



**International
Standard**

ISO/IEC 27040

Information technology — Security techniques — Storage security

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

**Second edition
2024-01**

Reference number
ISO/IEC 27040:2024(en)

Full document details: ISO IEC 27040-2024

 **Documents**
© ISO/IEC 2024 Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2024 – All rights reserved

Contents

Page

Foreword	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
3.1 General	1
3.2 Terms relating to storage technology	1
3.3 Terms relating to sanitization	3
3.4 Terms relating to availability	5
3.5 Terms relating to security and cryptography	5
3.6 Terms relating to archives and repositories	6
3.7 Miscellaneous terms	8
4 Symbols and abbreviated terms	8
5 Structure of this document	11
5.1 General	11
5.2 Controls	11
6 Overview and concepts	11
6.1 General	11
6.2 Storage concepts	12
6.3 Introduction to storage security	13
6.4 Storage security risks	15
6.4.1 Background	15
6.4.2 Data breaches	16
6.4.3 Data corruption or destruction	16
6.4.4 Temporary or permanent loss of access/availability	17
6.4.5 Failure to meet statutory, regulatory, or legal requirements	17
7 Organizational controls for storage	18
7.1 General	18
7.2 Align storage and policy	18
7.3 Business continuity management	18
7.4 Compliance	19
8 People controls for storage	20
9 Physical controls for storage	21
9.1 General	21
9.2 Physically secure storage	21
9.3 Protect physical interfaces to storage	21
9.4 Isolation of storage systems	22
10 Technological controls for storage	22
10.1 General	22
10.2 Design and implementation of storage security	22
10.2.1 General	22
10.2.2 Storage security design principles	23
10.2.3 Storage system quality attributes	25
10.2.4 Retention, preservation, and disposal of data	27
10.3 Storage systems security	28
10.3.1 System hardening	28
10.3.2 Security auditing, accounting, and monitoring	28
10.3.3 Storage vulnerability management	31
10.4 Storage management	31
10.4.1 Background	31
10.4.2 Authentication and authorization	32
10.4.3 Secure the management interfaces	34

10.5	Data confidentiality.....	35
10.5.1	General.....	35
10.5.2	Encryption and key management issues.....	36
10.5.3	Encryption of storage.....	37
10.5.4	Encrypting transferred data.....	40
10.5.5	Encrypting data at rest.....	41
10.6	Storage sanitization.....	42
10.6.1	General.....	42
10.6.2	Selection of sanitization methods.....	43
10.6.3	Media-based sanitization.....	44
10.6.4	Logical sanitization.....	44
10.6.5	Cryptographic erase.....	45
10.6.6	Verification of storage sanitization.....	46
10.6.7	Proof of sanitization.....	47
10.7	Direct attached storage.....	48
10.8	Storage networking.....	48
10.8.1	Background.....	48
10.8.2	Storage area networks.....	49
10.8.3	Network Attached Storage protocols.....	54
10.9	Block-based storage.....	55
10.9.1	Fibre Channel (FC) storage.....	55
10.9.2	IP storage.....	56
10.10	File-based storage.....	57
10.10.1	General.....	57
10.10.2	NFS-based NAS.....	57
10.10.3	SMB-based NAS.....	58
10.11	Cloud computing storage.....	59
10.11.1	Securing cloud computing storage.....	59
10.11.2	CDMI security.....	59
10.12	Object-based storage.....	60
10.13	Data reductions.....	61
10.14	Data protection and recovery.....	62
10.14.1	General.....	62
10.14.2	Storage backups.....	62
10.14.3	Storage replication.....	63
10.14.4	Storage snapshots.....	63
10.15	Data archives and repositories.....	64
10.15.1	General.....	64
10.15.2	Data archives.....	64
10.15.3	Data Repositories.....	68
10.16	Virtualization.....	68
10.16.1	Storage virtualization.....	68
10.16.2	Storage for virtualized systems.....	69
10.17	Secure multi-tenancy.....	70
10.18	Secure autonomous data movement.....	71
	Annex A (informative) Storage security controls summary.....	73
	Bibliography.....	82

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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 are as follows:

- the scope has been expanded to cover requirements;
- the clause structure has been more closely aligned with ISO/IEC 27002:2022;
- requirements have been added in [Clauses 7, 9](#), and [10](#);
- adjustments have been made regarding the storage technologies which are covered;
- a new controls labelling scheme has been added;
- former [Annex A](#), which provided guidance on sanitizing specific types of media, has been removed and text has been added in [Clause 10](#), recommending IEEE 2883 for this purpose;
- former Annex B, which included table to help prioritize the adoption of recommendation, has been replaced with [Annex A](#) that summarizes the requirements and guidance contained in this document;
- former Annex C, which provided tutorial oriented material, has been removed and references to appropriate materials have been added in [Clause 10](#).

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 and www.iec.ch/national-committees.

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 products 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 programme 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*

3 Terms and definitions

3.1 General

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

ISO and IEC maintain terminology 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 input/output interconnect capable of supporting multiple protocols, including access to open system *storage* (3.2.12), access to mainframe storage, 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 provision

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: The storage medium is used internally and independently by the storage device 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

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

3.2.14

storage device

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

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 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 magnetically 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* (3.3.16).

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

3.3.4

destruction

result of *destruct* (3.3.3) actions taken to ensure that the *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 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

logical storage sanitization (3.3.15) or *media sanitization* (3.3.16)

3.3.15

logical storage sanitization

virtual storage sanitization

sanitization (3.3.11) of virtualized storage (3.2.19)

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

Note 2 to entry: Logical 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 the cryptographic keys in a given system may remain in effect

[SOURCE: ISO 16609:2022, 3.6]

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:

- 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]

3.5.5

malware

malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity, and/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 infrastructure where data are encrypted on its way to *storage* ([3.2.12](#)) and, conversely, where data are decrypted when accessed from storage

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 can be preventive, detective, corrective, deterrent, recovery, or compensatory in nature.

3.5.9

strong authentication

authentication by means of cryptographically derived multi-factor credentials

[SOURCE: ISO 22600-1:2014, 3.23]

3.6 Terms relating to archives and repositories

3.6.1

archive

<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 — Notes to entry 1 to 4 have been omitted; term changed to singular from plural “archives”; domain <organization> has been added.]

3.6.2

archive

<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 at the start of the definition; Note 1 to entry has been omitted; term changed to singular from plural “archives”; domain <holdings> has been added.]

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 — “destruction” has been changed to “records destruction”.]

3.6.4 evidence

information that can 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, modified — Note 1 to entry has been omitted; “could” has been changed to “can”.]

3.6.5 preservation

measures taken to maintain the *usability* (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 usability

property of being able to be located, retrieved, presented and understood

Note 1 to entry: Usability 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 11179-1:2023, 3.2.26]

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 22123-1:2023, 3.4.3]

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
API	application programming interface
BCM	business continuity management
BMC	baseboard management controller
CCM	counter with cipher block chaining message authentication code
CDMI	Cloud Data Management Interface
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
DRAM	dynamic random access memory
ESP	encapsulating security payload
FC	fibre channel
FC-SP	fibre channel – security protocol
FCIP	fibre channel over TCP/IP
FCP	fibre channel protocol
GCM	Galois/Counter Mode
HBA	host bus adapter
HDD	hard disk drive
HMAC	hash-based message authentication code
HTTPS	hypertext transfer protocol secure
IB	InfiniBand™
ICT	information and communications technology
ID	identifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Security
IRBC	ICT readiness for business continuity
iSCSI	Internet Small Computer Systems Interface
ISMS	information security management system
iSNS	Internet Storage Name Service
KMIP	key management interoperability protocol
LAN	local area network
LUN	logical unit number

MTBF	mean time between failure
MTTF	mean time to failure
MTTR	mean time to repair
NAS	network attached storage
NFS	network file system
NTP	network time protocol
NVM	non-volatile memory
NVMe®	NVM Express®
NVMe-oF™	NVM Express® over Fabric
NVMe®/FC	NVMe® over Fibre Channel
NVMe®/RDMA	NVMe® over RDMA
NVMe®/TCP	NVMe® over TCP
OASIS	Organization for the Advancement of Structured Information Standards
PCIe®	PCI Express®
PII	personally identifiable information
RADIUS	remote authentication dial in user service
RAID	redundant array of independent disks
RDMA	remote direct memory access
REST	representational state transfer
RMCP	Remote Management Control Protocol
SAN	storage area network
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SLP	Service Locator Protocol
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSD	solid state drive
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

VLAN	virtual local area network
VM	virtual machine
VPN	virtual private network
WORM	write once read many
WWN	worldwide name
XEX	Xor-Encrypt-Xor
XTS	XEX-based Tweaked-codebook mode with ciphertext Stealing

5 Structure of this document

5.1 General

The basic structure of this document starts with an introduction of storage security in [Clause 6](#), followed by separate clauses that address organization controls ([Clause 7](#)), people controls ([Clause 8](#)), physical controls ([Clause 9](#)), and technological controls ([Clause 10](#)) that are relevant to storage systems and ecosystems.

5.2 Controls

The controls of ISO/IEC 27001 and ISO/IEC 27002 generally apply to storage ecosystems and the organizations that procure, manage, and operate them. This document provides additional guidance and requirements that expand upon these standards.

The requirements specified in this document represent a baseline set of storage security controls. To aid in identifying these baseline controls and key guidance, subheadings are used in the text. These subheadings include a control label with a description. The control labels take the form of xx-yyyy-cnn where:

- xx is “OC” for organizational controls, “SC” for people controls, “PC” for physical controls, or “TC” for technological controls;
- yyyy is associated with the topic;
- c is either “R” for a requirement or “G” for guidance;
- nn is a sequence number when multiple controls exist for a single topic; requirements and guidance are numbered independently of each other.

When multiple subheadings are included in a clause or sub-clause, they are presented in an order list to make easier to refer to them. A summary of the controls is listed in [Annex A](#).

Although this document is written from the perspective of consumers of storage technologies, it is important to note that many controls are dependent on vendors implementing certain security features or capabilities as a prerequisite to the use of these controls. The presence or absence of these features and capabilities can be an important consideration when making product selections.

6 Overview and concepts

6.1 General

Data storage or information storage, often called storage, refers to system components, storage devices, and storage media that retain digital data in durable (i.e. non-volatile) form. While both volatile and non-volatile forms of storage exist, this document is concerned primarily with non-volatile storage. Storage is a core function and fundamental component of ICT systems.

To secure storage infrastructure, a clear understanding of the storage technologies and concepts are necessary. In addition, the types of security controls and insights into how they impact and interact with the storage technologies are also important. Finally, the threats to this infrastructure and the major risks arising from these threats are factored into any efforts to mitigate risks to storage infrastructure or individual storage systems.

6.2 Storage concepts

In its simplest form, storage can be hard disk drives (HDD), solid state drives (SSD), or tape drives attached to an ICT system to store data. This approach, commonly called direct attached storage (DAS), is still in use within enterprise data centres as well as small office/home office environments. With the integration of networking technology, storage systems and ecosystems can be highly sophisticated technologies that provide solutions for managing, connecting, securing (i.e. making safe), sharing, and optimizing the storage of data. These solutions have become more feasible and cost effective as storage technology has evolved from non-intelligent internal and external DAS to intelligent networked storage. The use of networking in these solutions increases the attack surface of these solutions and requires additional attention to be paid to mitigate the associated risks.

Contemporary storage solutions include some or all of the following elements:

- Storage devices and media, consisting of materials which are magnetic, solid state, etc., on which data can be recorded or accessed;
- Block-based storage, which is the most basic and fundamental form of persistent digital data storage that is arranged in a sequence of blocks (each consisting of a sequence of bytes or bits) with offsets to represent locations of individual blocks of data;
- File-based storage, which is data storage that organizes data into files and directories on a file system, while abstracting the underlying hardware for local user access or access over a network, typically as network attached storage (NAS). NAS can enable multiple computer systems to have equal access to the stored contents regardless of their native operating system;
- Storage interfaces, which include specific storage direct attachment interfaces as well as storage networking interfaces;
- Object storage, which is a method of storing and subsequently retrieving sets of data as collections of single, uniquely identifiable indivisible items or objects. It applies to any forms of data that can be wrapped up and managed as an object;
- Cloud computing storage, which can be part of a data storage as a service (DSaaS), as defined in ISO/IEC 22123-1 and described in ISO/IEC 22123-2. Cloud storage can include the most basic storage of files or blocks of raw binary data, relational databases, and advanced big data platforms as well as offering automatic backup, disaster recovery, geographical redundancy, advanced failover, and other more sophisticated features;
- Data protection systems that create one or more copies of production data to enable the recovery of a system or its data following a catastrophic event;
- Persistent memory, which is non-volatile memory with densities greater than or equal to dynamic random access memory (DRAM) that resides on the memory bus and has DRAM-like access to data with nearly the same speed and latency of DRAM and the non-volatility of NAND flash.

Storage has become a prominent and independent layer of ICT infrastructure in enterprise class and midrange computing environments. The requirements for these environments frequently exceed simple data storage capabilities. Examples of applications and functions driving the emergence of new storage technology include:

- sharing of vast storage resources (measured in petabytes, exabytes, and yottabytes) between multiple systems via networks;
- need for more speed (lower latency);

- increased storage capacities;
- expanded storage client access (e.g. mobile devices and internet of things);
- support for distributed ICT architectures (e.g. edge computing);
- support for virtualized environments;
- data protection systems that backup data without the use of a local area network (LAN);
- remote, disaster tolerant, online mirroring of mission critical data;
- clustering of fault tolerant applications and related systems around a single copy of data;
- long-term retention of sensitive or high-value business information;
- distributed database and file systems;
- support for complying with regulatory and legal requirements;
- support for centralized data repositories for rapid recovery (e.g. backups) and archiving;
- resilience to cyber-attacks.

6.3 Introduction to storage security

Storage security is focused on mitigating risk associated with storage systems and infrastructure, as outlined in 6.2, through the use of safeguards and countermeasures (i.e. controls). The controls are categorized according to ISO/IEC 27002:2022, 4.2.

Storage security can also necessitate the introduction of specialized controls to address technologies such as:

- system security hardening;
- storage sanitization;
- virtualization security;
- self-encrypting storage devices and data encryption software;
- key management services;
- data authenticity and integrity services;
- data in motion protections (encryption and data reduction);
- directory services and other user management systems;
- data retention and preservation;
- data protection and recovery.

Knowing both how and why storage technologies are used can lead to a better understand of the security issues and implications for storage. As a starting point, the following points should be considered.

- The storage systems can function as nodes within storage networks, which can be based on, but not limited to, technologies such as Transmission Control Protocol/Internet Protocol (TCP/IP), Fibre Channel (FC), InfiniBand^{TM1)} (IB), etc. The potential threats can vary significantly based on the networking technology and their topologies.

1) This trademark is provided for reasons of public interest or public safety. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO.

- When stored, the data are typically represented and accessed as either blocks or as files/objects with significant differences between these two types of storage methods. Likewise, the associated security measures can have radical differences, especially with access controls, encryption, and data integrity.
- As part of normal storage operations, many storage device types have more internal media capacity than is exposed through the interface. SSDs typically over provision media, where data can be moved internally between physical media areas to improve write latencies and evenly distribute write activity. HDDs often contain spare areas where data can be moved internally between physical media areas when there is an access problem. User data can remain on over provision or spare areas even after subsequent writes to the device occur through its interface. Such data cannot be cleared by overwrites through the interface.
- Storage management is both an element of the storage infrastructure as well as an operation performed on that infrastructure. Commonly this infrastructure can have privileged users applying configuration changes, provisioning storage, tuning, monitoring, etc. Some of the management can be performed remotely and can involve third parties such as vendor support personnel.
- Data availability and integrity are key factors in an organization's storage architecture, so it is important that security measures are complementary rather than a trade-off and that they do not negate high-availability measures by introducing choke-points and single points of failure.
- Many organizations implement elaborate data resiliency strategies, which are integral to their business continuity management (BCM) plans. Security mechanisms like data at rest encryption can negatively impact these resiliency strategies if not implemented carefully.
- Virtualization within storage can take many forms and be implemented at different points within the storage infrastructure. This virtualization can mask the physical details associated with the presentation of storage [e.g. a logical unit (see NOTE below) or filesystem to a server], mask the true capacity of a device, perform policy-driven autonomous data movement (i.e. tiered storage), or completely abstract the storage infrastructure (i.e. cloud computing storage). Balancing security measures and virtualization to ensure they interoperate requires careful planning and selection of the right technologies.

NOTE In computer storage, a logical unit is a device addressed by the SCSI protocol or protocols which encapsulate SCSI, such as Fibre Channel or iSCSI. A logical unit number (LUN) is a number used to identify a logical unit. The LUN can be used with any device which supports read/write operations, such as a tape drive, but is most often used to refer to a logical storage as created on a SAN. Though not technically correct, the term LUN is often also used to refer to the logical storage itself.

- Data growth rates in some organizations are driving an increased use of data storage technologies. As an alternative to acquiring additional storage, organizations are employing data reduction technologies such as compression and deduplication. However, these data reduction technologies can be impacted by data at rest encryption mechanisms, and they in turn, can introduce data integrity problems during BCM operations.
- Additional copies of data can be created as a by-product of data protection strategies such as replicating data between systems and sites (see [10.14.3](#)), backups (see [10.14.2](#)), and snapshots (see [10.14.4](#)). Such data copies and residual data have the same sensitivity considerations as the original data.
- Sensitive and high-value data are often transmitted between and within systems (e.g. data in motion), increasing data protection considerations (see [10.5.4](#)).
- Many organizations are implementing data at rest encryption (see [10.5.5](#)) to protect sensitive and high-value data. The specific cryptographic mechanisms and the point of encryption are important factors in the actual data protection as well as for meeting compliance requirements.
- Successful use of encryption is often predicated on proper management of keying material throughout its lifecycle (see [10.5.2](#)). This includes correct generation of keys, secure storage and transmittal of key material, replicating keys as part of the normal strategy to ensure availability of the data, and proper disposal of the keying material when it is no longer needed. The sensitivity and importance of the data to be protected can also factor into the key management approach.

Ensuring adequate confidentiality, integrity, and availability of data stored and accessed on current and emerging storage technologies requires a concerted effort within this layer of ICT. Many of these security efforts focus on:

- protecting storage management (operations and interfaces);
- ensuring adequate credential and trust management;
- protecting data backup and recovery resources;
- data in motion protection;
- data at rest protection;
- data availability protection;
- BCM support;
- proper sanitization of storage and disposal of media;
- secure autonomous data movement;
- secure multi-tenancy.

6.4 Storage security risks

6.4.1 Background

Storage security risks are created by an organization's use of specific storage systems or infrastructures. Storage security risks arise from:

- threats targeting the data handled by the storage systems and infrastructure;
- vulnerabilities (both technical and non-technical);
- likelihood of performing a successful exploit of vulnerabilities by threats;
- impact of successful exploitation of vulnerabilities by threats.

Risk management is a key concept in information security. The information security risk management process presented in ISO/IEC 27005 consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review.

Threats for storage systems and infrastructure can include:

- unauthorized usage of storage resources;
- unauthorized access;
- liability due to regulatory non-compliance;
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on storage or networks;
- corruption/modification and destruction of data, including backup or recovery copies;
- unauthorized disclosure which can constitute a data breach;
- theft or accidental loss of storage media;
- malware attack or introduction of malicious code (e.g. ransomware);
- improper sanitization or disposal after end-of-use.

These threats can give rise to a wide assortment of risks. For storage systems and infrastructure however, the major concerns are the risks associated with data breaches, data corruption or destruction, temporary or permanent loss of access/availability, and failure to meet statutory, regulatory, or legal requirements.

6.4.2 Data breaches

This document defines a data breach as a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed. This definition goes significantly beyond more simplistic data breach definitions that focus on unauthorized access or disclosure of certain types of data.

Depending on the volume and type of data involved and the applicable laws and regulations, a data breach can expose the organization to significant risk arising from costs involved in investigating the data breach, making requisite notifications to affected individuals, litigation expenses, regulatory fines and other legal penalties as well as brand damage accruing from the public disclosure of the data breach.

There are economic and security risks to the entity that loses their or others' secured information. Such information can include:

- intellectual property or other sensitive business information;
- personally identifiable information (PII);
- financial account or record information;
- personally identifiable health record information.

Untrusted or unauthorized entities seeking this information can be well funded and have diverse motivations.

[Table 1](#) summarizes the likely storage-based security threats and lists the forms of data breaches that can result from these compromises.

Table 1 — Storage-oriented data breaches

Security threats	Potential forms of data breach
Theft or loss of storage device or storage media	Unlawful or unauthorized disclosure, data loss, or data destruction
Accidental configuration changes (e.g. storage management, storage/network resources, and incorrect patch management) by authorized personnel	Accidental access, accidental disclosure, accidental data destruction, accidental data alteration, or removal/denial of access
Malicious configuration changes (storage management, storage/network resources, and application tampering) by external or internal adversaries	Unlawful access, unlawful disclosure, unlawful data destruction, unlawful data alteration
Privileged user abuses by authorized users (e.g. inappropriate data snooping)	Unlawful/unauthorized access or disclosure
Malicious data tampering by external or internal adversaries	Unlawful data destruction or alteration
Denial of service attacks	Loss of access by legitimate users and unavailability of storage and data
Malicious monitoring of network traffic	Unlawful/unauthorized disclosure

6.4.3 Data corruption or destruction

Data corruption is the deterioration or damage of data (i.e. undesirable changes to the original data) caused by users, hardware, or software error. It can occur during writing, reading, retention, transmission, or processing. Early detection of data corruption can possibly enable the recovery of data or metadata under the right conditions. If left undetected or corrected, this data corruption can result in permanent data loss if the root cause persists. Data destruction on the other hand results in data loss, which can be permanent if data protection mechanisms like backups have not been employed. Both data corruption and

data destruction can be the result of unintentional or intentional events, and in the latter case, they can be further categorized as malicious or non-malicious.

Events such as fire, flood, power outages, and user errors are all examples of general, unintentional sources of data corruption and destruction. Background radiation, HDD head crashes, and aging or wear of the storage media are additional sources of problems that are more storage centric. Data corruption due to storage device or storage media failures can generally be detected by the use of checksums, and can often be corrected by using error correcting codes, but these silent corrections can lead to other problems if storage is not managed well (i.e. temporary correctable errors can turn into permanent ones as the storage device or media deteriorates).

Intentional attacks of a malicious nature can be perpetrated by external parties or insiders with the purpose of making some or all the affected data unusable or destroyed. In this context, unusable can mean that unauthorized modifications have been applied, modifications are suspected, or the data can be encrypted with an unknown key or mechanism (or the key used originally to encrypt the data can be destroyed). Non-malicious incidents typically result from carelessness, lack of knowledge, or intentional circumvention of security measures for such reasons as getting the job done. However, the impact of non-malicious incidents on the data can be as devastating as malicious attacks.

Employing appropriate mechanisms to detect and remedy data corruption is an important way of maintaining data integrity. Likewise, detecting data loss and recovering this data using data protection mechanisms can guard against the loss of data.

6.4.4 Temporary or permanent loss of access/availability

Availability is concerned with assuring that authorized users and systems have access to data at a required level of performance within a specified time frame. Loss of access, even when temporary, can cause significant harm to an organization. In addition, degraded access (e.g. minimum performance thresholds are not met) can be equally harmful to an organization.

Loss of access or availability can occur due to failures or issues associated with storage devices, storage network elements, stored data, data flows, services, and applications as well as attacks. In general, data availability is achieved through redundancy.

6.4.5 Failure to meet statutory, regulatory, or legal requirements

Organizations can incur significant liabilities and penalties for non-compliance with statutory, regulatory, or legal requirements. For multi-national organizations, country-specific legislation has an important influence on information security requirements.

Common compliance issues include:

- breach of country-specific privacy requirements;
- unlawful transfer of data (e.g. moving restricted data out of particular jurisdiction);
- breach of confidentiality;
- non-conformance with an organization's policies (e.g. sanitization);
- inadequate data retention and protection;
- insufficient evidence of security (e.g. audit logs and proof of encryption/sanitization).

These non-compliance issues can result in costly sanctions and remediation (e.g. breach notifications).

7 Organizational controls for storage

7.1 General

Users can refer to the extensive set of organizational controls listed in ISO/IEC 27002:2022, Clause 5. Some or all of these controls are relevant to storage systems and storage ecosystems.

7.2 Align storage and policy

The presence or absence of policy plays a major role in assuring both security and compliance.

The following policy guidance and requirements apply.

a) OC-PLCY-G01 Incorporating storage into policies

Storage should be incorporated into policies in order to:

- identify the most sensitive (PII, intellectual property, trade secrets, etc.) and business/mission critical data categories as well as protection requirements;
- integrate storage-specific policies with other policies (i.e. avoid creating a separate policy document for the storage ecosystem);
- address data retention and protection (e.g. WORM, authenticity, and access controls);
- address data destruction and storage media sanitization.

b) OC-PLCY-G02 Ensuring storage conforms with policies

Conformance with policies should:

- ensure that all elements of the storage ecosystem comply with policy (e.g. ISO/IEC 27001:2022, 5.2 and ISO/IEC 27002:2022, 5.1);
- give priority to the most sensitive/most critical data.

c) OC-PLCY-R01 Include storage in logging policy

Include storage in the logging policy such that the logging policy shall:

- clearly state that storage systems and devices participate in audit logging;
- identify the significant storage-related events to be collected;
- identify the preservation requirements for storage-related event logs;
- identify the retention and archival requirements for storage-related event logs;
- specify the time synchronization and use requirement for storage-related event logs;
- include evidentiary expectations (authenticity, chain of custody, etc.).

7.3 Business continuity management

ISO 22301 specifies the structure and requirements for implementing and maintaining a business continuity management system that develops business continuity appropriate to the amount and type of impact that the organization accepts following a disruption. The requirements specified in ISO 22301 are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity. The requirements specified in ISO 22301 address the context of the organization, leadership, planning, support, operations, performance evaluation, and improvement.

ISO/IEC 27002:2022, 5.30 identifies the importance of ICT readiness for business continuity (IRBC) to ensure the availability of the organization's information and other associated assets during disruption. ISO/IEC 27031 describes the concepts and principles of IRBC. It also provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. This framework applies to any organization (private, governmental, and non-governmental, irrespective of size) that is developing its ICT readiness for business continuity programme, and requires its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that can affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner.

Storage is typically a critical element of an organization's IRBC programme or informal BCM activities. The controls related to BCM are as follows:

a) OC-IRBC-G01 Factoring storage ecosystem into BCM planning and implementation

Organizations should ensure that the storage ecosystem is factored into the BCM planning and implementation.

b) OC-IRBC-G02 Preparing for limited disruption events

Organizations should prepare for limited disruption events (system failures, adversarial attacks, operator errors).

c) OC-IRBC-G03 Identifying and documenting the unique staffing and facility requirements

Organizations should identify and document the unique staffing and facility requirements associated with the storage ecosystem.

d) OC-IRBC-G04 Performing ongoing planning and testing of BCM

Organizations should perform ongoing planning and regular testing of assumptions, which are critical to successful BCM. Results of BCM testing should be fed back into ongoing maintenance of the BCM plan.

7.4 Compliance

The importance of complying with legal and regulatory requirements drives a significant portion of the security agenda and strategy of many organizations. The following elements are key compliance aspects of storage systems and infrastructure that are of concern to an information systems (IS) auditor.

The controls related to compliance are as follows:

a) OC-CPLC-R01 Ensure storage meets user accountability obligations

Make certain that user accountability obligations are met by ensuring that:

- users, especially privileged users, shall have unique user IDs (i.e. no shared accounts);
- users rights and privileges shall be explicitly granted based on their duties (e.g. roles) in accordance with the principle of least privilege (i.e. users are granted the minimum system resources and authorizations that they need to perform their function);
- all attempted (successful and unsuccessful) management events and transactions shall be logged.

b) OC-CPLC-G01 Ensuring storage meets user traceability obligations

Ensure that storage meets user traceability obligations such that:

- logged event/transaction data should contain sufficient application or system detail to clearly identify the source;
- user information should be traceable to a specific individual;

- when appropriate, log records should be treated as evidence (chain of custody, non-repudiation, authenticity, etc.).

c) OC-CPLC-G02 Ensuring storage meets user monitoring obligations

Ensure that storage meets user monitoring obligations such that:

- the storage layer should participate in the external audit logging measures;
- the audit logging events should be monitored and alert issues when appropriate.

d) OC-CPLC-G03 Ensuring storage meets data retention and sanitization obligations

Ensure that storage meets data retention and sanitization obligations such that:

- appropriate data retention measures should be implemented;
- appropriate data integrity and authenticity measures should be implemented;
- correct data sanitization should be implemented prior to the repurposing or decommissioning of hardware;
- correct sanitization of virtual server images, and their copies, should be implemented at their end of life.

e) OC-CPLC-G04 Ensuring storage meets privacy obligations

Ensure that storage meets privacy (see ISO/IEC 27701) obligations such that:

- appropriate data access control, based on least privilege, should be implemented to control access to data and metadata (e.g. search results);
- appropriate data confidentiality measures should be implemented to prevent unauthorized disclosure.

f) OC-CPLC-G05 Storage taking legal obligations into consideration

Legal obligations can apply to storage such that:

- use of data deduplication should not conflict with data authenticity requirements;
- use of data and storage media sanitization mechanisms should not violate preservation requirements;
- proper chain of custody procedures should be followed when evidentiary data (e.g. audit logs, metadata, mirror images, and point-in time copies) is handled.

8 People controls for storage

Users can refer to the extensive set of people controls listed in ISO/IEC 27002:2022, Clause 6. Some or all of these controls are relevant to storage systems and storage ecosystems.

ISO/IEC 27002:2022, 6.3 states that an organization should identify, prepare and implement an appropriate training plan for technical teams whose roles require specific skill sets and expertise. For individuals responsible for aspects of storage security, the skill and expertise can be highly specialized as demonstrated by this document.

The controls related to expertise are as follows:

a) SC-XPTS-G01 Ensuring adequate storage protection expertise

Storage teams and management should understand the technologies and practices associated with storage-based data protection technologies (see [10.14](#)). In addition, this understanding should include the applicability of data protection in the organization.

b) SC-XPTS-G02 Ensuring adequate storage security expertise

Storage teams and management should understand the technologies and practices for securing storage devices, systems and ecosystems, as well as leveraging storage-based security controls.

9 Physical controls for storage

9.1 General

Users can refer to the extensive set of physical controls listed in ISO/IEC 27002:2022, Clause 7. Some or all of these controls are relevant to storage systems and storage ecosystems.

9.2 Physically secure storage

Storage systems and ecosystems are particularly susceptible to physical threats. They can be subjected to theft, destruction, and unauthorized access unless protected when not in use or not under observation. The size of storage media, devices, and systems can vary significantly, so the methods to secure them can also vary.

The controls related to physically securing storage are as follows:

a) PC-PHYS-G01 Physically securing storage media

All storage media with recorded data should be stored in a safe, secure environment according to their information classification and which protects them against environmental threats (such as heat, moisture, humidity, electronic field or ageing), in accordance with manufacturers' specifications.

b) PC-PHYS-G02 Physically securing storage devices

Depending on their size and location, storage devices should be physically secured:

- small-size units in an office environment can be tethered to furniture or walls as well as being stored in locked cabinet or safes when not in use; or
- large-size units can be rack-mounted and resident in laboratory or data centres where they benefit from the security measures of the facility (e.g. locking covers or cages).

9.3 Protect physical interfaces to storage

Protecting the management interfaces from unauthorized access and reconnaissance is of paramount importance. Unauthorized access to management interfaces, occurring due to failure to implement appropriate controls, can result in data destruction, corruption, or denial of access.

Management interfaces for storage systems can take on several physical forms including serial ports, local area networks, modems, and even the technologies used for the data path (e.g. Fibre Channel). Hybrid interfaces (e.g. serial ports plugged into a console concentrator that provides an interface on a LAN) are also relatively common.

The controls related to protecting physical storage interfaces are as follows:

PC-PHYS-R01 Protect physical interfaces

To protect these physical interfaces, the organization shall:

- restrict physical access to management interfaces;
- disable and disconnect serial management ports when not in use;
- segregate LAN interfaces used for management from other LAN traffic, noting that physical isolation is preferred, but logical isolation (such as VLANs) is considered to be a best practice;
- disable modem ports when not needed.

9.4 Isolation of storage systems

Physical and logical isolation of storage devices (e.g. within a SAN) can also play an important role. The controls related to isolation of storage are as follows:

a) PC-PHYS-G03 Physically isolating storage systems

Physical isolation should be used to:

- segregate production from other system classes (e.g. quality assurance, development) including:
 - where possible, avoiding network connections between classes (e.g. a production server connected to both the production and development networks),
 - segregating networks and storage by class where appropriate,
 - physically separating systems in each class;
- isolate storage devices from other data centre devices, if practical.

b) PC-PHYS-G04 Logically isolating storage systems

Logical isolation should be used to:

- segregate storage traffic from normal server traffic using:
 - available network controls to create independent logical domains on common physical infrastructure,
 - trust and access controls to manage membership in the logical domains;
- segregate storage management traffic from all other traffic;
- configure network gateways for appropriate network segregation.

10 Technological controls for storage

10.1 General

Users can refer to the extensive set of physical controls listed in ISO/IEC 27002:2022, Clause 8. Some or all of these controls are relevant to storage systems and storage ecosystems.

10.2 Design and implementation of storage security

10.2.1 General

With enormous growth in volumes of critical data, many organizations have adopted storage-centric architectures for their ICT infrastructure. Consequently, storage security plays an important role in protecting this data, and in many instances, it serves as the last line of defence. The effectiveness of this storage security is often influenced by design considerations.

The controls related to storage design and implementation are as follows:

a) TC-DSGN-G01 Adhering to core security design principles

Designing and implementing storage security solutions requires adherence to core security design principles. In addition, the controls and guidance described in [Clauses 7, 8, and 9](#) should be integrated into the design and implementation of storage security solutions to counter applicable threats. Data sensitivity, criticality and value can also be an important consideration in designs (see [10.2.2](#)).

b) TC-DSGN-G02 Considering relevant threats in design