

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-SS 数据存储安全管理体系认证规则及相关公示信息

中标华信（北京）认证中心有限公司认证规则公开方式或可获取的途径：本中心认证规则信息依法依申请公开，如需获取经备案的认证项目认证规则全文请发函至本中心邮箱 cshcc@cshcc.cn 或拨打电话 010-88255986 联系本机构技术信息部获取。

中标华信（北京）认证中心有限公司认证依据用标准或技术规范名称公开方式或可获取的途径：本中心按国家认监委要求备案及公示认证依据的封面和目录等关键信息，获取全文请购买和使用正版标准文件。

【认证规则、认证依据及认证证书公示信息及相关附件】

认证类别	认证领域	认证规则名称	认证规则编号	认证规则版本信息	状态标识	认证规则发布单位	认证规则发布/实施/修订日期	认证规则来源信息	认证依据用标准或技术规范名称	认证依据用标准或技术规范编号	认证依据用标准或技术规范发布单位	认证依据用标准或技术规范发布/实施日期	认证依据用标准或技术规范公开方式或可获取的途径	认证证书名称	认证证书与认证标志发布/所有权单位	认证证书样式
管理体系	其他管理体系	数据存储 安全管理 体系认证 规则	CSHCC- RZGZ-SS	B0	新建	中标华信 (北京) 认证中心 有限公司	20251215	自行 制定	信息技术 安全技术 储存安全	ISO IEC 27040: 2024	国际标准化组织； 国际电工委员会	20240126	见附页	数据存储 安全管理 体系认证 证书	中标华信 (北京) 认证中心 有限公司	见附页
									数据存储安全管理体系认证技术规范	CTS CSHCC012-2025	中标华信 (北京) 认证中心有限公司	20260101				



数据存储安全管理体系认证规则

文件编号：CSHCC-RZGZ-SS

文件版本：B0

编 制：李岩、金鹏

审 核：伍倩惠

批 准：刘伯钊

2025-12-15 发布

2026-01-01 实施

中标华信（北京）认证中心有限公司 发布

CSHCC-RZGZ-SS 数据存储安全管理体系认证规则

目 录

1. 适用范围	3
2. 对认证人员的基本要求	3
3. 初次认证程序	3
4. 监督审核程序	9
5. 再认证程序	10
6. 认证证书状态管理	11
7. 认证证书及认证标志要求	13
8. 与其他管理体系的结合审核	14
9. 其他	14
附录 A. 审核时间要求	15
附录 B. 修订记录	17



International Standard

ISO/IEC 27040

Second edition
2024-01

Information technology — Security techniques — Storage security

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

Reference number
ISO/IEC 27040:2024(en)

© ISO/IEC 2024

ISO/IEC 27040:2024(en)	
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

© ISO/IEC 2024 – All rights reserved

ISO/IEC 27040:2024(en)	
Contents	Page
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 CDMF 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

© ISO/IEC 2024 – All rights reserved

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-SS 数据存储安全管理体系认证规则及相关公示信息



国际标准

ISO/IEC 27040

信息技术 - 安全技术 - 存储安全

信息技术 - 安全技术 - 存储安全

第二版 2024-01

参考编号
ISO/IEC 27040:2024(en)

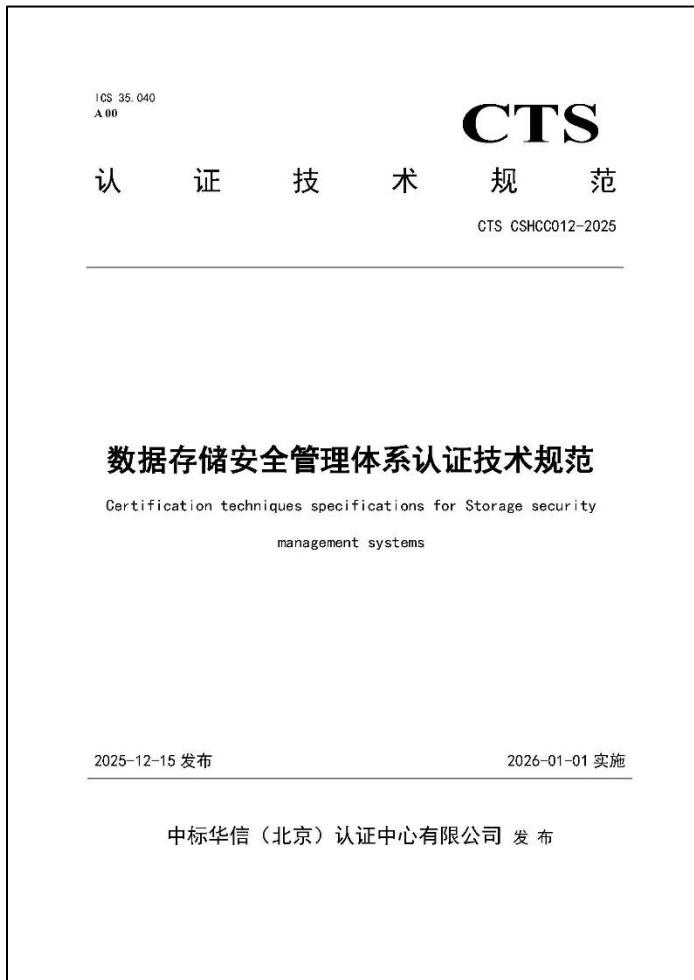
© ISO/IEC 2024

ISO/IEC 27040:2024(en)	
目录	页
前言	v
1 范围	1
2 规范性参考资料	1
3 术语和定义	1
3.1 一般	1
3.2 与存储技术有关的术语	1
3.3 与清理有关的术语	3
3.4 有关可用性的条款	5
3.5 与安全和密码学有关的术语	5
3.6 与档案馆和资料库有关的术语	6
3.7 其他术语	8
4 符号和缩略语	8
5 本文件的结构	11
5.1 总论	11
5.2 控制	11
6 概述和概念	11
6.1 总论	11
6.2 存储概念	12
6.3 存储安全简介	13
6.4 存储安全风险	15
6.4.1 背景介绍	15
6.4.2 数据泄露	16
6.4.3 数据损坏或损坏	16
6.4.4 暂时或永久丧失访问/可用性	17
6.4.5 云能满足法定、监管或法律要求	17
7 存储的组织控制	18
7.1 总论	18
7.2 调整存储和政策	18
7.3 业务连续性管理	18
7.4 合规性	19
8 存储的人员控制	20
9 存储的物理控制	21
9.1 总论	21
9.2 物理安全存储	21
9.3 保护存储的物理接口	21
9.4 限制对存储的访问	22
10 存储的技术控制	22
10.1 总论	22
10.2 设计和实施存储安全	22
10.2.1 总论	22
10.2.2 存储安全设计原则	22
10.2.3 存储系统质量属性	23
10.2.4 数据备份、保留和处置	25
10.3 存储系统设计	27
10.3.1 系统硬币	28
10.3.2 安全审计、预算和监控	28
10.3.3 存储漏洞管理	31
10.4 存储管理	31
10.4.1 行政情况	31
10.4.2 身份验证和授权	32

© ISO/IEC 2024 - 保留所有权利

ISO/IEC 27040:2024(en)	
10.4.3 痕迹管理接口安全	34
10.5 数据保密	35
10.5.1 一般服务	35
10.5.2 加密和密钥管理问题	36
10.5.3 存储加密	37
10.5.4 加密传输的数据	40
10.5.5 静态数据加密	41
10.6 仓库清理	42
10.6.1 一般	42
10.6.2 选择清理方法	43
10.6.3 基于介质的清理	44
10.6.4 逻辑清理	44
10.6.5 加密删除	45
10.6.6 核实储藏室清理情况	46
10.6.7 清理证明	47
10.7 直接连接存储	48
10.8 存储网络	48
10.8.1 背景介绍	48
10.8.2 存储区域网络	49
10.8.3 网络附加存储协议	54
10.9 基于块的存储	55
10.9.1 光纤通道(FC)存储	55
10.9.2 IP 存储	56
10.10 基于文件的存储	57
10.10.1 总论	57
10.10.2 基于 NFS 的 NAS	57
10.10.3 基于 SMB 的 NAS	58
10.11 云计算存储	59
10.11.1 确保云计算存储安全	59
10.11.2 CDMI 安全	59
10.12 基于对象的存储	60
10.13 减少数据	61
10.14 数据保护和恢复	62
10.14.1 总论	62
10.14.2 存储备份	62
10.14.3 存储复制	63
10.14.4 存储快照	63
10.15 数据档案和存储库	64
10.15.1 一般	64
10.15.2 数据档案	64
10.15.3 数据储存库	68
10.16 虚拟化	68
10.16.1 存储虚拟化	68
10.16.2 虚拟化系统的存储	69
10.17 安全多租户	70
10.18 安全的自旋数据移动	71
附件 A (信息性) 存储安全控制概要	73
参考项目	82

© ISO/IEC 2024 - 保留所有权利



CTS CSHCC012-2025

目录

1 范围	5
2 规范性引用文件	5
3 术语、定义和缩略语	5
4 组织环境	8
4.1 理解组织及其环境	8
4.2 理解相关方的需求和期望	8
4.3 确定管理体系范围	8
4.4 数据存储安全管理体系	8
5 领导作用	8
5.1 领导作用和承诺	8
5.2 方针	9
5.3 组织角色、责任和权限	9
6 策划	9
6.1 应对风险和机遇的措施	9
6.2 数据存储安全目标及其策划的实现	11
6.3 变更的策划	12
7 支持	12
7.1 意识	12
7.2 资源	12
7.3 能力	12
7.4 沟通	12
7.5 文件化信息	12
7.5.1 总则	12
7.5.2 创建和更新	13
7.5.3 文件化信息的控制	13
8 运行	13
8.1 运行策划和控制	13
8.2 数据存储安全管理内容结构	14
8.2.1 总则	14
8.2.2 控制	14
8.3 概述和概念	14
8.3.1 总则	14
8.3.2 存储概念	15
8.3.3 存储安全简介	16
8.3.4 存储安全风险	18

CTS CSHCC012-2025

8.4 存储的组织控制	21
8.4.1 总则	21
8.4.2 存储和政策的一致	21
8.4.3 业务连续性管理	22
8.4.4 合规性	22
8.5 存储的人员控制	23
8.6 存储的物理控制	24
8.6.1 总则	24
8.6.2 物理安全存储	24
8.6.3 保护存储的物理接口	24
8.6.4 存储系统的隔离	25
8.7 存储的技术控制	25
8.7.1 总则	26
8.7.2 设计和实施存储安全	26
8.7.3 存储系统安全	31
8.7.4 存储管理	35
8.7.5 数据保密	39
8.7.6 仓库清理	47
8.7.7 直接连接存储	52
8.7.8 存储网络	53
8.7.9 其他块的存储	61
8.7.10 基于文件的存储	62
8.7.11 云计算存储	64
8.7.12 基于对象的存储	65
8.7.13 数据缩减	66
8.7.14 数据保护和恢复	67
8.7.15 数据档案和存储库	69
8.7.16 虚拟化	74
8.7.17 安全多租户	76
8.7.18 安全的自主数据移动	77
9 绩效评价	78
9.1 监视、测量、分析和评价	78
9.2 内部审核	78
9.3 管理评审	79
10 改进	80
10.1 持续改进	80
10.2 不符合和纠正措施	80

