Information Systems Security Management: A Review and a Classification of the ISO Standards

Aggeliki Tsohou, Spyros Kokolakis, Costas Lambrinoudakis, and Stefanos Gritzalis

Dept. of Information and Communication Systems Engineering,
University of the Aegean, Samos GR-83200, Greece
{agt,sak,clam,sgritz}@aegean.gr

Abstract. The need for common understanding and agreement of functional and non-functional requirements is well known and understood by information system designers. This is necessary for both: designing the "correct" system and achieving interoperability with other systems. Security is maybe the best example of this need. If the understanding of the security requirements is not the same for all involved parties and the security mechanisms that will be implemented do not comply with some globally accepted rules and practices, then the system that will be designed will not necessarily achieve the desired security level and it will be very difficult to securely interoperate with other systems. It is therefore clear that the role and contribution of international standards to the design and implementation of security mechanisms is dominant. In this paper we provide a state of the art review on information security management standards published by the International Organization for Standardization and the International Electrotechnical Commission. Such an analysis is meaningful to security practitioners for an efficient management of information security. Moreover, the classification of the standards in the clauses of ISO/IEC 27001:2005 that results from our analysis is expected to provide assistance in dealing with the plethora of security standards.

Keywords: Information security management systems, standardization.

1 Introduction

Standardization is the process of developing and agreeing upon technical standards. A standard is a document that establishes uniform engineering or technical specifications, criteria, methods, processes, or practices [1]. Standards may fall into one of the following categories: International standard (a standard adopted by an international standards organization and made available to the general public), European standard (a standard adopted by a European standards organization and made available to the general public), and National standard (a standard adopted by a national standards organization and made available to the general public) [2]. The International Organization for Standardization's (ISO) [3] standards and guides for conformity assessment represent an international consensus on best practices. Their use contributes to the consistency of conformity assessment worldwide and so facilitates trade. Joint ISO/IEC International Standards and guides for conformity assessment, encourage best practice and consistency when products, services, systems, processes and materials need to be evaluated against standards, regulations or other specifications.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 220–235, 2010.

In this paper we provide a state of the art review of standards that guide information security management and its sub-areas. Such an enlisting of information security management standards would be useful to security practitioners in order to have a clear picture of current security standardization. Also in this paper, we reduce the complexity of the plethora of security standards by revealing the interrelation among them.

The paper is organized in five sections. The following two sections are dedicated to information security management systems and information security risk management standards and the information security management specific areas' standards respectively. Section 4 presents a classification of the standards according to the ISO/IEC 27001:2005 [4] security clauses. Finally, in section 5 we highlight the limitations of this work and we provide suggestions for future work.

2 Information Security Management Systems Standards

A series of security standards define and guide the procedures of implementing information security management. Information security management is the process by which an organization aims to achieve effective confidentiality, integrity and availability of its information and services. An information security management system (ISMS) refers to that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources (ISO/IEC 27001:2005 [4]).

2.1 Concepts and Models for Information and Communications Technology (ICT) Security Management

The ISO/IEC 13335-1:2004 [5] standard is dedicated in providing government and commercial organizations' managers a high-level management overview of an overall security program for ICT systems. It focuses on concepts and models for managing the planning, implementation and operations of ICT security. The series ISO/IEC 13335 also included ISO/IEC TR 13335-2:1997 [6] that has been withdrawn and revised by the ISO/IEC 13335-1:2004 [5]. It also included the ISO/IEC 13335-3:1998 [7] and ISO/IEC 13335-4:2000 [8] that have been withdrawn and revised by ISO/IEC 27005:2008 [9] (Section 2.3). Finally, it included ISO/IEC 13335-5:2001 [10] that has been revised by ISO/IEC 18028-1:2006 [11] (see Section 3.1).

2.2 Information Security Management Systems

Overview and Vocabulary

ISO/IEC 27000:2009 [12] provides an overview of information security management systems and defines terms which are related to the overall ISMS family of standards.

Code of Practice

ISO/IEC 27002:2005 [13] is highly interrelated to ISO/IEC 27001:2005 [4], and establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It provides general guidance on the commonly accepted goals of information security management. The control objectives and controls that it proposes are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 [13] revises the well-known ISO/IEC 17799:2005 [14] standard. The structure of the best practices includes 11 control clauses that contain 39 objectives aimed by 133 controls. The 11 clauses are:

- ✓ Security Policy
- ✓ Organizing Information Security
- ✓ Asset Management
- ✓ Human Resources Security
- ✓ Physical and Environmental Security
- ✓ Communications and Operations Management
- ✓ Access Control
- ✓ Information Systems Acquisition, Development and Maintenance
- ✓ Information Security Incident Management
- ✓ Business Continuity Management
- ✓ Compliance

Each main clause includes one (or more) control objectives stating what is to be achieved and one or more controls that can be applied to achieve the related control objective.

Requirements

ISO/IEC 27001:2005 [4] applies to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations), regardless of type, size and nature. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization’s overall business risks. ISO/IEC 27001:2005 [4] 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, as further described in the ISO/IEC 27002:2005 [13].

The standard proposes the application of a system of processes within an organization, together with the identification and interactions of these processes, and their management. Such a system is further referred to as a “*process approach*”, which is structured in the circular "Plan-Do-Check-Act" (PDCA) model. The processes of “Planning” an ISMS, begin with the definition of its scope, boundaries and an ISMS policy. Continuing, a systematic approach to information security risk management is necessary (see section 2.3). Such a risk management approach is described in the standard, but specified in detail in ISO/IEC 27005:2008 [9]. In sequence, the processes of obtaining management authorization to implement and operate the ISMS and preparing a Statement of Applicability (SOA[1]) are suggested. The processes of “Doing” include the

[1] SOA is a documented statement describing the control objectives and controls that are relevant and applicable to the organization’s ISMS.

implementation of risk treatment plan (described within the ISO/IEC 27005:2008 [9]), the definition of the way the effectiveness of the selected controls will be measured, the implementation of security awareness and training programs, and also managing the operation and resources of the ISMS and implementing procedures for prompt detection of response to security events. The third phase of the PDCA model includes continual monitoring and reviewing of risks (described in ISO/IEC 27005:2008 [9]), monitoring and reviewing procedures that promptly identify attempted and successful security breaches and incidents, and errors, undertaking regular reviews of the effectiveness of the ISMS, and measure the effectiveness of controls. The final “Act” phase refers to maintaining and improving the risk management process (described in the ISO/IEC 27005:2008 [9]), and also taking the appropriate corrective and preventive actions, communicating the actions and improvements to all interested parties and ensuring that the improvements achieve their intended objectives.

Implementation Guidance

Complementary advice on ISMS implementation will be provided by the ISO/IEC FCD 27003 [15], which is under development.

Guidelines for Telecommunications Organizations Based on ISO/IEC 27002

ISO/IEC 27011:2008 [16] provides guidelines for supporting the implementation of information security management in telecommunications organizations. The adoption of these guidelines will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security properties.

Auditing

Similarly, auditing guidance for ISMSs will be provided by the ISO/IEC WD 27007 [17], which is under development.

Certification

ISO/IEC 27006:2007 [18] specifies requirements and provides guidance for bodies providing audit and certification of ISMSs. It is primarily intended to support the accreditation of certification bodies providing ISMS certification. ISO/IEC 27006:2007 [18] strongly correlates to ISO/IEC 17021:2006 [19] which sets out criteria for bodies operating audit and certification of organizations' management systems. ISO/IEC 27006:2007 [18] is required because additional requirements and guidance to ISO/IEC 17021:2006 [19] are required for the auditing and certification of ISMSs according to ISO/IEC 27001:2005 [4].

2.3 Information Security Risk Management Standard

ISO/IEC 27005:2008 [9] provides guidelines for information security risk management and revises the former ISO/IEC 13335-3:1998 [7] and ISO/IEC 13335-4:2000 [8]. It supports the general concepts specified in ISO/IEC 27001:2005 [4] and describes a risk management approach to assist the implementation of information security. The concepts, models, processes and terminologies described in ISO/IEC 27001:2005 [4] and ISO/IEC 27002:2005 [13] are essential for the understanding of

ISO/IEC 27005:2008 [9]. ISO/IEC 27005:2008 is also applicable to all types of organizations.

Risk management process is described to include the activities of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review. Context establishment involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organization operating the information security risk management. Risk assessment involves the identification, description of risks (quantitatively or qualitatively), and prioritization of risks against risk evaluation criteria and objectives. Risk treatment contains the selection of controls to reduce, retain, avoid, or transfer the risks and the definition of a risk treatment plan. Risk acceptance includes the decision to accept the risks and the recording of accepted risks with justification for those that do not meet the organization's normal risk acceptance criteria (e.g. because the cost of risk reduction is too high). Risk communication refers to the exchange and sharing of information about risk between the decision-maker and other stakeholders. Finally, risk monitoring and review includes the monitoring of risks and their factors (i.e. value of assets, impacts) and their reviewing in case of any changes in the context of the organization.

3 Information Security Management Specific Areas' Standards

3.1 Network Security Management

ISO/IEC 18028 series include five standards that provide guidance for network security management. The series ISO/IEC 18028 will be revised by the upcoming ISO/IEC 27033. ISO/IEC 18028-1:2006 [11] provides detailed guidance on the security aspects of the management, operation and use of Information Technology (IT) networks, and their interconnections. To do so, it defines and describes the concepts associated with, and provides management guidance on, network security. Its audience includes anyone who owns, operates or uses a network. The standard will be revised by the upcoming ISO/IEC FCD 27033-1 [20]. ISO/IEC 18028-2:2006 [21], serves as a foundation for developing the detailed recommendations for end-to-end network security. The standard will be revised by ISO/IEC WD 27033-2 [22]. ISO/IEC 18028-3:2005 [23] outlines the techniques for security gateways to analyze network traffic. The techniques discussed are packet filtering, stateful packet inspection, application proxy, network address translation, content analyzing and filtering. Also, provides guidelines for the selection and configuration of security gateways. It will be revised by ISO/IEC NP 27033-4 [24]. The fourth part provides guidance for securely using remote access and its implication for IT security. It introduces the different types of remote access including the protocols in use, discusses the authentication issues related to remote access and provides support when setting up remote access securely. ISO/IEC 18028-4:2005 [25] will be revised by ISO/IEC NP 27033-5 [26]. The final part provides detailed guidance on the security aspects of the management, operation and use of IT networks, and their inter-connections. It defines techniques for securing inter-network connections that are established using virtual private networks (VPNs). ISO/IEC 18028-5:2006 [27] will be revised by the ISO/IEC NP 27033-6 [28]. Additionally, the series ISO/IEC 27033 will include ISO/IEC WD 27033-3 [29].

Intrusion Detection Systems

ISO/IEC 18043:2006 [30] provides guidance for including an intrusion detection capability within an organizations' IT infrastructure. ISO/IEC 18043:2006 [30] provides a brief overview of the intrusion detection process, discusses the benefits and limitations of an intrusion detection system, and provides a checklist that helps identify the best features for a specific IT environment, describes various deployment strategies, provides guidance on managing alerts and discusses management and legal considerations.

3.2 Auditing

Guidelines

As already mentioned in section 2.2, auditing guidelines for ISMSs will be provided ISO/IEC WD 27007.

Time-Stamping Services

ISO/IEC 18014 series specify time-stamping techniques. It consists of three parts, which include the general notion, models for a time-stamping service, data structures, and protocols. ISO/IEC 18014-1:2008 [31] describes a framework and defines the basic notion, the data structures, and protocols which are used for any time-stamping technique. It identifies the objective of a time-stamping authority, describes a general model on which time-stamping services are based, describes a process of generating and verifying time-stamp, defines the data structures of time-stamp token, defines the basic protocols of time-stamping and specifies the protocols between the involved entities. ISO/IEC 18014-2:2002 [32] describes time-stamping services producing independent tokens, time-stamps using digital signatures, message authentication codes and archiving. ISO/IEC 18014-3:2004 [33] describes time-stamping services producing linked tokens, that is, tokens that are cryptographically bound to other tokens produced by these time-stamping services.

3.3 Trusted Third Parties (TTPs)

ISO/IEC TR 14516:2002 [34] provides guidance for the use and management of TTPs, a clear definition of the basic duties and services provided their description and their purpose, and the roles and liabilities of TTPs and entities using their services. ISO/IEC TR 14516:2002 [34] identifies different major categories of TTP services including: time stamping, non-repudiation, key management, certificate management, and electronic notary public. The guidance for TTP services to support the application of digital signatures is provided by ISO/IEC 15945:2002 [35].

3.4 Incident Management

ISO/IEC TR 18044:2004 [65] does not possess the status of an International Standard, but rather it is published as a Technical Report. Technical reports can either be transformed into International Standards after being reviewed within three years of publication or are normally published as an International Standard until the data they provide are considered to be no longer valid or useful. The report is interrelated with the ISO/IEC 13335-1:2004 [5] and ISO/IEC 27002:2005 [13].

ISO/IEC TR 18044:2004 [65] provides advice and guidance on information security incident management for information security managers, and information system, service and network managers. After security controls and policies have been implemented, residual weaknesses are likely to remain. Residual weaknesses, together with the occurrence of new previously unidentified threats, make information security incidents possible. Information security incident management proposed by the technical report consists of processes structured in a model of four phases: Plan and Prepare, Use, Review, and Improve. "Plan and Prepare" includes the actions of developing, documenting and communicating an information security incident management policy, developing and documenting an information security incident management scheme (forms, procedures and support tools, for the detection, reporting, assessment and response to incidents), establishing an appropriate information security incident management organizational structure, and performing personnel training. "Use" refers to detecting, reporting the occurrence of information security events and evaluate their significance, making responses to the information security incidents. The "Review" step includes forensic analysis, identifying the lessons learnt from information security incidents, and identifying improvements. Finally, in the "Improve" phase improvements are realized and the organization's existing information security risk analysis and management review results are revised.

3.5 Business Continuity

Guidelines for Information and Communications Technology Disaster Recovery Services

ISO/IEC 24762:2008 [66] guides the provision of information and communications technology disaster recovery services as part of business continuity management. Business continuity management is an integral part of a holistic risk management process that safeguards the interests of an organization's key stakeholders, reputation, brand and value. It includes activities which identify potential threats that may cause adverse impacts on an organization's business operations, and associated risks, providing a framework for building resilience for business operations, providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and failures. The standard is interrelated with the ISO/IEC 27001:2005 [4] and ISO/IEC 27002:2005 [13].

ISO/IEC 24762:2008 [66] provides guidelines for both in-house and outsourced disaster recovery services. The guidelines are divides into two areas: disaster recovery guidelines and disaster recovery facilities. Disaster recovery guidelines include issues of environmental stability, asset management and protection, proximity of sites, vendor management, contractual agreements, activation and deactivation of disaster recovery plan, training and education etc. Disaster recovery facilities refer to the basic requirements that need to be fulfilled by disaster recovery service providers so that they can provide secure physical operating environments to facilitate organization recovery efforts. These include location of recovery sites (taking into account accessibility, natural hazards, weather changes etc.) physical access controls, physical facility security, environmental controls, telecommunications, power supply, fire protection etc.

3.6 Non-repudiation

ISO/IEC 13888-1:2004 [67] serves as a general model for subsequent parts of the series ISO/IEC 13888 by specifying non-repudiation mechanisms using cryptographic techniques. The goal of the non-repudiation service is to generate, collect, maintain, make available and verify evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. There are two main types of evidence, the nature of which depends on cryptographic techniques employed: a) the secure envelopes generated by an evidence-generating authority using symmetric cryptographic techniques, and b) the digital signatures generated by an evidence generator or an evidence generating authority using asymmetric cryptographic techniques. ISO/IEC 13888-2:1998 [68] and ISO/IEC 13888-3:1997 [69] provide non-repudiation mechanisms for the following phases of non-repudiation: evidence generation, transfer, storage, retrieval and verification. The non-repudiation mechanisms are then applied to a selection of specific non-repudiation services such as non-repudiation of origin, non-repudiation of delivery, non-repudiation of submission, and non-repudiation of transport.

3.7 Digital Signatures

Two types of digital signature mechanisms exist: a) signature mechanism with appendix and b) signature mechanism giving message recovery. In the first case the verification process needs the message as part of the input. A hash-function is used in the calculation of the appendix. In the second case the verification process reveals all or part of the message. A hash-function is also used in the generation and verification of these signatures.

ISO/IEC 14888 series specify digital signatures with appendix. ISO/IEC 14888-1:2008 [36] specifies general principles and requirements for digital signatures with appendix. ISO/IEC 14888-2:2008 [37] addresses digital signatures based on integer factoring, and ISO/IEC 14888-3:2006 [38] addresses digital signatures based on discrete logarithm. ISO/IEC 9796-2:2002 [39] specifies three digital signature schemes giving message recovery, two of which are deterministic (non-randomized) and one of which is randomized. Also specifies a method for key production for the three signature schemes. A complementary Annex has been provided by the ISO/IEC 9796-2:2002/Amd 1:2008 that provides an additional ASN.1 module. Finally, ISO/IEC 9796-3:2006 [40] gives the general model for digital signatures giving partial or total message recovery aiming at reducing storage and transmission overhead. It also, defines types of redundancy: natural redundancy, added redundancy, or both. ISO/IEC 9796-1:1991 [41] has been withdrawn.

3.8 Access Control

ISO/IEC 15816:2002 [42] defines guidelines for specifying the abstract syntax of generic and specific Security Information Objects (SIOs) for Access Control, specifying generic SIOs for Access Control and defining specific SIOs for Access Control.

Entity Authentication

ISO/IEC 9798-1:1997 [43] specifies an authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities, and where required, exchanges with a TTP. The subsequent five parts ISO/IEC 9798-2:2008 [44], ISO/IEC 9798-3:1998 [45], ISO/IEC 9798-4:1999 [46], ISO/IEC 9798-5:2004 [47] and ISO/IEC 9798-6:2005 [48] provide details of the mechanisms and the contents of the authentication exchanges.

3.9 Cryptographic Controls

Encryption Algorithms

ISO/IEC 18033 series specify encryption systems (ciphers). ISO/IEC 18033-1:2005 [49] specifies terms and definitions used throughout all parts of ISO/IEC 18033, the purpose of encryption, the differences between symmetric and asymmetric ciphers, and the key management problems associated with the use of ciphers, the uses and properties of encryption, and criteria for the inclusion of encryption algorithms in ISO/IEC 18033. ISO/IEC 18033-2:2006 [50] specifies the functional interface of an asymmetric (i.e. public-key) encryption scheme, and a number of particular schemes considered to be secure against chosen ciphertext attack. ISO/IEC 18033-3:2005 [51], along with its amendments ISO/IEC 18033-3:2005/Cor 1:2006, ISO/IEC 18033-3:2005/Cor 2:2007 and ISO/IEC 18033-3:2005/Cor 3:2008, specify block ciphers. Finally, ISO/IEC 18033-4:2005 [52] specifies stream cipher algorithms.

Key Management

The series ISO/IEC 11770 consists of three parts dedicated to key management of cryptographic controls. ISO/IEC 11770-1:1996 [53] defines a general model of key management that is independent of the use of any particular cryptographic algorithm. It identifies the objective of key management, basic concepts and key management services. It will be soon revised by a homonym standard (ISO/IEC CD 11770-1 [54]). ISO/IEC 11770-2:2008 [55] specifies a series of 13 mechanisms for establishing shared secret keys using symmetric cryptography. These mechanisms address three different environments for the establishment of shared secret keys: point-to-point key establishment schemes, mechanisms using a Key Distribution Centre (KDC), and techniques that use a Key Translation Centre (KTC). ISO/IEC 11770-3:2008 [56] defines key management mechanisms based on asymmetric cryptographic techniques. ISO/IEC 11770-4:2006 [57] defines key establishment mechanisms based on weak secrets. It specifies cryptographic techniques specifically designed to establish one or more secret keys based on a weak secret derived from a memorized password, while preventing off-line brute-force attacks associated with the weak secret.

Message Authentication Codes (MACs)

ISO/IEC 9797-1:1999 [58] specifies six MAC algorithms that use a secret key and an n-bit block cipher to calculate an m-bit MAC. ISO/IEC 9797-2:2002 [59] specifies three MAC algorithms that use a secret key and a hash-function (or its round-function) with an n-bit result to calculate an m-bit MAC. These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorized manner. They can also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key. The standards will be soon revised by homonym standards (ISO/IEC FCD 9797-1, ISO/IEC FCD 9797-2).

Hash Functions

ISO/IEC 10118 series specify hash-functions that are applicable to the provision of authentication, integrity and non-repudiation services. Hash-functions map arbitrary strings of bits to a fixed-length string of bits, using a specified algorithm. They can be used for reducing a message to a short imprint for input to a digital signature mechanism, and for committing the user to a given string of bits without revealing this string. ISO/IEC 10118-1:2000 [60] contains definitions, symbols, abbreviations and requirements, which are common to all the other parts of ISO/IEC 10118. ISO/IEC 10118-2:2000 [61], along with its amendment ISO/IEC 10118-2:2000/Cor 2:2007, specifies hash-functions which make use of an n-bit block cipher algorithm; therefore they are suitable for an environment in which such an algorithm is already implemented. This standard is also under revision (ISO/IEC CD 10118-2). ISO/IEC 10118-3:2004 [62] specifies seven dedicated hash-functions, e.g. RIPEMD-160 that provides hash-codes of lengths up to 160 bits. Finally, ISO/IEC 10118-4:1998 [63] specifies two hash-functions which make use of modular arithmetic.

3.10 Systems Security Engineering

ISO/IEC 21827:2008 [64] specifies the Systems Security Engineering - Capability Maturity Model, which describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering.

3.11 Assurance and Evaluation

Evaluation Criteria for IT Security

This multipart standard ISO/IEC 15408 defines criteria, which are known as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience. The CC is applicable to IT security measures implemented in hardware, firmware or software.

ISO/IEC FCD 15408-1.3 [71] is under development and will revise the ISO/IEC 15408-1:2005 [72]. That part of the ISO/IEC 15408 defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. ISO/IEC 15408-2:2008 [73] defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products. ISO/IEC 15408-3:2008 [74] defines the assurance requirements of the standard. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs).

ISO/IEC TR 19791:2006 [75] provides guidance and criteria for the security evaluation of operational systems. It provides an extension to the scope of ISO/IEC 15408, by taking into account a number of critical aspects of operational systems not addressed in ISO/IEC 15408 evaluation.

Methodology for IT Security Evaluation

ISO/IEC 18045:2008 [70] is a companion document to the evaluation criteria for IT security defined in ISO/IEC 15408. It defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation. The proposed evaluation process consists of the roles and responsibilities of the parties involved and the general evaluation model. The general roles involved are the sponsor, the developer, the evaluator and the evaluation authority. The general evaluation model consists of the evaluator performing the evaluation input task, the evaluation output task and the evaluation sub-activities. The evaluation input task ensures that the evaluator has available the correct version of the evaluation evidence necessary for the evaluation and that it is adequately protected. The evaluation output task refers to the documentation of the Observation Report[2] and the Evaluation Technical Report[3]. The evaluation sub-activities vary depending whether it is a Protection Profile (PP) or a Target of Evaluation (TOE) evaluation.

Assurance

ISO/IEC TR 15443 is also a technical report to guide the selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel. ISO/IEC TR 15443-1:2005 [76] describes the fundamentals of security assurance and its relation to other security concepts. It is under revision (ISO/IEC NP TR 15443-1). ISO/IEC TR 15443-2:2005 [77] describes a variety of IT security assurance methods and approaches and relates them to the IT security assurance framework in ISO/IEC TR 15443-1 [76]. It is under revision (ISO/IEC NP TR 15443-2). ISO/IEC TR 15443-3:2007 [77] provides general guidance to an assurance authority in the choice of the appropriate type of international communications technology assurance methods and to lay the framework for the analysis of specific assurance methods for specific environments. It will be revised by ISO/IEC NP TR 15443-3.

4 Classification of Information Security Management Standards

In this section we classify the various information security management specific areas standards, described in the previous sections, according to the clauses of ISO/IEC

[2] A report written by the evaluator requesting a clarification or identifying a problem during the evaluation.

[3] A report that documents the overall verdict and its justification, produced by the evaluator and submitted to an evaluation authority.

27001:2005 [4]. Such a categorization would enhance the application of information security management code of practice and would facilitate security managers aiming at conformance assessment.

Table 1. Information Security Management standards' classification

Areas of concern (based on ISO 27002: 2005)	**Published standards or series of standards**	**Standards under development**	**Will be revised by**
ISMSs	Series ISO/IEC 27000 ISO/IEC 13335-1:2004	ISO/IEC CD 27003 ISO/IEC WD 27007	
Security Policy	ISO 27002: 2005		
Organizing Information Security	ISO 27002: 2005 ISO/IEC TR 14516:2002 ISO/IEC 15945:2002		
Asset Management	ISO 27002: 2005		
Human Resources Security	ISO 27002: 2005		
Physical and Environmental Security	ISO 27002: 2005		
Communications and Operations Management	Series ISO/IEC 18028	ISO/IEC WD 27007	Series ISO/IEC 27033
	Series ISO/IEC 18014		
	ISO/IEC 18043:2006		
	ISO/IEC TR 14516:2002		
	ISO/IEC 15945:2002		
Access Control	ISO/IEC 15816:2002		
	Series ISO/IEC 9798		
Information Systems Acquisition, Development and Maintenance	Series ISO/IEC 11770		ISO/IEC CD 11770-1
	Series ISO/IEC 14888		
	Series ISO/IEC 9796		
	Series ISO/IEC 18033		
	Series ISO/IEC 9797		ISO/IEC FCD 9797-1 ISO/IEC FCD 9797-2
	Series ISO/IEC 10118		ISO/IEC CD 10118-2
	ISO/IEC 21827:2008		
	Series ISO/IEC 13888		
Information Security Incident Management	ISO/IEC TR 18044:2004		
Business Continuity Management	ISO/IEC 24762:2008		
	ISO/IEC 18045:2008		
	Series ISO/IEC 15408		ISO/IEC FCD 15408-1.3
	ISO/IEC TR 19791:2006		
	Series ISO/IEC TR 15443		ISO/IEC NP TR 15443-1 ISO/IEC NP TR 15443-2 ISO/IEC NP TR 15443-3
Compliance		ISO/IEC WD 27007	

5 Limitations and Further Research

In this paper we provided a state of the art review of exclusively ISO/IEC information security management published standards. The accuracy of the information provided in the paper is connected to the pace of standards' publications. However, this paper gives a structure of the international standards that shall guide managers in their attempt to follow the standards' advancements. In addition, we have included in our description several fore coming revisions and publications in order to assist security practitioners to keep pace with standards' validity. Finally, we should mention that other sub-areas of information security management are guided by national standardization organizations, such as NIST. The next step would be to extend our analysis, including such publications.

References

1. Standardization definition, `http://en.wikipedia.org/wiki/Standardization`
2. Guijarro, L.: ICT standardisation and public procurement in the United States and in the European Union: Influence on egovernment deployment. Telecommunications Policy 33(5-6), 285–295 (2009)
3. International Organization for Standardization, `http://www.iso.org/iso/home.htm`
4. ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements (2005)
5. ISO/IEC 13335-1:2004. Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management (2004)
6. ISO/IEC TR 13335-2:1997. Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security (1997)
7. ISO/IEC TR 13335-3:1998. Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security (1998)
8. ISO/IEC TR 13335-4:2000. Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards (2000)
9. ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management (2008)
10. ISO/IEC TR 13335-5:2001. Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security (2001)
11. ISO/IEC 18028-1:2006. Information technology – Security techniques – IT network security – Part 1: Network security management (2006)
12. ISO/IEC 27000:2009. Information technology – Security techniques – Information security management systems – Overview and vocabulary (2009)
13. ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management (2005)
14. ISO/IEC 17799:2005. Information technology – Security techniques – Code of practice for information security management (2005)
15. ISO/IEC FCD 27003. Information technology – Security techniques – Information security management system implementation guidance

16. ISO/IEC 27011:2008. Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (2008)
17. ISO/IEC WD 27007. Information technology – Security techniques – Guidelines for information security management systems auditing
18. ISO/IEC 27006:2007. Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems (2007)
19. ISO/IEC 17021:2006. Conformity assessment – Requirements for bodies providing audit and certification of management systems (2006)
20. ISO/IEC FCD 27033-1. Information technology – Security techniques – IT network security – Part 1: Guidelines for network security
21. ISO/IEC 18028-2:2006. Information technology – Security techniques – IT network security – Part 2: Network security architecture (2006)
22. ISO/IEC WD 27033-2. Information technology – Security techniques – IT network security – Part 2: Guidelines for the design and implementation of network security
23. ISO/IEC 18028-3:2005. Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways (2005)
24. ISO/IEC NP 27033-4. Information technology – Security techniques – IT network security – Part 4: Securing communications between networks using security gateways - Risks, design techniques and control issues
25. ISO/IEC 18028-4:2005. Information technology – Security techniques – IT network security – Part 4: Securing remote access (2005)
26. ISO/IEC NP 27033-5. Information technology – Security techniques – IT network security – Part 5: Securing Remote Access - Risks, design techniques and control issues
27. ISO/IEC 18028-5:2006. Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks (2006)
28. ISO/IEC NP 27033-6. Information technology – Security techniques – IT network security – Part 6: Securing communications across networks using Virtual Private Networks (VPNs) – Risks, design techniques and control issues
29. ISO/IEC WD 27033-3. Information technology – Security techniques – IT network security – Part 3: Reference networking scenarios – Risks, design techniques and control issues
30. ISO/IEC 18043:2006. Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (2006)
31. ISO/IEC 18014-1:2008. Information technology – Security techniques – Time-stamping services – Part 1: Framework (2008)
32. ISO/IEC 18014-2:2002. Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens (2002)
33. ISO/IEC 18014-3:2004. Information technology – Security techniques – Time-stamping services – Part 3: Mechanisms producing linked tokens (2004)
34. ISO/IEC TR 14516:2002. Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services (2002)
35. ISO/IEC 15945:2002. Information technology – Security techniques – Specification of TTP services to support the application of digital signatures (2002)
36. ISO/IEC 14888-1:2008. Information technology – Security techniques – Digital signatures with appendix – Part 1: General (2008)
37. ISO/IEC 14888-2:2008. Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms (2008)

38. ISO/IEC 14888-3:2006. Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms (2006)
39. ISO/IEC 9796-2:2002. Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms (2002)
40. ISO/IEC 9796-3:2006. Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms (2006)
41. ISO/IEC 9796-1:1991, Information technology–Security techniques–Digital signature scheme giving message recovery –Part 1: Mechanisms using redundancy (1991)
42. ISO/IEC 15816:2002. Information technology – Security techniques – Security information objects for access control (2002)
43. ISO/IEC 9798-1:1997. Information technology – Security techniques – Entity authentication – Part 1: General (1997)
44. ISO/IEC 9798-2:2008. Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms (2008)
45. ISO/IEC 9798-3:1998. Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques (1998)
46. ISO/IEC 9798-4:1999. Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function (1999)
47. ISO/IEC 9798-5:2004. Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge techniques (2004)
48. ISO/IEC 9798-6:2005. Information technology – Security techniques – Entity authentication – Part 6: Mechanisms using manual data transfer (2005)
49. ISO/IEC 18033-1:2005. Information technology – Security techniques – Encryption algorithms – Part 1: General (2005)
50. ISO/IEC 18033-2:2006. Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers (2006)
51. ISO/IEC 18033-3:2005. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers (2005)
52. ISO/IEC 18033-4:2005. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers (2005)
53. ISO/IEC 11770-1:1996. Information technology – Security techniques – Key management – Part 1: Framework (1996)
54. ISO/IEC CD 11770-1.Information technology – Security techniques – Key management – Part 1: Framework
55. ISO/IEC 11770-2:2008. Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques (2008)
56. ISO/IEC 11770-3:2008. Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques (2008)
57. ISO/IEC 11770-4:2006. Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets (2006)
58. ISO/IEC 9797-1:1999. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher (1999)
59. ISO/IEC 9797-2:2002. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function (2002)
60. ISO/IEC 10118-1:2000. Information technology – Security techniques – Hash-functions – Part 1: General (2000)
61. ISO/IEC 10118-2:2000. Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher (2000)

62. ISO/IEC 10118-3:2004. Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions (2004)
63. ISO/IEC 10118-4:1998. Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic (1998)
64. ISO/IEC 21827:2008. Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®) (2008)
65. ISO/IEC TR 18044:2004. Information technology – Security techniques – Information security incident management (2004)
66. ISO/IEC 24762:2008. Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services (2008)
67. ISO/IEC 13888-1:2004. IT security techniques – Non-repudiation – Part 1: General (2004)
68. ISO/IEC 13888-2:1998. Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques (1998)
69. ISO/IEC 13888-3:1997. Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques (1997)
70. ISO/IEC 18045:2008. Information technology – Security techniques – Methodology for IT security evaluation (2008)
71. ISO/IEC FCD 15408-1.3. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
72. ISO/IEC 15408-1:2005. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model (2005)
73. ISO/IEC 15408-2:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components (2008)
74. ISO/IEC 15408-3:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components (2008)
75. ISO/IEC TR 19791:2006. Information technology – Security techniques – Security assessment of operational systems (2006)
76. ISO/IEC TR 15443-1:2005. Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework (2005)
77. ISO/IEC TR 15443-2:2005. Information technology – Security techniques – A framework for IT security assurance – Part 2: Assurance methods (2005)
78. ISO/IEC TR 15443-3:2007. Information technology – Security techniques – A framework for IT security assurance – Part 3: Analysis of assurance methods (2007)