Information Management & Computer Security

Emerald Article: A security standards' framework to facilitate best practices' awareness and conformity

Aggeliki Tsohou, Spyros Kokolakis, Costas Lambrinoudakis, Stefanos Gritzalis

A security standards' framework to facilitate best practices' awareness and conformity

Aggeliki Tsohou and Spyros Kokolakis
Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece
Costas Lambrinoudakis
Department of Digital Systems, University of Piraeus, Piraeus, Greece, and
Stefanos Gritzalis
Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece

Abstract

Purpose – Recent information security surveys indicate that both the acceptance of international standards and the relative certifications increase continuously. However, it is noted that still the majority of organizations does not know the dominant security standards or does not fully implement them. The aim of this paper is to facilitate the awareness of information security practitioners regarding globally known and accepted security standards, and thus, contribute to their adoption.

Design/methodology/approach – The paper adopts a conceptual approach and results in a classification framework for categorizing available information security standards. The classification framework is built in four layers of abstraction, where the initial layer is founded in ISO/IEC 27001:2005 information security management system.

Findings – The paper presents a framework for conceptualizing, categorizing and interconnecting available information security standards dynamically.

Research limitations/implications – The completeness of the information provided in the paper relies on the pace of standards' publications; thus the information security standards that have been classified in this paper need to be updated when new standards are published. However, the proposed framework can be utilized for this constant effort.

Practical implications – Information security practitioners can benefit by the proposed framework for available security standards and effectively invoke the relevant standard each time. Guidelines for utilizing the proposed framework are presented through a case study.

Originality/value – Although the practices proposed are not innovative by themselves, the originality of this work lies on the best practices' linkage into a coherent framework that can facilitate the standards diffusion and systematic adoption.

Keywords Data security, International standards, Best practice

Paper type General review

Information Management & Computer Security
Vol. 18 No. 5, 2010
pp. 350-365

0968-5227
DOI 10.1108/09685221011095263

This paper was first presented at the South African Information Security Multi-conference (SAISMC) held on 17-18 May 2010 at the Tsitsikamma Conference Centre, Port Elizabeth, South Africa.

1. Introduction

Standardization is a way to promote the best practices and the requirements that products or services must meet on world markets transparently. At the same time, it is a way to provide conformity assessment mechanisms for checking whether these products or services measure up to the standards International Organization for Standardization (ISO, 2008a). Moreover, information system standards contribute to several advantages, such as:

- establishing a consensus on terminology;
- establishing a common understanding and agreement of functional and non-functional requirements for the design of systems that ensure the compatibility of equipment of diverse origins; and
- strengthening interoperability, etc.

These advantages also apply to information systems security, since standards promote the common understanding of security requirements and ensure that the security mechanisms implemented do comply with globally accepted rules and practices. In this way, the systems that are being implemented reach a commonly accepted security level and interoperate with other systems in an efficient and secure way[1].

Currently a number of standardization organizations exist, which can be divided according to their range in international, regional or national organizations. Organizations which have published information security standards that gained great acceptance include ISO, Information Systems Audit and Control Association (ISACA), Information Systems Security Association (ISSA), National Institute of Standards and Technology (NIST), British Standards Institution (BSI), Information Security Forum (ISF), Payment Card Industry Security Standards Council and others. Several security standards are continuously published and gain acceptance; some of them provide guidelines, others promote best practices, while a few can be used as a basis for certification. The latter include the well-known ISO/IEC 27001:2005, the NIST FIPS 140-2 (2001), common criteria (CC) or ISO/IEC 15408 series, COBITv4.1, Payment Card Industry Data Security Standard (PCI DSS), etc. Information security breaches survey (Department for Business, Enterprise and Regulatory Reform (BERR, 2010)) reveals that organizations in the UK are increasingly required by their customers to demonstrate compliance with information security standards or guidelines (41 per cent for large and 31 per cent of small organizations were required to comply to a recognized standard such as ISO/IEC 27001). Moreover, as the survey states "ISO 27001 is becoming the lingua franca for information security". Ernst & Young (2008) international survey reveals that international information security standards are enjoying greater acceptance and adoption; ISO/IEC 27001:2005 has a 15 per cent rise, ISO/IEC 27002:2005 a 9 per cent rise and ISF – Standard of Good Practice for information security a 7 per cent rise from 2007 to 2008. The increasing adoption of ISO/IEC 27001:2005 is also evident from the growing number of certifications world widely. The ISO Survey of Certifications (ISO, 2008b) reports that ISO/IEC 27001:2005 certifications keep an increasing pace; certifications have increased by approximately 20 per cent from 2007 to 2008.

However, the awareness and the compliance to the widely accepted standards remain quite small. According to information security breaches survey (BERR, 2008) only 21 per cent of overall UK business are aware of ISO 27000 series and only 30 per cent of the aware ones have fully implemented them. The same conclusions derive from

Ernst and Young (2010) international survey; only 8 per cent have achieved formal certification and only 36 per cent is using ISO/IEC 27001:2005 as a basis for their information security management system (ISMS). Therefore, recent surveys indicate that even for widely accepted information security standards awareness rates remain high.

The aim of this paper is to enhance the awareness of organizations about the security standards through a framework of information security standards conceptualization, interconnection and categorization. The four-layer framework is based on ISO/IEC 27001:2005 and is used for the classification of several information security standards. The framework serves two main purposes:

(1) links together existing security standards in a coherent and systematic way; and

(2) provides guidelines, in regard with the security management decisions and actions, that are mainly based on the security management code of practice (ISO/IEC 27002:2005) and requirements specification (ISO/IEC 27001:2005) standards.

The way that information security practitioners can benefit by the proposed framework for informing themselves regarding security standards and each time effectively inquiring the adequate security standard, is presented through a case study of a Payroll and Pensioner Information System (PPIS). The authors have conducted a risk analysis and management study for the specific information system using the CCTA Risk Analysis and Management Methodology (CRAMM) method[2]. However, since the aim is to demonstrate the usefulness of the proposed framework, and not to describe in detail the specific information system, we only address a subset of the system's functionality, software, hardware and data assets. The same is done for the risk analysis and management results;, i.e. only a subset of the identified security requirements will be considered together with the resulting technical, organizational and procedural security measures.

The paper is structured into seven sections. After this section, we present the proposed information security standards framework, and we describe its layers. In sequence, a brief overview of the information system used as a case study is given. In Sections 4 and 5, we demonstrate how the ISMS for the case study system can be developed according to the proposed framework. Finally, conclusions and limitations of the paper are provided followed by the paper's references.

2. A framework of security standards

The proposed security framework consists of four interleaved layers, as shown in Figure 1. The first layer of the framework is associated with the ISO/IEC 27001:2005 and prescribes its adoption in order to collect security requirements and implement, operate, monitor, review, maintain and improve an ISMS. This leads to a plan-do-check-act (PDCA) process that results in the realization of a number of new actions (e.g. specification of the systems' boundaries). Most of these additional actions are in fact extending or/and complementing or/and customizing or/and specializing the high level guidelines of ISO/IEC 27001:2005 and are in turn guided by other, more focused, ISO standards that are, in turn, associated with the remaining layers of the framework. The fact that all these additional actions are caused by the guidelines of ISO/IEC 27001:2005 explains why Layer 1 encapsulates the remaining layers of the proposed framework.

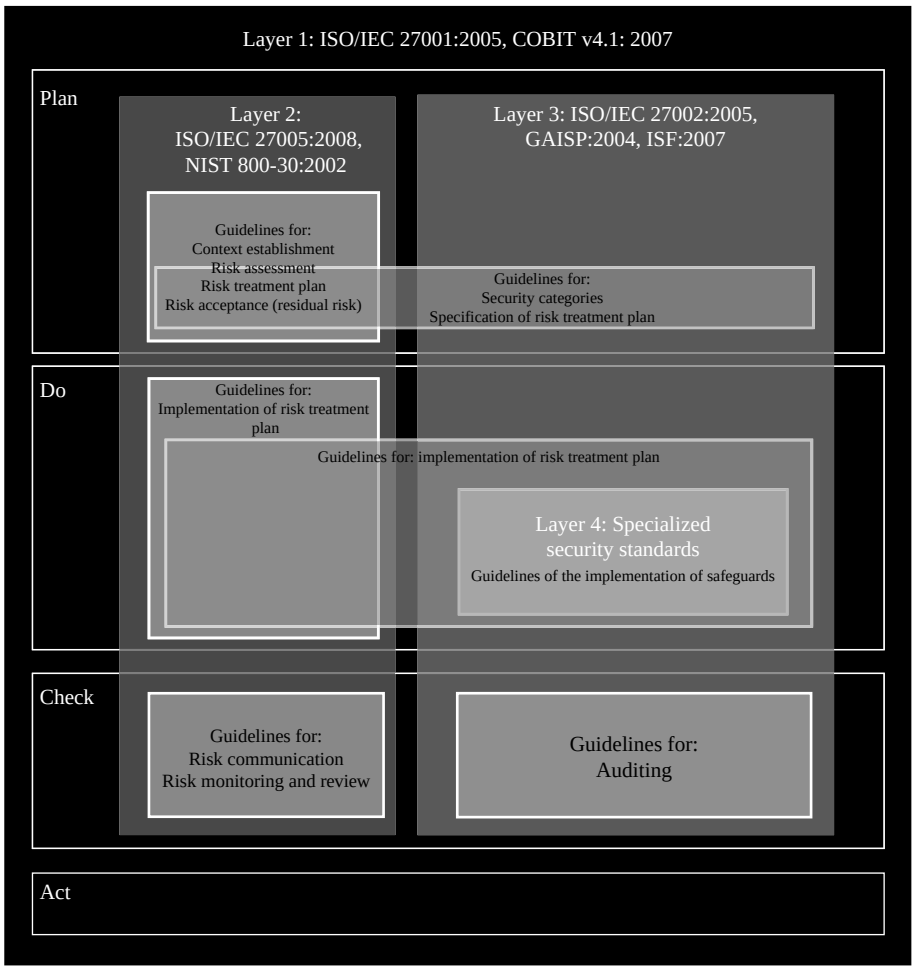

Figure 1.
The framework of information security standards

At the same level of abstraction practitioners could also find guidelines by COBIT v4.1:2007. However, we will base our analysis on ISO/IEC 27001:2005 since surveys indicate that it dominates information security management guidance.

Among the first actions of the Plan phase is the identification of the system boundaries (context establishment), the realization of risk assessment and the specification of the risk treatment plan. All these actions are guided by ISO/IEC 27005:2008 and *NIST Special Publication 800-30:2002* which, as shown in Figure 1, are associated with the second layer of the framework. Specifically, for the structure and the required characteristics of the risk treatment plan, and while still in the Plan phase, there are more specialized guidelines provided by ISO/IEC 27002:2005, GAISP:2004 and ISF Standard of Good Practice:2007 that have been associated with the third layer of the proposed framework.

Continuing, according to the ISO/IEC 27001:2005 the Plan phase is followed by the Do phase, during which the risk treatment plan that has been already specified

is implemented. The risk treatment plan will clearly identify the organizational, procedural and technical safeguards for the organization. The proper implementation of these safeguards is described in detail in the ISO/IEC 27002:2005, GAISP:2004 and ISF Standard of Good Practice:2007 (Layer 3), even though there are more specialized guidelines for specific countermeasure categories that are provided by other ISO standards (Figure 1). This additional, more specialized, set of standards is associated with the fourth layer of the proposed security framework.

After completion of the Do phase, the first layer (ISO/IEC 27001:2005) requires continuous monitoring and reviewing of the developed ISMS. Also, internal and external auditing of the ISMS is necessary. All these tasks are part of the Check phase. More focused guidelines for their realization are provided by *ISO/IEC 27005:2008, NIST Special Publication 800-30:2002* and ISO/IEC 27002:2005 (Layers 2 and 3).

Finally, during the Act phase, improvement or/and corrective actions are implemented (if necessary) according to the guidelines of ISO/IEC 27001:2005.

As a result, we propose a framework that guides security management by using the best practices published by established standards.

3. The payroll and pensioner information system

The information system used as a case study is a typical PPIS that also provides web-based services to retired public servants (electronic PPIS (e-PPIS)). We identify its security requirements and we illustrate how the proposed ISO-based security framework can guide the implementation and maintenance of the e-PPIS ISMS.

The aim of the e-PPIS is to automate the interaction of public servants and pensioners with the appropriate governmental departments. The offered services will be available 24 hours per day, seven days a week. One of the main system functionalities is to monitor the salaries of public servants and when an employee applies for retirement to change her state from worker to pensioner and continue monitoring her payoffs. Indicative functionality of the system is:

- Retirement application (approval/disapproval).
- count of longevity.
- Payments calculation (according to retirement decision, stoppages, allowances, etc.).
- Turnovers (e.g. retirement handover to family member or cancelation of retirement grant in case of death).
- Updates to the pensioner (e.g. certificates), to the department (e.g. statistical data) and to other services (e.g. insurance conservancies).

The system operates in two modes: off-line and on-line. During the off-line operation, it supports the aforementioned functionality within the scope of the appropriate governmental department. However, it is also offering several web-based public services (online mode of operation) for the retired persons, like:

- Information regarding retirement procedure, rights, conditions, answers to frequently asked questions (FAQs), etc.
- Downloadable application forms.

- Capability to fill and submit applications, to apply for the provision of various types of certificates, to monitor the status of an application, to calculate the pension amount, etc.
- Analysis of pensioner's stoppages/allowances and online payments.

4. Developing the E-PPIS ISMS

The development of the e-PPIS ISMS according to the proposed security framework begins with the implementation of the actions described in the PDCA model (Layer 1). Subsequent actions of each phase of the PDCA model are further specialized and guided by the ISO standards associated with the Layers 2-4 of the framework.

4.1 Plan phase

In this phase, the decision makers begin with the definition of the system's scope, boundaries and overall policy, in accordance with the guidelines provided by ISO/IEC 27005:2008 and NIST 800-30:2002 (Layer 2). Continuing, a systematic approach to information security risk planning and management is necessary; such a risk assessment approach is described by ISO/IEC 27005:2008 and NIST 800-30:2002 (Layer 2) and a risk management approach in more detail by ISO/IEC 27002:2005, GAISP:2004 and ISF Standard of Good Practice:2007 (Layer 3). Finally, the processes of obtaining management authorization to implement and operate the ISMS and preparing a statement of applicability are suggested. The statement of applicability is a document describing the control objectives and controls that are relevant and applicable to the organization's ISMS.

4.1.1 The e-PPIS scope, boundaries and policy. The aim of e-PPIS is to manage the retirement cycle, to process the pensioner's data and to offer online public services to the retired persons. The e-PPIS includes a hardware infrastructure of web servers, application servers, database servers, Domain Name System servers, mail servers, firewalls and switches and other peripherals or network devices. Furthermore, e-PPIS works using subsystems such as retirement software, payroll, human resources and a web-portal. In general, during this phase hardware and software resources are recorded in detail. In addition, any interoperability with other systems is also recorded (for example, the e-PPIS interoperates with the information systems of insurance companies). Finally, the e-PPIS processes different types of data, including personal information of public servants or pensioners, their job status, salary, allowances, family status, bank accounts, potential disabilities or illnesses. Some of these data are categorized as personal or/and sensitive data according to Art. 8§1 of the data protection directive Greek e-government interoperability framework (Greek e-GIF, 2008). The users of the system are: end-users (citizens), advanced users (employees of governmental departments), managers and system administrators.

Furthermore, during this phase the security policy is defined only in a very high level manner; it reflects the general perception of top management about security and will be further specialized in an e-PPIS security policy during the "Do" phase.

4.1.2 Risk management. Following the scope and boundaries of e-PPIS, the risk management activities should take place. According to the ISO/IEC 27005:2008 and NIST 800-30:2002 (Layer 2), these include context establishment, risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review. Within the Plan phase the activities of context establishment, risk assessment, risk treatment

plan development and risk acceptance take place. Context establishment has been already described (4.1.1). Risk assessment involves the identification, description of risks (quantitatively or qualitatively) and prioritization of risks against risk evaluation criteria and objectives. For the e-PPIS system a subset of the identified risk levels is listed in Table I.

The next step is the risk treatment plan that incorporates controls to reduce, contain, avoid or transfer the risks. For that purpose, ISO/IEC 27002:2005 (Layer 3) provides a list of control objectives and controls structured in the 11 control clauses (ISO/IEC 27002:2005) that follow:

(1) security policy;
(2) organizing information security;
(3) asset management;
(4) human resources security;
(5) physical and environmental security;
(6) communications and operations management;
(7) access control;
(8) information systems acquisition, development and maintenance;
(9) information security incident management;
(10) business continuity management; and
(11) compliance.

Threat	Possibility	Vulnerability	Asset	Impact	Risk levels
Application software failure	High	High	Web portal	Information disclosure	High
Masquerading of user identity by insiders	High	High	Payroll application	Loss of availability information disclosure deliberate modification of information	High
Unauthorized use of an application	Very high	High	Retirement application	Loss of availability information disclosure	Very high
Embedding of malicious code	Very high	Low	Web portal	Loss of availability small-scale error in data, information disclosure	Very high
System and network software failure	High	High	Application servers	Loss of availability	High
Communications manipulation	Very high	High	Payroll application retirement application	Loss of availability information disclosure deliberate modification of information	Very high
User errors	Very high	Medium	Payroll data, retirement data, web portal data	Deliberate modification, small-scale errors, widespread errors	High

Table I.
e-PPIS indicative risk assessment results

The security countermeasures depend on the specific hardware and software implementation and the specific organizational environment where the system functions. In the "Do" phase, we present a subset of the e-PPIS countermeasures list, focusing on the description of the ISO standards that are applicable to these security measures and thus guide their implementation.

4.1.3 Statement of applicability. The Plan phase is completed with the preparation of a statement of applicability that describes the Layer 3 (ISO/IEC 27002:2005) controls that are applicable and the ones that after appropriate justification have been excluded.

4.2 Do phase

The Do phase (Layer 1 – ISO/IEC 27001:2005) includes the implementation of the risk treatment plan, the definition of the way the effectiveness of the selected controls will be measured and the implementation of security awareness and training program. Also, it includes the management of the operation and resources of the ISMS and the implementation of procedures for prompt detection or response to security events.

As already described in Section 4.1.2 above, the e-PPIS risk treatment plan incorporates countermeasures belonging to all 11 clauses of ISO/IEC 27002:2005, GAISP:2004 and ISF Standard of Good Practice:2007 (Layer 3). An indicative subset of them is presented in the following sub-sections.

4.2.1 Security policy. The e-PPIS organization owner has established a security policy that has been approved by top management. That security policy defines security as "the protection of information integrity, availability and confidentiality, and the protection of human assets and infrastructures required for the collection, process and transmission of that information". The scope of the security policy refers to the overall information that the e-PPIS processes as well as to the related software, hardware and staff that directly or indirectly participate in that processing.

4.2.2 Organizing information security. The internal e-PPIS security has been supported through the role of a Security Officer who is responsible for the communication and coordination of all security issues, the supervision of countermeasures' implementation, the planning of awareness and training programms', the realization of regular and unscheduled audits, the incident management and the formulation of an annual e-PPIS security report.

4.2.3 Asset management. A list of e-PPIS assets has been compiled including software, hardware and documentation. The asset list must be reviewed and updated every six months.

4.2.4 Human resources security. According to the risk treatment plan, employees of the organization that are granted with e-PPIS use privileges must be informed of their accountability and should be trained accordingly. The staff should sign a confidentiality agreement. Finally, in case of staff leave their access rights should be removed, and any keys, access cards or equipment should be returned. In addition, specially adapted awareness and training programs have been designed and delivered including posters, leaflets, presentations, security events, etc.

4.2.5 Physical and environmental security. The entrance to the building should be controlled 24 hours a day. Access to the computer room should be controlled with a card-based access control system. Fire detection mechanisms, air-conditioning and uninterruptible power supply should be used in the computer room. Instructions

for managing bomb threats and the procedures for treating such incidents should be documented. Procedures for building evacuation should also be in place.

4.2.6 Communications and operations management. All software changes should be authorized by the e-PPIS Security Officer and a register should be maintained, monitoring at least a change ID, date, responsible person and justification. Procedures for preventing and dealing with malicious code or disruptive software should be established. The remote access of users should be only allowed through a virtual private network (VPN, 5.1). Furthermore, it is necessary to implement mechanisms employing digital certificates (5.4) for mutual authentication among the communicating entities (especially in cases of users/applications from interconnected systems), as well as encryption mechanisms (5.3) for protecting the confidentiality of the data. Also, in order to protect the integrity of data, it has been proposed to develop some integrity check mechanisms based on internationally approved algorithms (5.5 and 5.6). The internal network internet protocol addresses should not be visible to external networks and thus network address translation (NAT; 5.1) has been suggested. Firewalls (5.1) were proposed for implementing demilitarized zone architecture and restricting packets acceptance. An intrusion detection system (5.2) is also required for detecting any unauthorized attempt to access, manipulate, and/or disable the system via web. There should be a contract with the internet services provider that specifies the responsibilities and security requirements of the provider.

4.2.7 Access control. An access control policy that specifies the access rights of each user or each user group has been suggested. The access control policy grants to users only the access rights that are necessary for performing the tasks associated with their job (5.8). The policy should be reviewed every six months from the Security Officer. It has been proposed the e-PPIS users to be divided into two main categories: the internal users (administrators, super-user and advanced users) and the external users (end-users land end-users from interconnected systems). The registration process of new users should be documented in detail. The internal users should access the e-PPIS applications through a password scheme with the exception of selected applications (i.e. retirement application) for which they will also need digital certificates (5.4). The use of digital certificates (5.4) is mandatory for the external users. The users' passwords should change every two months, while the administrators' passwords every month. All passwords should follow documented rules (e.g. not contain usernames, have special characters) and be stored in encrypted form (5.3).

4.2.8 Information systems acquisition, development and maintenance. Risk analysis has resulted in high non-repudiation and integrity requirements. In order to satisfy these requirements it has been decided to implement non-repudiation mechanisms based on digital signatures (5.4 and 5.7) in certain software components. Moreover, according to the risk treatment plan a risk analysis is mandatory for any new application incorporated in the e-PPIS. A registry of the development and maintenance activities (with records of persons, date and tasks) should be kept. In case of development outsourcing an assessment of the new applications security level is compulsory.

4.2.9 Information security incident management. Any potential security incident or detected vulnerability should be reported to the Security Officer via predetermined communication channels. The report should contain information regarding the date/time and incident type. Procedures of managing security incidents (5.10) should be documented. In case of a security incident, a back-up of the event and audit records should be taken immediately.

4.2.10 Business continuity management. A business continuity plan (5.11) based on an impact analysis has been scheduled. It will determine the procedures/infrastructures for recovering in case of a major disruption.

4.2.11 Compliance. The e-PPIS should be compliant with the 95/46/EC Directive (1995) and 2006/24/EC Directive (2006) and the amending 2002/58/EC Directive (2002), since it stores, processes and communicates personal or/and sensitive data.

4.3 Check phase

The third phase of the "Plan-Do-Check-Act" model includes continual monitoring and reviewing of risks, monitoring and reviewing procedures that promptly identify attempted and successful security breaches, undertaking regular reviews of the effectiveness of the ISMS and measuring the effectiveness of controls (Layer 2 – ISO/IEC 27005:2008, *NIST Special Publication 800-30:2002*). Therefore, appropriate auditing procedures (5.12) for the e-PPIS have been established (Layer 3 – ISO/IEC 27002:2005, GAISP: 2004 and ISF Standard of Good Practice: 2007). The event and audit logs should be analyzed at least once a week in order to detect any unusual activity. In addition, the evaluation criteria (5.12) to measure the effectiveness of security controls have been established.

4.4 Act phase

The final "Act" phase refers to maintaining the risk management process and also taking the appropriate corrective and preventive actions, communicating these actions and improvements to all interested parties and ensuring that these achieve their intended objectives.

5. Specialized guidance for the implementation of e-PPIS safeguards

The implementation of the e-PPIS safeguards during the "Do" phase, according to ISO/IEC 27002:2005, GAISP:2004 and ISF Standard of Good Practice:2007 (Layer 3), is further supported and guided by a set of specialized ISO standards (Layer 4) for specific countermeasure categories.

5.1 Network security management

The resulting countermeasures for the communications and operations clause, include the introduction of network security safeguards, such as NAT. For the purposes of network security management the ISO/IEC 18028 series can be used, according to the specific safeguards. ISO/IEC 18028-1:2006 provides detailed guidance on the security aspects of the management, operation and use of IT networks and their interconnections. ISO/IEC 18028-2:2006 could be instructed concerning end-to-end network security. ISO/IEC 18028-3:2005 outlines the techniques for security gateways to analyze network traffic as well as guidelines for selecting and configuring these gateways. ISO/IEC 18028-4:2005 is specialized on secure remote access and its implications for IT security. Finally, ISO/IEC 18028-5:2006 defines techniques for securing inter-network connections that are established using VPNs.

5.2 Intrusion detection systems

One countermeasure resulted from the risk management process is the employment of an intrusion detection system. Therefore, guidelines from the ISO/IEC 18043:2006

for including an intrusion detection capability within an organizations' IT infrastructure could be used. The standard 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 to identify the best features for a specific IT environment. Moreover, it describes various deployment strategies, provides guidance on managing alerts and discusses management and legal considerations.

5.3 Encryption systems

Encryption systems were acknowledged as necessary for both data transmission and password storage. The applicable security standards can be found in the ISO/IEC 18033 series, which specify encryption systems (ciphers). ISO/IEC 18033-1:2005 should be used for instructions about the proper terminology and definitions used throughout all parts of ISO/IEC 18033, the differences between symmetric and asymmetric ciphers and the key management problems associated with the use of ciphers and encryption in general. ISO/IEC 18033-2:2006 guides asymmetric (i.e. public-key) encryption schemes while ISO/IEC 18033-3:2005 specify block ciphers. Finally, ISO/IEC 18033-4:2005 specifies stream cipher algorithms.

5.4 Digital signatures

Digital signatures are needed within e-PPIS in order to fulfill non-repudiation, integrity and authentication requirements. Two types of digital signature mechanisms exist:

(1) signature mechanism with appendix; and

(2) 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, ISO/IEC 14888-2:2008 and ISO/IEC 14888-3:2006), while ISO/IEC 9796 series specify signature mechanisms giving message recovery (ISO/IEC 9796-2:2002 and ISO/IEC 9796-3:2006).

5.5 Hash-functions

ISO/IEC 10118 series specify hash-functions that are applicable to the provision of authentication, integrity and non-repudiation services. ISO/IEC 10118 series include four standards that contain general concepts and definitions (ISO/IEC 10118-1:2000), and also specific implementations of hash-functions (ISO/IEC 10118-2:2000, ISO/IEC 10118-3:2004, ISO/IEC 10118-4:1998).

5.6 Message authentication codes

ISO/IEC 9797 series are dedicated to message authentication codes (MACs). MACs have been proposed to the e-PPIS as integrity and authentication mechanisms. ISO/IEC 9797-1:1999 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 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.

5.7 Non-repudiation

Non-repudiation requirements concerning the exchange of information (send or receive) are introduced in the information systems acquisition, development and maintenance clause of the e-PPIS. Assistance for the non-repudiation requirements is offered by the ISO/IEC 13888 series. ISO/IEC 13888-1:2004 serves as a general model and specifies non-repudiation mechanisms using cryptographic techniques. Two main types of non-repudiation evidence exist:

(1) the secure envelopes generated by an evidence-generating authority using symmetric cryptographic techniques (guided by ISO/IEC 13888-2:1998); and

(2) the digital signatures generated by an evidence generator or an evidence generating authority using asymmetric cryptographic techniques (guided by ISO/IEC 13888-3:1997).

5.8 Access control

For the purposes of defining an access control policy, ISO/IEC 15816:2002 could be employed 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.

5.9 TTPs and key management

The necessity of digital certificates and cryptographic mechanisms for e-PPIS introduces the need for key management. This can be done in-house or through some third party (TTP) certification authority. In case of an in-house implementation the series ISO/IEC 11770 could be consulted. ISO/IEC 11770 consists of three parts dedicated to key management of cryptographic mechanisms. ISO/IEC 11770-1:1996 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. According to the symmetric or asymmetric cryptographic needs, ISO/IEC 11770-2:2008 (which specifies a series of 13 mechanisms for establishing shared secret keys using symmetric cryptography) or ISO/IEC 11770-3:2008 (which defines key management mechanisms based on asymmetric cryptographic techniques) should be used. In addition, ISO/IEC 11770-4:2006 that defines key establishment mechanisms based on weak secrets may be advised.

5.10 Incident management

The e-PPIS risk treatment plan includes the development and establishment of an incident management framework. Guidance for that activity is provided by the ISO/IEC TR 18044:2004. The proposed model is structured in 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, 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 refinements are realized and the organization's existing information security risk analysis and management review results are revised. Moreover, NIST 800-61:2004 provides a *Computer Security Incident Handling Guide* aiming at mitigating the risks from information security incidents by providing practical guidance on responding to incidents effectively and efficiently. It includes guidance on establishing an effective incident response program; primarily focusing on guidelines for detecting, analyzing, prioritizing and handling incidents.

5.11 Business continuity management

The e-PPIS risk treatment plan also includes the development and establishment of a business continuity plan. ISO/IEC 24762:2008 guides the provision of information and communications technology disaster recovery services as part of business continuity management. 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 provides guidelines for both in-house and outsourced disaster recovery services. The guidelines are divided 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. Similar guidelines are provided by the BS 25999 series. The series included two standards; the first presents a code of practice for in a form of general guidance that seek to establish processes, principles and terminology for business continuity management, and the second specifies requirements for implementing, operating and improving a documented business continuity management system, describing only requirements that can be objectively and independently audited.

5.12 Auditing

Auditing requirements result mainly from the "Check" phase of the ISMS. Currently ISO has not published standard providing auditing guidelines, but ISO/IEC WD 27007 will soon be published. In addition, practitioners can find guidelines for auditing such as COBIT v4.1:2007, ISACA IS Auditing Guideline:2008, VITA IT Security Audit Guideline:2007.

5.13 Evaluation criteria and a methodology of IT security evaluation

During the "Check" phase, regular review of the control effectiveness is necessary. For that purpose the multipart standard ISO/IEC 15408 and the ISO/IEC 18045:2008 could be used. The three parts of ISO/IEC 15408 series (ISO/IEC 15408-1:2005, ISO/IEC

15408-2:2008 and ISO/IEC 15408-3:2008) define criteria, which are known as the CC, to be used as the basis for evaluation of security properties of IT products and systems. The ISO/IEC 18045:2008 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.

6. Conclusions

The standards and guides for conformity assessment published by standardization organizations and institutes reflect an international, regional or national consensus on best practices. Their use contributes to the consistency of conformity assessment worldwide. In this paper, we have introduced a framework for classifying information security standards. It has been illustrated how such a framework is useful to security practitioners for organizing security management procedures in accordance to current security standardization activities. It should be noted that the practices proposed are not innovative by themselves; however their integration into a coherent framework will facilitate the standards' diffusion and systematic adoption. The applicability of the resulting four-layer security framework has been demonstrated through a case study. In Table II, we present the standards analyzed in this paper, in relation to their position at the proposed framework and the specific guidance that they provide. It should be stressed that the completeness of the information provided in the paper relies to the pace of standards' publications.

Layer in framework	Standard	Guidance topic
Layer 1	ISO/IEC 27001:2005, COBIT v4.1:2007	ISMS requirements
Layer 2	ISO/IEC 27005:2008, NIST 800-30:2002	Risk management
Layer 3	ISO/IEC 27002:2005, GAISP:2004 ISF Standard of Good Practice:2007	Risk treatment plan
Layer 4	ISO/IEC 18028 series	Network security management
	ISO/IEC 18043:2006	Intrusion detection systems
	ISO/IEC 18033 series	Encryption systems
	ISO/IEC 14888 series ISO/IEC 9796 series	Digital signatures
	ISO/IEC 10118 series	Hash-functions
	ISO/IEC 9797 series	Message authentication codes (MACs)
	ISO/IEC 13888 series	Non-repudiation
	ISO/IEC 15816:2002	Access control
	ISO/IEC 11770 series	TTPs and key management
	ISO/IEC TR 18044:2004, NIST 800-61:2004	Incident management
	ISO/IEC 24762:2008, BS 25999 series	Business continuity management
	ISO/IEC WD 27007, COBIT v4.1:2007, ISACA IS Auditing Guideline:2008, VITA IT Security Audit Guideline:2007	Auditing
	ISO/IEC 15408, ISO/IEC 18045:2008	Evaluation

Table II. Classified information security standards according to the framework

Notes

1. ISO – web site http://iso.org/ (accessed 13 August 2010).
2. CRAMM – web site http://cramm.com/ (accessed 13 August 2010).

References

BERR (2008), "Information Security Breaches Survey", Technical Report, PriceWaterHouseCoopers, in association with Symantec, HP and The Security Company, London, available at: http://pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf (accessed 13 August 2010).

BERR (2010), "Information Security Breaches Survey", PriceWaterHouseCoopers, in association with Infosecurity Europe, and Reed Exhibitions, London, available at: http://uk.sitestat.com/pwc/uk/s?ukws.eng_publications.pdf.isbs_survey_2010.technical_report&ns_type=pdf (accessed 13 August 2010).

Ernst & Young (2008), *Global Information Security Survey: Moving Beyond Compliance*, Ernst & Young, London.

Ernst & Young (2010), "12th annual global information security survey: outpacing change", available at: http://ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf (accessed 13 August 2010).

Greek e-GIF (2008), "Digital authentication framework, Greek e-government interoperability framework", available at: http://e-gif.gov.gr/portal/pls/portal/docs/210989.PDF (accessed 13 August 2010).

ISO (2008a), "ISO in brief", available at: http://iso.org/iso/isoinbrief_2008.pdf (accessed 13 August 2010).

ISO (2008b), "The ISO Survey of Certifications", available at: http://oudarlesteyn.nl/nieuws/ISO%20survey%20certifications%202008.pdf (accessed 13 August 2010).

95/46/EC Directive (1995), Directive of the European Parliament and of the Council of 24 October on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2002/58/EC Directive (2002), Directive European Parliament and of the Council of 12 July concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications).

2006/24/EC (2006), Directive European Parliament and of the Council of 15 March on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

About the authors

Aggeliki Tsohou is currently a Researcher at the University of the Aegean, Department of Information and Communication Systems Engineering. She holds a BSc in Informatics and a MSc in Information Systems, both acquired from Athens University of Economics and Business, and a PhD in Information Security Management from the University of the Aegean, Department of Information and Communication Systems Engineering. Her research interests include information systems security management, risk management, security standards and security awareness. Aggeliki Tsohou is the corresponding author and can be contacted at: agt@aegean.gr

Spyros Kokolakis is an Assistant Professor at the Department of Information and Communication Systems Engineering at the University of the Aegean, Greece. He received a BSc in Informatics from the Athens University of Economics and Business in 1991 and a PhD

in Information Systems from the same university in 2000. His current research interests include information systems security management, risk analysis and security policies design and implementation. He is a member of IEEE and ACM.

Costas Lambrinoudakis is an Assistant Professor at the Department of Digital Systems, University of Piraeus, Greece. He holds a BSc (Electrical and Electronic Engineering) degree from the University of Salford (The UK), an MSc (Control Systems) and a PhD (Computer Science) degree from the University of London (The UK). He has been involved in several national and EU- funded R&D projects in the areas of Information and Communication Systems Security.

Stefanos Gritzalis is a Professor at the Department of Information and Communication Systems Engineering at the University of the Aegean, Greece. He holds a BSc in Physics, an MSc in Electronic Automation and a PhD in Informatics all from the University of Athens, Greece. His published scientific work includes several books on Information and Communication Technologies topics, and more than 190 journals and national and international conference papers. He has leaded more than 25 international conferences and workshops as General Chair or Program Committee Chair, and has served on more than 170 Program Committees of international conferences and workshops. He acts as an Editor-in-Chief for one journal, an Editorial Advisory Board member for more than 12 journals and a Reviewer for more than 35 journals. He has been involved in several national and EU-funded R&D ICT projects. He was an elected member of the Board (Secretary General, Treasurer) of the Greek Computer Society. He is a member of the ACM and the IEEE.