

**INFOTEHNOLOOGIA. TURBEMEETODID.  
INFOTURBEMEETODITE TAVAKOODEKS**

**Information technology - Security techniques - Code of  
practice for information security controls (ISO/IEC  
27002:2013 including Cor 1:2014 and Cor 2:2015)**

**EESTI STANDARDI EESSÕNA****NATIONAL FOREWORD**

See Eesti standard EVS-EN ISO/IEC 27002:2017 sisaldab Euroopa standardi EN ISO/IEC 27002:2017 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 27002:2017 consists of the English text of the European standard EN ISO/IEC 27002:2017.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 22.02.2017.	Date of Availability of the European standard is 22.02.2017.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile [standardiosakond@evs.ee](mailto:standardiosakond@evs.ee).

ICS 03.100.70, 35.030

**Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele**

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:  
Koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto:info@evs.ee)

**The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation**

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

English Version

Information technology - Security techniques - Code of  
practice for information security controls (ISO/IEC  
27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information - Techniques de sécurité  
- Code de bonne pratique pour le management de la  
sécurité de l'information (ISO/IEC 27002:2013 y  
compris Cor 1:2014 et Cor 2:2015)

Informationstechnik - Sicherheitsverfahren - Leitfaden  
für Informationssicherheitsmaßnahmen (ISO/IEC  
27002:2013 einschließlich Cor 1:2014 und Cor 2:2015)

This European Standard was approved by CEN on 26 January 2017.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

## European foreword

The text of ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015 has been prepared by Technical Committee ISO/IEC JTC 1 “Information technology” of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27002:2017.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2017, and conflicting national standards shall be withdrawn at the latest by August 2017.

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

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

### Endorsement notice

The text of ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015 has been approved by CEN as EN ISO/IEC 27002:2017 without any modification.

# Contents

Page

<b>Foreword</b>	<b>v</b>
<b>0 Introduction</b>	<b>vi</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Structure of this standard</b>	<b>1</b>
4.1 Clauses	1
4.2 Control categories	1
<b>5 Information security policies</b>	<b>2</b>
5.1 Management direction for information security	2
<b>6 Organization of information security</b>	<b>4</b>
6.1 Internal organization	4
6.2 Mobile devices and teleworking	6
<b>7 Human resource security</b>	<b>9</b>
7.1 Prior to employment	9
7.2 During employment	10
7.3 Termination and change of employment	13
<b>8 Asset management</b>	<b>13</b>
8.1 Responsibility for assets	13
8.2 Information classification	15
8.3 Media handling	17
<b>9 Access control</b>	<b>19</b>
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
<b>10 Cryptography</b>	<b>28</b>
10.1 Cryptographic controls	28
<b>11 Physical and environmental security</b>	<b>30</b>
11.1 Secure areas	30
11.2 Equipment	33
<b>12 Operations security</b>	<b>38</b>
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
<b>13 Communications security</b>	<b>49</b>
13.1 Network security management	49
13.2 Information transfer	50
<b>14 System acquisition, development and maintenance</b>	<b>54</b>
14.1 Security requirements of information systems	54
14.2 Security in development and support processes	57
14.3 Test data	62
<b>15 Supplier relationships</b>	<b>62</b>
15.1 Information security in supplier relationships	62

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

## 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<sup>[11]</sup> 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.<sup>[11]</sup>

### **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;<sup>[10]</sup>
- 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.