PECB

When Recognition Matters

WHITEPAPER

ISO/IEC 27002:2013

INFORMATION TECHNOLOGY - SECURITY TECHNIQUES
CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

CONTENT

PRINCIPAL AUTHORS
Eric LACHAPELLE, PECB
Mustafë BISLIMI, PECB

EDITORS:
Anders CARLSTEDT, Parabellum Cyber Security
Rreze HALILI, PECB

Published on February 26, 2016

INTRODUCTION

The Information Security standard ISO/IEC 27002:2013 is the "Code of Practice for Information Security Controls". First it was published by the International Organization for Standardization (ISO) and by the International Electro Technical Commission (IEC) in December 2000 as ISO 17799. Today, ISO/IEC 27002 is part of the ISO27XXX series. The document provides best practice recommendations and guidance for organizations selecting and implementing information security controls within the process of initiating, implementing and maintaining an Information Security Management System (ISMS).

The establishment and implementation of an ISMS depends on a strategic orientation of the organization and is influenced by a number of aspects including its needs, objectives, security requirements, the organizational processes used, the size and the structure of the organization.

An ISMS such as specified in ISO/IEC 27001 is an integrated part of organization's processes and overall management structure, with the main objective to ensure the necessary levels of confidentiality, integrity and availability of information. This objective is achieved by applying a supporting risk management process within the ISMS and by implementing a suite of information security controls as part of the risk treatment under the overall framework of a coherent management system.

The normative requirements of ISMS are addressed in clauses 4 to 11 of 27001:2013 that define the ISMS. Furthermore, organizations need to consider the set of 144 controls which are found in Annex A of the same standard.

In ISO/IEC 27002, you will find more detailed guidance on the application of the controls of Annex A including areas such as policies, processes, procedures, organizational structures and software and hardware functions. All these information security controls may need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific established security and business objectives of the organization are met.

ISO/IEC 27002 provides general guidance on the controls of ISO 27001, and should be combined and used with other standards of the information security management system family of standards, including ISO/IEC 27003 (implementation), ISO/IEC 27004 (measurement), and ISO/IEC 27005 (risk management).

Information and the need for its security

The importance of information security and emerging threats has changed dramatically in the last eight years. Everyday information is being collected, processed, stored and transmitted in many forms including electronic, physical and verbal formats, within all types of organizations. All this is accomplished by using a huge range of devices, systems and services including smartphones, tablets personal computers, servers, workstations, personal digital assistants, telecommunication network systems, industrial/process control systems, environmental control systems, etc. Therefore, organizations are trying to achieve their missions, objectives and business functions in a very complex atmosphere.

Information systems and the services they provide allow competitive advantages to organizations, however, now it is a known fact that same platforms and solutions have become subjects to serious threats where the ultimate consequences might include losing functions, or affecting image or reputation of the organization.

Information Security

Preservation of confidentiality, integrity and availability of information

To efficiently negotiate these complex issues, it is very important that leaders and managers at all levels go beyond understanding and thinking about information system. They have to acknowledge and accept their responsibilities and understand that they are held accountable for ensuring information security. ISO 27001 has been published to provide requirements for establishing, implementing, maintaining and continually improving information security levels against identified needs by means of an information security management system. This international standard defines the requirements regarding policy, roles, definitions, responsibilities and authorities of participants connected with information security. Furthermore, it requires processes, procedures and organizational structures that will prevent, detect, and respond to different types of threats. This management system typically preserves the confidentiality, integrity and availability of information by applying a risk management process, and gives confidence to interested parties that risks are adequately managed.

For each identified threat and vulnerability, from which will result a risk scenario, ISO/IEC 27002 may help to provide guidelines for controls that should be considered to identify, asses, evaluate, reduce and mitigate risk. This information security standard can be used to select information security controls, to improve security practices and to develop security guidelines and standards. It gives information security responsibilities, precise explanation of control objectives, and detailed guideline on how to implement these controls.

An overview of ISO/IEC 27002:2013

ISO/IEC 27002 applies to all types and sizes of organizations, including public and private sectors, commercial and non-profit that collect, process, store and transmit information in many forms including electronic, physical and verbal.

This standard should be used as a reference for the consideration of controls within the process of implementing an Information Security Management System based on ISO/IEC 27001, it implements commonly accepted information security controls, and develops the organization's own information security management guidelines.

What is Information Security Control?

Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks related to personal property, or computer software.

The standard contains 14 security control clauses, collectively containing a total of 35 main security categories and 114 controls.

In each section of the ISO/IEC 27002 standard, there is a security control category that contains:

- a control objective stating what is to be achieved;
- one or more controls that can be applied to achieve the control objective;
- implementation guidance and any other pertinent information useful for understanding the controls and implementation process.

The order of the clauses in this standard does not relate to their criticality or importance.

Relation between 27002 and 27001 and other standards

Each standard from ISO/IEC 27000 series is designed with a certain focus: if you want to create the foundations of information security in your organization, and devise its framework, you should use ISO/IEC 27001; whereas if you want to focus on the implementation controls, you should use ISO/IEC 27002, or to improve information security risk management, then use ISO/IEC 27005, etc.

Information Security Management Systems

Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

Without the normative requirements and management framework approach of ISO/IEC 27001, and the supporting Annex A, ISO/IEC 27002 could be considered just another best practice control matrix for information security. With this link however, ISO/IEC 27002 may very well be regarded as de facto the most important individual document proving guidance on information security controls.

So, by implementing ISO/IEC 27001 correctly, an organization will have management system that will assist in efficiently planning, implementing, monitoring, reviewing and improving information security in scope. On the other hand, ISO/IEC 27002 can assist to implement and maintain controls to achieve objectives for all requirements as required by ISO/IEC 27001. For every risk situation identified in ISO 27001, ISO/IEC 27002 will give a set of controls how to decrease the risks and how to maintain it in an accepted level.

There are other well-known standards which are related to ISO/IEC 27002:

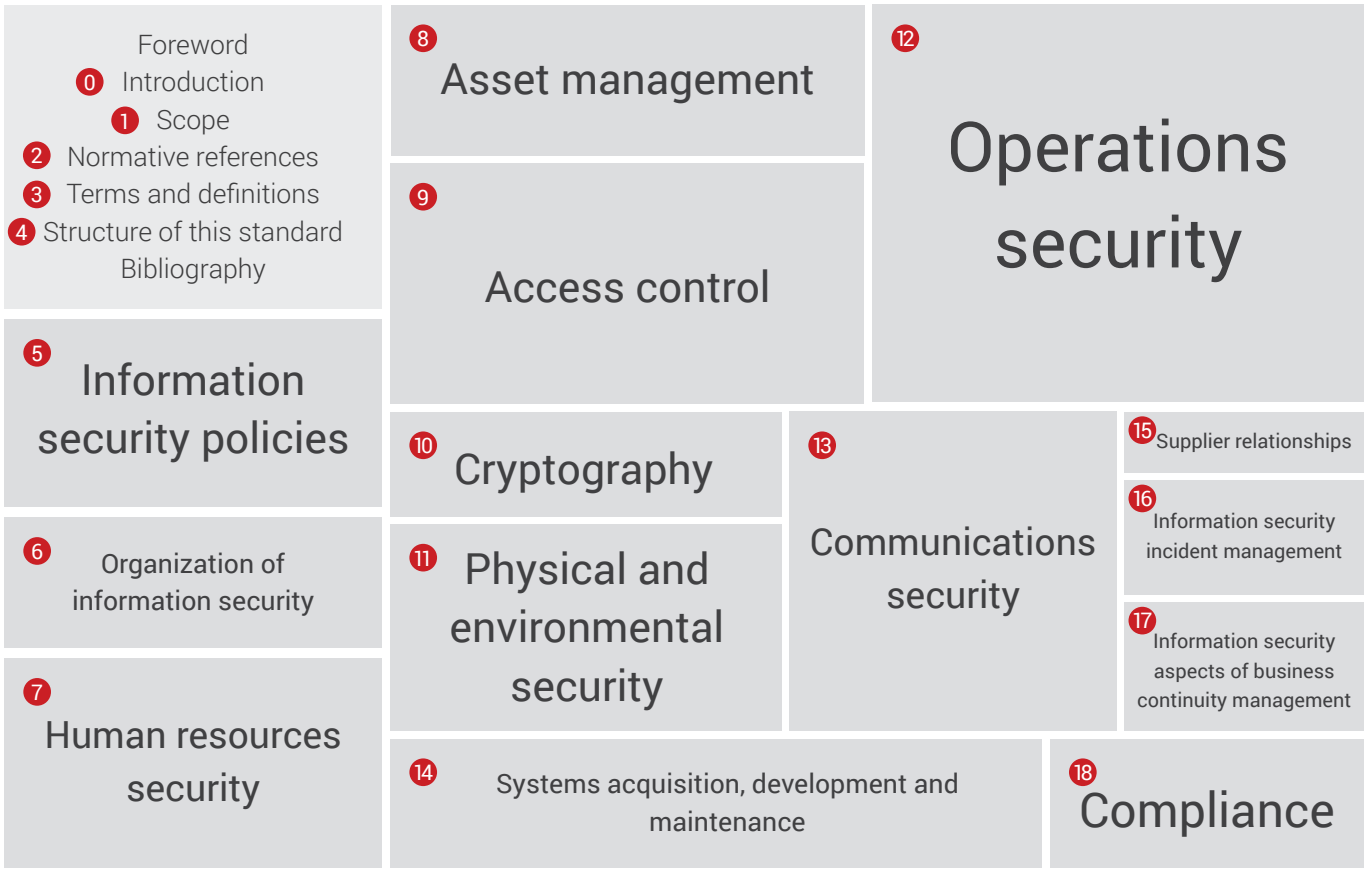
- OECD Principles (2002)
- PCI-DSS - Payment Card Industry Data Security Standard (2004)
- Basel II (2004)
- COBIT – Control Objectives for Business and related Technology (1994+)
- ITIL – Information Technology Infrastructure Library (1980+)

Key clauses of ISO/IEC 27002:2013

ISO/IEC 27002 is organized into the following main clauses:

The standard contains 14 security control clauses, collectively containing a total of 35 main security categories and 114 controls.

- Clause 5: Information Security Policies
- Clause 6: Organization of Information Security
- Clause 7: Human Resource Security
- Clause 8: Asset Management
- Clause 9: Access Control
- Clause 10: Cryptography
- Clause 11: Physical and Environmental Security
- Clause 12: Operations Security
- Clause 13: Communication Security
- Clause 14: System Acquisition, Development and Maintenance
- Clause 15: Supplier Relationships
- Clause 16: Information Security Incident Management
- Clause 17: Information Security Aspects of Business Continuity Management
- Clause 18: Compliance



Each of the objectives, and the required controls, are listed and described below.

Clause 5: Information Security Policies

Objectives:

- To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

The Information Security Policies clause addresses the need to define, publish and review different types of policies required for information security management

Clause 6: Organization of Information Security

Objectives:

- To establish a management framework, to initiate and control the implementation and operation of information security within the organization.
- To ensure the security of teleworking and use of mobile devices.

The Organization of Information Security clause addresses the need to define and allocate the necessary roles and responsibilities for information security management processes and activities. This includes controls related to the definition of information security roles and responsibilities, segregation of duties, contact with authorities, contact with special interest groups, information security in project management and mobile devices and teleworking.

Clause 7: Human Resource Security

Objectives:

- To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
- To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
- To protect the organization's interests as part of the process of changing or terminating employment.

The Human Resource Security clause addresses the required controls for processes related to staff recruiting, their job during employment and after the termination of their contracts. These considerations should include information security coordination, allocation of information security responsibilities, authorization processes for information processing facilities, confidentiality agreements, contact with authorities, contact with special interest groups, independent review of information security, identification of risks related to external parties, addressing security when dealing with customers, addressing security on contractors' agreements, etc.

Clause 8: Asset Management

Objectives:

- To identify organizational assets and define appropriate protection responsibilities.
- To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
- To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

The Asset Management clause addresses the required responsibilities to be defined and allocated for the asset management processes and procedures.

The owner of the assets and other parts involved in this matter should be identified to be held accountable for assets' security, including classification, labelling, and handling of information; and information processing facilities should be identified and maintained. Moreover, this clause addresses controls on management of removable media, disposal of media, and physical media transfer.

Clause 9: Access Control

Objectives:

- To limit access to information and information processing facilities.
- To ensure authorized user access and to prevent unauthorized access to systems and services.

- To make users accountable for safeguarding their authentication information.
- To prevent unauthorized access to systems and applications.

The Access controls clause addresses requirements to control access to information assets and information processing facilities. The controls are focused on the protection against accidental damage or loss, overheating, threats, etc.

This requires a documented control policy and procedures, registration, removal and review of user access rights, including here physical access, network access and the control over privileged utilities and restriction of access to program source code.

Clause 10: Cryptography

Objectives:

- To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

The Cryptography clause addresses policies on cryptographic controls for protection of information to ensure proper and effective use of cryptography in order to protect the confidentiality, authenticity, integrity, non-repudiation and authentication of the information. It also includes the need for digital signatures and message authentication codes, and cryptographic key management.

Clause 11: Physical and Environmental Security

Objectives:

- To prevent unauthorized physical access, damage and interference to the organization's
- information and information processing facilities.
- To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

The Physical and Environmental Security clause addresses the need to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

Controls cover: to physically secure the perimeter of office rooms and facilities, protection against external and environmental threats, prevent loss, damage, theft or compromise of assets, protect the equipment from power failures, cabling should be protected from interception or damage, maintenance of equipment, etc.

Clause 12: Operations Security

Objectives:

- To ensure correct and secure operations of information processing facilities.
- To ensure that information and information processing facilities are protected against malware.
- To protect against loss of data.
- To record events and generate evidence.
- To ensure the integrity of operational systems.
- To prevent exploitation of technical vulnerabilities.
- To minimize the impact of audit activities on operational systems.

The Operations security clause addresses the organization's ability to ensure correct and secure operations. The controls cover the need for operational procedures and responsibilities, protection from malware, backup, logging and monitoring, control of operational software, technical vulnerability management, information systems audit considerations.

Clause 13: Communication Security

Objectives:

- To ensure the protection of information in networks and its supporting information processing facilities.
- To maintain the security of information transferred within an organization and with any external entity.

The Communication Security clause addresses the organization's ability to ensure protection of information in systems and applications in networks and its supporting information processing facilities. Controls cover security of information in networks and connected services from unauthorized access, transfer policies and procedures, secure transfer of business information between the organization and external parties, information involved in electronic messaging, the need for confidentiality or non-disclosure agreements.

Clause 14: System Acquisition, Development and Maintenance

Objectives:

- To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.
- To ensure that information security is designed and implemented within the development lifecycle of information systems.
- To ensure the protection of data used for testing.

The System Acquisition, Development and Maintenance clause covers controls for identification, analyses and specification of information security requirements, securing application services in development and support processes, technical review restrictions on changes to software packages, secure system engineering principles, secure development environment, outsourced development, system security testing, system acceptance testing and protection of test data.

Clause 15: Supplier Relationships

Objectives:

- To ensure protection of the organization's assets that is accessible by suppliers.
- To maintain an agreed level of information security and service delivery in line with supplier agreements.

The Supplier Relationships clause addresses controls for supplier's relationship issues, including here information security policies and procedures, addressing security within supplier agreements, communication and awareness about technology supply chain and service delivery management.

Clause 16: Information Security Incident Management

Objective:

- To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

The Information Security Incident Management clause covers controls for responsibilities and procedures, reporting information and security weaknesses, assessment of and decision on information security events, response to information security incidents, learning from information security incidents, and collection of evidence.

Clause 17: Information Security Aspects of Business Continuity Management

Objectives:

- Information security continuity should be embedded in the organization's business continuity management systems.
- To ensure availability of information processing facilities.

The Business Continuity Management clause addresses the organization's ability to counteract interruptions to normal operations, including availability of information processing facilities, verify, review and evaluate information security continuity, implementing information security continuity, and planning information security continuity.

Clause 18: Compliance

Objectives:

- To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.
- To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

The Compliance clause addresses the organization's ability to remain in compliance with regulatory, statutory, contractual, and security requirements, including: identification of applicable legislation and contractual requirements, intellectual property rights, protection of records, privacy and protection of personally identifiable information, regulation of cryptographic controls, independent review of information security, compliance with security policies and standards, and technical compliance review.

Code of Practice for Information Security Controls The Business Benefits

Benefits from ISO/IEC 27002 are applicable to organizations of all sizes and all security maturity levels. It offers flexible set of controls to be used in the way an organization wants to protect itself (either stand-alone, with ISO/IEC 27001 or other methodologies), and reflects the new threats an organization faces.

The point of ISO/IEC 27002 is to prepare and/or improve the security framework that controls the compliance initiatives, security controls, and future information security plans. Employees enjoy a more reliable data access environment, with fewer work interruptions and far less frustration.

Today, good information security controls are not about being forced into taking action to address external pressures, but about recognizing the positive value of Information Security Controls good practice being embedded throughout your organization.

Predictable and effective response to information security assets	Protection of people	Maintenance of vital activities of the organization	Better understanding of the organization
Cost reduction	Respect of the interested parties	Protection of the reputation and brand	Confidence of clients
Competitive advantage	Legal compliance	Regulatory compliance	Contract compliance

The adoption of an effective information security controls process within an organization will have benefits in a number of areas, examples of which include:

1. Providing a framework for resolving security issues
2. Enhancing client confidence & perception of your organization
3. Enhancing business partners' confidence & perception of your organization
4. Enhancing security awareness within an organization
5. A defined process for implementation, management, maintenance and ISMS evaluation
6. Compliance advantages for participation in Global business opportunities

Why is PECB a Worthy Choice?

Professional Evaluation and Certification Board (PECB) is a certification body for persons and management systems on a wide range of professional standards. It offers ISO 27001, ISO 27005, ISO 29100 and ISO/IEC 27002 training and certification services for professionals wanting to support organizations on the implementation of these management systems.

PECB offers ISO/IEC 27002 trainings on how to implement information security controls and information security management practices.

This, above all, is intended to help reduce information security risks, by initiating, implementing, maintaining, and improving information security management within an organization by using potential controls and control mechanisms which can be found within PECB Certified ISO/IEC 27001 training courses.

ISO Standards and Professional Trainings offered by PECB:

- PECB Certified ISO/IEC 27002 Introduction
- PECB Certified ISO/IEC 27002 Foundation
- PECB Certified ISO/IEC 27002 Manager
- PECB Certified ISO/IEC 27002 Lead Manager

Various professions may apply for this certification:

- Managers or consultants wanting to implement an Information Security Management System (ISMS)
- Project managers or consultants wanting to master the Information Security Management System implementation process
- Persons responsible for the information security or conformity in an organization
- Members of information security teams
- Expert advisors in information technology
- Technical experts wanting to prepare for an Information Security Audit function

For further details relating the types of trainings and certifications that PECB offers, please visit our website: www.pecb.com.

PECB

+1-844-426-7322

customer@pecb.com

Customer Service