DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27040

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2022-07-11

Voting terminates on:
2022-10-03

Information technology — Security techniques — Storage security

ICS: 35.030

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27040:2022(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27040:2015), which has been technically revised.

The main changes compared to the previous edition are as follows:

— Clause 1 (Scope) has been expanded to include requirements;

— the structure of the clauses is more closely aligned with ISO/IEC 27002:2022;

— requirements have been added in Clauses 7, 9, and 9.4;

— adjustments have been made as to what storage technologies are covered;

— a new controls labelling scheme has been added;

— the original Annex A, which provided guidance on sanitizing specific types of media, was removed and text was added in Clause 9.4, recommending IEEE Std 2883 for this purpose;

— the original Annex B, which included table to help prioritize the adoption of recommendation, has been replaced with Annex A that summarizes the requirements and guidance;

— the original Annex C, which provided tutorial oriented material, was removed and references to appropriate materials were added to the document.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document provides implementation requirements and guidance for storage security in meeting the requirements of an information security management system (ISMS) according to ISO/IEC 27001. This document 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, and industry sector. A number of existing methodologies can be used under the framework described in this document to implement the requirements of an ISMS.

This document 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 document are the following:

— highlight the risks arising out of potential threats and attack surfaces;

— assist organizations in better securing their data;

— provide a basis for designing, auditing, and reviewing storage security controls.

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

Information technology — Security techniques — Storage security

1 Scope

This document provides detailed technical requirements and guidance on how organizations can achieve 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 of data both while stored in information and communications technology (ICT) systems and while in transit across the communication links associated with storage. Storage security includes the security of devices and media, management activities related to the devices and media, applications and services, and controlling or monitoring user activities during the lifetime of devices and media and after end of use or end of life.

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 services, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information 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 document provides an overview of storage security concepts and related definitions. It includes requirements and guidance on the threats, 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 are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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*

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

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

3 Terms and definitions

3.1 General

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.2 Terms relating to storage technology

3.2.1
block
unit in which data is *stored* (3.2.17) and retrieved on *storage devices* (3.2.14) and *storage media* (3.2.16)

3.2.2
compression
reduction in the number of bits used to represent an item of data

Note 1 to entry: For *storage* (3.2.12), 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 used.

3.2.3
data at rest
data recorded on stable, *non-volatile storage* (3.2.11)

3.2.4
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 outside of an interface, chip, or device).

3.2.5
deduplication
method of reducing *storage* (3.2.12) 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 data reduction.

3.2.6
device
mechanical, electrical, or electronic contrivance with a specific purpose

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

3.2.7
Fibre Channel
serial I/O interconnect capable of supporting multiple protocols, including access to open system *storage* (3.2.12), access to mainframe *storage* (3.2.12), 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 128 gigabits per second.

3.2.8
Fibre Channel Protocol
Serial Small Computer System Interface (SCSI) transport protocol used on *Fibre Channel* (3.2.7) interconnects

3.2.9
over provisioning
technique used by *storage devices* (3.2.14) in which a subset of the available *storage medium* (3.2.16) is exposed through the interface

Note 1 to entry: *Storage medium* (3.2.16) is used internally and independently by the *storage device* (3.2.14) to improve performance, endurance, or reliability.

3.2.10
network attached storage
storage device (3.2.14) or system that connects to a network and provides file access services to computer systems

3.2.11
non-volatile storage
storage (3.2.12) that retains its contents after power is removed

3.2.12
storage
device (3.2.6), function, or service supporting data entry or retrieval

3.2.13
storage area network
network whose primary purpose is the transfer of data between computer systems and *storage devices* (3.2.14) and among *storage devices* (3.2.14)

Note 1 to entry: A SAN consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, *storage devices* (3.2.14), and computer systems so that data transfer is secure and robust.

3.2.14
storage device
any component or aggregation of components made up of one or more *devices* (3.2.6) containing *storage media* (3.2.16), designed and built primarily for the purpose for accessing *non-volatile storage* (3.2.11)

3.2.15
storage ecosystem
system of interdependent components that work together to enable *storage* (3.2.12) services and capabilities

Note 1 to entry: The components often include *storage devices* (3.2.14), storage networks, storage management, and other information and communications technology (ICT) infrastructure.

3.2.16
storage medium
storage media
material on which digital data are, or can be, recorded or retrieved

3.2.17
store
record data on *volatile storage* (3.2.20) or *non-volatile storage* (3.2.11)

3.2.18
target data
information subject to a given process, typically including most or all information on *storage* (3.2.12)

3.2.19
virtualized storage
logical storage
abstraction of physical *storage devices* (3.2.14) or *storage media* (3.2.16) that masks the characteristics and boundaries of the physical *storage* (3.2.12)

Note 1 to entry: Virtualized storage can employ multiple levels of virtualization prior to presenting the virtualized storage to a system or an application.

3.2.20
volatile storage
storage (3.2.12) that fails to retain its contents after power is removed

3.3 Terms relating to sanitization

3.3.1
clear
sanitize (3.3.12) using logical techniques on user data on all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same host interface available to the user

3.3.2
degauss
render magentically stored data unreadable by applying a strong magnetic field to the *storage medium* (3.2.16) with an organizationally approved field strength

3.3.3
destruct
sanitize (3.3.12) using physical techniques that make recovery of *target data* (3.2.18) infeasible using state of the art laboratory techniques and results in the subsequent inability to use the *storage medium* (3.2.16) for *storage* (3.2.12)

Note 1 to entry: *Disintegrate* (3.3.5), *incinerate* (3.3.6), *melt* (3.3.7), *pulverize* (3.3.9), and *shred* (3.3.13) are destruct forms of *media sanitization* (3.2.16).

Note 2 to entry: If the *storage medium* (3.2.16) cannot be removed, then the *storage device* (3.2.14) can be subjected to the destruct technique; a *storage device* (3.2.14) can contain multiple *storage media* (3.2.16)

3.3.4
destruction
result of *destruct* (3.3.3) actions taken to ensure that *storage medium* (3.2.16) cannot be reused as originally intended and that user data is virtually impossible or prohibitively expensive to recover

3.3.5
disintegrate
destruct (3.3.3) by separating *storage medium* (3.2.16) into its component parts

3.3.6
incinerate
destruct (3.3.3) by burning *storage medium* (3.2.16) completely

3.3.7
melt
destruct (3.3.3) by changing *storage medium* (3.2.16) from a solid to a liquid state generally by the application of heat

3.3.8
cryptographic erase
method of sanitization in which the encryption key for the encrypted *target data* (3.2.18) is *sanitized* (3.3.12), making recovery of the decrypted *target data* (3.2.18) infeasible

3.3.9
pulverize
destruct (3.3.3) by grinding *storage medium* (3.2.16) to a powder or appropriately small particles

3.3.10
purge
sanitize (3.3.12) using physical or logical techniques that make recovery of *target data* (3.2.18) infeasible using state of the art laboratory techniques, but which preserves the *storage media* (3.2.16) and *storage device* (3.2.14) in a potentially reusable state

3.3.11
sanitization
process or method to *sanitize* (3.3.12)

3.3.12
sanitize
render access to *target data* (3.2.18) on *storage* (3.2.12) infeasible for a given level of effort

3.3.13
shred
destruct (3.3.3) by cutting or tearing *storage medium* (3.2.16) into small particles

3.3.14
storage sanitization
virtual storage sanitization (3.3.15) or *media sanitization* (3.3.16)

3.3.15
virtual storage sanitization
logical storage sanitization
sanitization (3.3.11) of virtual storage

Note 1 to entry: *Clear* (3.3.1) and *purge* (3.3.10) are actions that can be taken to *sanitize* (3.3.12) virtual storage.

Note 2 to entry: Virtual storage sanitization is a subset of *storage sanitization* (3.3.14).

3.3.16
media sanitization
sanitization (3.3.11) of *storage media* (3.2.16)

Note 1 to entry: *Clear* (3.3.1), *purge* (3.3.10), and *destruct* (3.3.3) are actions that can be taken to *sanitize* (3.3.12) *storage media* (3.2.16).

Note 2 to entry: Media sanitization is a subset of *storage sanitization* (3.3.14).

3.4 Terms relating to availability

3.4.1
resilience
ability to anticipate and adapt to, resist or quickly recover from a potentially disruptive event, whether natural or man-made

[SOURCE: ISO 15392:2019, 3.21.]

3.5 Terms relating to security and cryptography

3.5.1
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 16609:2012, 3.9.]

3.5.2
data breach
compromise of security that leads to the accidental or unlawful *destruction* (3.3.4), loss, alteration, unauthorized disclosure of, or access to protected data transmitted, *stored* (3.2.17), or otherwise processed

3.5.3
data integrity
property that data has not been altered or destroyed in an unauthorized manner

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

3.5.4
multi-factor authentication
authentication using two or more of the following factors:

a) knowledge factor, something an individual knows;

b) possession factor, something an individual has;

c) biometric factor, something an individual is or is able to do.

[SOURCE: ISO 19092:2008, 4.42.]

3.5.5
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 27033-1:2015, 3.22.]

3.5.6
point of encryption
location within the information and communications technology (ICT) infrastructure where data are encrypted on its way to *storage* (3.2.12) and, conversely, where data are decrypted when accessed from *storage* (3.2.12)

Note 1 to entry: The point of encryption is only applicable for *data at rest* (3.2.3).

3.5.7
security strength
number associated with the amount of work that is required to break a cryptographic algorithm or system

3.5.8
storage security
application of physical, technical, and administrative controls to protect storage systems and infrastructure as well as the data *stored* (3.2.17) within them

Note 1 to entry: Storage security is focused on protecting data (and its storage infrastructure) against unauthorized disclosure, modification, or destruction while assuring its availability to authorized users.

Note 2 to entry: These controls may be preventive, detective, corrective, deterrent, recovery, or compensatory in nature.

3.5.9
strong authentication
authentication by means of cryptographically derived credentials

[SOURCE: ISO/TS 22600-1:2006, 2.23.]

3.6 Terms relating to archives and repositories

3.6.1
archives
<organization>organization or part of an organization responsible for selection, acquisition, *preservation* (3.6.5), and availability of one or more *archives* (3.6.2)

[SOURCE: ISO 5127:2017, 3.2.3.01, modified — Note 1 to entry until Note 4 to entry has been omitted]

3.6.2
archives
<holdings>materials, items, *records* (3.6.6) or documents created or received by a person, family or organization, public or private, in the conduct of their affairs and preserved because of the enduring value contained in them or as evidence of the functions and responsibilities of their creator, especially those materials maintained using the principles of provenance, original order and collective control

[SOURCE: ISO 5127:2017, 3.6.1.03, modified — Items, records or documents have been included to define archives. Note 1 to entry has been omitted]

3.6.3
disposition
range of records processes associated with implementing *records* (3.6.6) *retention* (3.6.9), *records destruction* (3.6.7) or transfer decisions which are documented in disposition authorities or other instruments

[SOURCE: ISO 30300:2020, 3.4.8, modified—changed "destruction" to "records destruction".]

3.6.4
evidence
information that could be used either by itself or in conjunction with other information, to establish proof about an event or action

[SOURCE: ISO 30300:2020, 3.2.6.]

3.6.5
preservation
measures taken to maintain the *useability* (3.6.10), authenticity, reliability and integrity of *records* (3.6.6) over time

Note 1 to entry: Measures include principles, policies, rules, strategies, processes and operations.

[SOURCE: ISO 30300:2020, 3.4.11.]

3.6.6
record
information created or received and maintained as *evidence* (3.6.4) and as an asset by an organization, in pursuit of legal obligations or in the course of conducting business

Note 1 to entry: Records are normally used in plural.

Note 2 to entry: In a management system standard (MSS) implementation, the records created to conduct and direct the management system and to document its implementation are called documented information.

[SOURCE: ISO 30300:2020, 3.2.10.]

3.6.7
records destruction
eliminating or deleting a *record* (3.6.6), beyond any possible reconstruction

[SOURCE: ISO 30300:2020, 3.4.7, modified—changed the term "destruction" to "records destruction".]

3.6.8
records requirement
requirement for *evidence* (3.6.4) of a business function, activity or transaction and for records processes including how, and how long, *records* (3.6.6) need to be kept

[SOURCE: ISO 30300:2020, 3.3.2.]

3.6.9
retention
keeping a *record* (3.6.6) according to *records requirements* (3.6.8)

[SOURCE: ISO 30300:2020, 3.4.14.]

3.6.10
useability (preferred term)
usability (admitted term)
property of being able to be located, retrieved, presented and understood

Note 1 to entry: Useability may also refer to the extent to which a system, product, or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.

[SOURCE: ISO 30300:2020, 3.2.12.]

3.7 Miscellaneous terms

3.7.1
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.

3.7.2
metadata
data that defines and describes other data

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

3.7.3
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: ISO/IEC 22123-1:2021, 3.5.3.]

3.7.4
out-of-band
communication or transmission that occurs outside of a previously established communication method or channel

3.7.5
secure multi-tenancy
type of *multi-tenancy* (3.7.3) that employs security controls to explicitly guard against *data breaches* (3.5.2) and provides validation of these controls for proper governance

Note 1 to entry: Secure multi-tenancy exists when the risk profile of an individual tenant is no greater than in a dedicated, single-tenant environment.

Note 2 to entry: In very secure environments even the identity of the tenants is kept secret.

4 Symbols and abbreviated terms

ACL	access control list
AES	Advanced Encryption Standard

BC	business continuity
BCM	Business Continuity Management
BMC	baseboard management controller
CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining Message authentication code
CDMI	Cloud Data Management Interface
CDP	continuous data protection
CHAP	Challenge Handshake Authentication Protocol
CLI	command line interface
CNA	converged network adaptor
DAS	direct attached storage
DDoS	distributed denial of service
DH-CHAP	Diffie Hellman – Challenge Handshake Authentication Protocol
DNS	Domain Name System
DoS	denial of service
DR	disaster recovery
EHR	electronic healthcare record
ESP	Encapsulating Security Payload
FC	Fibre Channel
FC-NVMe	NVMe over Fibre Channel
FC-SP	Fibre Channel – Security Protocol
FCAP	Fibre Channel Certificate Authentication Protocol
FCEAP	Fibre Channel Extensible Authentication Protocol
FCIP	Fibre Channel over TCP/IP
FCP	Fibre Channel Protocol
FCPAP	Fibre Channel Password Authentication Protocol
GCM	Galois/Counter Mode
GUI	graphical user interface
HBA	host bus adapter
HDD	hard disk drive
HTTPS	Hypertext Transfer Protocol Secure