed in Section 5. Finally, Section 6 concludes the paper.

2. Related Work

Some references of related controls are included in the Implementation guidance section of particular controls in ISO/IEC 27002 [3]. But, this is not an exhaustive reference list. It has been left for the security analyst to apply his judgment and skill in determining the complete inter-dependency of security controls. To the best of our knowledge, there has not been any exhaustive study to detail this inter-dependency that will help to implement a fool-proof control implementation programme.

Our study addresses this research problem and proposes a comprehensive inter-dependency list of the security controls of ISO/IEC 27002.

3. Structure of ISO/IEC 27002:2005

ISO/IEC 27002 consists of 11 clauses (excluding an introductory clause on Risk Assessment and Treatment) as shown in Table I. Each clause consists of several main security categories [3]. Each main security category contains:

a. a control objective stating what is to be achieved; and

b. one or more controls that can be applied to achieve the control objective.

Table I
Clauses of ISO/IEC 27002:2005

Clause No.	Clause Name
5	Security Policy
6	Organization of Information Security
7	Asset Management
8	Human Resources Security
9	Physical and Environmental Security
10	Communications and Operations Management
11	Access Control
12	Information Systems Acquisition, Development and Maintenance
13	Information Security Incident Management
14	Business Continuity Management
15	Compliance

The control structure of ISO/IEC 27002 is illustrated in Fig. 1, where a main security category is shown along with its controls.

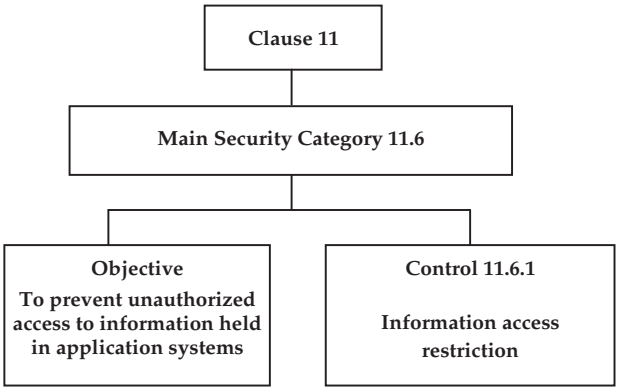

Fig. 1 Control structure of ISO/IEC 27002:2005

ISO/IEC 27002 consists of 133 security controls grouped into 39 main security categories. A control can be either of four types: administrative, management, technical, or legal. Administrative controls suggest measures that are either supervisory in nature or deal with critical policy decisions (e.g. Information security policy document and Management commitment to information security). Management controls pertain to organizational measures (e.g. Capacity management and Password use). Technical controls suggest specific tools and techniques to achieve security (e.g. Segregation in networks and Session time-out). Legal controls contain references to laws and regulations that are needed to maintain security and achieve compliance (e.g. Confidentiality agreements and Intellectual property rights). It is important to note that some controls are hybrid in nature; they suggest more than one type of measure. E.g. Control of operational software suggests both management (monitoring of users) as well as technical (access control techniques) measures. Based on the above criteria, we have categorized the controls of ISO/IEC 27002 as shown in Table II.

Table 2 Controls of ISO/IEC 27002:2005 and their types (A – Administrative, M – Management, T – Technical, L - Legal)

Control No.	Type	Control No.	Type	Control No.	Type
5.1.1	A	10.2.2	A, L	11.5.4	M, T
5.1.2	A	10.2.3	M, L	11.5.5	T
6.1.1	A	10.3.1	M	11.5.6	T
6.1.2	M	10.3.2	M	11.6.1	M, T, L
6.1.3	M	10.4.1	M, T	11.6.2	M, T
6.1.4	M, T	10.4.2	M, T	11.7.1	A, M, T
6.1.5	L	10.5.1	M, T, L	11.7.2	A, M, T
6.1.6	M, L	10.6.1	M, T	12.1.1	A, M
6.1.7	M	10.6.2	M, T	12.2.1	M, T
6.1.8	A	10.7.1	M, T, L	12.2.2	M, T
6.2.1	M	10.7.2	M, T, L	12.2.3	M, T
6.2.2	M, T, L	10.7.3	M, T, L	12.2.4	M, T
6.2.3	M, T, L	10.7.4	M, T	12.3.1	M, L
7.1.1	M	10.8.1	M	12.3.2	M, T, L
7.1.2	M, L	10.8.2	L	12.4.1	M, T
7.1.3	M, T, L	10.8.3	M, T	12.4.2	M, T
7.2.1	A	10.8.4	M, T	12.4.3	M, T
7.2.2	M, T, L	10.8.5	A, M, T	12.5.1	M
8.1.1	M	10.9.1	A, M, T	12.5.2	M, T
8.1.2	M	10.9.2	M, T, L	12.5.3	M, T
8.1.3	L	10.9.3	A, M, T	12.5.4	M, T
8.2.1	M	10.10.1	M, T	12.5.5	A, M, T, L
8.2.2	A	10.10.2	A, T	12.6.1	M, T
8.2.3	A, L	10.10.3	M, T, L	13.1.1	M
8.3.1	M	10.10.4	M, T, L	13.1.2	M
8.3.2	M, L	10.10.5	M, T, L	13.2.1	A, M
8.3.3	M, T, L	10.10.6	M, T, L	13.2.2	M
9.1.1	M, T	11.1.1	A, M, L	13.2.3	M, T, L
9.1.2	M, T	11.2.1	M, T	14.1.1	A, L
9.1.3	M, T	11.2.2	M, T	14.1.2	M, T
9.1.4	M, T	11.2.3	M, T	14.1.3	M, T, L
9.1.5	A, M, T	11.2.4	M	14.1.4	A, M, L
9.1.6	M	11.3.1	M	14.1.5	M, T, L
9.2.1	M, T	11.3.2	M, T	15.1.1	A, L
9.2.2	M, T	11.3.3	M, T	15.1.2	L
9.2.3	M, T	11.4.1	M, L	15.1.3	M, T, L
9.2.4	M, T, L	11.4.2	T	15.1.4	M, T, L
9.2.5	M, T, L	11.4.3	T	15.1.5	M, T, L
9.2.6	M, T, L	11.4.4	T	15.1.6	M, T, L
9.2.7	M, T, L	11.4.5	T	15.2.1	M, L
10.1.1	M, L	11.4.6	T	15.2.2	M, T, L
10.1.2	M, T, L	11.4.7	T	15.3.1	M, T, L
10.1.3	M, T, L	11.5.1	M, L	15.3.2	M, T, L
10.1.4	M, T, L	11.5.2	T		
10.2.1	M, L	11.5.3	M, T		

The inter-and intra-dependence of these controls are detailed in subsequent sections.

4. Inter-dependence of Controls

Analysis of the controls of ISO/IEC 27002 reveals an interesting inter-dependence pattern. In case of 29 main security categories (out of total 39 categories), the presence (or absence) of the first control determines the need of all other controls of that category. In other words, if the first control of a main security category (belonging to the set of 29 main security categories, as mentioned) is not required for a particular enterprise, then none of the other controls in that particular category can be present. The need of these other controls is inter-dependent on that of the first control of their main security category. This is illustrated by an example in Fig. 2.

Main security category 10.2 (Third Party Service Delivery Management) consists of 3 controls. The first control is Service delivery (10.2.1), while the second and third controls are Monitoring and review of third party services (10.2.2) and Managing changes to third party services (10.2.3), respectively. As is obvious, the presence of controls 10.2.2 and 10.2.3 depend on the presence (or absence) of the first control 10.2.1 (since, if there is no control for third party service delivery, the question of monitoring and managing those services does not arise).

But, there are 10 main security categories that do not follow the pattern stated above. These categories and the corresponding controls are listed in Table III. All controls in main security categories 10.3, 10.7, 11.3, 11.7, 12.2, 12.4, 13.1, 15.2, and 15.3 are independent. However, in case of main security category 12.5, only two controls (12.5.4 and 12.5.5) are independent. Controls 12.5.2 and 12.5.3 are dependent on the first control (12.5.1) of this category.

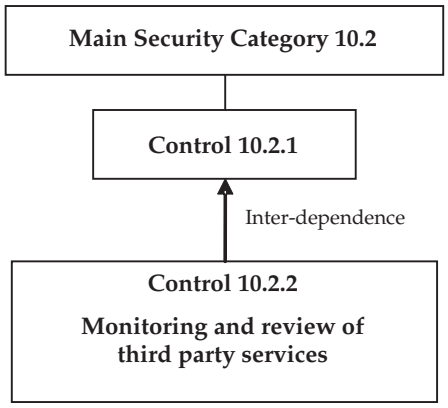

Fig. 2 Inter-dependence of controls of ISO/IEC 27002:2005

It may be noted that there is no inter-dependence of controls across main security categories (and hence, clauses). In other words, a control belonging to a main security category, say A, will not be dependent on a control belonging to another main security category, say B. This is due to the fact that the objectives of different main security categories are different; they do not overlap.

Table 3
Independent Controls of ISO/IEC 27002:2005

Main Security Category	Independent Controls
10.3: System Planning and Acceptance	10.3.1: Capacity management 10.3.2: System acceptance
10.7: Media Handling	10.7.1: Management of removable media 10.7.2: Disposal of media 10.7.3: Information handling procedures 10.7.4: Security of system documentation
11.3: User Responsibilities	11.3.1: Password use 11.3.2: Unattended user equipment 11.3.3: Clear desk and clear screen policy
11.7: Mobile Computing and Teleworking	11.7.1: Mobile computing and communications 11.7.2: Teleworking
12.2: Correct Processing in Applications	12.2.1: Input data validation 12.2.2: Control of internal processing 12.2.3: Message integrity 12.2.4: Output data validation
12.4: Security of System Files	12.4.1: Control of operational software 12.4.2: Protection of system test data 12.4.3: Access control to program source code
12.5: Security in Development and Support Processes	12.5.4: Information leakage 12.5.5: Outsourced software development
13.1: Reporting Information Security Events and Weaknesses	13.1.1: Reporting information security events 13.1.2: Reporting security weaknesses
15.2: Compliance with Security Policies and Standards, and Technical Compliance	15.2.1: Compliance with security policies and standards 15.2.2: Technical compliance checking
15.3: Information Systems Audit Considerations	15.3.1: Information systems audit controls 15.3.2: Protection of information systems audit tools

A. Inter-dependence in Hybrid Controls

In case of hybrid controls, there exists some intra-dependence between elements of a single control. As described in Section 3 above, a hybrid control suggests more than one type of measure. E.g. Input data validation (Control 12.2.1 in Table II) suggests both management (implementation and monitoring of validation checks) as well as technical (validation checks) measures. It may be observed that the technical measure depends on the presence of the management measure. If a management function does not implement the validation check, then the technical measure will not be in place. Such intra-dependence exists between the control elements (suggested measures) of all hybrid controls. The intra-dependence rules for hybrid controls are stated as follows:

(R4.1.1) If a hybrid control, say CH, suggests an administrative measure, say CHa, then the need of all other measures suggested by CH, namely management (CHm), technical (CHt), and/or legal (CHl), will depend on the presence of CHa.

(R4.1.2) If a hybrid control, say CH, suggests a management measure, say CHm, then the need of any other technical (CHt) and/or legal (CHl) measures suggested by CH, will depend on the presence of CHm.

These rules are illustrated in Fig. 3 below.

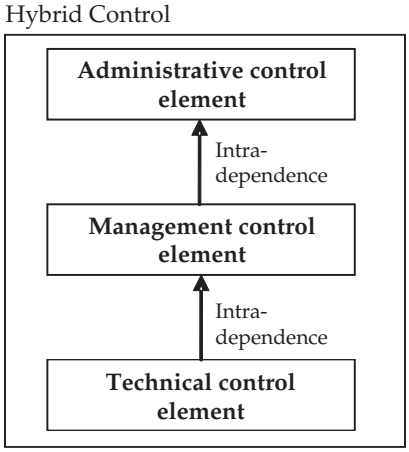

Fig. 3 Inter-dependence of elements of hybrid controls

5. Utility of Proposed Control Dependency Model

As has been stated in Section 1 above, an enterprise needs to implement security controls in order to mitigate risks. This is usually carried out as part of an Information Security Management System (ISMS) of an enterprise [8]. ISO/IEC 27001:2005 security standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving ISMS within an enterprise [8]. It suggests several controls in an annexure, which are further detailed in ISO/IEC 27002 [3]. After implementing ISMS and security controls as per ISO/IEC 27001 and 27002, an enterprise may apply for a formal security certification. One of the primary requirements of compliance with ISO/IEC 27001 and 27002 is the preparation of a Statement of Applicability (SoA), which justifies the need for each security control. A sample SoA is shown in Table IV. A complete SoA of an enterprise consists of 133 rows (each row corresponding to a security control of ISO/IEC 27002).

Table 4 : Sample Statement of Applicability (SOA) based on the controls of ISO/IEC 27002:2005

Control No.	Control Name	Applicable (Y/N)	Justification
5.1.1	Information security policy document	Y	The enterprise deals with sensitive information and hence, needs an information security policy document.
7.1.1	Inventory of assets	Y	The enterprise consists of several critical assets, and hence needs to maintain an inventory.
10.9.1	Electronic commerce	N	The enterprise does not practice electronic commerce
11.2.1	User registration	Y	The enterprise has numerous users of information systems.
12.5.5	Outsourced software development	N	The enterprise does not outsource any software development.

It is extremely important to prepare the SoA judiciously and correctly, since the control implementation programme uses this as its reference point. Implementation of irrelevant controls may lead to overkill and unnecessary investment. Similarly, ignoring necessary controls may lead to security breaches in an enterprise. Also, certifying authorities check the SoA thoroughly; an incorrect SoA will result in an enterprise failing to get ISO/IEC 27001 certification.

Often, lack of knowledge of dependent controls leads to the preparation of incorrect SoA. Our proposed control dependency model will help enterprises in choosing security controls of ISO/IEC 27002 properly. In order to illustrate this, we consider two cases, namely a data centre and the branch office of a banking enterprise, and two security controls, namely Information security policy document (5.1.1) and Information exchange policies and procedures (10.8.1). In case of the branch office of a bank, both of these security controls (and hence, all of their dependent controls) are applicable. But, in case of a data centre, information exchange with another entity should not be allowed. Hence, control 10.8.1 is not applicable. Now, based on our proposed model of control dependency (as illustrated in Fig. 2 above), the need of all other controls of main security category 10.8, namely controls 10.8.2, 10.8.3, 10.8.4, and 10.8.5 (as listed in Table II above) depend on the need of control 10.8.1. Since, control 10.8.1 is not applicable for a data centre, all other controls of main security category 10.8 are also not applicable. Thus, our control dependency model helps an enterprise to select the controls that are applicable and necessary for its business functions. This leads to the preparation of a correct SoA, and the implementation of a proper control implementation programme and ISMS.

6. Conclusion and Future Work

This paper begins by classifying the security controls of ISO/IEC 27002:2005. Then, the inter-dependence of these controls has been detailed. It has been shown that in most cases, the first control of a main security category determines the need of the other controls in that category. There are a few exceptions, which have been listed in Table III. The intra-dependence of the control elements of a hybrid control has also been described. The paper ends with a discussion on the usefulness of the proposed control dependency model.

Thus, in this paper, we have attempted to model the dependencies of security controls of ISO/IEC 27002. This will help security analysts and implementers to design a fool-proof control implementation programme, where all necessary controls are addressed. As has been stated in Section 1, incomplete or missing controls create vulnerabilities in enterprise information systems. Often, this occurs due to the implementers' inability to determine all dependent controls. This paper tries to ease this task by presenting a generic model of control dependency.

Future work is geared towards designing and developing a tool suite that will use our control dependency model to suggest appropriate security controls for an enterprise.

Acknowledgment
Most of the concepts presented in this paper have evolved during the execution of a couple of R&D Projects sponsored by the Department of Information Technology, Govt. of India.

7. References

1. *C. Soanes, and A. Stevenson, (eds.), "Concise Oxford English Dictionary", Eleventh Edition, Oxford University Press, New York, USA, pp. 475, 2006.*
2. *Federal Office for Information Security, "IT Baseline Protection Manual", Germany, 2007.*
3. *The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC), "ISO/IEC 27002:2005, Information technology – Security techniques - Code of practice for information security management", Edition 1, Switzerland, 2005.*
4. *T.R. Peltier, "Information Security Risk Analysis", Third Edition, Auerbach Publications, USA, 2010.*
5. *T.R. Peltier, "Information Security Policies and Procedures", Second Edition, Auerbach Publications, USA, 2004.*
6. *IT Governance Institute, "Control Objectives for Information and related Technology (COBIT) 4.1", IL, USA, 2007.*
7. *R. Ross, et. al., "Recommended Security Controls for Federal Information Systems", NIST Special Publication 800-53 Revision 3, MD, USA, 2009.*
8. *The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC), "ISO/IEC 27001:2005, Information technology – Security techniques - Information security management systems – Requirements", Edition 1, Switzerland, 2005.*