
**Information technology — Security
techniques — Storage security**

*Technologie de l'information — Techniques de sécurité — Sécurité de
stockage*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 |
| Introduction | vi |
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 3 Terms and definitions | 1 |
| 4 Symbols and abbreviated terms | 7 |
| 5 Overview and concepts | 11 |
| 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 |
| 6 Supporting controls | 17 |
| 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 |

| | | |
|----------|--|------------|
| 7 | Guidelines for the design and implementation of storage security | 43 |
| 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 |
| | Annex A (normative) Media sanitization | 60 |
| | Annex B (informative) Selecting appropriate storage security controls | 75 |
| | Annex C (informative) Important security concepts | 96 |
| | Bibliography | 109 |

This is a free 10 page sample. Access the full version online.

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology, SC 27, Security techniques*.

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)

3.2 clear

sanitize (3.38) using logical techniques on data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user

3.3 compression

process of removing redundancies in digital data to reduce the amount that should be *stored* (3.50) or transmitted

[SOURCE: ISO/TR 12033:2009, 3.1]

Note 1 to entry: For *storage* (3.43), lossless compression (i.e., compression using a technique that preserves the entire content of the original data, and from which the original data can be reconstructed exactly) is required.

3.4 cryptographic erase

method of *sanitization* (3.37) in which the encryption key for the encrypted *target data* (3.52) is *sanitized* (3.38), making recovery of the decrypted *target data* (3.52) infeasible

3.5 cryptoperiod

defined period of time during which a specific cryptographic key is authorized for use, or during which time the cryptographic keys in a given system can remain in effect

[SOURCE: ISO 16609:2004, 3.9]

3.6 data at rest

data *stored* (3.50) on stable *non-volatile storage* (3.30)

3.7 data breach

compromise of security that leads to the accidental or unlawful *destruction* (3.13), loss, alteration, unauthorized disclosure of, or access to protected data transmitted, *stored* (3.50), or otherwise processed

3.8 data in motion

data being transferred from one location to another

Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e., never exposed to outside of an interface, chip, or device).

3.9 data integrity

property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, 3.3.21]

3.10 deduplication

method of reducing *storage* (3.43) needs by eliminating redundant data, which is replaced with a pointer to the unique data copy

Note 1 to entry: Deduplication is sometimes considered a form of *compression* (3.3).

3.11 degauss

render data unreadable by applying a strong magnetic field to the media

3.12**destruct**

sanitize (3.38) using physical techniques that make recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for *storage* (3.43) of data

Note 1 to entry: *Disintegrate* (3.15), *incinerate* (3.21), *melt* (3.25), *pulverize* (3.34), and *shred* (3.41) are destruct forms of *sanitization* (3.37).

3.13**destruction**

result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible or prohibitively expensive to recover

3.14**device**

mechanical, electrical, or electronic contrivance with a specific purpose

[SOURCE: ISO/IEC 14776-372:2011, 3.1.10]

3.15**disintegrate**

destruct (3.12) by separating media into its component parts

3.16**Electronically Stored Information**

data or information of any kind and from any source, whose temporal existence is evidenced by being *stored* (3.50) in, or on, any electronic medium

Note 1 to entry: Electronically Stored Information (ESI) includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations, and other electronic formats commonly found on a computer. ESI also includes system, application, and file-associated *metadata* (3.26) such as timestamps, revision history, file type, etc.

Note 2 to entry: Electronic medium can take the form of, but is not limited to, *storage devices* (3.45) and *storage elements* (3.47).

3.17**Fibre Channel**

serial I/O interconnect capable of supporting multiple protocols, including access to open system *storage* (3.43), access to mainframe *storage* (3.43), and networking

Note 1 to entry: Fibre Channel supports point to point, arbitrated loop, and switched topologies with a variety of copper and optical links running at speeds from 1 gigabit per second to over 10 gigabits per second.

3.18**Fibre Channel Protocol**

serial Small Computer System Interface (SCSI) transport protocol used on *Fibre Channel* (3.17) interconnects

3.19**gateway**

device (3.14) that converts a protocol to another protocol

3.20**in-band**

communication or transmission that occurs within a previously established communication method or channel

Note 1 to entry: The communications or transmissions often take the form of a separate protocol, such as a management protocol over the same medium as the primary data protocol.

3.21

incinerate

destruct (3.12) by burning media completely to ashes

3.22

malware

malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity, or availability

Note 1 to entry: Viruses and Trojan horses are examples of malware.

[SOURCE: ISO/IEC 27033-1:2009, 3.22]

3.23

Mean Time Between Failures

expected time between consecutive failures in a system or component

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.1713, modified — The term was capitalized.]

3.24

Mean Time To Repair

expected or observed duration to return a malfunctioning system or component to normal operations

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.1714, modified — The term was capitalized.]

3.25

melt

destruct (3.12) by changing media from a solid to a liquid state generally by the application of heat

3.26

metadata

data that define and describe other data

[SOURCE: ISO/IEC 11179-1:2004, 3.2.16]

3.27

multi-factor authentication

authentication using two or more of the following factors:

- knowledge factor, “something an individual knows”;
- possession factor, “something an individual has”;
- biometric factor, “something an individual is or is able to do”.

[SOURCE: ISO 19092:2008, 4.42]

3.28

multi-tenancy

allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another

[SOURCE: Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.27]

3.29

Network Attached Storage

storage device (3.45) or system that connects to a network and provide file access services to computer systems

3.30

non-volatile storage

storage (3.43) that retains its contents even after power is removed

This is a free preview. Purchase the entire publication at the link below:

-
- ▶ Looking for additional Standards? Visit [SAI Global Infostore](#)
 - ▶ Subscribe to our [Free Newsletters about Australian Standards® in Legislation; ISO, IEC, BSI and more](#)
 - ▶ Do you need to [Manage Standards Collections Online?](#)
 - ▶ Learn about [LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
 - ▶ Do you want to [know when a Standard has changed?](#)
 - ▶ Want to [become an SAI Global Standards Sales Affiliate?](#)

Learn about other SAI Global Services:

- ▶ [LOGICOM Military Parts and Supplier Database](#)
- ▶ [Metals Infobase Database of Metal Grades, Standards and Manufacturers](#)
- ▶ [Materials Infobase Database of Materials, Standards and Suppliers](#)
- ▶ [Database of European Law, CELEX and Court Decisions](#)

Need to speak with a Customer Service Representative - [Contact Us](#)