International Standard

ISO/IEC 27040

Second edition
2024-01

Information technology—Security techniques —Storage security

Technologie de I'information—Techniques de sécurité — Sécurité de stockage

Reference number
ISO/IEC 27040:2024(en)

ISO copyright office
CP 401·Ch.de Blandonnet 8
CH-1214 Vernier,Geneva
Phone:+41227490111
Email:copyright@iso.org
Website:www,iso.org

Published in Switzerland

Contents

Page

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 SC27,Information security,cybersecurity and privacyprotection.

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 moreclosely aligned with ISO/IEC 27002:2022;
- requirements have been added in Clauses Z,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 ofmedia,has been removed and texthas 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 informationor 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 thataddress 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/IEC27000 and the following apply.

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

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

— IECElectropedia: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)

国际标准

ISO / IEC 27040

信息技术-安全技术–存储安全

第二版2024-01

参考号码
ISO/IEC 27040:2024（中文）

内容

页面

前言

ISO（国际标准化组织）和IEC（国际电工委员会）组成了专门的全球标准化体系。作为ISO或IEC成员的国家机构通过各自组织建立的技术委员会参与国际标准的制定，以处理特定领域的技术活动。ISO和IEC技术委员会在共同感兴趣的领域进行合作。其他与ISO和IEC保持联系的政府和非政府国际组织也参与了这项工作。

ISO/IEC指令第1部分描述了用于开发本文件和进一步维护本文件的程序。特别要注意的是，不同类型的文件需要不同的批准标准。本文档按照ISO/ IEC指令第2部分的编辑规则起草（参见www.iso.org/directives或www.iec.ch/members experts/refdocs）。

ISO和IEC提请注意本文件的实施可能涉及使用(a)项专利。ISO和IEC对任何声称的专利权的证据、有效性或适用性不采取任何立场。截至本文件发布之日，ISO和IEC尚未收到实施本文件可能需要的专利通知。但是，实施者要注意，这可能不代表最新的信息，这些信息可以从www.iso.org/patents和https://patents.iec.ch上的专利数据库中获得。iso和IEC不负责识别任何或所有此类专利权。

本文件中使用的任何商品名称都是为方便用户而提供的信息，并不构成认可。

有关标准自愿性的解释，ISO与合格评定相关的特定术语和表达的含义，以及有关ISO遵守世界贸易组织（WTO）技术贸易壁垒（TBT）原则的信息，请参见www.iso.org/iso/foreword.html在IEC中，请参见www.iec.ch/understanding-standards。

本文件由ISO/IEC JTC 1信息技术分委员会SC27信息安全、网络安全和隐私保护起草。

第二版取消并取代了第一版（ISO/IEC 27040:2015），第一版在技术上进行了修订。

主要变化如下：

范围扩大到涵盖要求；

条款结构更接近ISO/IEC 27002:2022；在条款Z、9和10中增加了要求；

对所涵盖的存储技术进行了调整；增加了新的控制标签方案；

前附件A提供了对特定类型介质消毒的指导，已被删除，并在第10条款中添加了文本，建议为此目的使用IEEE 2883；

前附件B，其中包括有助于优先采用建议的表格，已被附件A取代，该附件A总结了本文件中包含的要求和指导；

在第10条中删除了提供教程材料的前附件C，并添加了对适当材料的参考。

关于本文档的任何反馈或问题应直接向用户所在的国家标准机构提出。这些机构的完整列表可以在www.iso.org/members.html和www.iec.ch/national-committees上找到。

信息技术-安全技术-存储安全

1范围

本文档提供了详细的技术要求和指导，说明组织如何通过采用经过充分验证的一致方法来规划、设计、编写文档和实现数据存储安全性，从而达到适当的风险缓解级别。存储安全既适用于存储在信息通信技术（ICT）系统中的数据，也适用于通过与存储相关的通信链路传输的数据的保护。存储安全包括设备和媒体的安全，与设备和媒体相关的管理活动，应用程序和服务，以及在设备和媒体的生命周期内以及结束使用或生命周期后控制或监视用户活动。

存储安全与任何参与拥有、操作或使用数据存储设备、媒体和网络的人都相关。这包括高级管理人员、存储产品和服务的采购人员以及其他非技术管理人员或用户，此外还包括对信息或存储安全、存储操作或负责组织整体安全计划和安全策略制定的管理人员和管理员。它也与任何参与存储网络安全体系结构方面的规划、设计和实施的人相关。

本文档概述了存储安全的概念和相关定义。包括典型存储场景和存储技术领域相关的威胁、设计和控制方面的要求和指导。此外，它还提供了对其他国际标准和技术报告的参考，这些标准和技术报告涉及可应用于存储安全的现有实践和技术。

2规范性参考

在本文中引用以下文件时，其部分或全部内容构成了本文件的要求。对于注明日期的参考文献，只适用所引用的版本。对于未注明日期的参考文献，引用文件的最新版本（包括任何修订）适用。

ISO/IEC 27000，信息技术-安全技术-信息安全管理系统-概述和词汇

3术语和定义

3.1总则

就本文件而言，ISO/IEC27000和以下给出的术语和定义适用。ISO和IEC在以下地址维护用于标准化的术语数据库：

—ISO在线浏览平台：athttps://www.iso.org/obp—

IECElectropedia:https://www.electropedia.org/

3.2存储技术相关术语

3.2.1
块
在存储设备（3.2.14）和存储介质（3.2.16）上存储（3.2.17）和检索数据的单元OISO/IEC

3.2.2
压缩
减少用于表示一项数据的位数

注1：对于存储（3.2.12），使用无损压缩（即使用保留原始数据的全部内容的技术进行压缩，并且可以从中精确地重构原始数据）。

3.2.3
静态数据
记录在稳定、非易失性存储器上的数据（3.2.11）

3.2.4
动态数据
数据从一个地方转移到另一个地方

注1：这些传输通常涉及可访问的接口，不包括内部传输（即从未暴露在接口、芯片或设备之外）。

3.2.5
重复数据删除
通过消除冗余数据来减少存储（3.2.12）需求的方法，将冗余数据替换为指向唯一数据副本的指针

注1：重复数据删除有时被认为是数据缩减的一种形式。

3.2.6
设备
具有特定用途的机械、电气或电子装置[来源：ISO/IEC 14776-

372:2011,3.1.10]

3.2.7
光纤通道
串行输入/输出互连能够支持多种协议，包括访问开放系统存储（3.2.12），访问大型机存储和网络

注1：光纤通道支持点对点、仲裁环路和交换拓扑，具有各种铜和光链路，运行速度从每秒1千兆位到每秒128千兆位以上。

3.2.8
光纤通道协议
串行小型计算机系统接口（SCSI）传输协议，用于光纤通道（3.2.7）互连

3.2.9
在规定
存储设备（3.2.14）使用的技术，其中可用存储介质（3.2.16）的子集通过接口暴露

注1：存储介质在存储设备内部独立使用，以提高性能、耐用性或可靠性。

3.2.10
网络附加存储
连接到网络并向计算机系统提供文件访问服务的存储设备（3.2.14）或系统

3.2.11
非易失性存储
在断电后仍能保留其内容的存储器（3.2.12）

3.2.12
存储
支持数据输入或检索的设备（3.2.6），功能或服务@ISO/IEC

3.2.13
存储区域网络
其主要目的是在计算机系统和存储设备（3.2.14）之间以及存储设备之间传输数据的网络

注1：存储区域网络由提供物理连接的通信基础设施和管理层组成，管理层组织连接、存储设备和计算机系统，以便数据传输是安全和健壮的。

3.2.14
存储设备
包含存储介质（3.2.16）的一个或多个设备（3.2.6）组成的组件或组件的集合，主要设计和构建用于访问非易失性存储（3.2.11）

3.2.15
存储生态系统
由相互依赖的组件组成的系统，这些组件协同工作以实现存储（3.2.12）服务和功能

注1：这些组件通常包括存储设备（3.2.14）、存储网络、存储管理和其他信息通信技术（ICT）基础设施

3.2.16
存储介质
记录或检索数字数据的材料

3.2.17
商店
在易失性存储器（3.2.20）或非易失性存储器（3.2.11）上记录数据

3.2.18
目标数据
服从于给定过程的信息，通常包括存储的大部分或全部信息（3.2.12）

3.2.19
虚拟化存储逻辑存储
物理存储设备（3.2.14）或存储介质（3.2.16）的抽象，它掩盖了物理存储（3.2.12）的特征和边界

注1：虚拟化存储可以在将虚拟化存储呈现给系统或应用程序之前采用多个级别的虚拟化。

3.2.20
易失性存储器
断电后无法保留内容的存储器（3.2.12）

3.3与卫生处理有关的术语

3.3.1
清晰
使用逻辑技术对所有可寻址存储位置上的用户数据进行消毒（3.3.12），以防止使用用户可用的相同主机接口进行简单的非侵入性数据恢复技术

3.3.2
消磁
通过向存储介质（3.2.16）施加具有组织批准的场强的强磁场，使磁性存储的数据不可读

3.3.3
自毁
使用物理技术消毒（3.3.12），使目标数据（3.2.18）无法使用最先进的实验室技术恢复，并导致随后无法使用存储介质（3.2.16）
用于存储（3.2.12）

注1:Disintegrate (3.3.5),incinerate (3.3.6),melt (3.3.7), powder (3.3.9), shred（3.3.13）是介质消毒（3.3.16）的破坏形式。

入境须知2：如果存储介质不能被移除，则存储设备（3.2.14）可以进行破坏技术；一个存储设备可以包含多个存储介质。

3.3.4
破坏
销毁（3.3.3）为确保存储介质（3.2.16）不能按原计划重复使用而采取的行动的结果，并且用户数据几乎不可能或代价高昂地恢复

3.3.5
分解
通过将存储介质（3.2.16）分离成其组成部分来破坏（3.3.3）

3.3.6
烧成灰
通过完全燃烧存储介质（3.2.16）来破坏（3.3.3）

3.3.7
融化
通过将存储介质（3.2.16）从固体状态变为液体状态，通常通过加热来破坏（3.3.3）

3.3.8
加密擦掉
一种消毒处理方法，对加密的目标数据（3.2.18）的加密密钥（3.3.12）进行消毒处理，使解密后的目标数据无法恢复

3.3.9
粉碎
将（3.3.3）存储介质（3.2.16）粉碎成粉末或适当的小颗粒

3.3.10
清洗
使用物理或逻辑技术对（3.3.12）进行消毒，使目标数据（3.2.18）的恢复无法使用最先进的实验室技术，但将存储介质（3.2.16）和存储设备（3.2.14）保持在潜在的可重用状态

3.3.11
卫生处理
消毒的过程或方法（3.3.12）

3.3.12
清洁
在给定的努力水平下，使访问存储（3.2.12）上的目标数据（3.2.18）变得不可行

3.3.13
分解
通过切割或撕裂存储介质（3.2.16）将其破坏（3.3.3）成小颗粒

3.3.14
存储卫生处理
逻辑存储消毒（3.3.15）或介质消毒（3.3.16）

3.3.15
逻辑存储卫生处理
虚拟存储清理处理
虚拟化存储（3219）的卫生处理（3311）

入口注1：清除（3.3.1）和清除（3.3.10）可用于净化（3.3.12）虚拟化存储的反应

注2：逻辑存储清理是存储清理的一个子集（3.3.14）

3.3.16
媒体卫生处理
存储介质（3.2.16）的卫生处理（3.3.11）

注1：清除（3.3.1）、吹扫（3.3.10）和销毁（3.3.3）是对存储介质（3.2.16）进行消毒（3.3.12）时可以采取的措施。

注2：介质卫生处理是存储卫生处理（3.3.14）的一个子集。

3.4与可用性有关的术语

3.4.1
弹性
预测和适应、抵御或迅速从潜在破坏性事件中恢复的能力，无论是自然的还是人为的

(来源:ISO 15392:2019, 3.21)

3.5与安全和密码学相关的术语

3.5.1
cryptoperiod
指定的一段时间，在这段时间内，特定的密码密钥被授权使用，或者在这段时间内，给定系统中的密码密钥可以保持有效

(来源:ISO 16609:2022, 3.6)

3.5.2
数据泄露
安全漏洞导致意外或非法破坏（3.3.4）、丢失、更改、
未经授权披露或访问传输、存储（3.2.17）或以其他方式处理的受保护数据

3.5.3
数据完整性
未以未经授权的方式更改或销毁数据的属性[SOURCE：ISO 7498-

2:1989,3.3.21]

3.5.4
多因素身份验证
身份验证使用以下两个或多个因素：-知识因素，个

人知道的事情；

—占有因素，个人拥有的东西；

-生物特征因子，个人正在或能够做的事情[SOURCE：

ISO 19092:2008,4.42]

3.5.5
恶意软件
恶意软件，专门用于破坏或破坏系统，攻击机密性、完整性和/或可用性

注1：病毒和特洛伊木马都是恶意软件的例子。(来源:ISO / IEC27033-1:2015, 3.22)

3.5.6
加密点
信息和通信技术基础设施中对数据进行加密的位置

注1：加密点仅适用于静态数据（3.2.3）。

3.5.7
安全力量
与破解密码算法或系统所需工作量相关的数字

3.5.8
存储安全
应用物理、技术和管理控制来保护存储系统和基础设施以及存储在其中的数据（3.2.17）

注1：存储安全的重点是保护数据（及其存储基础设施）免遭未经授权的披露、修改或破坏，同时确保授权用户可以使用数据。

注2：这些控制在性质上可以是预防性、侦查性、纠正性、威慑性、恢复性或补偿性。

3.5.9
强认证
通过加密衍生的多因素凭据进行身份验证[SOURCE：ISO 22600-1:2014,3.23]

3.6与存档和存储库相关的术语

3.6.1
存档
<组织>负责一个或多个档案（3.6.2）的选择、获取、保存（3.6.5）和可用性的组织或组织的一部分

[SOURCE：ISO 5127:2017,3.2.3.01，修改-条目1至4的注释已被省略；术语从复数“archives”改为单数；已添加域<组织>。]

操作
存档
<持有>个人、家庭或公共或私人组织在处理其事务时创造或收到的材料、物品、记录（3.6.6）或文件，并因其所包含的持久价值或作为其创建者的职能和责任的证据而保存，特别是那些使用出处、原始顺序和集体控制原则保存的材料

[SOURCE：IS05127:2017,3.6.1.03，修改-“项目、记录或文件”已包含在定义开头；条目注释1已被省略；术语从复数“archives”改为单数；添加了域名<holdings>。]

3.6.3
性格
与实施记录（3.6.6）保存（3.6.9）、记录销毁（3.6.7）或转移决定相关的记录过程范围，这些记录已记录在处置文件或其他文件中

[SOURCE：ISO 30300:2020,3.4.8，修改-“销毁”已更改为“记录销毁”]

3.6.4
证据
可以单独使用或与其他信息结合使用的信息，以建立对事件或行为的证据

[来源：ISO 30300:2020,3.2.6，修改-注1条目已被省略；“could”已更改为“can”]

3.6.5
保存
为长期保持记录（3.6.6）的可用性（3.6.10）、真实性、可靠性和完整性而采取的措施

注1：措施包括原则、方针、规则、战略、过程和运行。[SOURCE：ISO 30300:2020,3.4.11]

3.6.6
记录
组织作为证据（3.6.4）和资产创建或接收并保持的信息

注1：记录通常以复数形式使用。

注2：在实施管理体系标准（MSS）时，为实施和指导管理体系并将其实施形成文件而创建的记录称为形成文件的信息。

[SOURCE：ISO 30300:2020,3.2.10]

3.6.7
记录销毁
删除或删除一条记录（3.6.6），超出任何可能的重建

[SOURCE：ISO 30300:2020,3.4.7，修改-将术语“销毁”改为“记录销毁”]

3.6.8
记录要求
对业务功能、活动或交易的证据（3.6.4）和记录过程的要求，包括记录（3.6.6）需要保存的方式和时间

[SOURCE：ISO 30300:2020,3.3.2]

3.6.9
保留
根据记录要求（3.6.8）保持记录（3.6.6）[SOURCE：ISO 30300:2020,3.4.14]

3.6.10
可用性
能够被定位、检索、呈现和理解的属性

注1：可用性也可指系统、产品或服务在特定的使用环境中，为有效、高效和满意地实现特定目标而被特定用户使用的程度。

[SOURCE：ISO 30300:2020,3.2.12]

3.7杂项

3.7.1
带内
在先前建立的通信方法中发生的通信或传输
通道

注1：通信或传输通常采用单独协议的形式，例如在与主数据协议相同的介质上的管理协议。

3.7.2章
元数据
定义和描述其他数据的数据[SOURCE：

ISO/IEC11179-1:2023,3.2.26]

3.7.3
多租户
分配物理或虚拟资源，使多个租户及其计算和数据相互隔离并不可访问

[SOURCE：ISO / iec 22123-1:2023,3.4.3]

3.7.4
带外
发生在先前建立的通信方法或信道之外的通信或传输

3.7.5
安全的多租户
多租户类型（3.7.3），它采用安全控制来明确地防止数据泄露（3.5.2），并为适当的治理提供这些控制的验证

注1：当单个租户的风险状况不大于专用的单租户环境时，存在安全的多租户。

注2：在非常安全的环境中，甚至租户的身份也是保密的。

4符号和缩写

ACL访问控制列表

AES高级加密标准

API应用程序编程接口

BCM业务连续性管理

BMC底板管理控制器

CCM计数器用密码块链消息验证码

CDMI云数据管理接口

CHAP挑战握手认证协议

CLI命令行接口

CNA融合网卡

DAS直连存储

DDoS	分布式拒绝服务
DH-CHAP	Diffie Hellman-Challenge Handshake Authentication Protocol
DNS	域名系统
DoS	拒绝服务
DRAM	动态随机存取存储器
ESP	封装安全负载
FC	光纤通道
FC-SP	光纤通道安全协议
FCIP	通过TCP/IP的光纤通道
FCP	光纤通道协议
GCM	伽罗瓦/计数器模式
HBA	主机总线适配器
HDD	硬盘驱动器
HMAC	基于哈希的消息验证码
HTTPS	超文本传输协议安全
IB	InfiniBandTM
ICT	信息和通信技术
ID	标识符
IEEE	电气和电子工程师学会
IETF	互联网工程任务组
IKE	互联网密钥交换
IP	互联网协议
IPMI	智能平台管理接口
IPsec	互联网协议安全
IRBC	为业务连续性做好ICT准备
iSCSI	Internet小型计算机系统接口
主义	信息安全管理体系
不是	互联网存储名称服务
KMIP	密钥管理互操作协议
LAN	局域网
LUN	逻辑单元号

MTBF平均故障间隔时间

MTTF平均故障间隔时间

MTTR平均修复时间

NAS网络附加存储

NFS网络文件系统

NTP网络时间协议

NVM	非易失性内存
NVMe⑩	NVM浓咖啡
NVMe-oFTM	NVM Express over Fabric
NVMe@ / FC	NVMe@over光纤通道
RDMA NVMe⑧/	RDMA NVMe⑧在
NVMe@ / TCP	NVMe over TCP
OASIS	结构化信息标准促进组织
PCIe⑧	PCI Express@
PII	个人身份信息
RADIUS	远程认证拨入用户服务
RAID	冗余的arrayofindependent磁盘
RDMA	远程直接内存访问
REST	表征状态转移
RMCP	远程管理控制协议
SAN	存储区域网络
SCSI	小型计算机系统接口
SHA	安全哈希算法
SLP	服务定位协议
SMB	服务器消息块
SNMP	简单网络管理协议
SSD固态硬盘	固态硬盘
SSH	Secure Shell
TCP	传输控制协议
TLS	传输层安全
UDP	用户数据报协议

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。