

Information technology - Security techniques - Storage security (ISO/IEC 27040:2015)

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 27040:2016 sisaldab Euroopa standardi EN ISO/IEC 27040:2016 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 27040:2016 consists of the English text of the European standard EN ISO/IEC 27040:2016.
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 24.08.2016.	Date of Availability of the European standard is 24.08.2016.
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 35.040

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:

Aru 10, 10317 Tallinn, Eesti; 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:

Aru 10, 10317 Tallinn, Estonia; 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 - Storage  
security (ISO/IEC 27040:2015)

Technologie de l'information - Techniques de sécurité -  
Sécurité de stockage (ISO/IEC 27040:2015)

Informationstechnik - IT-Sicherheitsverfahren -  
Speichersicherheit (ISO/IEC 27040:2015)

This European Standard was approved by CEN on 19 June 2016.

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, 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 27040:2015 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 27040:2016.

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 February 2017, and conflicting national standards shall be withdrawn at the latest by February 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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

### Endorsement notice

The text of ISO/IEC 27040:2015 has been approved by CEN as EN ISO/IEC 27040:2016 without any modification.

# Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>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 Symbols and abbreviated terms</b> .....	<b>7</b>
<b>5 Overview and concepts</b> .....	<b>11</b>
5.1 General.....	11
5.2 Storage concepts.....	12
5.3 Introduction to storage security.....	12
5.4 Storage security risks.....	14
5.4.1 Background.....	14
5.4.2 Data breaches.....	15
5.4.3 Data corruption or destruction.....	16
5.4.4 Temporary or permanent loss of access/availability.....	16
5.4.5 Failure to meet statutory, regulatory, or legal requirements.....	17
<b>6 Supporting controls</b> .....	<b>17</b>
6.1 General.....	17
6.2 Direct Attached Storage (DAS).....	17
6.3 Storage networking.....	18
6.3.1 Background.....	18
6.3.2 Storage Area Networks (SAN).....	18
6.3.3 Network Attached Storage (NAS).....	23
6.4 Storage management.....	24
6.4.1 Background.....	24
6.4.2 Authentication and authorization.....	26
6.4.3 Secure the management interfaces.....	27
6.4.4 Security auditing, accounting, and monitoring.....	28
6.4.5 System hardening.....	30
6.5 Block-based storage.....	31
6.5.1 Fibre Channel (FC) storage.....	31
6.5.2 IP storage.....	31
6.6 File-based storage.....	32
6.6.1 NFS-based NAS.....	32
6.6.2 SMB/CIFS-based NAS.....	33
6.6.3 Parallel NFS-based NAS.....	33
6.7 Object-based storage.....	34
6.7.1 Cloud computing storage.....	34
6.7.2 Object-based Storage Device (OSD).....	35
6.7.3 Content Addressable Storage (CAS).....	36
6.8 Storage security services.....	37
6.8.1 Data sanitization.....	37
6.8.2 Data confidentiality.....	40
6.8.3 Data reductions.....	42

<b>7</b>	<b>Guidelines for the design and implementation of storage security</b>	<b>43</b>
7.1	General	43
7.2	Storage security design principles	43
7.2.1	Defence in depth	43
7.2.2	Security domains	44
7.2.3	Design resilience	45
7.2.4	Secure initialization	45
7.3	Data reliability, availability, and resilience	45
7.3.1	Reliability	45
7.3.2	Availability	46
7.3.3	Backups and replication	46
7.3.4	Disaster Recovery and Business Continuity	47
7.3.5	Resilience	48
7.4	Data retention	48
7.4.1	Long-term retention	48
7.4.2	Short to medium-term retention	49
7.5	Data confidentiality and integrity	50
7.6	Virtualization	52
7.6.1	Storage virtualization	52
7.6.2	Storage for virtualized systems	53
7.7	Design and implementation considerations	54
7.7.1	Encryption and key management issues	54
7.7.2	Align storage and policy	55
7.7.3	Compliance	55
7.7.4	Secure multi-tenancy	56
7.7.5	Secure autonomous data movement	57
<b>Annex A</b>	<b>(normative) Media sanitization</b>	<b>60</b>
<b>Annex B</b>	<b>(informative) Selecting appropriate storage security controls</b>	<b>75</b>
<b>Annex C</b>	<b>(informative) Important security concepts</b>	<b>96</b>
<b>Bibliography</b>		<b>109</b>

## Introduction

Many organizations face the challenge of implementing data protection and security measures to meet a wide range of requirements, including statutory and regulatory compliance. Too often the security associated with storage systems and infrastructure has been missed because of misconceptions and limited familiarity with the storage technology, or in the case of storage managers and administrators, a limited understanding of the inherent risks or basic security concepts. The net result of this situation is that digital assets are needlessly placed at risk of compromise due to data breaches, intentional corruption, being held hostage, or other malicious events.

Data storage has matured in an environment where security has been a secondary concern due to its historical reliance on isolated connectivity, specialized technologies, and the physical security of data centres. Even as storage connectivity evolved to use technologies such as storage protocols over Transmission Control Protocol/Internet Protocol (TCP/IP), few users took advantage of either the inherent security mechanisms or the recommended security measures.

This International Standard provides guidelines for storage security in an organization, supporting in particular the requirements of an Information Security Management System (ISMS) according to ISO/IEC 27001. This International Standard recommends the information security risk management approach as defined in ISO/IEC 27005. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS.

This International Standard is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.

The objectives for this International Standard are the following:

- help draw attention to the risks;
- assist organizations in better securing their data when stored;
- provide a basis for auditing, designing, and reviewing storage security controls.

It is emphasized that ISO/IEC 27040 provides further detailed implementation guidance on the storage security controls that are described at a basic standardized level in ISO/IEC 27002.

It should be noted that this International Standard is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

# Information technology — Security techniques — Storage security

## 1 Scope

This International Standard provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.

Storage security is relevant to anyone involved in owning, operating, or using data storage devices, media, and networks. This includes senior managers, acquirers of storage product and service, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security or storage security, storage operation, or who are responsible for an organization's overall security program and security policy development. It is also relevant to anyone involved in the planning, design, and implementation of the architectural aspects of storage network security.

This International Standard provides an overview of storage security concepts and related definitions. It includes guidance on the threat, design, and control aspects associated with typical storage scenarios and storage technology areas. In addition, it provides references to other International Standards and technical reports that address existing practices and techniques that can be applied to storage security.

## 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.

ITU-TY.3500 | ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

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

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27005, and the following apply.

### 3.1

#### block

unit in which data is *stored* (3.50) and retrieved on disk and tape *devices* (3.14)