SLOVENSKI STANDARD

oSIST prEN ISO/IEC 27002:2016

01-december-2016

Informacijska tehnologija - Varnostne tehnike - Pravila obnašanja pri kontrolah informacijske varnosti (ISO/IEC 27002:2013)

Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013)

Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013)

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information (ISO/IEC 27002:2013)

Ta slovenski standard je istoveten z: prEN ISO/IEC 27002

ICS:

03.100.70	Sistemi vodenja	Management systems
35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 27002:2016 en,fr,de

INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

Information technology — Security techniques — Code of practice for information security controls

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Reference number
ISO/IEC 27002:2013(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**

0 Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Structure of this standard **1**
4.1 Clauses 1
4.2 Control categories 1

5 Information security policies **2**
5.1 Management direction for information security 2

6 Organization of information security **4**
6.1 Internal organization 4
6.2 Mobile devices and teleworking 6

7 Human resource security **9**
7.1 Prior to employment 9
7.2 During employment 10
7.3 Termination and change of employment 13

8 Asset management **13**
8.1 Responsibility for assets 13
8.2 Information classification 15
8.3 Media handling 17

9 Access control **19**
9.1 Business requirements of access control 19
9.2 User access management 21
9.3 User responsibilities 24
9.4 System and application access control 25

10 Cryptography **28**
10.1 Cryptographic controls 28

11 Physical and environmental security **30**
11.1 Secure areas 30
11.2 Equipment 33

12 Operations security **38**
12.1 Operational procedures and responsibilities 38
12.2 Protection from malware 41
12.3 Backup 42
12.4 Logging and monitoring 43
12.5 Control of operational software 45
12.6 Technical vulnerability management 46
12.7 Information systems audit considerations 48

13 Communications security **49**
13.1 Network security management 49
13.2 Information transfer 50

14 System acquisition, development and maintenance **54**
14.1 Security requirements of information systems 54
14.2 Security in development and support processes 57
14.3 Test data 62

15 Supplier relationships **62**
15.1 Information security in supplier relationships 62

15.2 Supplier service delivery management 66
16 Information security incident management 67
16.1 Management of information security incidents and improvements 67
17 Information security aspects of business continuity management 71
17.1 Information security continuity 71
17.2 Redundancies 73
18 Compliance 74
18.1 Compliance with legal and contractual requirements 74
18.2 Information security reviews 77
Bibliography 79

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

ISO/IEC 27002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

This second edition cancels and replaces the first edition (ISO/IEC 27002:2005), which has been technically and structurally revised.

0 Introduction

0.1 Background and context

This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).

Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. An ISMS such as that specified in ISO/IEC 27001[10] takes a holistic, coordinated view of the organization's information security risks in order to implement a comprehensive suite of information security controls under the overall framework of a coherent management system.

Many information systems have not been designed to be secure in the sense of ISO/IEC 27001[10] and this standard. The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.

In a more general sense, effective information security also assures management and other stakeholders that the organization's assets are reasonably safe and protected against harm, thereby acting as a business enabler.

0.2 Information security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements:

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;

b) the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;

c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

ISO/IEC 27005[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

0.3 Selecting controls

Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate.

The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations. Control selection also depends on the manner in which controls interact to provide defence in depth.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. The controls are explained in more detail below along with implementation guidance. More information about selecting controls and other risk treatment options can be found in ISO/IEC 27005.[11]

0.4 Developing your own guidelines

This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

0.5 Lifecycle considerations

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a company's financial accounts is far less significant after they have been formally published) but information security remains important to some extent at all stages.

Information systems have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be taken into account at every stage. New system developments and changes to existing systems present opportunities for organizations to update and improve security controls, taking actual incidents and current and projected information security risks into account.

0.6 Related standards

While this standard offers guidance on a broad range of information security controls that are commonly applied in many different organizations, the remaining standards in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMSs and the family of standards. ISO/IEC 27000 provides a glossary, formally defining most of the terms used throughout the ISO/IEC 27000 family of standards, and describes the scope and objectives for each member of the family.

Information technology — Security techniques — Code of practice for information security controls

1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;[10]

b) implement commonly accepted information security controls;

c) develop their own information security management guidelines.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4 Structure of this standard

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

4.1 Clauses

Each clause defining security controls contains one or more main security categories.

The order of the clauses in this standard does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important, therefore each organization applying this standard should identify applicable controls, how important these are and their application to individual business processes. Furthermore, lists in this standard are not in priority order.

4.2 Control categories

Each main security control category contains:

a) a control objective stating what is to be achieved;

b) one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

Control

Defines the specific control statement, to satisfy the control objective.

Implementation guidance

Provides more detailed information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the organization's specific control requirements. .

Other information

Provides further information that may need to be considered, for example legal considerations and references to other standards. If there is no other information to be provided this part is not shown.

5 Information security policies

5.1 Management direction for information security

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

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

a) business strategy;

b) regulations, legislation and contracts;

c) the current and projected information security threat environment.

The information security policy should contain statements concerning:

a) definition of information security, objectives and principles to guide all activities relating to information security;

b) assignment of general and specific responsibilities for information security management to defined roles;

c) processes for handling deviations and exceptions.

At a lower level, the information security policy should be supported by topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics.

Examples of such policy topics include:

a) access control (see Clause 9);

b) information classification (and handling) (see 8.2);

c) physical and environmental security (see Clause 11);

d) end user oriented topics such as:

   1) acceptable use of assets (see 8.1.3);

   2) clear desk and clear screen (see 11.2.9);

   3) information transfer (see 13.2.1);

   4) mobile devices and teleworking (see 6.2);

   5) restrictions on software installations and use (see 12.6.2);

e) backup (see 12.3);

f) information transfer (see 13.2);

g) protection from malware (see 12.2);

h) management of technical vulnerabilities (see 12.6.1);

i) cryptographic controls (see Clause 10);

j) communications security (see Clause 13);

k) privacy and protection of personally identifiable information (see 18.1.4);

l) supplier relationships (see Clause 15).

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme" (see 7.2.2).

Other information

The need for internal policies for information security varies across organizations. Internal policies are especially useful in larger and more complex organizations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organization. Policies for information security can be issued in a single "information security policy" document or as a set of individual but related documents.

If any of the information security policies are distributed outside the organization, care should be taken not to disclose confidential information.

Some organizations use other terms for these policy documents, such as "Standards", "Directives" or "Rules".

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

The review of policies for information security should take the results of management reviews into account.

Management approval for a revised policy should be obtained.

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

Control

All information security responsibilities should be defined and allocated.

Implementation guidance

Allocation of information security responsibilities should be done in accordance with the information security policies (see 5.1.1). Responsibilities for the protection of individual assets and for carrying out specific information security processes should be identified. Responsibilities for information security risk management activities and in particular for acceptance of residual risks should be defined. These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Local responsibilities for the protection of assets and for carrying out specific security processes should be defined.

Individuals with allocated information security responsibilities may delegate security tasks to others. Nevertheless they remain accountable and should determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible should be stated. In particular the following should take place:

a) the assets and information security processes should be identified and defined;

b) the entity responsible for each asset or information security process should be assigned and the details of this responsibility should be documented (see 8.1.2);

c) authorization levels should be defined and documented;

d) to be able to fulfil responsibilities in the information security area the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments;

e) coordination and oversight of information security aspects of supplier relationships should be identified and documented.

Other information

Many organizations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the identification of controls.

However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Implementation guidance

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

Other information

Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.

6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities should be maintained.

Implementation guidance

Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner (e.g. if it is suspected that laws may have been broken).

Other information

Organizations under attack from the Internet may need authorities to take action against the attack source.

Maintaining such contacts may be a requirement to support information security incident management (see Clause 16) or the business continuity and contingency planning process (see Clause 17). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in laws or regulations, which have to be implemented by the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment).

6.1.4 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

Implementation guidance

Membership in special interest groups or forums should be considered as a means to:

a) improve knowledge about best practices and stay up to date with relevant security information;

b) ensure the understanding of the information security environment is current and complete;

c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;

d) gain access to specialist information security advice;