*The 7th International Scientific Conference*
*"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"*
**Braşov, November 15th 2012**

# SECURING IT NETWORKS WITH ISMS FAMILY OF STANDARDS (ISO 27001 SERIES)

**LTC Military professor eng. Daniel SORA, PhD**

National Defence University of Romania "Carol I"/ The Regional Department of Defense Resources Management Studies / Braşov / România

**Abstract:**
An organization's information is dependent upon information and communications technology. This technology is an essential element in any organization and assists in facilitating the creation, processing, storing, transmitting, protection and destruction of information. Where the extent of the interconnected global business environment expands so does the requirement to protect information as this information is now exposed to a wider variety of threats and vulnerabilities.
International Standards for Management Systems incorporates the features on which experts in the field have reached a consensus as being the international state of the art. Through the use of the Information Security Management System (ISMS) family of standards, organizations can develop and implement a framework for managing the security of their information assets and prepare for an independent assessment of their ISMS applied to the protection of information, such as financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties.

*Key words: information, networks, protection, risks*

## 1. Introduction

All information held and processed by an organization is subject to threats of attack, error, nature (for example, flood or fire), etc, and is subject to vulnerabilities inherent in its use. The term information security is generally based on information being considered as an asset which has a value requiring appropriate protection, for example, against the loss of availability, confidentiality and integrity. Enabling accurate and complete information to be available in a timely manner to those with an authorized need is a catalyst for business efficiency.

Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its objectives, and maintain and enhance its legal compliance and image. These coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are generally known as elements of information security management.

As information security risks and the effectiveness of controls change depending on shifting circumstances, organizations need to:

a) monitor and evaluate the effectiveness of implemented controls and procedures;
b) identify emerging risks to be treated; and
c) select, implement and improve appropriate controls as needed.

# *SECURING IT NETWORKS WITH ISMS FAMILY OF STANDARDS (ISO 27000 SERIES)*

To interrelate and coordinate such information security activities, each organization needs to establish its policy and objectives for information security and achieve those objectives effectively by using a management system.

An ISMS (Information Security Management System) provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets to achieve business objectives based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS:

a) awareness of the need for information security;
b) assignment of responsibility for information security;
c) incorporating management commitment and the interests of stakeholders;
d) enhancing societal values;
e) risk assessments determining appropriate controls to reach acceptable levels of risk;
f) security incorporated as an essential element of information networks and systems;
g) active prevention and detection of information security incidents;
h) ensuring a comprehensive approach to information security management; and
i) continual reassessment of information security and making of modifications as appropriate.

The ISMS family of standards is intended to assist organizations of all types and sizes to implement and operate an ISMS. The ISMS family of standards consists of the following International Standards, under the general title *Information technology — Security techniques*:

- ISO/IEC 27000:2009, *Information security management systems — Overview and vocabulary*
- ISO/IEC 27001:2005, *Information security management systems — Requirements*
- ISO/IEC 27002:2005, *Code of practice for information security management*
- ISO/IEC 27003:2010, *Information security management system implementation guidance*
- ISO/IEC 27004:2009, *Information security management — Measurement*
- ISO/IEC 27005:2008, *Information security risk management (Second edition)*
- ISO/IEC 27006:2011, *Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27007:2011, *Guidelines for information security management systems auditing*
- ISO/IEC 27008:2011, *Guidelines for auditors on information security management systems controls*
- ISO/IEC 27010:2012, *Information security management for inter-sector and inter-organisational communications*

An organization needs to maintain and improve the ISMS through monitoring and assessing performance against organization policy and objectives, and reporting the results to management for review. This ISMS review will allow evidence of validation, verification, and traceability of corrective, preventive and improvement actions based on the records of these monitored areas, including the monitoring of information security controls.

## 2. The ISMS family of standards description

The ISMS family of standards consists of inter-related standards, either already published or under development, and contains a number of significant structural components. These components are focused upon normative standards describing ISMS requirements (ISO/IEC 27001) and certification body requirements (ISO/IEC 27006) for those certifying compliance with ISO/IEC 27001. Other standards provide guidance for various aspects of an ISMS implementation, addressing a generic process, control-related guidelines as well as sector-specific guidance. Relationships between the ISMS family of standards are illustrated in Figure 1.

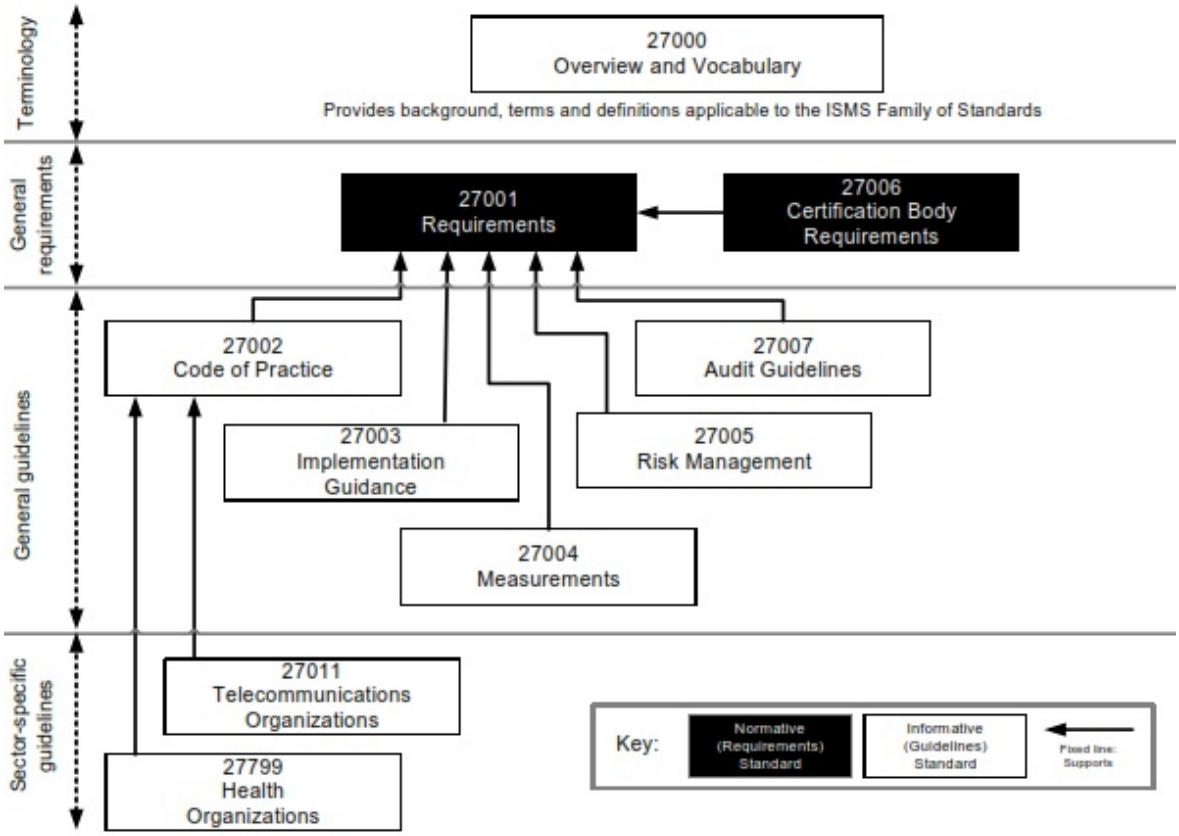


Fig.1 ISMS Family of Standards Relationships

**ISO/IEC 27000** *Information security management systems — Overview and vocabulary* describes the fundamentals of information security management systems, which form the subject of the ISMS family of standards, and defines related terms.

### 2.1 Standards specifying requirements

**ISO/IEC 27001** *Information security management systems — Requirements* specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. This International Standard is universal for all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations).

# *SECURING IT NETWORKS WITH ISMS FAMILY OF STANDARDS (ISO 27000 SERIES)*

ISO/IEC 27001 provides normative requirements for the development and operation of an ISMS, including a ***set of controls*** for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS. Organizations operating an ISMS may have its conformity audited and certified. The control objectives and controls from Annex A (ISO/IEC 27001) shall be selected as part of this ISMS process as appropriate to cover the identified requirements.

Annex A of ISO 27001 is probably the most mentioned annex of any management standard, containing the following clauses (sometimes called ISO 27001 Annex A domains):

- A.5 Security policy
- A.6 Organization of information security
- A.7 Asset management
- A.8 Human resources security
- A.9 Physical and environmental security
- A.10 Communications and operations management
- A.11 Access control
- A.12 Information systems acquisition, development and maintenance
- A.13 Information security incident management
- A.14 Business continuity management
- A.15 Compliance

Annex A contains 133 controls which, as can be seen from the names of the clauses, are not focused solely on IT - they also cover physical security, legal protection, human resources management, organizational issues, etc.

Therefore, you could consider Annex A as a form of a catalog of security measures to be used during your treatment process - once you identify unacceptable risks in risk assessment, Annex A will help you choose the right control(s) to decrease those risks. And ensure you don't forget any important control.

Annex A is where ISO 27001 and ISO 27002 come together - the controls in ISO 27002 are named the same as in Annex A of ISO 27001, but the difference is in the level of detail - ISO 27001 gives only a short definition of a control, while ISO 27002 gives detailed guidelines on how to implement the control. ISO27001 are ***the requirements*** needed to eventually have your ISMS (Information Security Management System) certified by an accredited company. ISO-27002 is considered best practices document, meaning that if you don't know how to comply with 27001 Annex A controls - you can use 27002 to get ideas how to implement the control.

**ISO/IEC 27006** *Requirements for bodies providing audit and certification of information security management systems* specifies requirements and provides guidance for bodies providing audit and ISMS certification in accordance with ISO/IEC 27001, in addition to the requirements contained within ISO/IEC 17021. It is primarily intended to support the accreditation of certification bodies providing ISMS certification according to ISO/IEC 27001. The document supplements ISO/IEC 17021 in providing the requirements by which certification organizations are accredited, thus permitting these organizations to provide compliance certifications consistently against the requirements set forth in ISO/IEC 27001.

### 2.2 Standards describing general guidelines

**ISO/IEC 27002** *Code of practice for information security management* provides a list of commonly accepted control objectives and best practice controls to be used as

implementation guidance when selecting and implementing controls for achieving information security.

**ISO/IEC 27003** *Information security management system implementation guidance* provides practical implementation guidance and provide a process oriented approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS in accordance with ISO/IEC 27001.

**ISO/IEC 27004** *Information security management — Measurement* provides guidance and advice on the development and use of measurements in order to assess the effectiveness of ISMS, control objectives, and controls used to implement and manage information security, as specified in ISO/IEC 27001.

**ISO/IEC 27005** *Information security risk management* provides guidelines on implementing a process oriented information security risk management. The approach described within this International Standard supports the general concepts specified in ISO/IEC 27001.

**ISO/IEC 27007** *Guidelines for information security management systems auditing* provides guidance on conducting internal or external ISMS audits, as well as guidance on the competence of information security management system auditors, in addition to the guidance contained in ISO 19011, which is applicable to managements systems in general.

**ISO/IEC 27008** *Guidelines for auditors on information security management systems controls* complements ISO/IEC 27007. It concentrates on auditing the information security controls, whereas ’27007 concentrates on auditing the management system. This standard provides guidance for all auditors regarding “information security management systems controls” selected through a risk-based approach for information security management. It supports the information security risk management process and internal, external and third-party audits of an ISMS by explaining the relationship between the ISMS and its supporting controls. It provides guidance on how to verify the extent to which required “ISMS controls” are implemented. Furthermore, it supports any organization using ISO/IEC 27001 and ISO/IEC 27002 to satisfy assurance requirements, and as a strategic platform for Information Security Governance.

## 3.Conclusion

As part of an organization's ISMS, risks associated with an organization's information assets need to be addressed. Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the organization.

The adoption of an ISMS is expected to be a strategic decision for an organization and it is necessary that this decision is seamlessly integrated, scaled and updated in accordance with the needs of the organization.

The design and implementation of an organization's ISMS is influenced by the needs and objectives of the organization, security requirements, the business processes employed and the size and structure of the organization. The design and operation of an ISMS needs to reflect the interests and information security requirements of all of the organization's stakeholders including customers, suppliers, business partners, shareholders and other relevant third parties.

# *SECURING IT NETWORKS WITH ISMS FAMILY OF STANDARDS (ISO 27000 SERIES)*

In an interconnected world, information and related processes, systems, and networks constitute critical business assets. Organizations and their information systems and networks face security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire and flood. Damage to information systems and networks caused by malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

An ISMS is important to both public and private sector businesses. In any industry, an ISMS is an enabler that supports e-business and is essential for risk management activities. The interconnection of public and private networks and the sharing of information assets increases the difficulty of controlling access to and handling of information. In addition, the distribution of mobile storage devices containing information assets can weaken the effectiveness of traditional controls. When organizations adopt the ISMS family of standards the ability to apply consistent and mutually-recognisable information security principles can be demonstrated to business partners and other interested parties.

Information security is not always taken into account in the design and development of information systems. Further, information security is often thought of as being a technical solution. However, the security that can be achieved through technical means is limited, and may be ineffective without being supported by appropriate management and procedures within the context of an ISMS. Integrating security into an information system after the fact could be cumbersome and costly. An ISMS involves identifying which controls are in place and requires careful planning and attention to detail. As an example, access controls, which may be technical (logical), physical, administrative (managerial) or a combination, provide a means to ensure that access to information assets is authorized and restricted based on the business and security requirements.

The successful adoption of an ISMS is important to protect information assets allowing an organization to:

a) achieve greater assurance that its information assets are adequately protected against information security risks on a continual basis;
b) maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness;
c) continually improve its control environment; and
d) effectively achieve legal and regulatory compliance.

## References:


[1] http://www.iso27001security.com
[2] http://standards.iso.org
[3] http://www.noticebored.com/html/policy_manual.html
[4] http://en.wikipedia.org/wiki/ISO/IEC_27001
[5] http://blog.iso27001standard.com/tag/annex-a/
[6] Alan Calder, Steve Watkins - ***IT Governance: an international guide to data security and ISO27001/ISO27002***, Kogan Page, 2012, ISBN 978-0-7494-6485-1
[7] Edward Humphreys - ***Information Security Risk Management: Handbook for ISO/IEC 27001,*** BSI (London), 2010, ISBN: 978-0-580-60745-5
[8] Edward Humphreys - ***ISO/IEC 27001 for Small Businesses: Practical Advice***, ISO/IEC, 2010, ISBN: 978-92-67-10517-8