Information Security Standards

Dan Constantin Tofan
Academy of Economic Studies Bucharest
Romana Square, district 1, Bucharest 010374,
ROMANIA
tofandan@yahoo.com

Abstract: The use of standards is unanimously accepted and gives the possibility of comparing a personal security system with a given frame of reference adopted at an international level. A good example is the ISO 9000 set of standards regarding the quality management system, which is a common reference regardless of the industry in which a certain company activates. Just like quality control standards for other industrial processes such as manufacturing and customer service, information security standards demonstrate in a methodical and certifiable manner that an organization conforms to industry best practices and procedures. This article offers a review of the world's most used information security standards.

Key-Words: Information Security Standards, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 17799, COBIT, NIST SP-800 series, Federal Office for Information Security (BSI), ISF – Standard of good practice for Information Security.

1. What is an information security standard?

Generally speaking a standard, whether it is an accountability standard, a technical standard or an information security standard, it represents a set of requirements that a product or a system must achieve. Assuming the conformity of a product or system with a certain standard demonstrates that it fulfills all the standard's specifications.

There are currently some primary standards in place governing information security.

First of them is the ISO/IEC 27000 series of standards. It is the most recognizable standard as it bears the internationally prestigious name of the International Organization for Standardization and the International Electrotechnical Commission.

It was initiated by British Standard Institute in 1995 through BS7799 (Information Security Management System), and later was taken over by the ISO (International Organization for Standardization) and released under the name of ISO/IEC 27000 series (ISMS Family of Standards) and ISO/IEC 17799:2005 "Information Technology – Code of practice for information security management". Secondly, there is the NIST SP800 group of standards, published by the National Institute of Standards and Technology (NIST) from USA.

Another information security standard is the Information Security Forum's Standard of Good Practice for Information Security.

This document also includes a description of COBIT and BSI Standards 100 series. Due to the lack of space other international security standards like ITIL could not be presented.

This is a post conference paper. Parts of this paper have been published in the Proceedings of the 3rd International Conference on Security for Information Technology and Communications, SECITC 2010 Conference (printed version).

2. Why do we need an information security standard?

The use of standards is unanimously accepted and gives the possibility of comparing a personal security system with a given frame of reference adopted at an international level. A good example is the ISO 9000 set of standards regarding the quality management system, which is a common reference regardless of the industry in which a certain company activates.

Standards ensure desirable characteristics of products and services such as quality, safety, reliability, efficiency and interchangeability - and at an economical cost.

We need information security standards in order to implement information security controls to meet an organizations requirements as well as a set of controls for business relationships with other organizations and the most effective way to do this is to have a common standard on best practice for information security management such as ISO/IEC 17799:2005. Organizations can then benefit from common best practice at an international level, and can prove the protection of their business processes and activities in order to satisfy business needs.

Anyone responsible for designing or implementing information security systems knows that it can sometimes be difficult to demonstrate the effectiveness of their solutions, either to their organization's decision makers, or to its clients. Decision makers need to know that the budgets they assign are being directed at worthwhile targets, while clients demand the sense of confidence that comes with knowing their sensitive data and confidential details are in safe hands.

This is where the role of information security standards becomes essential. Similarly to quality control standards for other industrial branches such as customer service, information security standards demonstrate in a methodical and certifiable manner that an organization conforms to industry best practices and procedures.

3. The ISO/IEC 27000 standards series

The International Organization for Standardization (Organization internationale de normalization), known as ISO, is an international-standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, the organization promulgates world-wide proprietary industrial and commercial standards. ISO’s headquarters are in Geneva, Switzerland ISO is defined as a non-governmental organization, but its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations.

The ISO International Standards are published in accordance with the following format: ISO[/IEC][/ASTM] [IS] nnnnn[:yyyy] Title, where nnnnn is the number of the standard, yyyy is the year published, and Title describes the subject. IEC stands for International Electrotechnical Commission and is included if the standard results from the work of ISO/IEC JTC1 (the ISO/IEC Joint Technical Committee). For standards developed in cooperation with ASTM International, ASTM is used.

ISO has 157 national members, out of the 195 total countries in the world. ISO has three membership categories:

Member bodies are national bodies that are considered to be the most representative standards body in each country. These are the only members of ISO that have voting rights.

Correspondent members are countries that do not have their own standards organization. These members are informed about ISO's work, but do not participate in standards promulgation.

Subscriber members are countries with small economies. They pay reduced membership fees, but can follow the development of standards.

The ISO/IEC 27000-series (also known as the 'ISMS Family of Standards' or 'ISO27k' for short) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The series provides recommendations on information security management, risk handling and controls implementation within the context of an overall Information Security Management System (ISMS). Management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series) are also similar in design to the ISO/IEC 27000- series of standards.

The series is applicable to organizations of all shapes and sizes covering more than just privacy, confidentiality and IT or technical security issues.

The first of the 27000 series of standards (27001) was published in 2005. However, its predecessor -- ISO/IEC 17799 - dates back to 2000, a time when the growth of the Internet caused a rapidly increasing awareness of the importance of security in the IT industry.

There are currently four published standards in the series: 27001, 27002, 27005 and 27006. Ten more are at various draft stages.

3.1. ISO/IEC27001

The 27001 standard sets out the steps required for an organization's Information Security Management Systems (ISMS) to achieve certification. The standard specifies seven key elements in the creation of a certified ISMS. These are to establish, implement, operate, monitor, review, maintain and improve the system. As a management standard it doesn't mandate the use of specific controls so much as specify the management processes required to identify controls that are appropriate to the organization.

It is intended to be used along with ISO/IEC 27002 (formerly ISO/IEC 17799), the Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls. Organizations that implement an ISMS in accordance with ISO/IEC 27002 are likely to simultaneously meet the requirements of ISO/IEC 27001 but certification is entirely optional.

3.2. ISO/IEC 27002

ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799:2005 and subsequently renumbered ISO/IEC 27002:2005 in July 2007, bringing it into line with the other ISO/IEC 27000-series standards. It is entitled Information technology - Security techniques - Code of practice for information security management. The current standard is a revision of the version first published by ISO/IEC in 2000, which was a word-for-word copy of the British Standard (BS) 7799-1:1999.

The purpose of the 27002 standard is to set out a structured set of literally hundreds of information security controls, the use of which will help to achieve conformity with 27001. However, it is not an compulsory list: organizations are free to implement controls not specifically listed, so long as they are effective and conform to the requirements outlined in 27001.

ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad: the preservation of **confidentiality** (ensuring that information is accessible only to those authorised to have access), **integrity** (safeguarding the accuracy and completeness of information and processing methods) and **availability** (ensuring that authorised users have access to information and associated assets when required).

ISO/IEC 27002 contains best practices and security controls in the following areas of information security management:

- security policy;
- organization of 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.

3.3. ISO/IEC 27005

ISO/IEC 27005:2008 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the implementation of information security based on a risk management approach. Knowledge of the concepts and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is very important for a complete understanding of ISO/IEC 27005:2008. ISO/IEC 27005:2008 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

3.4. ISO/IEC 27006

The 27006 standard outlines the certification and registration processes that must be followed by certifying bodies. Its chief purpose is to guide accredited certification bodies on the formal processes for certifying or registering other organizations information security management systems.

The scope of ISO/IEC 27006 is "to specify general requirements a third-party body operating ISMS certification/registration has to meet, if it is to be recognized as competent and reliable in the operation of ISMS certification / registration."

The following standards are under development by the ISO/IEC JTC1:

- ISO/IEC 27000 - an introduction and overview for the ISMS Family of Standards, plus a glossary of common terms
- ISO/IEC 27003 - an ISMS implementation guide
- ISO/IEC 27004 - a standard for information security management measurements
- ISO/IEC 27007 - a guideline for ISMS auditing (focusing on the management system)
- ISO/IEC 27008 - a guideline for Information Security Management auditing (focusing on the security controls)
- ISO/IEC 27011 - an ISMS implementation guideline for the telecommunications industry (also known as X.1051)
- ISO/IEC 27031 - a specification for ICT readiness for business continuity
- ISO/IEC 27032 - a guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
- ISO/IEC 27033 - IT network security, a multi-part standard currently known as ISO/IEC 18028:2006
- ISO/IEC 27034 - a guideline for application security

4. The SP800 standard series

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life.

NIST has a total budget of $931.5 million and employs about 2,900 scientists, engineers, technicians, and support and administrative personnel. 2

NIST Laboratories provide measurements and standards for U.S. industry:

- Building and fire research
- Chemical science and technology
- Electronics and electrical engineering
- Information technology
- Manufacturing engineering
- Materials science and engineering
- Nanoscale science and technology
- Neutron research
- Physics
- Technology services

Established in 1990 the NIST Special Publications 800 group of documents is the oldest of all the information security standards. It consists of over a hundred documents covering almost every aspect of information security. The most representative among all these documents is the computer security handbook SP800-12 which provides a good idea of the NIST approach.

4.1. SP800-12

The core document of the series, SP800-12, is a handbook that covers the central principles of information security in details. It summarizes NIST's approach to the subject, identifying the following eight major guiding elements:

1. Computer security should support the organization's mission

2. Computer security is a central element of sound management
3. Computer security should be cost effective
4. Computer security responsibilities and accountability should be made explicit
5. System owners have security responsibilities outside their own organizations
6. Computer security requires a comprehensive and integrated approach
7. Computer security should be periodically reassessed
8. Computer security is constrained by societal factors

The document, along with the rest of the series, goes on to outline in detail the specific strategies, procedures and controls by which security issues can be addressed in compliance with these principles. They cover areas such as Guidelines on Electronic Mail Security (SP800-45), Building an Information Technology Security Awareness and Training Program (SP800-50), Electronic Authentication Guidelines (SP800-63) and Guidelines for Secure Web Services (SP800-95) to mention just a few. By explaining important concepts, cost considerations, and interrelationships of security controls the handbook provides assistance in securing computer-based resources (including hardware, software, and information).

Although NIST doesn't itself provide a certification program, it provides support for a range of initiatives in the areas of awareness, training and education.

5. ISF Standard of Good Practice for Information Security

The Information Security Forum (ISF) is an international, independent, non-profit organization dedicated to benchmarking and best practices in information security. It was established in 1989 as the European Security Forum but expanded its mission and membership in the 1990s, so that it now includes hundreds of members, including a large number of Fortune 500 companies, from North America, Asia, and other locations around the world. Groups of members are organized as chapters throughout Europe, Africa, Asia, the Middle East, and North America. The ISF is headquartered in London, England, but also has staff based in New York City.

The membership of the ISF is international and includes large organizations in transportation, financial services, chemical/pharmaceutical, manufacturing, government, retail, media, telecommunications, energy, transportation, professional services, and other sectors.

The Standard of Good Practice (SoGP) was first released in 1996 by the Information Security Forum (ISF) and it represents a detailed documentation of best practice for information security. The Standard is published and revised biannually.

Standard of Good Practice, which is freely available, derives from the ISO/IEC 27002 and COBIT v4.1. standards and outlines a functional information security methodology based on both research and real world experience. The standard is centered around the following six key aspects:

1. Computer installations. This aspect is targeted chiefly at IT specialists, and addresses the hardware and software that supports the critical business applications.
2. Critical business applications. These are the applications on which the organization's activities depend. This aspect is primarily targeted at the CBA owners, the individuals in charge of business processes and systems integrators.
3. Security management. The security management aspect is targeted at security decision makers and auditors. It handles management level decision making in relation to security implementations across the organization.
4. Networks. Networks form a special category due to their unique security vulnerabilities. Its target is typically

network managers, network service specialists and network service providers. The network aspect addresses the nature and implementation of an organization's networking requirements.

5. Systems development. This aspect addresses to system developers and deals with the identification, design and implementation of system requirements.
6. End user environment. The end user environment is the point at which individuals are using the organization's systems and applications to support business processes. This aspect therefore tends to target business managers and individuals who work within such end user environments.

Computer Installations and **Networks** address the underlying IT infrastructure on which **Critical Business Applications** run. The **End-User Environment** covers the arrangements associated with protecting corporate and workstation applications at the endpoint in use by individuals. **Systems Development** deals with how new applications and systems are created, and **Security Management** addresses high- level direction and control.

The standard itself consists of a statement of principles and objectives, completed by an extensive documentation covering implementation recommendations. In order to maintain currency in the fast changing world of information security the standard is reviewed and updated biannually. In addition to the Standard of Good Practice, the ISF also supervises a biannual benchmarking program known as the Information Security Status Survey. The participating organizations are examined on the effectiveness of the security systems and the results are measured against each other.

6. Control Objectives for Information and related Technology (COBIT)

The ISACA (Information Systems Audit and Control Association) was founded in the USA in 1967 by a group of individuals dealing with auditing controls in the computer systems, when they realized the need for a standard in the field. In 1969, Stuart Tyrnauer founded an entity named EDP Auditors Association. In 1976 the association developed as an education foundation with the scope of expanding the knowledge and value of the IT governance and control field.

Today, ISACA’s membership is composed of more than 75,000 members worldwide. Members live and work in more than 160 countries and cover a variety of professional IT-related positions.

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI).

COBIT was first released in 1996. Its mission is “to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.” COBIT helps Managers, auditors, and other users to understand their IT systems and decide the level of security and control that is necessary to protect their companies’ assets through the development of an IT governance model.

COBIT is an IT governance framework that allows managers to fill in the gap between control requirements, technical issues and business risks. The latest update COBIT 4.1 helps organizations to increase the value attained from IT, highlights links between business and IT goals, and simplifies implementation of the COBIT framework. COBIT 4.1 is a fine-tuning of the COBIT framework and can be used to enhance work already done based upon earlier versions of COBIT.

COBIT 4.1 has 34 high level processes that cover 210 control objectives categorized in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation:

1. Plan and Organize. The Plan and Organize domain describes how IT can

be used to help achieve the company's goals and objectives.

2. Acquire and Implement. This domain covers activities such as identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes.
3. Deliver and Support. It covers areas such as the execution of the applications within the IT system and its results, as well as, the processes that enable the efficient execution of these IT systems.
4. Monitor and Evaluate. This domain deals with the strategy of assessing the needs of the company and establishes whether or not the current IT system still meets the objectives for which it was designed.

1. COBIT and ISO/IEC 27002 do not compete with each other and actually complement one another. COBIT typically covers a broader area than ISO/IEC 27002.

7. BSI IT-Grundschutz - IT baseline protection

The Bundesamt für Sicherheit in der Informationstechnik (abbreviated BSI - in English: Federal Office for Information Security) is the German government agency in charge of managing computer and communication security for the German government. Its areas of expertise and responsibility include the security of computer applications, critical infrastructure protection, Internet security, cryptography, counter eavesdropping, certification of security products and the accreditation of security test laboratories. It is located in Bonn and has over 400 employees.

BSI's predecessor was the cryptographic department of Germany's foreign intelligence agency (BND). BSI still designs cryptographic algorithms such as the Libelle cipher.

The BSI Standards contains recommendations on methods, processes, procedures and approaches relating to information security. For accomplishing that the BSI standards contains fundamentally

important areas for information security regarding public authorities and companies and for which appropriate practical approaches have been established.

BSI Standard 100-1 is the first standard of the BSI IT-Grundschutz series and defines the general requirements for implementing an ISMS. It is completely compatible with ISO Standard 27001 and also takes into consideration the recommendations within ISO Standards 13335 and 27002.

BSI-Standard 100-2 also known as The IT-Grundschutz Methodology is a step by step description of how IT security management can be set up and operated in practice.

The IT-Grundschutz Methodology provides a detailed description of how to select appropriate IT security measures, how to produce a practical IT security concept, and how to implement the IT security concept. IT-Grundschutz interprets the general requirements of the ISO Standards 27001, 27002 and 13335 and provides many notes, background expertise and examples in order to help users implement them in practice. The IT-Grundschutz Catalogues not only explain what has to be done, they also provide very specific information as to what implementation may look like.

BSI-Standard 100-3: The third standard from the BSI series deals with a method of risk analysis based on IT-Grundschutz. This approach can be used when organizations are already working successfully with the IT-Grundschutz Manual and would like to add an additional risk analysis to the IT- Grundschutz analysis.

8. Conclusions

Information security standards are needed in order to implement information security controls to meet an organizations requirements as well as a set of controls for business relationships with other organizations. The most effective way to do this is to have a common standard on best practice for information security management such as the standards described above. By implementing one of these standards organizations can benefit from common best practice at an international level, and can prove the protection of their business processes and activities in order to satisfy business needs. The only problem is to choose which of the standards is appropriate for an organization judging by the nature and field of activity. Although there are a number of information security standards available, an organization can only benefit if those standards are implemented properly. Security is something that all parties should be involved in. Senior management, information security practitioners, IT professionals and users all have a role to play in securing the assets of an organization. The success of information security can only be achieved by full cooperation at all levels of an organization, both inside and outside.

References

[1] International Organization for Standardization - International Electrotechnical Commission Joint Technical Committee1, *ISO/IEC 27002- Information technology -- Security techniques -- Information security management systems -- Requirements*, 2007.

[2] International Organization for Standardization-International Electrotechnical Commission Joint Technical Committee1, *ISO/IEC 17799 Information technology — Security techniques — Code of practice for information security management*, 2005.

[3] National Institute for Standards and Technology, *An introduction to Computer Security – The NIST Handbook – SP 800-12*, NIST 1995, http://csrc.nist.gov.

[4] Information Security Forum, *The Standard of Good Practice for Information Security*, ISF 2007, https://www.isfsecuritystandard.com/SOGP07/index.htm.

[5] Erik Guldentops, Tony Betts, Gary Hodgkiss, *Aligning COBIT, ITIL and ISO 17799 for Business Benefit*, http://www.isaca.org 2007

[6] Jimmy Heschl, *Cobit Mapping: Overview Of International IT Guidance - 2nd edition*, IT Governance Institute USA http://www.isaca.org 2007

[7] Federal Office for Information Security (BSI), *BSI Standard 100-1 Information Security Management System*, http://www.bsi.de/english/publications/bsi_st andards/index.htm 2008

[8] Federal Office for Information Security (BSI), *BSI Standard 100-2 IT-Grundschutz Methodology*, http://www.bsi.de/english/publications/bsi_st andards/index.htm 2008

[10] Federal Office for Information Security (BSI), *BSI Standard 100-3 Risk Analysis based on IT-Grundschutz*, http://www.bsi.de/english/publications/bsi_st andards/index.htm 2008.

[11] An Overview of Information Security Standards, The Government of the Hong Kong Special Administrative Region, 2008, www.infosec.gov.hk/english/technical/files/overview.pdf

[12] http://en.wikipedia.org