Journal of Information Security, **2013, 4, 92-100**
http://dx.doi.org/10.4236/jis.2013.42011 Published Online April 2013 (http://www.scirp.org/journal/jis)

Scientific Research

ISO/IEC 27000, 27001 and 27002 for Information Security Management

Georg Disterer
Department of Business Administration and Computer Science, University of Applied Sciences and Arts, Hannover, Germany
Email: georg.disterer@hs-hannover.de

Received March 15, 2013; revised April 11, 2013; accepted April 16, 2013

ABSTRACT

With the increasing significance of information technology, there is an urgent need for adequate measures of information security. Systematic information security management is one of most important initiatives for IT management. At least since reports about privacy and security breaches, fraudulent accounting practices, and attacks on IT systems appeared in public, organizations have recognized their responsibilities to safeguard physical and information assets. Security standards can be used as guideline or framework to develop and maintain an adequate information security management system (ISMS). The standards ISO/IEC 27000, 27001 and 27002 are international standards that are receiving growing recognition and adoption. They are referred to as "common language of organizations around the world" for information security [1]. With ISO/IEC 27001 companies can have their ISMS certified by a third-party organization and thus show their customers evidence of their security measures.

Keywords: Security; Standards; ISO/IEC 27000; ISO 27001; ISO 27002; ISO 27 K

1. Introduction

Information and information systems are an important foundation for companies. In particular more and more internal and inter-company data transfer and utilization of open networks increase the risks that information and information systems are exposed to. In order to reduce risks and avoid damages to companies care must be taken to assure adequate information security [2]. For the protection of the information and information systems the standards ISO 27000, ISO 27001 and ISO 27002 provide control objectives, specific controls, requirements and guidelines, with which the company can achieve adequate information security. In doing so ISO 27001 enables the company to be certified against the standard, whereby information security can be documented as being rigorously applied and managed in accordance with an internationally recognized organizational standard.

With a certification against ISO 27001 a company verifies the fulfillment of well-known and accepted security standards and thus promotes customers' trust. Likewise a verification of compliance with an international standard reduces the risk of fines or compensation payments as a result of legal disputes, since legal requirements such as provisioning according to "state-of-the-art" and with "due care and diligence" can be countered with standards compliance [3]. We present the ISO 27000 to ISO 27002 standards, their development and actual dissemination, and the ISO 27 K family of standards.

2. International Standards

Standards arise through the development of detailed descriptions of particular characteristics of a product or service by experts from companies and scientific institutions. They represent a consensus on characteristics such as quality, security and reliability that should remain applicable for an extended period of time and thus are documented and published. The objective of the development of standards is to support both individuals and companies when procuring products and services. Providers of products and services can boost their reputation by having certified their compliance with standards.

ISO is an organization founded in 1946 and supported by 159 countries; ISO is the leading issuing body for international standards. The standards ISO 27000 to ISO 27002 were developed in cooperation with the "International Electrotechnical Commission" (IEC), which is a leading global issuer of international standards in the electronics and electronic-related technologies sector.

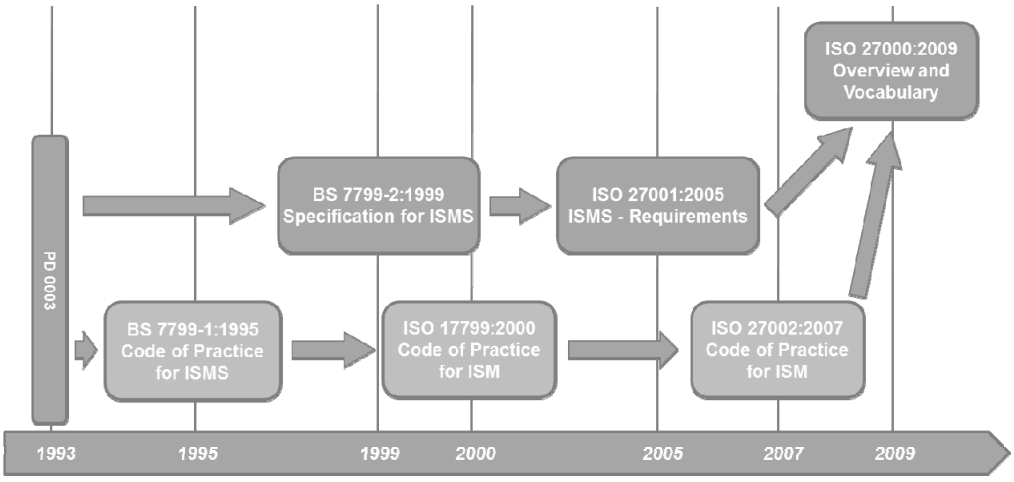

Figure 1. Development of standards ISO 27000, ISO 27001, and ISO 27002.

3. Development and Dissemination of ISO 27000 to ISO 27002 Standards

3.1. Development of Standards

The existence of the ISO 27000 to ISO 27002 standards can be traced back to 1993 (**Figure 1**), whereby a British professional association, the National Computing Centre (NCC), published a document titled "PD 0003 A Code of Practice for Information Security Management". The British Standards Institute (BSI) adopted this and issued "BS 7799-1 IT—Security techniques—Code of practice for information security management" as national standard in 1995.

The complementary part "BS 7799-2 Information security management systems—Specification with guidance for use" enables companies to certificate their processes. ISO harmonized this standard with others like ISO 9001 and developed the ISO 27001 in October 2005. Since then, companies can certify their processes according to this international standard.

ISO 27001 formed the foundation for the ISO 27 K family of standards, which encompass various standards for information security. In 2007 the old ISO 17799 standard was assigned to the ISO 27 K family as ISO 27002. In 2009 ISO 27000 was issued to provide an overview, introduction and explanation of terminology with the title "IT—Security techniques—Information security management systems—Overview and Vocabulary".

3.2. Current Dissemination of ISO 27001 Certification

At the end of year 2010 worldwide 15.625 certificates according to ISO 27001 are valid [4], more recent and reliable information do not exist. **Figure 2** shows the development from 2006 to 2010 and the large increase in the dissemination. With the high number of certificates in 2006 it should be noted that organizations that held certificates according to prior standards were able to convert these to ISO 27001 in a simplified process.

All our figures show the number of certificates according to ISO 27001, not the number of certified organizations. The number of organizations holding certificates cannot be given, because some organizations do have several certificates, e.g. for several sites or groups, other organizations do have one certificates for several sites.

The distribution of the certificates issued per region is shown in **Figure 3**. Alone 6.264 certificates were registered in Japan caused by local national legislations in Japan that often require the submission of proof or verification of security management conformance with standards. Furthermore, the surprisingly high number of certificates in Asia aside from Japan can be explained in part as follows: One objective of companies in Europe and North America is cost reduction through outsourcing of IT services. IT providers in Asia strive to achieve this objective primarily through the utilization of lower personnel costs. However, these providers are largely unknown in Europe and North America and have neither image nor reputation. Managers who are heading to outsource some of their IT activities need confidence in the reliability and professionalism of Asian IT providers. Normally they try to secure this by detailed and costly contracts and agreements, verifications, assessments, and reviews [5].

Independent attestations of the providers can be supportive and reinforcing. With a certificate according to ISO 27001 IT providers can thus document the conformity of their security processes with a recognized standard. The certificate serves as verification from an independent body and provides sureness about appropriate security measures; it serves as quality seal increasing the

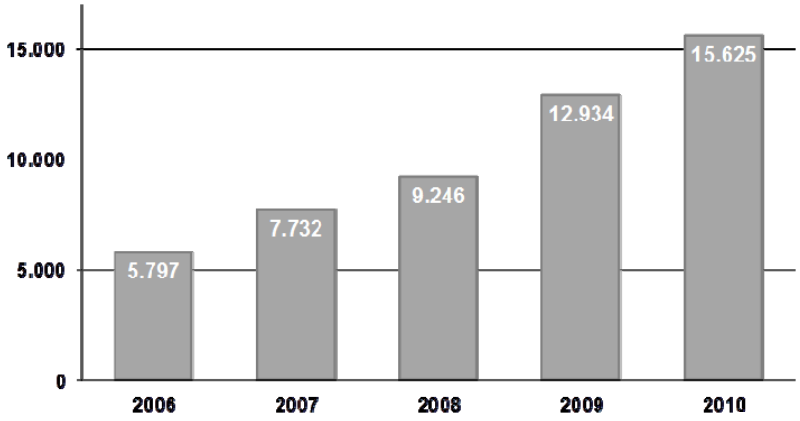

Figure 2. Number of certificates accord. ISO 27001 [4].

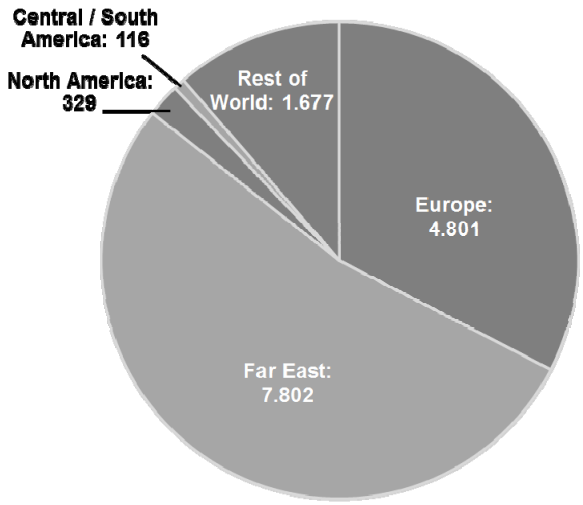

Figure 3. Number of certificates accord. ISO 27001 by regions [4].

Table 1. Number of certificates [4].

Top Countries in 2010	
Japan	6.264
India	1.281
United Kingdom	1.157
Taipei	1.028
China	957
Spain	711
Czech Republic	529
Italy	374
Germany	357
Romania	350

competitiveness of an IT provider [6].

The low number of 329 certificates registered in North America confirms the common assumption that international IT standards do not currently draw much attention there [7]. In Europe ISO 27001 has been widely disseminated, many European countries are in the list given in **Table 1**. The high number of certificates in the UK can also be explained by the fact that a British standard was the basis for the international ISO 27001 standard and so there is a longer tradition of certification according to security standards.

4. ISO 27000

The ISO 27000 standard was issued in 2009 to provide an overview for the ISO 27 K family of standards and a common conceptual foundation [8]. 46 basic information security terms are defined and differentiated in the "Terms and conditions" section. The meaning of information security and systematic engagement with security aspects is derived from the risk for companies whose business processes are increasingly dependent on information processing and whose complex and interlinked IT infrastructures are vulnerable to failures and disruptions. As with other IT standards, the ISO 27 K family of standards refer directly to the "Plan-Do-Check-Act" (PDCA cycle) cycle—well known from Deming's classic quality management (**Figure 4**), which emphasizes the necessity of process orientation as well as integration of the planning of operations and the constant checking of planing-compliant implementation [6].

In the planning phase for an ISMS the requirements for protection of the information and the information systems will be defined, risks identified and evaluated, and suitable procedures and measures for reducing risks developed. These procedures and measures will be implemented during implementation and operations. The reports generated through continuous monitoring of operations will be used to derive improvements and for further development of the ISMS.

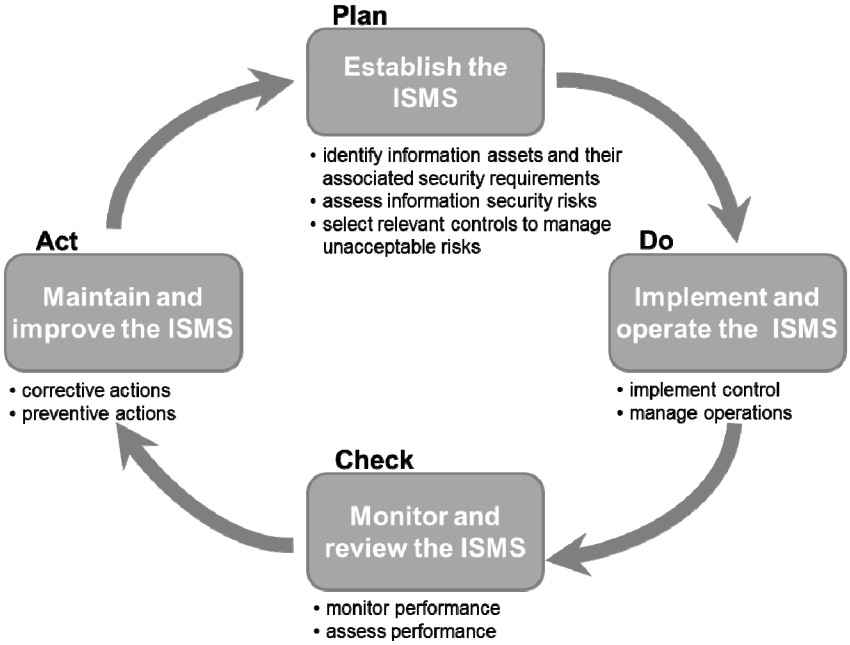

Figure 4. PDCA cycle in ISO 27000 [9].

5. ISO 27001

5.1. Content

The ISO 27001 standard was published in 2005 under the title "Information technology—Security techniques—Information security management systems—Requirements". In 42 pages it describes the requirements that an ISMS must fulfill in order to achieve certification. As a framework, the standard is aimed at companies from all sectors and of all sizes. However, there is some doubt over the suitability for SMEs [10]. Concrete measures for the fulfillment of requirements are not be stipulated by the standard but rather must be developed and implemented on a company-specific basis. Certification requirements of ISO 27001 are elucidated through the elaboration of terms and concepts and supplemented with a implementation guideline within ISO 27002.

The focal point of ISO 27001 is the requirement for planning, implementation, operation and continuous monitoring and improving of a process-oriented ISMS. The approach should be aligned with the PDCA cycle (**Figure 4**). The coverage and scope of an ISMS should be defined for planning and implementation. Risks should be identified and assessed [8] and control objectives should be defined for the information and information systems. Suitable measures for protecting operations should be derived from these. In annex A of the standard a total of 39 control objectives and 134 measures for security management are listed and thus expressly stipulated. The control objectives are listed in **Table 2**, subdivided by domains. These are described further and detailed in the ISO 27002 standard [11].

Adequate training should be developed for the implementation in order to push though the stipulated procedures and to establish them, and to generate awareness of their necessity [8]. The compliance with the procedures must be continuously monitored. The measures should be checked and improved in the course of continuous improvement and security risks should be identified and assessed in order to continuously increase the effectiveness and efficiency of the ISMS [8].

Requirements, which are to be applied to the ISMS documentation, are described in the standard through the stipulation of essential content, necessary documents as well as specifications and monitoring structures for document management, such as:

- Change and approvals processes
- Version control
- Rules for access rights and access protection
- Specifications for filing systems [8]

Responsibilities of top management in all phases of the PDCA cycle are listed [8]. They encompass determination and implementation of a security policy, the definition of roles and responsibilities, the recruitment and preparation of necessary personnel and material resources as well as decisions on risks management.

The improvement and further development of the ISMS is to be implemented continuously, based on the security policy, the logging and evaluation of operations, the results of testing as well as the results from improvement measures. In addition the improvement and further development should be pushed forward through

Table 2. ISO 27001 control objectives [8].

Domain	Control objectives
Security policy	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
Organization of information security	To manage information security within the organization.
	To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
Asset management	To achieve and maintain appropriate protection of organizational assets.
	To ensure that information receives an appropriate level of protection.
Human resources security	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
	To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
	To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.
Physical and environmental security	To prevent unauthorized physical access, damage and interference to organization's premises and information.
	To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.
Communications and operations management	To ensure the correct and secure operation of information processing facilities.
	To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
	To minimize the risk of systems failures.
	To protect the integrity of software and information.
	To maintain the integrity and availability of information and information processing facilities.
	To ensure the protection of information in networks and the protection of the supporting infrastructure.
	To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.
	To maintain security of information and software exchanged within an organization and with external entities.
	To ensure the security of electronic commerce services, and their secure use.
	To detect unauthorized information processing activities.
Access control	To control access to information.
	To ensure authorized user access and to prevent unauthorized access to information systems.
	To prevent unauthorized user access, compromise or theft of information and information processing facilities.
	To prevent unauthorized access to networked services.
	To prevent unauthorized access to operating systems.
	To prevent unauthorized access to information held in application systems.
	To ensure information security when using mobile computing and teleworking facilities.
Information systems acquisition, development and maintenance	To ensure that security is an integral part of information systems.
	To prevent errors, loss, unauthorized modification or misuse of information in applications.
	To protect the confidentiality, authenticity or integrity of information by cryptographic means.
	To ensure the security of system files.
	To maintain the security of application system software and information.
	To reduce risks resulting from exploitation of published technical vulnerabilities.
Information security incident management	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
	To ensure a consistent and effective approach is applied to the management of information security incidents.
Business continuity management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
Compliance	To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
	To ensure compliance of systems with organizational security policies and standards.
	To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

regular internal audits. Adequate implementation of the security policy as well as its suitability and completeness [8] are to be assured through annually management reviews.

5.2. Certification Process

To verify the compliance of the ISMS with ISO 27001 a company has to pass a certification procedure steered by an authorized certification organization (Registered Certification Bodies RCB), ISO provides a list of RCBs. The company initiates the procedure by selecting an RCB. In a preliminary examination with the support of the RCS a determination can be made to ascertain the extent to which there already is conformity according the standard and which needs for actions still exist for successful certification. Correspondingly, the measures necessary for ISMS conformity should be carried out in a preparation project. Appropriate knowledge and experience with certification processes as well as special expertise in information security is necessary for this and should be obtained by calling in external experts if required.

In the first instance the examination for certification (audit) comprises of a check of all documents (security policy, process descriptions, etc.) by the RCB, therefor the documents are to be sent to the certificating organization. Checking the documentation serves as a preparation for the main audit, where representatives of the certification organization carry out a detailed examination during an on-site visit lasting several days. This will include interviews being conducted with all responsible persons whereby they will explain their understanding of the security policy, describe processes, present details and features on a random basis, explain process documentation as well as discuss known weaknesses and improvement measures initiated.

Then the certification organization will generate a report in which the audit results are explained and improvement measures to be implemented necessarily before the next audit are listed. In case of a positive overall result the company receives the official certificate to attest the ISMS conformity with the requirements of ISO 27001.

The implementation of an appropriate ISMS can take a few months to some years, depending largely on the maturity of IT security management within an organization. When processes according framework like COBIT, ISO 20000, or ITIL are already established, time and costs of implementation will be lower. The process of certification will take a few months additionally [12].

The certificate has validity for 3 years; after this a re-certification can be applied for generally requiring less effort than the initial certification. The continuous observance of the requirements of standard ISO 27001 and continuous improvement of the ISMS is assured through annual monitoring audits. These audits are carried out by auditors from the RCB, whereby the first monitoring audit must take place before 12 months have passed since issuing the certificate. If serious deviations from the requirements of the standard should be discovered during a monitoring audit then the RCB can suspend or even withdraw the certificate until the deviations are rectified.

Some national alternatives exist. For German companies the federal office for information security (BSI) offers since 1994 a procedural guideline—so-called “IT-Grundschutz”—to support authorities and companies regarding security. In 2006 this specifications were been revised based on ISO 27001 and the concordance between “IT-Grundschutz” of BSI and the ISO 27001 standard was verified officially. Since 2006 BSI assigns this “ISO 27001 certification based on IT-Grundschutz” with which both the conformity with ISO 27001 and an assessment of the IT security measures against IT-Grundschutz catalogues are certified.

6. ISO 27002

The codified requirements in ISO 27001 are expanded and explained in ISO 27002 in the form of a guideline. The manual was first issued in the year 2000—at that time with the designation “ISO 17799”, under the title “Information technology—Security techniques—Code of practice for information security management”. In 2007 this was revised and aligned to the 27 K family of standards and the designation was changed to ISO 27002. With the development of ISO 27002 common practices—often also known as best practices—were offered as procedures and methods proven in practice, which could be adapted to the specific requirements within companies. In order to explain the importance of information security for companies, risks for the information security of a company and the necessity to have targeted and agreed measures (“controls”) within the framework of an ISMS [11] are set out. Necessary steps for identification and evaluation of security risks are described in order to ascertain the requirement to protect information and information systems [11]. The continuing development of ISO 27002 is based on the presentation of ISO 27001, whereby the 39 control objectives listed in the annex to ISO 27001 (**Table 2**) are explained in more detail. A total of 134 measures, which are justified and described in detail, are assigned to these objectives [11].

The fundamental guidelines for ensure information security are to be defined and specified in the form of security policies by the management of the company. The distribution and enforcement of these policies within the company also serves to emphasize the importance of information security and the management attention for

this topics. The information security must be organizationally anchored in the company so that the measures for information security can be efficiently promoted and established. So roles and responsibilities are to be defined and in particular duties for maintaining confidentiality and rules for the communications with external parties (customer, suppliers, authorities etc.) are to be specified. All tangible and intangible assets that are to be protected by the measures for information security are to be identified and classified in order to draw up specific responsibilities and handling rules.

Security risks are also caused by vulnerabilities of the IT systems. Here it must be assumed that more than half of all attacks are initiated by internal personnel—however a large proportion will also be initiated by joint actions from internal and external personnel [13]. Because internal personnel can use insider knowledge (on internal processes, habits, weak points, social relations etc.) for attacks they should be considered to have a higher potential for success and damage [14]. Corresponding risks must be taken into account with personnel measures such as recruiting, decruiting and allocating. So, for example, the access rights for a user must be restricted to the extent necessary to carry out the work that the user is assigned to. With changes in responsibilities, duties or jobs the access rights should be adapted accordingly and if personnel are laid off then the access rights should be revoked promptly.

Physical security measures should be provided to protect the infrastructure from unauthorized entry, access, theft, damage and destruction. To ensure proper and correct operation of the IT systems the ideal routine operations should be documented in a manual (standard operating procedures). Likewise, processes and procedures for exceptional circumstances, delays, outages, faults or catastrophic events should be specified and documented. Technical or organizational changes should be checked for potential effects on the operations of the IT systems before being implemented. Likewise security incidents should be documented, analyzed and evaluated for possible or essential improvements to the security system. Lastly, suitable measures must be implemented to fulfill compliance requirements. In particular copyrights and exploitation rights, requirements for data security and data protection are cited in the standard—these must be regulated and assured in a verifiable manner.

7. Further Standards in the ISO 27 K Family

The 27 K family of standards (also designated as “ISO 27 K” or “ISO 27000 series”) is managed under the title: “Information technology—Security techniques” and describes the requirements for an information security management system (ISMS) as well as for certifications in a comprehensive and detailed manner [9]. The family of standards represents a collection of both new and already well-known standards, which have been reworked and revised to bring them up to date and also to harmonize their content and format. With this collection ISO follows the objective of having cohesive standards in the area of information security as well as a compatibility with the various standards. This achieves the goal of offering comprehensive support to companies of all sizes, sector and types in ensuring information security [9]. The publishing of the 27 K family of standards is not completed or closed at this point in time—many standards are in the drafting or development stage, further supplements will follow. **Table 3** shows the current status as well as the immediate planning.

Figure 5 shows the interrelations of the standards in the 27 K family, separated into requirements and guidelines. ISO 27001 contains requirements that must be verified for certification according to this standard. ISO 27006 contains the requirements that must be fulfilled in order to be accredited as a certification organization. All further standards can be considered as guidelines for different domains to ensure information security.

8. Summary

Information and information systems are exposed to risks more and more through the increasing support to business processes provided by information technology as well as the increased level of networking within companies and with external parties. An effective ISMS helps to reduce risks and to prevent security breaches.

The ISO 27000, 27001 and 27002 standards form a framework to design and operate an ISMS, based on long lasting experiences of development. With this companies are offered the opportunity to align their IT procedures and methods for ensuring an adequate level of information security with an international standard.

Certification of an ISMS according to ISO 27001 also projects a positive image through the verification of a systematic management of information security. This standard is also called upon in legal rulings as a yardstick and a basis for assessment on the subject of information security—here a certificate according to ISO 27001 proves a “provision of state-of the-art services” regarding information security. Organizations can demonstrate that they are “fit-enough” to provide IT services in a secure way [1]. With the certificate a verification of compliance with respect to information security can be rendered.

The ISO 27000, 27001 and 27002 standards have been widely disseminated in Europe and Asia. The significance of a certification of compliant information security with procurement decisions for IT services will increase and so a further increase in the number of certifications

Table 3. The ISO 27 K family of standards [15].

ISO-Norm	Title	Status
ISO 27000	Information security management systems—Overview and vocabulary	published 2009
ISO 27001	Information security management systems—Requirements	published 2005
ISO 27002	Code of practice for information security management	published 2007
ISO 27003	Information security management system implementation guidance	published 2010
ISO 27004	Information security management—Measurement	published 2009
ISO 27005	Information security risk management	published 2011
ISO 27006	Requirements for bodies providing audit and certification of ISMSs	published 2011
ISO 27007	Guidelines for ISMS auditing	published 2011
ISO 27008	Guidelines for auditors on ISMS controls	published 2011
ISO 27010	ISMSs for inter-sector and inter-organizational communications	published 2012
ISO 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	published 2008
ISO 27013	Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001	under development
ISO 27014	Proposal on an information security governance (ISG) framework	under development
ISO 27016	Information security management—Organizational economics	under development
ISO 27017	Guidelines on information security controls for use of cloud computing	under development
ISO 27018	Code of practice for data protection controls for public cloud computing	under development
ISO 27031	Guidelines for ICT readiness for business continuity	under development
ISO 27032	Guidelines for cyber security	under development
ISO 27033-1	Network security—Part 1: Overview and concepts	published 2009
ISO 27033-2	Network security—Part 2: Guidelines for the design and implementation	published 2012
ISO 27033-3	Network security—Part 3: Reference networking scenarios	published 2010
ISO 27033-4	Network security—Part 4: Securing communications between networks	under development
ISO 27033-5	Network security—Part 5: Securing communications across networks using VPNs	under development
ISO 27033-6	Network security—Part 6: Securing IP network access using wireless	under development
ISO 27034-1	Application security—Part 1: Overview and concepts	published 2011
ISO 27034-2	Application security—Part 2: Organization normative framework	under development
ISO 27034-3	Application security—Part 3: Application security management process	under development
ISO 27034-4	Application security—Part 4: Application security validation	under development
ISO 27034-5	Application security—Part 5: Application security controls data structure	under development
ISO 27035	Information security incident management	under development
ISO 27036	Information security for supplier relationships	under development
ISO 27037	Guidelines for identification, collection and/or acquisition and preservation of digital evidence	under development
ISO 27038	Specification for digital redaction	under development
ISO 27039	Selection, deployment and operations of intrusion detection systems	under development
ISO 27040	Storage security	under development
ISO 27041	Guidance on assuring suitability and adequacy of investigation methods	under development
ISO 27042	Guidelines for the analysis and interpretation of digital evidence	under development
ISO 27043	Investigation principles and processes	under development

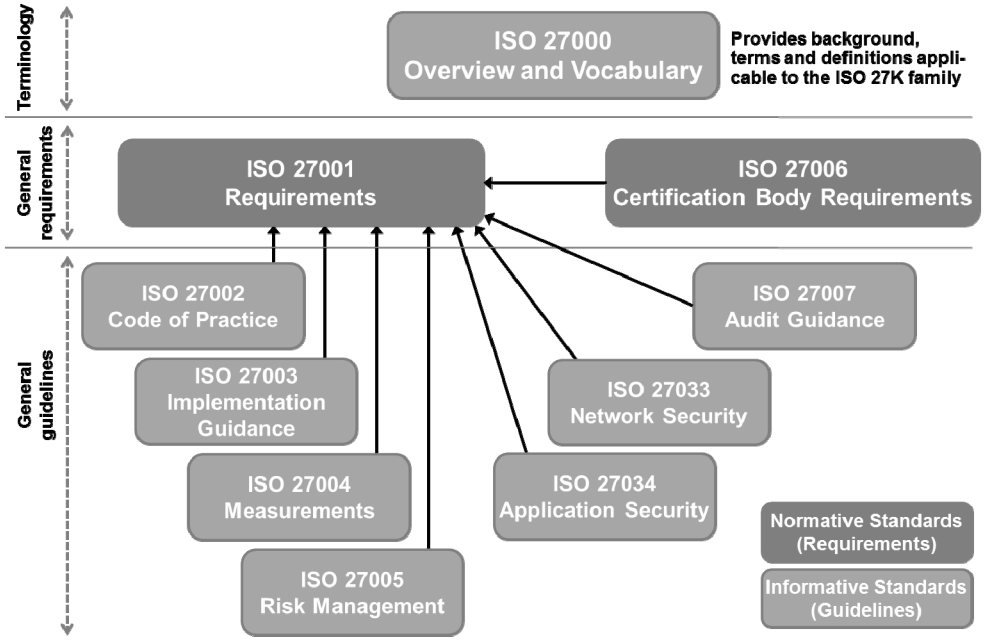

Figure 5. Interrelations within the ISO 27 K family of standards [9].

according to ISO 27001 is also to be expected.

REFERENCES

[1] E. Humphreys, "Information Security Management System Standards," *Datenschutz und Datensicherheit*, Vol. 35, No. 1, 2011, pp. 7-11. doi:10.1007/s11623-011-0004-3

[2] BSI, "IT-Sicherheitsmanagement und IT-Grundschutz, BSI-Standards zur IT-Sicherheit," Köln, 2005.

[3] C. Pelnekar, "Planning for and Implementing ISO 27001," *ISACA Journal*, Vol. 4, No. 4, 2011, pp. 1-8.

[4] ISO/Nielsen, "The ISO Survey of Certifications," International Organization for Standardization ISO, Geneve, 2011.

[5] Deloitte, "Financial Services Global Security Study," Deloitte, London, 2010.

[6] G. Disterer, "Zertifizierung der IT Nach ISO 20000," *Wirtschaftsinformatik*, Vol. 51, No. 6, 2009, pp. 530-534.

[7] M. Winniford, S. Conger and L. Erickson-Harris, "Confusion in the Ranks," *Information Systems Management*, Vol. 26, No. 2, 2009, pp. 153-163. doi:10.1080/10580530902797532

[8] ISO 27001, "Information Technology, Security Techniques, Information Security Management Systems, Requirements," International Organization for Standardization ISO, Geneve, 2005.

[9] ISO 27000, "Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary," International Organization for Standardization ISO, Geneve, 2009.

[10] Y. Barlette and V. Fomin, "Exploring the suitability of IS Security Management Standards for SMEs," In: R. H. Sprague, Ed., *Proceeding of* 41*st Hawaii International Conference on System Sciences* (*HICSS*), Los Alamitos, 2008, pp. 308- 317.

[11] ISO 27002, "Information Technology, Security Techniques, Code of Practice for Information Security Management," International Organization for Standardization ISO, Geneve, 2005.

[12] A. Teubner and T. Feller, "Informationstechnologie, Governance und Compliance," *Wirtschaftsinformatik*, Vol. 50, No. 5, 2008, pp. 400-407. doi:10.1007/s11576-008-0081-6

[13] R. Richardson, "CSI Computer Crime and Security Survey," Computer Security Institute and Federal Bureau of Investigation, Washington, 2008.

[14] J. D'Arcy and A. Hovav, "Deterring internal information systems misuse," *Communications of the ACM*, Vol. 50, No. 10, 2007, pp. 113-117. doi:10.1145/1290958.1290971

[15] "ISO IT Security Techniques," 8 August 2012. www.iso.org

