ISO/IEC 27040:2015

信息技术-安全技术-存储安全

Information technology — Security techniques — Storage security

(ISO /IEC 27040:2015)

目录

前言

ISO（国际标准化组织）和IEC（国际电工委员会）构成了全球标准化的专业体系。作为ISO或IEC成员的国家机构通过由各自组织建立的技术委员会参与国际标准的制定，这些委员会处理特定的技术领域活动。ISO和IEC技术委员会在共同感兴趣的领域进行合作。其他国际组织，政府和非政府组织与ISO和IEC保持联系，也参与其中的工作。在信息技术领域，ISO和IEC建立了一个联合技术委员会，即ISO/IEC JTC 1。

制定本文件的程序以及其进一步维护的程序在ISO/IEC准则第1部分中有所描述。特别要注意的是，不同类型的文件需要不同的批准标准。本文件是根据ISO/IEC准则第2部分的编辑规则草拟的（参见www.iso.org/directives）。

请注意，本文件的某些元素可能涉及专利权。ISO和IEC不负责识别任何或所有此类专利权。在文件制定过程中发现的任何专利权的详细信息将在引言和/或ISO收到的专利声明清单上列出（参见www.iso.org/patents）。

本文件中使用的任何商标名称均为为用户方便提供信息，并不构成认可。

关于ISO特定术语和与符合性评估相关的表达式的含义解释，以及有关ISO遵守《技术性贸易壁垒协议》中的WTO原则的信息，请参阅以下网址：前言 - 附加信息。

负责本文件的委员会是ISO/IEC JTC 1，信息技术，SC 27，安全技术委员会。

引言

许多组织面临着实施数据保护和安全措施的挑战，以满足广泛的要求，包括法定和监管合规性。然而，由于对存储技术的误解和有限的了解，或者在存储管理人员和管理员的情况下，对潜在风险或基本安全概念的认识有限，与存储系统和基础设施相关的安全往往被忽视。由于这种情况，数字资产不必要地面临着因数据泄漏、故意损坏、被勒索或其他恶意事件而受到威胁的风险。

数据存储在一个安全性在其历史上依赖于隔离连接、专用技术和数据中心的物理安全的环境中成熟。即使存储连接发展到使用诸如传输控制协议/互联网协议（TCP/IP）上的存储协议等技术，很少有用户利用其中固有的安全机制或建议的安全措施。

本国际标准为组织中的存储安全提供指导，特别支持根据ISO/IEC 27001的信息安全管理体系（ISMS）的要求。本国际标准推荐了ISO/IEC 27005中定义的信息安全风险管理方法。组织可根据ISMS的范围、风险管理的背景或行业部门等来定义其风险管理方法。在本国际标准描述的框架下，许多现有的方法可以用于实施ISMS的要求。

本国际标准与组织内有关信息安全风险管理的管理者和员工以及在适当情况下支持此类活动的外部方面有关。

本国际标准的目标如下：

- 帮助引起注意与风险相关的问题；
- 协助组织更好地保护其存储的数据；
- 为审计、设计和审查存储安全控制提供基础。

值得强调的是，ISO/IEC 27040提供了更详细的实施指导，涉及ISO/IEC 27002中基本标准化级别描述的存储安全控制。

应当注意，本国际标准不是监管和法律安全要求的参考或规范性文件。虽然它强调了这些影响的重要性，但由于这些要求依赖于国家、业务类型等情况，它不能具体说明它们。

信息技术-安全技术-存储安全

1 范围

本国际标准通过采用经过充分验证的一致方法来规划，设计，记录和实施数据存储安全性，为组织如何定义适当的风险缓解水平提供详细的技术指导。存储安全性适用于存储信息的保护(安全性)以及通过与存储相关的通信链路传输的信息的安全性。存储安全性包括设备和介质的安全性，与设备和介质相关的管理活动的安全性，应用程序和服务的安全性，以及在设备和介质的使用寿命期间以及使用结束后与最终用户相关的安全性。

存储安全性与参与拥有，操作或使用数据存储设备，介质和网络的任何人相关。这包括高级管理人员，存储产品和服务的接收者以及其他非技术经理或用户，以及对信息安全或存储安全，存储操作或负责组织整体安全性负有特定职责的经理和管理员。计划和安全政策的制定。它还涉及参与存储网络安全结构方面的规划，设计和实现的任何人。

本国际标准概述了存储安全性概念和相关定义。它包括与典型存储方案和存储技术领域相关的威胁，设计和控制方面的指导。此外，它还提供了其他国际标准和技术报告的参考，这些报告涉及可应用于存储安全的现有实践和技术。

2 规范性引用文件

以下文件的全部或部分内容在本文件中作了规范性引用，并且对于其应用是必不可少的。凡是注日期的引用文件，仅引用的版本适用。凡是不注日期的引用文件，其最新版本适用于引用文件(包括附议案修改)。ITU-TY.3500|ISO/IEC 17788：2014，信息技术-云计算-概述和词汇。

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

ISO/IEC 27001:2013，信息技术-安全技术-信息安全管理系统-要求

ISO/IEC 27005，信息技术-安全技术-信息安全风险管理

3 术语和定义

ISO / IEC 27000,ISO/IEC 27005中给出的术语和定义适用于本文件

3.1
块（block）
存储（3.50）和检索在磁盘和磁带设备（3.14）上的数据的单元。

3.2
清除（clear）
使用逻辑技术对所有用户可寻址存储位置上的数据进行消除（3.38），以保护免受简单的非侵入性数据恢复技术的影响，这些技术使用用户可用的相同接口。

3.3
压缩（compression）
去除数字数据中的冗余，以减少应存储（3.50）或传输的数据量。
[来源：ISO/TR 12033:2009，3.1]
注1：对于存储（3.43），需要使用无损压缩（即使用保留原始数据完整内容的技术进行压缩，并可从中完全重构原始数据）。

3.4
加密擦除（cryptographic erase）
一种清理（3.37）方法，其中针对加密目标数据（3.52）的加密密钥进行消除（3.38），使得无法恢复解密的目标数据（3.52）。

3.5
密钥周期（cryptoperiod）
授权使用特定加密密钥的定义时间段,或在此期间加密密钥在给定系统中保持有效的时间段。
[来源：ISO 16609:2004，3.9]

3.6
静态数据（data at rest）
存储在稳定的非易失性存储（3.30）上的数据。

3.7
数据泄漏（data breach）
导致受保护数据传输、存储（3.50）或其他处理的意外或非法破坏（3.13）、丢失、更改、未经授权的披露或访问的安全侵害。

3.8
动态数据（data in motion）
数据从一个位置传输到另一个位置。
注1：这些传输通常涉及可访问的接口，不包括内部传输（即不暴露给接口、芯片或设备的外部）。

3.9
数据完整性（data integrity）
数据未经未经授权的更改或破坏的属性。
[来源：ISO 7498- 2:1989，3.3.21]

3.10
去重（deduplication）
通过消除冗余数据的方法，减少存储（3.43）需求，并用指向唯一数据副本的指针替代。
注1：去重有时被视为一种压缩（3.3）形式。

3.11
消磁（degauss）
通过向介质施加强磁场，使数据无法读取。

3.12
摧毁（destruct）
使用物理技术进行消除（3.38），以使恢复变得不可行，使用先进的实验室技术，并导致媒体不能再用于数据的存储（3.43）。
注1：分解（3.15）、焚毁（3.21）、熔化（3.25）、粉碎（3.34）和撕毁（3.41）是清理（3.37）的销毁形式。

3.13
销毁（destruction）
采取措施确保媒体不能如原本意图那样重新使用，并且信息在实际上几乎不可能或成本过高地恢复。

3.14
设备（device）
具有特定目的的机械、电气或电子装置。
[来源：ISO/IEC 14776- 372:2011，3.1.10]

3.15
分解（disintegrate）
通过将介质分解成其组成部分，进行销毁（3.12）。

3.16
电子存储信息（Electronically Stored Information，ESI）
任何来源、任何类型的数据或信息，通过存储在任何电子介质上来证明其存在的时间性。
注1：电子存储信息（ESI）包括传统的电子邮件、备忘录、信件、电子表格、数据库、办公文档、演示文稿以及计算机上常见的其他电子格式。ESI还包括系统、应用程序和文件相关的元数据（3.26），如时间戳、修订历史、文件类型等。
注2：电子媒体
可以采取多种形式，但不限于存储设备（3.45）和存储元素（3.47）。

3.17
光纤通道（Fibre Channel）
串行I/O互连，支持多种协议，包括访问开放式系统存储（3.43）、访问主机存储（3.43）和网络。
注1：光纤通道支持点对点、仲裁环和交换拓扑，具有多种铜缆和光纤链路，速率从每秒1千兆位到超过10千兆位。

3.18
光纤通道协议（Fibre Channel Protocol）
用于光纤通道（3.17）互连的串行小型计算机系统接口（SCSI）传输协议。

3.19
网关（gateway）
将一个协议转换为另一个协议的设备（3.14）。

3.20
内带（in-band）
在先前建立的通信方法或通道内进行的通信或传输。
注1：通信或传输通常采用单独的协议，例如在主数据协议的相同媒介上进行管理协议。

3.21
焚毁（incinerate）
通过将介质完全燃烧成灰烬进行销毁（3.12）。

3.22
恶意软件（malware）
专门设计用于损坏或破坏系统、攻击机密性、完整性或可用性的恶意软件。
注1：病毒和木马是恶意软件的示例。
[来源：ISO/IEC 27033- 1:2009，3.22]

3.23
平均故障间隔时间（Mean Time Between Failures，MTBF）
系统或组件连续故障之间的预期时间。

3.24
平均修复时间（Mean Time To Repair，MTTR）
将故障的系统或组件恢复到正常运行状态的预期或观察持续时间。

3.25
熔化（melt）
通过应用热量，将介质从固态变为液态进行销毁（3.12）。

3.26
元数据（metadata）
定义和描述其他数据的数据。
[来源：ISO/IEC 11179- 1:2004，3.2.16]

3.27
多因素认证（multi-factor authentication）
使用以下两个或更多因素进行认证：
— 知识因素：“个体所知道的”；
— 持有因素：“个体所拥有的”；
— 生物特征因素：“个体所是或所能做的”。
[来源：ISO 19092:2008，4.42]

3.28
多租户（multi-tenancy）
分配物理或虚拟资源，使多个租户及其计算和数据彼此隔离和无法访问。
[来源：ITU-T Y.3500 | ISO/IEC 17788:2014，3.2.27]

3.29
网络附加存储（Network Attached Storage，NAS）

连接到网络并为计算机系统提供文件访问服务的存储设备（3.45）或系统。

3.30
非易失性存储（non-volatile storage）
断电后仍保留其内容的存储（3.43）。

3.31
带外（out-of-band）
在先前建立的通信方法或通道之外进行的通信或传输。

3.32
过量预分配（over provisioning）
存储元素（3.47）和存储设备（3.45）使用的一种技术，通过暴露可用介质的子集来提高性能、耐用性或可靠性。
注1：存储介质（3.48）在存储元素（3.47）内部独立使用，以改善性能、耐用性或可靠性。

3.33
加密点（point of encryption）
信息和通信技术（ICT）基础设施中的位置，在数据存储（3.43）过程中对数据进行加密，反之，在从数据存储（3.43）中访问数据时对数据进行解密。
注1：加密点仅适用于静态数据（3.6）。

3.34
粉碎（pulverize）
通过将介质研磨成粉末或尘埃进行销毁（3.12）。

3.35
清洗（purge）
使用物理技术进行消除（3.38），使恢复变得不可行，使用先进的实验室技术，并使存储介质（3.48）保持在可能可重用的状态。

3.36
可靠性（reliability）
系统或组件在规定条件下在指定时间段内执行其所需功能的能力。

3.37
清理（sanitization）

对数据进行消除（3.38）的过程或方法。

3.38
消除（sanitize）
对存储介质（3.48）上的目标数据（3.52）的访问变得对于给定的努力程度而言不可能。

注1：清除（3.2）、清洗（3.35）和销毁（3.12）是可以用于对存储介质（3.48）进行消除（3.38）的操作。

3.39
安全多租户（secure multi-tenancy）
多租户（3.28）的一种类型，采用安全控制明确防范数据泄漏（3.7），并对这些控制进行适当治理的验证。
注1：当个体租户的风险配置与专用的单租户环境中的风险配置相同时，存在安全多租户。
注2：在非常安全的环境中，甚至将租户的身份保密。

3.40
安全强度（security strength）
与破译加密算法或系统所需工作量相关联的数字。

3.41
撕毁（shred）
通过切割或撕碎介质成小颗粒进行销毁（3.12）。

3.42
单点故障（single point of failure）
系统的一个元素、组件的一个路径或一个系统，在其故障时，整个系统或一组系统将无法执行其主要功能。
注1：单点故障通常被视为与关键元素相关的设计缺陷。

3.43
存储（storage）
支持数据输入和检索的设备（3.14）、功能或服务。

3.44
存储区域网络（Storage Area Network，SAN）

其主要目的是在计算机系统和存储设备（3.45）之间以及存储设备（3.45）之间传输数据的网络。
注1：SAN包括通信基础设施（提供物理连接）和管理层（组织连接、存储设备（3.45）和计算机系统，以使数据传输安全稳定。

3.45
存储设备（storage device）
为数据存储（3.43）和交付而设计和构建的任何存储介质（3.48）或存储元素（3.47）的聚合。

3.46
存储生态系统（storage ecosystem）
相互依赖的复杂系统组件，共同实现存储（3.43）服务和功能。
注1：这些组件通常包括存储设备（3.45）、存储元素（3.47）、存储网络、存储管理和其他信息和通信技术（ICT）基础设施。

3.47
存储元素（storage element）
用于构建存储设备（3.45）的组件，有助于数据存储（3.43）和交付。
注1：存储元素的常见示例包括磁盘或磁带驱动器。

3.48
存储介质（storage medium）
存储（3.16）或可以记录电子存储信息（3.16）或数字数据的材料。

3.49
存储安全（storage security）
对存储系统和基础设施以及存储其中的数据应用物理、技术和管理控制，以保护数据，并确保其对授权用户的可用性。
注1：这些控制可能是预防性、检测性、纠正性、威慑性、恢复性或补偿性的。

3.50
存储（store）
将数据记录在易失性存储（3.53）或非易失性存储（3.30）上。

3.51
强认证（strong authentication）
使用基于密码学的派生凭证进行认证。

[来源：ISO/TS 22600- 1:2006，2.23]

3.52
目标数据（target data）
在给定过程中受到影响的信息，通常包括存储介质（3.48）上的大多数或全部信息。

3.53
易失性存储（volatile storage）
断电后失去其内容的存储（3.43）。

3.54
弱密钥（weak key）
与特定密码本身的定义相互作用的密钥，从而削弱了密码的安全强度（3.40）。

4 符号和缩写术语

ACE 访问控制项（Access Control Entry）
ACL 访问控制列表（Access Control List）
AD 活动目录（Active Directory）
AES 高级加密标准（Advanced Encryption Standard）
ATA 高级技术附件（Advanced Technology Attachment）
BC 业务连续性（Business Continuity）
BCM 业务连续性管理（Business Continuity Management）
CAS 内容寻址存储（Content Addressable Storage）
CBC 密码块链接（Cipher Block Chaining）
CCM 计数器与密码块链接消息认证码（Counter with Cipher block chaining Message authentication code）
CDMI 云数据管理接口（Cloud Data Management Interface）
CDP 连续数据保护（Continuous Data Protection）
CHAP 挑战-握手认证协议（Challenge Handshake Authentication Protocol）
CIFS 通用互联网文件系统（Common Internet File System）
CLI 命令行界面（Command Line Interface）
CNA 融合网络适配器（Converged Network Adaptor）
DAC 自主访问控制（Discretionary Access Control）
DAS 直接连接存储（Direct Attached Storage）
DDoS 分布式拒绝服务（Distributed Denial of Service）
DH-CHAP 迪菲-赫尔曼 - 挑战握手认证协议（Diffie Hellman - Challenge Handshake Authentication Protocol）

DES 数据加密标准（Data Encryption Standard）
DLM 数据生命周期管理（Data Lifecycle Management）
DMZ 非军事化区域（De-Militarized Zone）
DNS 域名系统（Domain Name System）
DoS 拒绝服务（Denial of Service）
DR 灾难恢复（Disaster Recovery）
DRP 灾难恢复规划（Disaster Recovery Planning）
EHR 电子医疗保健记录（Electronic Healthcare Record）
ESI 电子存储信息（Electronically Stored Information）
ESP 封装安全载荷（Encapsulating Security Payload）
FC 光纤通道（Fibre Channel）
FC-SP 光纤通道 - 安全协议（Fibre Channel - Security Protocol）
FCAP 光纤通道证书认证协议（Fibre Channel Certificate Authentication Protocol）
FCEAP 光纤通道可扩展认证协议（Fibre Channel Extensible Authentication Protocol）
FCIP 光纤通道通过TCP/IP（Fibre Channel over TCP/IP）
FCoE 光纤通道通过以太网（Fibre Channel over Ethernet）
FCP 光纤通道协议（Fibre Channel Protocol）
FCPAP 光纤通道密码认证协议（Fibre Channel Password Authentication Protocol）
FCS 固定内容存储（Fixed Content Storage）
FDE 全盘加密（Full Disk Encryption）
GCM 盖洛瓦/计数器模式（Galois/Counter Mode）
GUI 图形用户界面（Graphical User Interface）
HAMR 加热辅助磁记录（Heat Assisted Magnetic Recording）
HBA 主机总线适配器（Host Bus Adapter）
HDD 硬盘驱动器（Hard Disk Drive）
HTTPS 安全超文本传输协议（Hypertext Transfer Protocol Secure）
ICT 信息与通信技术（Information and Communications Technology）
ID 标识符（Identifier）
IDS 入侵检测系统（Intrusion Detection System）
IEEE 电气和电子工程师学会（Institute of Electrical and Electronics Engineers）
IETF 互联网工程任务组（Internet Engineering Task Force）
IKE 互联网密钥交换（Internet Key Exchange）
ILM 信息生命周期管理（Information Lifecycle Management）
I/O 输入/输出（Input/Output）
IP 互联网协议（Internet Protocol）
IPS 入侵防御系统（Intrusion Prevention System）
IPOCM 事件准备和运营连续性管理（Incident Preparedness and Operational Continuity Management）

IPsec 互联网协议安全（Internet Protocol Security）
IRBC 信息与通信技术的业务连续性准备（ICT Readiness for Business Continuity）
iSCSI 互联网小型计算机系统接口（Internet Small Computer Systems Interface）
ISL 交换机之间的连接（Inter-Switch Link）
ISMS 信息安全管理系统（Information Security Management System）
iSNS 互联网存储名称服务（Internet Storage Name Service）
KEK 密钥加密密钥（Key Encryption Key）
KMIP 密钥管理互操作性协议（Key Management Interoperability Protocol）
LAN 局域网（Local Area Network）
LBA 逻辑块地址（Logical Block Address）
LDAP 轻量级目录访问协议（Lightweight Directory Access Protocol）
LUN 逻辑单元（Logical Unit）
MAC 强制访问控制（Mandatory Access Control）
MD5 消息摘要算法5（Message-Digest algorithm 5）
MEK 媒体加密密钥（Media Encryption Key）
MTBF 故障间隔时间（Mean Time Between Failure）
MTTF 故障平均时间（Mean Time To Failure）
MTTR 平均修复时间（Mean Time To Repair）
NAS 网络附加存储（Network Attached Storage）
NAT 网络地址转换（Network Address Translation）
NFS 网络文件系统（Network File System）
NIC 网络接口卡（Network Interface Card）
NIS 网络信息服务（Network Information Service）
NPIV N端口ID虚拟化（N_Port_ID Virtualization）
NTLM NT LAN Manager
NTP 网络时间协议（Network Time Protocol）
NVM 非易失性存储器（Non-Volatile Memory）
OASIS 结构化信息标准推进组织（Organization for the Advancement of Structured Information Standards）
OID 对象标识符（Object IDentifier）
OSD 基于对象的存储设备（Object-based Storage Device）
PCIe 外围组件互连快速通道（Peripheral Component Interconnect express）
PII 个人身份信息（Personally Identifiable Information）
PKI 公钥基础设施（Public Key Infrastructure）
pNFS 并行网络文件系统（parallel Network File System）
PRNG 伪随机数发生器（Pseudo-Random Number Generator）
RADIUS 远程身份验证拨号用户服务（Remote Authentication Dial In User Service）
RAID 独立磁盘冗余阵列（Redundant Array of Independent Disks）

RAM 随机存取存储器（Random Access Memory）
RBAC 基于角色的访问控制（Role-Based Access Control）
REST 表述性状态转移（REpresentational State Transfer）
RNG 随机数生成器（Random Number Generator）
ROM 只读存储器（Read-Only Memory）
RPC 远程过程调用（Remote Procedure Call）
SAN 存储区域网络（Storage Area Network）
SAS 串行附加SCSI（Serial Attached SCSI）
SCSI 小型计算机系统接口（Small Computer System Interface）
SED 自加密驱动器（Self-Encrypting Drive）
SHA 安全哈希算法（Secure Hash Algorithm）
SIEM 安全信息与事件管理（Security Information and Event Management）
SLP 服务定位器协议（Service Locator Protocol）
SMB 服务器信息块（Server Message Block）
SMI-S 存储管理倡议 – 规范（Storage Management Initiative – Specification）
SNIA 存储网络行业协会（Storage Networking Industry Association）
SNMP 简单网络管理协议（Simple Network Management Protocol）
SOHO 小型办公室/家庭办公室（Small Office/Home Office）
SSC 安全子系统类（Security Subsystem Class）
SSD 固态硬盘（Solid State Drive）
SSH 安全外壳协议（Secure SHell）
SSHD 固态硬盘驱动器（Solid State Hard Drive）
SSO 单点登录（Single Sign-On）
TCG 可信计算组织（Trusted Computing Group）
TCP 传输控制协议（Transmission Control Protocol）
TLS 传输层安全（Transport Layer Security）
UDP 用户数据报协议（User Datagram Protocol）
USB 通用串行总线（Universal Serial Bus）
VLAN 虚拟局域网（Virtual Local Area Network）
VM 虚拟机（Virtual Machine）
VSAN 虚拟存储区域网络（Virtual Storage Area Network）
VPN 虚拟专用网络（Virtual Private Network）
WAN 广域网（Wide Area Network）
WORM 只写不读（Write Once Read Many）
WWN 世界范围名称（World Wide Name）
WWPN 世界范围端口名称（World Wide Port Name）
XEX 异或-加密-异或（Xor-Encrypt-Xor）

XTS 基于XEX的代码本模式（XEX-based Tweaked-codebook mode with ciphertext Stealing）

5 概述与概念

5.1 总则

计算机数据存储或信息存储通常被称为存储，指的是计算机组件、存储元素、存储设备和存储介质，用于保留电子存储信息（ESI）或数字数据。虽然存在易失性和非易失性存储形式，但这个国际标准主要关注非易失性存储。存储是计算机的核心功能和基本组成部分。

为了保护存储基础设施，必须对存储技术和概念有清晰的理解。此外，对于安全控制的类型以及它们如何影响和与存储技术相互作用，也非常重要。最后，对于这个基础设施面临的威胁以及由这些威胁产生的主要风险，都必须考虑在保护存储基础设施或个别存储系统的努力中。

5.2 存储概念

在过去，存储仅被视为连接到计算机以存储数据的硬盘驱动器（HDD）和磁带驱动器。这种方法通常称为直接连接存储（DAS），在企业数据中心以及小型办公室/家庭办公室（SOHO）环境中仍在使用。随着高度复杂的技术可用于提供管理、连接、保护、安全、共享和优化数据存储的解决方案，基于网络技术的备用方法也出现了。随着存储技术从非智能的内部和外部DAS演变为智能网络存储，这些解决方案变得更加可行和具有成本效益。在这些解决方案中使用网络增加了攻击面，需要额外关注其安全性。

当代存储解决方案包括以下一些或所有元素：
- 带有存储网络接口的存储阵列；
- 网络附加存储（NAS）；
- 可寻址内容存储（CAS）；
- 基于对象的存储设备（OSD）；
- 备份/恢复系统，连续数据保护（CDP）等（即数据保护系统）。

在企业级和中档计算环境中，存储已成为信息与通信技术（ICT）基础设施中显著而独立的层。这些环境对存储的需求通常超出了简单的数据存储能力。推动新存储技术涌现的应用和功能的例子包括：
- 通过网络在多个系统之间共享大量存储资源（以PB和EB为单位）；
- 不需要使用局域网（LAN）的备份；

- 对关键业务数据进行远程、容灾性的在线镜像；
- 将容错应用和相关系统聚集在单个数据副本周围；
- 长期保留敏感或高价值的业务信息；
- 分布式数据库和文件系统；
- 支持法规和法律合规性要求；
- 支持集中的数据存储库用于快速恢复（例如备份）和归档。

5.3 存储安全简介

存储安全涉及与第5.2节中所述存储系统和基础设施相关的物理、技术和行政控制，以及预防性、检测性和纠正性控制。存储安全还可以引入特定的技术，例如：

- 介质消毒；
- 虚拟化安全；
- 自加密存储设备（见C.3），如HDD、固态硬盘（SSD）和固态硬盘（SSHD）；
- 密钥管理服务；
- 数据真实性和完整性服务；
- 数据传输时的保护（加密和数据压缩）；
- 目录服务和其他用户管理系统。

为了更好地理解存储的安全问题和影响，人们应该了解存储技术的使用方式和原因。以下是一些起点考虑的因素：

- 存储系统可以作为存储网络中的节点，这些网络可以基于各种技术，如传输控制协议/互联网协议（TCP/IP）、光纤通道（FC）、以太网上的光纤通道（FCoE）和InfiniBand。潜在的威胁因网络技术和拓扑结构的不同而有显著差异。
- 存储的数据通常表示为块数据或文件/对象，并以此进行访问；这两种存储方法之间存在显著差异。同样，与每种方法相关的安全措施可能存在根本性的差异，特别是在访问控制、加密和数据完整性方面。
- 在正常的存储操作中，许多存储设备类型具有比接口暴露出来的更多的内部媒体功能。SSD和SSHD通常是过度配置的，内部可能会在物理媒体区域之间移动数据以提高写入延迟。HDD通常含有备用区域，当出现临时访问问题时，数据可能会在物理媒体区域之间进行内部移动。即使设备通过接口进行写入，用户数据可能仍然存在于这些区域中。此类设备可能无法通过接口进行覆盖清除。
- 存储管理既是存储基础设施的一部分，也是许多系统上执行的操作。通常会有特权用户应用配置更改、配置存储、调整、监控等操作于该基础设施上。某些管理操作可以远程执行，还可能涉及第三方，如供应商支持人员。
- 数据可用性和完整性是组织存储架构的关键因素，因此安全性应该与之相辅相成，而不是相互制衡，并且不能通过引入瓶颈和附加的单点故障来否定高可用性措施。

- 许多组织实施复杂的数据弹性策略，这是其灾难恢复（DR）和业务连续性（BC）计划的一部分。必须小心实施诸如静止数据加密之类的安全机制，以确保不会影响弹性策略。
- 存储中的虚拟化可以采取许多形式，并且可以在存储基础设施的不同点实施。这种虚拟化可以隐藏与存储呈现相关的物理细节（例如，对服务器的逻辑单元或文件系统进行呈现）、隐藏设备的真实容量、执行基于策略的自主数据移动（如分层存储）或完全抽象化存储基础设施（如云计算存储）。要使安全性和虚拟化共存，需要仔细规划和选择合适的技术。
- 一些组织的数据增长速度正在推动对数据存储技术的增加使用。为了避免额外采购存储，组织正在采用数据压缩和去重等数据减少技术。然而，这些数据减少技术可能受到静止数据加密机制的影响，并且反过来可能会在灾难恢复和业务连续性操作中引入数据完整性问题。
- 作为正常数据保护策略的一部分，会创建许多数据副本（例如，在系统和站点之间复制、备份、快照等）。在使用期间必须适当地保护这些副本，并在其使用价值结束时进行适当的消毒。
- 在系统之间传输敏感和高价值数据时，通常需要进行保护，使用的机制可以包括Internet协议安全（IPsec）。IPsec可能会对某些技术（如网络地址转换（NAT）、入侵检测系统（IDS）、入侵防御系统（IPS）或其他深入分析网络流量的系统）产生不利影响。是否依赖IPsec或其他传输保护协议可能取决于可能抵消其他技术价值的权衡，以及在网络中的部署位置。

— 许多组织正在实施静止数据加密以保护敏感和高价值数据。具体的加密机制和加密点是实际数据保护以及满足合规要求的重要因素。

— 成功使用加密往往取决于在其整个生命周期内对密钥材料进行正确的管理。这包括正确生成密钥、安全存储和传输密钥材料、将密钥复制作为正常策略的一部分，以确保数据的可用性，并在不再需要时适当地处置密钥材料。要保护的数据的敏感性和重要性也可能影响密钥管理方法。

确保当前和新兴存储技术上存储和访问的数据具有足够的保密性、完整性和可用性，需要在ICT的这一层中进行协调的努力。其中许多安全工作将集中在以下方面：

— 保护存储管理（操作和接口）；
— 确保足够的凭据和信任管理；
— 保护数据备份和恢复资源；
— 数据在传输中的保护；
— 数据静态保护；
— 数据可用性保护；
— 灾难恢复和业务连续性支持；
— 适当的消毒和处置；
— 安全的自主数据移动；
— 安全的多租户。

5.4 存储安全风险

5.4.1 背景

存储安全风险是由组织对特定存储系统或基础设施的使用而产生的。存储安全风险源于：
a）针对存储系统和基础设施处理的信息的威胁；
b）脆弱性（技术和非技术）；以及
c）威胁成功利用脆弱性的影响。
风险管理是信息安全的一个关键概念。根据ISO/IEC 27005，“信息安全风险管理过程可应用于整个组织、组织的任何离散部分（例如部门、实体位置、服务）、任何现有或计划中的信息系统或特定的控制方面（例如业务连续性计划）。” ISO/IEC 27005中提出的信息安全风险管理过程包括上下文建立、风险评估、风险处理、风险接受、风险沟通以及风险监测和审查。
存储系统和基础设施的威胁包括但不限于：
— 未经授权的使用；
— 未经授权的访问；
— 由于违反监管合规性而导致的责任；
— 对存储的拒绝服务（DoS）和分布式拒绝服务（DDoS）攻击；
— 数据损坏/修改和数据破坏；
— 数据泄漏/违规；
— 媒体丢失或意外丢失；
— 恶意软件攻击或引入；
— 终止使用后的不当处理或消毒。
这些威胁可能导致各种各样的风险。然而，对于存储系统和基础设施来说，与数据泄露、数据损坏或破坏、临时或永久性的访问/可用性丧失以及未能满足法定、监管或法律要求相关的风险是主要的关注点。

5.4.2 数据泄露

数据泄露可能是安全妥协的结果，并且可能采取多种形式。未经授权访问或披露受保护信息是两种常见认可的数据泄露形式，但重要的是要理解，较少人知道的形式可能包括意外或非法销毁、丢失或更改数据。
根据涉及的信息量和类型（例如个人身份信息、受保护的健康信息等）以及适用的法律法规，数据泄露可能会使组织面临很大风险，包括调查数据泄露所需的成本、向受影响的个人进行必要的通知、诉讼费用、监管罚款和其他法律处罚，以及因数据泄露公开披露而造成的品牌损害。
对于失去自己或他人受保护信息的实体，存在经济和安全风险，因为信息的丢失可能包括以下内容：

— 机密信息（例如密码、加密密钥等）；
— 知识产权或其他敏感的商业信息；
— 可以识别个人的信息（PII）；
— 金融账户或记录信息；
— 可以识别个人的健康记录信息。

寻求这些泄露或溢出信息的不受信任或未经授权的实体可以来自广泛的来源，资金充足且动机各异。

表1总结了更有可能发生的基于存储的安全威胁，并列出了可能由这些妥协造成的数据泄露形式。

表1 — 存储相关的数据泄露

安全威胁	潜在的数据泄露形式
存储元件或媒体被盗	非法访问、非法披露、非法数据丢失、非法数据销毁
存储元件或媒体丢失	未经授权访问、未经授权披露、意外数据丢失、意外数据销毁
数据丢失	非法、未经授权或意外数据销毁或破坏
被授权人员意外更改配置（例如存储管理、存储/网络资源、不正确的补丁管理等）	意外访问、意外披露、意外数据销毁、意外数据更改
恶意配置更改（存储管理、存储/网络资源、应用程序篡改等）由外部或内部对手	非法访问、非法披露、非法数据销毁、非法数据更改
授权用户滥用特权 (例如不恰当的数据窥探)	非法/未经授权访问或披露
恶意数据篡改由外部或内部对手	非法数据销毁或更改
拒绝服务攻击	非法数据销毁、丢失或更改
恶意监控网络流量	非法/未经授权披露

5.4.3 数据损坏或销毁

数据损坏是由人为、硬件和软件错误引起的计算机数据（即原始数据的意外更改）的恶化或损坏。它可能发生在写入、读取、存储、传输或处理过程中。数据损坏可能仅影响数据或元数据的一小部分，但这在适当条件下可以进行恢复；如果根本原因得不到解决，它也可能导致永久数据丢失。另一方面，数据销毁导致数据丢失，如果没有采取数据备份等数据保护机制，这种丢失可能是永久的。数据损坏和销毁都可能是无意或有意事件的结果，在后一种情况下，它们可以进一步被归类为恶意或非恶意。

事件，如火灾、洪水、停电、编程错误和用户错误，都是数据损坏和销毁的一般性、非故意的例子。背景辐射、磁头碰撞以及存储硬件的老化或磨损是更加存储中心化的其他问题来源。基于硬件的数据损坏通常可以通过使用校验和进行检测，并且通常可以通过使用纠错码进行纠正，但是如果存储管理不当，这些"悄悄纠正"可能会导致其他问题（即，暂时可纠正的错误可能会随着存储设备或媒体的恶化而变为永久性错误）。

恶意性质的故意攻击/事件可能由外部方或内部人员实施，目的是使部分或全部受影响的数据无法使用或被销毁。在这种情况下，"无法使用"可能意味着未经授权的修改已经应用，存在可疑的修改，或者数据可以被未知的密钥或机制加密。非恶意攻击通常由于粗心、缺乏知识或故意绕过安全措施而发生，比如出于完成任务的目的，但对数据的影响可能与恶意攻击一样具有破坏性。

采用适当的机制来检测和修复数据损坏是保持数据完整性的重要途径。同样，利用数据保护机制来检测数据丢失并恢复这些数据可以防范数据的完全丢失。

5.4.4 临时或永久性的访问/可用性丧失

可用性涉及确保对存储元素、存储网络元素、存储信息、信息流、服务和应用程序的授权访问1）不受限制或受到有限的拒绝。一般来说，数据可用性是通过数据存储的冗余性和可访问性的实现来实现的。

可用性丧失通常可以归因于以下一个或多个问题：
- 可靠性；
- 可访问性；
— 及时性。

5.4.5 未能满足法定、监管或法律要求

组织可能因未遵守法定、监管或法律要求而承担重大责任和处罚。不同司法管辖区的要求可能有很大差异，对于跨国组织来说，各国特定的立法对信息安全要求有更大的影响。

常见的合规问题包括：
- 违反特定国家的隐私要求；
- 非法转移数据（即将受限制的数据移出特定管辖区）；
- 违反保密性；
- 不符合组织的政策（例如，消除数据的操作）；
- 数据保留和保护不足；
- 安全证据不足（例如，审计日志，加密/消除的证明等）。

这些不合规问题可能导致昂贵的制裁和整改（例如，数据泄露通知）。

6 支持控制

6.1 总则

第6条提供了支持存储安全技术架构及其相关技术控制以及其他控制（技术和非技术控制），这些控制不仅适用于存储。关于许多此类控制的信息可以在ISO/IEC 27002中找到。下面的6.2到6.8条对于使用存储特别重要的控制进行了详细阐述。它们涉及保护直接连接存储、存储网络、存储网络安全管理、不同类型存储（块存储、文件存储和对象存储）的技术控制以及存储安全服务。数据的敏感性、重要性和价值在选择和使用控制时也可能是一个重要考虑因素，因此还应查阅附录B，特别是B.1.2。

6.2 直接连接存储（DAS）

直接连接存储设备是一种存储元素（例如硬盘驱动器、磁带等），直接连接到计算机而没有存储网络介于其中（即两者之间没有类似集线器、路由器或交换机的网络设备）。DAS设备可以是内部存储（即计算机系统的组成部分）或外部存储（即辅助存储）。此外，它们通常专用于与之连接的系统；一个DAS设备可以在多台计算机之间共享，只要它提供多个接口（端口）以允许并发和直接访问。

这些存储元素具有有限的数据访问和管理接口（后者通常是带内的）。因此，保护DAS的选项往往是有限的，包括：

- DAS通常在物理上较小，并且可能位于办公环境中，可能受到恶意攻击（例如被盗、毁坏、未经授权访问等），因此应该进行物理安全保护。
- 为了防止对DAS上的敏感和高价值数据的未经授权访问，应使用某种形式的加密来保护数据的静态存储，包括：
- 集成了加密和访问控制功能的存储元素，也称为自加密驱动器（SEDs）。
- 计算机或应用程序加密，包括全盘加密（FDE）。
- 对所有涉及敏感或高价值数据的DAS，应使用媒体消除（参见6.8.1.2和附录A获取更多信息），可以采用以下任一方法：
  - 使用存储元素中集成的消除功能；
  - 使用基于计算机或应用程序的消除。
- 如有可能，应使用认证（例如Fibre Channel - 安全协议 - 22）（FC-SP-2）的认证-A认证（参见C.7.2）来防止对敏感和高价值数据的未经授权访问。
- 为了防范意外或故意的数据丢失或损坏，应定期对DAS的内容进行备份。

6.3 存储网络

6.3.1 背景

除了DAS可能有例外外，网络在存储基础设施中扮演着重要角色，这些网络可以包括常见的网络技术（例如局域网和广域网），使用这些技术的存储特定网络协议，以及存储特定技术（例如光纤通道）。对于前者，在ISO/IEC 27033提供的安全指南对于保护使用这些技术的存储资源至关重要。存储特定的网络协议和技术在本国际标准中进行了介绍。

存储系统使用网络主要用于三个目的：1）存储和检索数据，2）数据保护，3）存储系统管理。这些用途并未强制要求采用特定的网络技术或方法。例如，某些存储管理可以通过与服务器用于访问数据的相同光纤通道接口（即带内）执行，同时还可以通过TCP/IP连接到存储系统的管理接口执行。

6.3.2 存储区域网络（SAN）

6.3.2.1 总则

存储区域网络（SAN）是一种专用的高速网络，为存储提供块级别的网络访问。SAN通常由服务器、交换机、存储元素和存储设备组成，它们使用各种技术、拓扑和协议进行连接。SAN也可以跨越多个站点。

SAN通常用于提高应用程序可用性（例如多个数据路径）、提高应用程序性能（例如卸载存储功能、使用独立的网络等）、增加存储利用率和效率（例如合并存储资源、分层存储等）以及改善数据保护和安全性。此外，SAN通常在组织的灾难恢复和业务连续性活动中发挥重要作用（参见图1）。

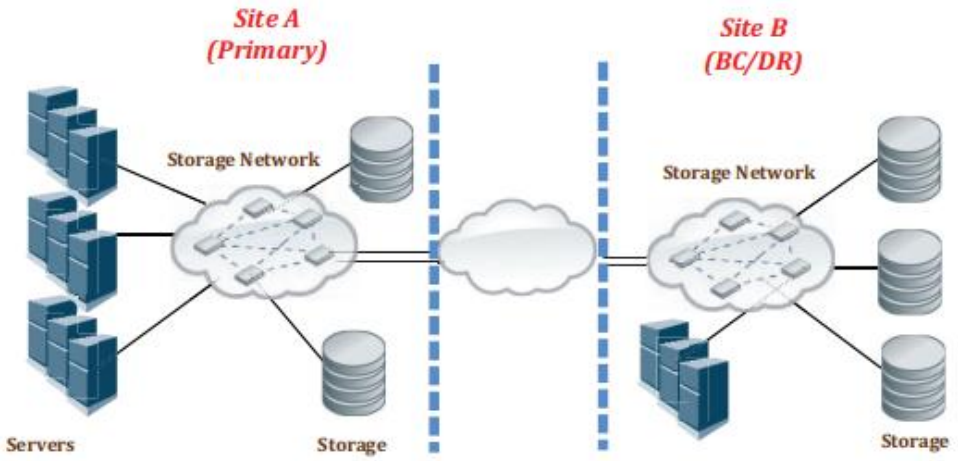


图1 存储区域网络（SAN）示例
Figure 1 — Storage Area Network (SAN) example

SAN（存储区域网络）向服务器操作系统呈现存储设备（如磁盘阵列和磁带库），使服务器看起来存储似乎是本地连接的。通过使用不同类型的虚拟化，可以实现将存储简化呈现给服务器的目的。

SAN通常基于光纤通道（FC）技术，该技术利用光纤通道协议（FCP）用于开放系统，利用专有变体用于主机。此外，使用以太网上的光纤通道（FCoE）可以将FC流量传输到现有高速以太网基础架构，并将存储和IP协议融合到单个电缆传输和接口中。其他技术，如用于小型和中型组织的Internet Small Computing System Interface（iSCSI）作为比FC更便宜的选择，以及在高性能计算环境中常用的InfiniBand，也可以被使用。利用扩展器和交换机的串行连接SCSI（SAS）和外围组件互连（PCIe）等互连技术也开始拥有SAN的特征。此外，通过使用网关，还可以在不同的SAN技术之间传输数据（参见图2）。

与SAN相关的安全控制被分为以下几类：
- 访问控制：通过应用区域划分、逻辑单元（LUN）掩码和端口绑定机制实现SAN的访问控制。
- 端口绑定：在SAN中使用全球唯一标识符（WWN）来进行识别。端口绑定是一种SAN安全机制，它将物理端口ID与连接设备的WWN关联起来。此关联可以减轻潜在对手的监听尝试，因此应尽可能使用。
- 区域划分：SAN布局可以划分为不同的区域，以限制特定服务器和存储设备对SAN的可见性。软区域划分基于将SAN布局名称服务器响应限制为基于服务器不会通过名称服务器联系未被发现的存储设备的假设。硬区域划分使用SAN交换机上的物理端口号来限制流量转发，是一种更安全的区域划分方法，因为它不依赖于正确的服务器行为，特别是不容易受到伪造服务器身份的攻击。

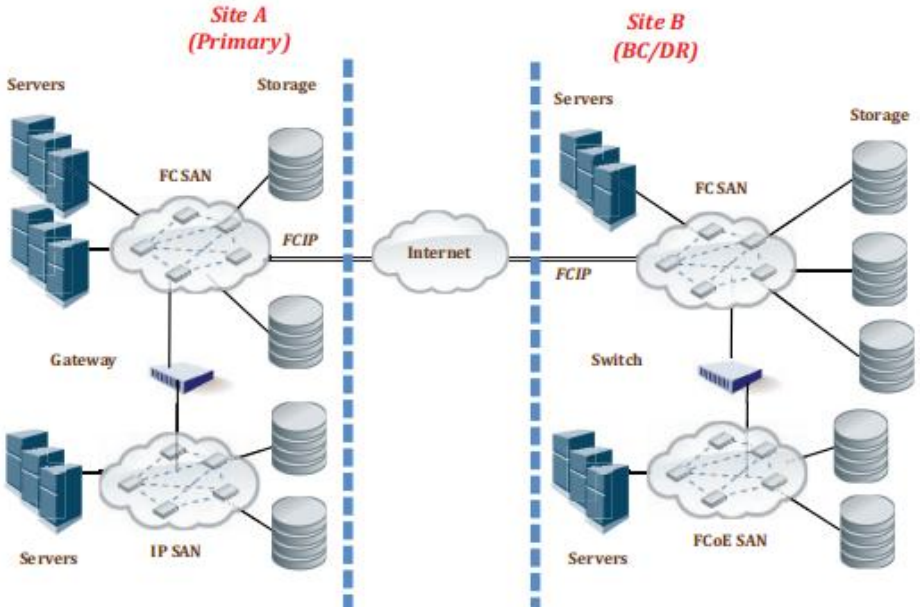


图2-存储区域网络（SAN）示例
Figure 2 — Storage Area Network (SAN) example

-LUN掩码和映射：存储设备可以被划分为不同的逻辑单元（LUNs），每个LUN由逻辑单元号码进务器能够看到一个LUN，而使其他服务器看不到该LUN。

- 认证：对于SAN来说，交换机需要验证与其通信的SAN中其他交换机的身份。如果未实施交换机认证，恶意交换机可能加入SAN并潜在地危害SAN数据。同样，SAN中的节点（如存储设备和服务器）需要使用认证来防范数据泄露。

- 加密：SAN中数据的机密性有两个主要组成部分：1）数据在传输时的状态（数据在运动中）；2）数据在存储设备上的状态（数据静止状态）。敏感和高价值的数据在在运动中和在存储设备上时都需要进行加密保护。这可能需要使用专用硬件来加密发送到存储设备的数据。更多有关在传输时保护数据的指导信息请参阅6.8.2.2，有关在存储设备上保护数据的指导信息请参阅6.8.2.3。

深度防御策略（参见7.2.1）有助于减轻与一个安全控制失败（可能导致单点故障）可能损害受保护资产的风险。
物理和逻辑隔离在SAN中的存储元素中也起着重要的作用，可以采取以下形式：
- 物理隔离包括：
  - 将生产环境与其他系统类别（例如质量保证、开发）隔离开；
  - 在可能的情况下，避免类别之间的网络连接（例如生产服务器同时连接到生产和开发网络）；
  - 适当时通过类别对网络和存储进行隔离；
  - 在每个类别中对系统进行物理分隔；
  - 如可行，将存储设备与其他数据中心设备隔离。
- 逻辑隔离包括：
  - 使用可用的网络控制在共同的物理基础设施上创建独立的逻辑域，将存储流量与普通服务器流量隔离开；
  - 使用信任和访问控制来管理逻辑域的成员资格；
  - 将存储管理流量与所有其他流量隔离开；
  - 确保网络网关的配置维持适当的网络隔离。

6.3.2.2 光纤通道SAN

光纤通道是一种用于块存储的多千兆速度网络技术。有三种主要的光纤通道拓扑结构，描述了如何将多个端口连接在一起：点对点（两个设备直接连接）、仲裁环和交换结构。从安全的角度来看，交换结构拓扑和光纤通道协议（FCP）（是用于在该网络技术上传输SCSI流量的接口协议）更为有趣。

管理员应采取以下措施：

– 控制FCP节点访问，包括：
– 使用访问控制列表（ACLs）、绑定列表和FC-SP-2交换机策略（见C.7.1）等技术限制交换机上的服务器访问；
– 使用启用了NPIV（N_Port_ID虚拟化）的HBA为虚拟服务器分配单独的N_Port_IDs。
– 实施基于交换机的控制，包括：
– 使用ACLs、绑定列表和FC-SP-2交换机策略（见C.7.1）等技术限制交换机之间的连接；
– 在FC SAN布局中应使用区域划分，并优先考虑硬区域划分；
– 确定基本区域划分是否是目标环境的足够强大的安全措施，如果不是，则在供应商支持的情况下使用更强大的技术，例如FC-SP区域划分（见C.7.5）；
– 禁用未使用的端口；
– 谨慎使用默认区域和区域集（假设最小权限原则）。
– 通过配置交换机、扩展器、路由器和网关来安全地互联存储网络，以满足要求。
子条款6.5.1提供了有关基于块的光纤通道存储的指导。

6.3.2.3 IP SAN

Internet SCSI（iSCSI），在IETF RFC 3720中进行了描述，它是一种运行在TCP上的连接导向的命令/响应协议，用于访问磁盘、磁带和其他设备。
通过以下方式控制iSCSI网络访问和协议：
– 避免将iSCSI接口连接到通用LAN，进行安全性和性能上的隔离；
– 在不能使用物理隔离的情况下，使用虚拟局域网（VLANs）。

基于TCP/IP的光纤通道（FCIP），在IETF RFC 3821中定义，是一种纯光纤通道封装协议。它允许通过基于IP的网络将光纤通道存储区域网络的孤立岛屿相互连接，形成一个统一的存储区域网络。
FCIP网络访问和协议控制应通过以下方式进行控制：
– 在FCIP实体之间建立点对点关系，并认识到安全策略将被统一应用；
– 在可能的情况下，由FCIP实体独占使用私有IP网络。

结合FCIP实施IPsec安全措施，包括：
– 至少执行加密认证和数据完整性；
– 通过适当的保密措施保护敏感数据。

IETF RFC 3723《在IP上保护块存储协议》为iSCSI和FCIP提供了额外有用的信息。子条款6.5.2提供了基于块的IP存储的指导。此外，IETF RFC 7146《在IP上保护块存储协议：IPsec v3的RFC 3723要求更新》为IETF RFC 3720、3723和3821提供了重要的安全更新。

6.3.2.4 FCoE SAN

以太网上的光纤通道（FCoE）是一种协议规范，用于在以太网数据包中封装光纤通道帧。支持FCoE的以太网网络必须是无丢包的以太网网络，并且具有内部架构设计，以提供无丢包的数据包能力和网络流量控制机制，以实现在以太网基础架构上无丢包传输数据包。

FCoE SAN应通过以下方式保护：

- 利用光纤通道的安全机制（参见C.7）；
- 防范以太网广播风暴（例如分配足够的输入缓冲区），以防止吞吐量和超时问题；
- 使用ACLs控制网络访问（例如拒绝特定计算机的不必要或不需要的流量）；
- 在不能使用物理隔离的情况下，使用FCoE VLANs。

6.3.3 网络附加存储（NAS）

6.3.3.1 总则

网络附加存储（NAS）是一种数据存储技术，为异构客户端提供基于文件级的网络访问。NAS使得物理上存储在一台服务器或设备上的文件系统可以被远程客户端计算机访问，并对用户呈现为本地文件系统。NAS系统通常专门为NAS目的而设计和构建，但也可以使用通用服务器计算机。

NAS系统可以实现为单个存储服务器，也可以实现为由多个存储服务器组成的集群，通过在集群存储服务器上分片或条带化数据和元数据来动态分配客户端连接（见图3）；并行NFS（pNFS）系统是集群NAS系统的示例。

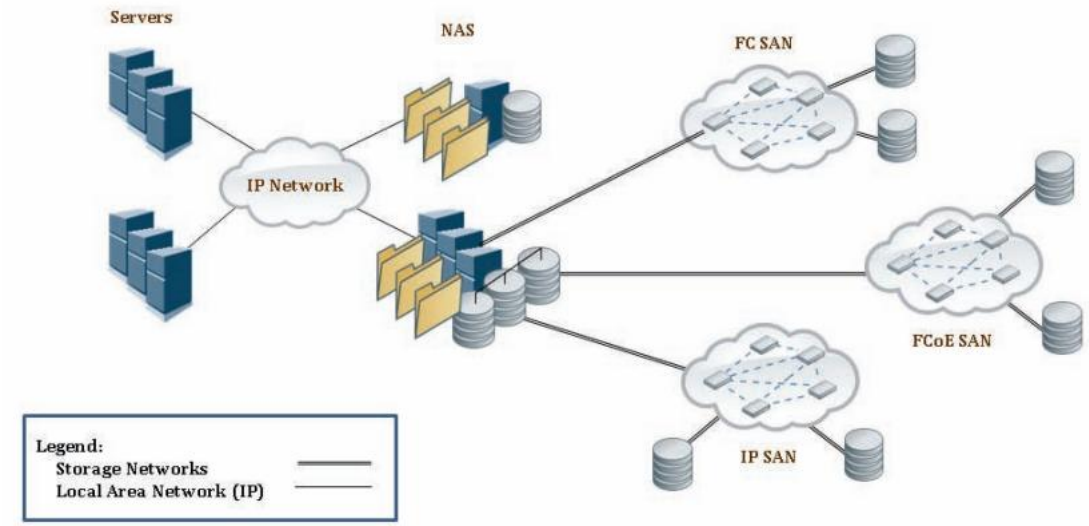


图3-网络连接存储（NAS）示例

Figure 3 — Network Attached Storage (NAS) Example

常见的文件系统实现包括网络文件系统（NFS）和服务器消息块（SMB）/常用互联网文件系统（CIFS），但也存在其他技术，如基于对象的存储设备（OSD）和云计算存储。

与NAS相关的安全控制分为以下几类：
- 授权控制，如ACLs，限制用户对NAS设备提供的文件和文件夹资源的访问；
- 对数据的加密，包括在数据传输时和数据静态存储时进行加密；
- 身份验证控制，如Kerberos，用于验证试图访问NAS数据的用户的身份。

有关NAS和基于文件的存储的更多实施指导，请参阅6.6。

6.3.3.2 网络文件系统（NFS）

NFS是一个客户端/服务器应用程序，使用基于远程过程调用（RPC）的协议进行通信。已经指定和使用了多个版本的NFS，包括NFS版本3（在IETF RFC 1813中指定）、NFS版本4（在IETF RFC 3530中指定）和NFS版本4.1（在IETF RFC 5661中指定）。从安全角度来看，NFS版本3（NFSv3）被认为不太安全，因此在使用敏感或高价值数据时应格外小心。

以下网络指导适用于基于NFS的NAS，并应遵循：
- 通过以下方式控制NFS网络访问和协议：
  - 仅在需要时启用NFS。这样可以消除它作为入侵者可能利用的攻击矢量；
  - 尽可能使用NFSv4（或更高版本），并限制NFSv3的使用；
  - 对客户端和管理访问进行IP地址过滤，以提供额外的安全性；
- 必要时对客户端数据访问进行加密（例如使用IPsec）。

6.3.3.3 服务器消息块（SMB/CIFS）

服务器消息块（SMB）3.0是CIFS（Common Internet File System）的继任者，而CIFS本身是SMB 1.0的继任者。SMB 3.0是一种旨在为客户端系统提供跨平台机制的协议，使其可以通过网络从服务器系统请求文件服务。它基于广泛使用于个人计算机和工作站的标准SMB协议，这些计算机和工作站运行各种操作系统。

以下网络指导适用于基于SMB/CIFS的NAS，并应遵循：
- 使用更高版本的SMB协议；
- 关闭低安全性会话协商协议，例如NT LAN Manager（NTLM）v1，LanMan和明文，并改用NTLM v2或Kerberos；
- 保持更新的补丁级别；
- 使用SMB签名；
- 安全地维护活动目录（AD）服务；
- 在可能的情况下，使用单向信任，从子域到父域；

- 通过以下方式控制SMB/CIFS网络访问和协议：
- 仅在需要时启用SMB/CIFS。这样可以消除它作为入侵者可能利用的攻击矢量；
- 必要时对客户端数据访问进行加密。

6.4 存储管理

6.4.1 总则

存储网络和基础设施元素是复杂的架构，可能对管理员施加严格的管理要求。为了满足这些要求，组织实施存储基础设施管理工具和流程，以确保所有存储元素的可用性和性能，提供更好的数据保护和安全性，集中审计，并满足合规性要求（见图4）。

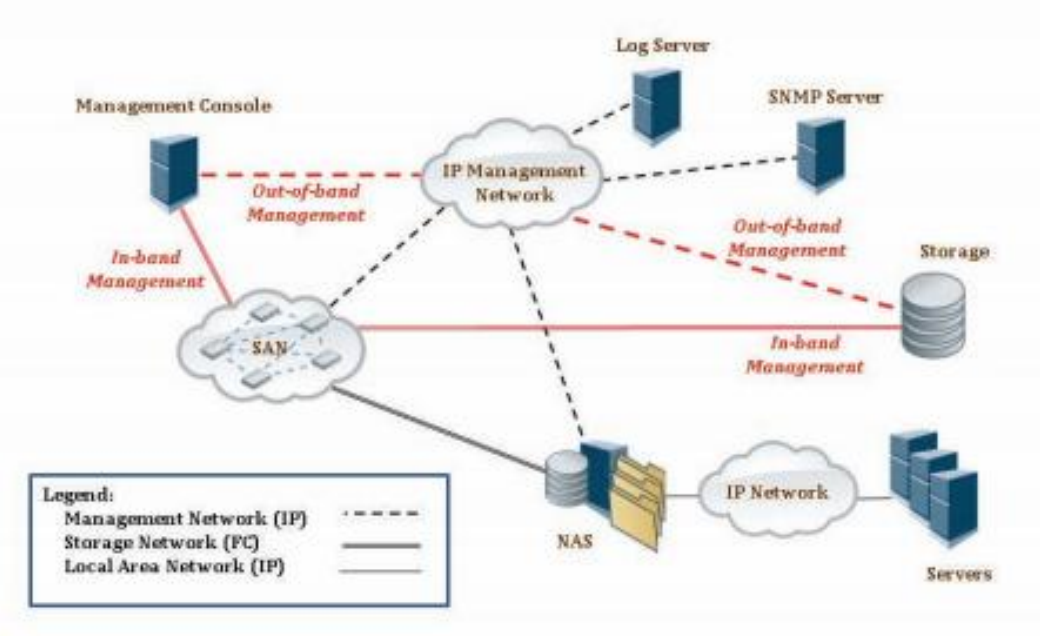


图4-存储管理示例

Figure 4 — Storage Management Example

类似于ISO/IEC 27033- 2中对网络管理的描述，存储管理也涉及与存储系统的操作、管理、维护、配置和清除相关的活动、方法、流程和工具。

- 操作涉及保持存储（以及存储基础设施提供的服务）平稳运行。这包括监控存储以尽早发现问题，最好是在用户受到影响之前。
- 管理涉及跟踪存储基础设施中的资源以及它们的分配情况。这包括所有必要的“管家婆”工作，以控制存储。

– 维护涉及进行维修和升级，例如更换设备、对存储阵列进行微码更新或将新交换机添加到存储网络时。维护还包括纠正和预防措施，以使存储运行得更好，例如调整设备配置参数。
– 配置涉及初始化和装备系统，以准备为其提供服务。
– 清除涉及在媒体从服务中移除或重新用于其他用途时，通过使数据不可读（例如通过用随机数据覆写数据、销毁加密密钥或物理销毁设备）来保护信息的机密性。
安全地执行这些存储管理活动需要与身份验证和授权(6.4.2)、保护存储管理接口(6.4.3)、维护系统和用户的可追溯性（6.4.4）以及确保用于存储管理的底层系统得到充分加固（6.4.5）相关的控制措施。有关每个主题的指导，请参阅本条款6.4内的子条款。

6.4.2 身份验证和授权

6.4.2.1 验证

管理存储系统和基础设施的个人通常是特权用户。根据ISO/IEC 27002:2013的9.2.3条款，特权访问权的分配和使用应受到限制和控制。对信息系统的系统管理权限（允许用户覆盖系统或应用程序控制的任何功能或设施)的不当使用可能是系统故障或违规事件的重要因素。为了减轻这些威胁，可能需要采用ISO/IEC 27002:2013的9.4.2条款中所描述的安全登录过程，并配合附加的身份验证措施（见附录C.1），其中包括但不限于：
– 所有用户应为其个人使用而具有唯一的标识符（用户ID）；
– 应选择适当的身份验证技术来证实用户所声称的身份，其中包括：
  – 强密码（增加最小字符数，增加复杂性等）并缩短使用期限；
  – 强身份验证（例如挑战–响应协议）；或
  – 多因素身份验证，例如生物识别数据（例如指纹验证、签名验证）和使用硬件令牌（例如智能卡）。
– 对于所有远程访问，使用强身份验证或多因素身份验证以及安全通道；
– 在可能的情况下，使用集中式身份验证解决方案（例如远程认证拨号用户服务或RADIUS，单点登录或SSO等）以提高监视和控制能力；
– 在管理敏感和高价值数据时使用多因素身份验证；
– 禁用对root账户的登录。远程记录所有特权升级操作。

除了用户身份验证外，存储系统有时还会采用实体身份验证，即分布式系统中的代理获取对通信伙伴身份的信任过程。实体身份验证可以在传输层安全（TLS）和IPsec连接中以及存储协议内（例如使用iSCSI的挑战握手身份验证协议、FCP中的Diffie–Hellman挑战握手身份验证协议等）进行。在可能的情况下，应使用这些实体身份验证机制。有关这些机制的更多指导，请参阅相关部分。

6.4.2.2 授权和访问控制

在金融服务和医疗保健等市场领域，有将授权和访问控制（参见C.2）与最小权限模型相结合的趋势，利用特定角色。在存储技术中应实施和使用以下角色：
– 安全管理员 – 该角色具有查看和修改权限，用于建立和管理帐户，创建和关联角色/权限，配置和内容的审计日志（审计日志事件条目永远不能更改），与IT基础设施建立信任关系（例如RADIUS的共享密钥），管理证书和密钥库，管理加密和密钥管理，并设置访问控制。
– 存储管理员 – 该角色具有对存储系统所有方面的查看和修改权限。不允许访问与安全相关的元素或数据。
– 安全审计员 – 该角色具有查看权限，允许进行授权审查，验证安全参数和配置，并检查审计日志。不允许访问存储、配置或数据。
– 存储审计员 – 该类似操作员的角色具有查看权限，允许验证存储参数和配置，并检查健康/故障日志。不允许访问与安全相关的元素或数据。
每个存储管理事务应与“安全”或“存储”角色相关联。这些角色可以是重要的控制措施，以确保在管理能力方面分离职责。

6.4.3 保护管理接口

保护管理接口免受未经授权的访问和侦察是非常重要的。由于未能实施适当的控制而导致对管理接口的未经授权访问可能导致数据破坏、损坏和拒绝访问。

存储系统的管理接口可以采用多种物理形式，包括串行端口（例如RS-232、DB9、DB25等）、局域网、调制解调器，甚至用于数据路径的技术（例如光纤通道）。混合接口（例如连接到局域网的串行端口，提供LAN接口的控制台聚合器）也相对常见。为了保护这些物理接口，组织应该：
– 限制对管理接口的物理访问；
– 在不使用时禁用和断开串行管理端口；
– 将用于管理的LAN接口与其他LAN流量隔离，注意物理隔离更可取，但最低限度应使用逻辑隔离（例如VLAN）。

除了物理接口外，存储系统还采用各种软件和固件来实现对存储系统的管理。这些软件接口可以包括简单的命令行界面（CLI）、基于Web的图形用户界面（GUI）、支持简单网络管理协议（SNMP）以及处理带内管理（即通过数据路径进行管理）的服务器代理。为了保护这些软件/固件接口，组织应该：
– 使用防火墙和TCP封装器来限制对管理网络的访问，只允许授权的系统和协议；
– 使用实体身份验证来建立存储系统与管理系统之间的信任关系（例如使用FC-SP-2 AUTH-A来对带内管理执行实体身份验证，如C.7.1中所述）；
– 利用IDS和IPS机制识别异常行为并防范它们；

- 使用带有适当安全控制的ICT基础设施（例如域名系统或DNS，服务定位协议或SLP，网络时间协议或NTP）以避免间接攻击；
- 使用适当的特权用户控制，包括身份验证（见6.4.2.1）、授权（见6.4.2.2）和安全审计/监控（见6.4.4）；
- 确保操作系统和应用程序是最新的，并经过足够的硬化防范攻击（见6.4.5）。

当远程管理存储系统时，应采取以下额外的安全措施：
- 对所有远程访问使用安全通道（虚拟私人网络或VPN、TLS、安全外壳或SSH、安全超文本传输协议或HTTPS）；
- 使用强身份验证或多因素身份验证；
- 将特权限制为所需的最低限度（即最小特权）。

组织应该制定组织和技术控制措施，限制用于远程（非本地）供应商维护会话的管理接口。通过外部网络（例如互联网）进行的远程供应商维护操作会带来重大风险，不仅涉及可用性，还涉及完整性和机密性。

技术控制措施应该限制远程供应商维护操作所需的通信流量（即系统、端口和协议）至最低限度。在验证访问方之后，应该在访问点设计附加控制措施来授权供应商维护会话。这些控制措施包括接受、请求批准或拒绝请求的会话。应该生成包含供应商操作审计记录的适当日志。

组织应该限制拨号接入线路，只允许授权的访问方进行访问。这包括强制实施调制解调器回拨协议，并在供应商请求维护会话并且经过组织授权之前禁用连接建立。

6.4.4 安全审计、会计和监控

合规法规和合同条款通常包含监控和报告要求。事件日志记录和系统会计是帮助满足这些要求的关键功能（参见C.5）。在这两者中，从存储安全的角度来看，事件日志记录可能更有用，因为它可以用于实时监控和事件调查。因此，存储系统和基础设施需要参与组织的事件日志记录计划（也参见ISO/IEC 27002:2013，12.4提供相关指导）。

以下日志记录指导适用于存储系统，应予以使用：
- 将存储包含在日志记录策略中，如下所示：
  - 关于存储系统和设备，应该解决以下策略要素：
    - 存储系统和设备应参与审计日志记录；
    - 应收集所有重要的存储管理事件；
    - 日志数据应得到保留；
    - 日志数据应按照日志数据保留策略进行存档和保留；和

- 设备时间应与可靠的外部来源同步。
- 日志记录策略（参见7.7.2）应包括证据期望（真实性、保管链等）。
- 通过以下方式将外部或集中的事件日志记录到可信任的远程源头：
  - 实施集中化的审计日志记录，将所有来源的事件收集到一个单一的存储库中；
  - 在整个环境中建立和使用一个共同的准确时间源，以确保可以对来自不同来源的事件记录进行关联；
  - 避免使用设备自带的日志记录用于除系统健康监测和调试之外的任何其他用途，因为它们更容易遭到篡改或破坏，日志记录的存储空间有限，并且不能使用集中式自动化分析、警报和存档；
  - 将事件日志直接记录到一个或者最好是多个外部日志服务器。
— 使用支持可靠传输和安全传输的标准日志记录协议，如syslog9）（例如TLS）；
— 将设备配置为在事件发生时立即记录日志（即不进行缓冲），当主要的审计日志记录驱动因素是合规性、问责制或安全性时；
— 实施分析协议，以在事件源之间关联审计日志记录，以识别提供安全事件指示的重要安全事件；
— 在部署此类技术时，确保将存储日志记录纳入安全信息与事件管理（SIEM）解决方案。
— 确保完整的事件日志记录；
— 一旦确定要记录的事件类型，那么应该记录所有这些事件的发生情况（无论是在带内还是带外）；
— 应该记录以下类型的事件（最小安全事件集）：
  — 失败和成功的登录尝试；
  — 对敏感和高价值数据的文件和对象访问尝试失败；
  — 帐户和组配置文件的添加、更改和删除；
  — 系统安全配置的更改（例如审计日志记录、网络过滤、分区更改）；
  — 安全服务器使用的更改（例如syslog、网络时间协议NTP、域名系统DNS、身份验证）；
  — 系统关闭和重新启动；
  — 特权操作（即管理员发起的更改）；
  — 使用敏感工具（例如特权升级命令）；
  — 访问关键数据文件；
  — 虚拟服务器在物理服务器之间的移动。
— 每个日志条目应包括：
  — 时间戳（日期和时间）；
  — 严重程度级别；
  — 日志条目的来源（区分名称、IP地址等）；
  — 事件ID以及文本描述（必要时以启用事件的本地化/国际化-其中事件ID保持不变，但文本描述可以翻译为不同的语言）；以及目的地降低了意外丢失的风险。

— 事件的描述。
— 在过滤“严重性”等字段时要小心，企业的日志记录策略应作为确定何种过滤适合以及什么级别的信息需要长期存储的指南。
— 实施适当的保留和保护措施，如下所示：
— 具有证据价值的审计日志数据应正确处理（例如，保持责任链、可验证的完整性和真实性等）；
— 具有特定保留要求的审计日志数据（例如，用于合规性监管）应按照组织的数据保留解决方案（见7.4）保存；
— 实施适当的措施来保护日志的完整性并防止其修改或破坏（无论是恶意还是意外）；
— 当审计日志条目包含敏感信息时，应使用适当的机密性机制10）保护审计日志数据；
— 对于独特的审计日志记录要求（例如，高容量、特殊保留、事件签名等），应使用专用和经过特殊硬化和配置的系统；
— 利用日志中继和日志过滤，以最小化专用存储要求（例如，只读一次写入或WORM）的影响。

6.4.5 系统硬化

所有操作系统、虚拟化程序和应用程序应相对于存储系统进行硬化。除了ISO/IEC 27002:2013第12.6节中的技术漏洞管理指导外，还有许多现有的最佳实践适用于各种操作系统，应根据所使用的操作系统参考这些最佳实践。一些适用于任何操作系统的最佳实践包括：
— 删除不需要/未使用的软件；
— 删除不必要的账户；
— 对任何预定义或默认账户进行更改（例如重命名、禁用、更改任何默认密码等）；
— 仅打开所需的网络端口；
— 从可信源安装最新的补丁；
— 从可信源更新固件；
— 安装和维护恶意软件防护措施（也参考ISO/IEC 27002:2013第12.2节）。

当存储基础架构的元素接收更新（例如微码）或补丁时，应确保将要应用的软件来自于可信源。否则，攻击者可以编写自己的“更新”，其中包含他们选择的恶意代码，例如rootkit、botnet或其他恶意软件。

供应商应对其控制下的元素执行6.4.5中描述的操作。

6.5 基于块的存储

6.5.1 光纤通道（Fibre Channel，FC）存储

光纤通道存储系统使用专门的网络技术（见6.3.2.2）将基于块的存储资源呈现给计算机。这些资源通常采用逻辑单元（Logical Units，LUNs）和磁带设备（包括虚拟磁带）的形式。

对于光纤通道系统，应考虑以下事项：
- 应使用LUN掩码和映射（WWN过滤）等访问控制机制来限制对存储的访问；
- 实施FCP安全措施，包括：
  - 与所有服务器和交换机使用FC-SP-2 AUTH-A进行相互认证（见C.7），在可能时利用集中式认证服务；
  - 如果可能，应使用ESP_Header11）加密对离开受保护区域（例如受物理控制的数据中心限制）的光纤通道连接（见6.8.2.2和C.7.3）。
- 实施数据静态加密措施（见6.8.2.3），包括：
  - 敏感和高价值数据在存储设备或介质12）上应进行加密；
  - 应在可能接触到敏感或受管制数据的存储设备中实施加密，以及为便于快速消除数据（见A.3）。
- 实施数据消除措施（见6.8.1和附录A），包括：
  - 对于敏感和受管制数据，应使用媒体对齐的消除方法（见6.8.1.2）；
  - 应使用逻辑消除方法（见6.8.1.3）来清除虚拟化存储（见7.6.1），特别是当无法确定实际存储设备和介质时。

供应商应在其产品中实施6.5.1中描述的访问控制、认证、数据消除和加密功能。

6.5.2 IP存储

与光纤通道存储不同，IP存储使用TCP/IP网络技术（见6.3.2.3），具体来说是iSCSI，向计算机呈现基于块的存储资源。

对于IP存储系统，应考虑以下事项：
- 通过基于源IP地址和协议进行过滤来控制iSCSI启动器的访问；
- 实施iSCSI安全措施，包括：
  - 对所有iSCSI实现中的启动器和目标使用双向挑战-握手认证协议（CHAP），使用随机挑战（即不重复的）；
  - 当可能会暴露敏感或高价值数据时，应使用IPsec来保护通信通道（见6.8.2.2）。
  - 互联网存储名称服务 (iSNS)，SLP，DNS基础设施应该使用适当的安全控制来避免间接攻击。
— 实施数据静态加密措施（见6.8.2.3）。
  — 敏感和高价值数据在存储设备或介质上应进行加密13）；

— 加密应该在可能接触到敏感或受管制数据的存储设备中实施，以及为便于快速消除数据（见A.3）。

— 实施数据消除措施（见6.8.1和附录A）。

— 应对敏感和受管制数据使用媒体对齐的消除方法（见6.8.1.2）；

— 应在无法确定实际存储设备和介质时，使用逻辑消除方法（见6.8.1.3）来清除虚拟化存储。

供应商应在其产品中实施6.5.2中描述的访问控制、认证、数据消除和加密功能。

6.6 基于文件的存储

6.6.1 基于NFS的网络附加存储（NAS）

这种类型的存储是一个通过网络协议NFS（见6.3.3.2）呈现文件的局域网附加文件服务器。它包括一个实现文件服务的引擎和一个或多个存储设备，用于存储数据。NAS系统也可以是SAN连接的，这种情况下NAS系统被视为SAN上的任何其他服务器（例如，提供对存储的访问、无LAN备份等）。基于NFS的NAS系统可以采用许多不同的形式（例如，简单的NAS服务器到高度可扩展的集群），它们通常被高度优化以处理大量同时的文件访问。

对于基于NFS的NAS系统，应考虑以下事项：

- 对NFS导出的文件系统应用访问控制，包括：
  - 尽可能使用用户级认证（例如，NFSv4与Kerberos V5）；
  - 配置NFS服务器以明确为授权用户导出文件系统；
  - 配置NFS服务器以导出具有最小所需特权的文件系统；
  - 避免授予网络文件系统上的文件“root”或“administrator”访问权限；
  - 确保正确分配NFSv4 ACL（访问控制列表）；
  - 对于NFSv3，使用Kerberos认证；
  - 考虑使用Kerberos的安全和私密模式对NFS流量进行签名和加密。
- 限制NFS客户端行为
  - 尽可能过滤客户端对NFS共享的访问；
  - 不要允许NFS客户端在导出的文件系统上运行suid和sgid程序。
- 安全地处理NFS服务器上的数据
  - 导出的文件系统应位于自己的分区中，以防止攻击者通过向导出的文件系统写入数据直到其满为止而造成系统退化。
  - 在必要时加密数据在静态状态下；
  - 不允许导出管理文件系统的NFS（例如，/etc）；
  - 防范恶意软件（例如，病毒，蠕虫，Rootkit等）；
  - 持续监控放置在NFS共享和相关访问控制中的内容。

供应商应在其产品中实施6.6.1中描述的访问控制、认证和加密功能。

6.6.2 基于SMB/CIFS的网络附加存储（NAS）

与基于NFS的NAS（见6.6.1）类似，基于SMB/CIFS的NAS是一个局域网附加文件服务器，用于提供文件服务，但其使用的网络协议是SMB/CIFS（见6.3.3.3）。

对于基于SMB/CIFS的NAS系统，应考虑以下事项：
- 对SMB/CIFS导出的文件系统应用访问控制
  - 禁用未经身份验证的对CIFS共享和NAS设备的访问（即限制匿名访问）；
  - 禁用对所有CIFS共享的“Guest”和“Everyone”访问；
  - 通过集中化机制（例如RADIUS，轻量级目录访问协议或LDAP）实施认证和访问控制。
- 通过为客户端和NAS设备启用SMB签名来限制SMB/CIFS客户端行为；
- 保护SMB/CIFS服务器上的数据：
  - 尽可能启用CIFS审计；
  - 持续审查放置在CIFS共享和相关访问控制中的内容；
  - 在必要时加密数据在静态状态下；
  - 防范恶意软件（例如，病毒，蠕虫，Rootkit等）。
- 使用强认证（NTLMv2，Kerberos）实施CIFS认证。

供应商应在其产品中实施6.6.2中描述的访问控制、认证和加密功能。

6.6.3 基于Parallel NFS的网络附加存储（NAS）

如6.3.3.1中所述，NAS设备可以作为独立的存储服务器或成为一个集群的存储服务器。这些集群有两种类型：对称和非对称，并且两者可以结合使用。对称集群允许所有文件服务器都成为完整的文件服务器，通过重定向或类似技术来选择基于客户端和客户端所需访问的文件来选择合适的服务器。一个常见的技术是使用不同的服务器来负责不同部分的文件系统命名空间-在这样的结构中，文件名解析可能导致客户端遍历涉及多个文件服务器的命名空间路径。非对称集群将功能分割到多个服务器上-并行NFS至少使用一个主文件服务器和多个从属存储服务器，这些存储服务器受主服务器的控制（客户端必须与主文件服务器联系，以了解存储在从属存储服务器上的数据以及如何访问它）。

对于对称集群，包括对pNFS主文件服务器进行集群化，主要的指导方针是在集群服务器之间一致应用控制和控制机制（例如认证和授权），以便安全保证性质不依赖于客户端访问哪个文件服务器。

对于非对称集群，控制和控制机制的一致应用非常重要，但是服务器的不同角色可能会给客户端带来一些在对称集群中不存在的责任。对于pNFS来说，一个特定的复杂性是从属存储服务器可能不使用与主文件服务器相同的协议（NFS），需要在两个协议之间以一致的方式实施控制。另一个重要的例子是，pNFS块/卷布局需要信任客户端尊重从主

服务器获取的布局信息，并且不访问其没有布局的块存储 – 这应该以某种方式纳入控制中，以执行不在不能依赖客户端执行此操作时使用pNFS块/卷布局的建议 – 参见IETF RFC 5663中的安全考虑（第4节）。

在这两种情况下，控制不应依赖于文件系统命名空间在服务器之间的路径遍历 – 客户端直接访问客户端不应该“从”启动的服务器是有效应用控制的一个重要考虑因素，因为某些服务器可以导出部分文件系统命名空间（没有客户端预期从“根”开始的命名空间）或者根本不导出文件系统命名空间。后一种情况的一个具体例子是，对于不能导出文件系统命名空间的服务器（例如pNFS存储服务器），不应该对控制有限制或没有限制。另一个例子是，阻止命名空间路径遍历的目录ACL可能不足以控制命名空间路径跨越到另一个文件服务器 – 有效的控制必须处理客户端直接访问后者文件服务器的情况，因为这种访问将绕过目录ACL。

对于pNFS系统，应考虑以下事项：
– 控制和控制机制应在集群（包括对称和非对称）中一致应用；
– 安全保证性质不应依赖于客户端访问特定的文件服务器；
– 对于非对称集群，应实施一致的控制，以确保在不同的协议上具有一致性；
– 安全控制不应依赖于文件系统命名空间在服务器之间的路径遍历。

6.7 对象存储

6.7.1 云计算存储

6.7.1.1 保护云计算存储

使用专有和基于标准的云计算存储服务时，通常会提供复制功能（例如，镜像系统上的一部分或全部存储），备份和恢复功能，长期保留功能（例如，存档）以及多系统同步功能（例如，允许用户在多个可能不同类型设备上同步数据）。然而，除非他们确信相关的安全威胁和挑战已得到解决，否则个人和组织将不愿将其数据托管到云计算存储中。14）其中一些云计算实现是基于对象的，通常依赖HTTPS（HTTP over TLS）来保护底层通信。可能会指定其他安全功能，但实际实现与最终使用可能存在显著差异。

安全使用云计算存储应涉及以下一些或全部步骤：
– 确保所有交易都使用传输安全性，例如IPsec或传输层安全（TLS）（参见6.8.2.2）；
– 当敏感数据存储在第三方云环境中时，应使用数据静态状态加密（和适当的密钥管理流程）以防止未经授权的访问（例如，云服务提供商人员，其他租户，对手等）。
— 确保用户注册安全，并使用强密码认证来保护对数据的访问；
— 使用访问控制来防止其他租户的未经授权访问，同时为被允许访问数据的用户提供适当的访问权限；

— 使用提供的消除敏感数据功能来清除云计算存储中的敏感数据。
注意：在某些司法管辖区，隐私要求（如“被遗忘权”或“被删除权”）可能需要额外的安全控制。
云计算实现通常利用不同形式的虚拟化，因此7.6中的指导也可能相关。

厂商应在其产品中实施适当的云计算存储功能，包括访问控制、身份认证、加密、日志记录、消除敏感数据等，这些功能在6.7.1.1中进行了描述。

6.7.1.2 CDMI安全性

基于ISO/IEC 17826:2012云数据管理接口（CDMI）规范的云计算存储是一种基于对象的存储技术，使用RESTful HTTP接口。它具有足够详细的安全元素，可以提供具体的指导。CDMI内部的安全措施可以概括为传输安全、用户和实体认证、授权和访问控制、数据完整性、数据和介质消除、数据保留、防御恶意软件、数据静态状态加密和安全性能力查询。除了必须实施的传输安全和安全性能力查询（用法始终是可选的）外，安全措施在不同的实现中可能会有很大的差异。

CDMI客户端应：
— 确保所有交易都使用传输层安全性（TLS）（参见6.8.2.2）；
— 查询云服务提供商的CDMI实现的安全能力，并基于风险进行决策，判断所提供的安全性是否足够；
— 对CDMI实体进行认证（对于服务器使用证书，对于客户端使用HTTP基本认证）；
— 使用CDMI域提供外部认证提供者的认证映射位置；
— 启用CDMI安全日志记录，并定期及时地检索安全事件数据；
— 与组织的数据保留策略相一致，调整自动删除功能（CDMI删除）；
— 在使用CDMI Holds之前，了解解除CDMI Hold的过程和机制；
— 使用数据静态状态加密措施保护敏感和高价值数据；
— 对于加密功能，始终验证实现是否使用了请求的CDMI功能（支持的操作），而不是其他功能；
— 使用提供的消除敏感数据设施清除云服务提供商存储中的敏感数据。

厂商应在其产品中实施适当的CDMI功能，包括访问控制、身份认证、加密、日志记录、消除敏感数据等，这些功能在6.7.1.2中进行了描述。

6.7.2 基于对象的存储设备（OSD）

基于对象的存储设备（OSD）是一种计算机存储设备，类似于磁盘存储，但在更高的层面工作（即，物理存储位置在对象接口下隐藏，并由存储设备自身管理）。与提供以块

为导向的接口读写固定大小的数据块不同，OSD将数据组织成灵活大小的数据容器，称为对象。
每个对象都包含数据（字节的线性序列）和元数据（描述对象的可扩展属性集），可以通过指定对象标识符（OID）和（偏移量、长度）元组来访问。OSD接口包括用于创建和删除对象、将字节写入和从单个对象读取字节以及在对象上设置和获取属性的命令。OSD负责管理对象及其元数据的存储。OSD实现了一种安全机制，提供了基于对象和基于命令的访问控制。

为了确保对存储的安全访问，每个命令都附带着一个加密安全性能力，用于标识对特定对象的操作列表。性能力不仅提供了典型块存储中缺少的设备级别安全性，而且还能实现对单个对象的细粒度访问。这使得存储设备可以在具有独特安全需求的多种应用程序之间共享。

OSD使用基于凭证的访问控制系统，由三个活动实体组成：对象存储（OSD）、安全管理器和客户端。作为一种基于性能力的访问控制系统，所有对对象存储的请求都伴随着一个性能力，其中编码了持有者对对象的一组权限，并具有加密安全性。

要安全地使用OSD：
— 在涉及敏感数据的所有事务中应使用IPsec来保护不安全的网络；
— 对象存储在执行操作之前应验证性能力的真实性；
— OSD和安全管理器之间的时钟同步应使用安全协议来实现；
— 性能力到期时间应设定限制，以最小化受到损害的性能力可以使用的时间；
— 工作密钥（用于生成性能力密钥）应定期刷新。

厂商应在其产品中实施适当的OSD功能，包括访问控制、身份认证、加密等，这些功能在6.7.2中进行了描述。

6.7.3 内容寻址存储（CAS）

内容寻址存储（CAS），有时也称为固定内容存储（FCS），技术旨在存储不随时间改变的数据（即，它在时间上是固定的）。CAS通常会暴露通过加密哈希函数（如MD5或SHA-1）从所指的文档生成的摘要。CAS技术的主要优势在于用户无需知道实际数据的位置和存储的副本数量。

CAS支持通过其内容摘要检索文档，并确保检索到的文档与最初存储的文档完全相同。（如果文档不同，则其内容地址将不同。）此外，由于数据是通过其包含的内容存储到CAS系统中，因此永远不会存在多个完全相同文档的情况。根据定义，两个相同的文档具有相同的内容地址。

如果CAS系统使用的哈希函数较弱，这种方法可能在对抗环境中发生冲突（不同的文档生成相同的哈希）。因此，对于CAS系统来说，使用强大的哈希机制非常重要。

在授予CAS系统访问权限之前，用户和应用程序应进行身份认证和授权。这样可以防止未经授权的用户存储数据或检索数据。此外，CAS系统应确保内容在其整个生命周期内可读和可访问。最后，CAS系统应采用强大的哈希机制。
CAS是在满足短期和中期保留需求时特别有用的技术（参见7.4.2）。

厂商应在其产品中实施适当的CAS功能，包括身份认证、授权、可用性、哈希等，这些功能在6.7.3中进行了描述。

6.8 存储安全服务

6.8.1 数据消除

6.8.1.1 总则

在处理媒体的指南中，重要的元素是确保在不再需要媒体时，其内容变得无法恢复。消除（sanitization）是指一般过程，将先前写入存储媒体的数据变得不可检索，以合理保证数据不能轻易地被恢复或重建（参见C.4）。

为了有效地使用这个标准来处理所有类型的媒体，组织和个人应对其信息进行分类，评估其记录媒介的性质，评估对机密性的风险，并确定媒体的未来计划（例如，重复使用）。然后决定适当的消除类型。所选类型应根据成本、环境影响等进行评估，并作出能最好地减轻对机密性风险的决策，以满足对该过程施加的其他约束。

只有在信息披露对组织任务没有影响、不会对组织资产造成损害、不会导致财务损失或对任何个人造成伤害的情况下，才应考虑不消除存储设备或存储元素的处理。

清除（clear）、清洗（purge）和销毁（destroy）是可以用于消除存储的操作。A.1描述了每种方法，并在适当的情况下提供了其他选项。A.2通过提供有关消除硬拷贝和电子（软）拷贝媒体的具体指导，补充了这些信息。

消除操作可能是昂贵和耗时的，但出于安全原因是必要的。消除操作的级别应与风险相平衡。应特别注意个人身份信息（PII）和电子医疗记录（EHR）以及业务或任务关键数据（例如，商业机密、知识产权等）。

当消除是合规性的一个要素时，应当审查具体的要求和相关规范，以确定它们是否强制要求特定的覆写技术、消除证明等。这些要求可以采取特定的覆写技术、消除证明等形式。

为了提供适当的消除功能，厂商应在其产品中实施6.8.1.2、6.8.1.3、6.8.1.4、6.8.1.5和附件A中描述的功能。

6.8.1.2 基于媒体的消除

当存储介质被转移、变得过时、无法再使用或信息系统不再需要时，应该消除介质上残留的磁性、光学、电气或其他数据表示。

附录A应该被用来确定特定介质的推荐消除方法。虽然在这里强烈推荐使用附录A，但还存在其他方法来满足清除、清洗（在某些情况下仍然相关）和销毁的意图，并且没有在附录A中指定的方法可能是合适的，只要它们经过审查并被组织认可为令人满意的。并非所有类型的可用介质都在本国际标准中指定，对于未包含的介质，组织应识别和使用能够满足清除、清洗或销毁介质意图的过程。

建议在使用加密方法时，也应对媒体进行消除，即使使用加密擦除来消除设备上的数据，仍建议对介质本身进行消除。

6.8.1.3 逻辑消除

许多存储设备将底层存储介质虚拟化，并将其呈现为逻辑存储。一个众所周知的例子是存储阵列上的逻辑单元（LUN），其大小可以远远超过单个存储元素的容量。当逻辑存储被复制（即存在多个数据副本）以支持服务器虚拟化（参见7.6.2）和灾难恢复（参见7.3.4）时，情况可能进一步复杂化。在这些情况下，几乎不可能识别出所有底层存储介质。此外，消除所有物理介质可能不合适，因为多个逻辑存储实例可以存在于共享的物理介质上。

如果逻辑存储（例如，逻辑单元、文件系统或对象存储）是可写的，那么应使用覆写或加密擦除技术对逻辑存储使用的底层存储介质进行消除；加密擦除的成功应用（参见A.3）前提是在数据被记录到逻辑存储之前激活了加密。数据保护技术（参见7.3.3），其中包括复制、备份和连续数据保护存储，通常与逻辑存储一起使用，因此应对与数据保护机制相关的存储执行单独的消除操作。

6.8.1.4 消除验证

组织应记录消除活动的记录，记录哪些媒体被消除、何时消除、如何消除以及媒体的最终处理方式。通常情况下，当组织被怀疑失去对其信息的控制时，这是因为媒体消除的记录不足。

消除验证至少有两种形式：1）审计日志追踪和2）消除证书。这些消除记录是组织应该为合规/法律目的保留的证据，否则可能面临制裁或昂贵的数据泄露通知。消除证书以及与记录消除证据相关的溯源或链条传递要求的重要性是将消除置于安全人员控制之下的主要原因。

消除证书应至少包含以下信息：
— 制造商；
— 型号；
— 序列号；
— 媒体类型（例如，磁性、闪存、混合等）；
— 媒体来源（即媒体来自的用户或系统）；
— 消除描述（即清除、清洗、销毁）；
— 使用的消除方法（例如，去磁、覆写、块消除、加密擦除等）；
— 使用的工具（包括版本）；
— 验证方法（例如，全面、快速抽样等）；
— 对于消除和验证：
    — 人员姓名；
    — 人员职位/头衔；
    — 日期和时间（完成时间）；
    — 地点；
    — 联系信息（例如，电话号码、电子邮件地址等）；
    — 执行消除操作的人员签名字段。

除了与消除证书相关的详细信息外，审计日志应记录与消除相关的时间戳事务和进展情况。例如，消除操作的启动和结束以及中间覆写和验证进度应该得到反映。

在媒体处于不可操作状态且需要进行物理销毁的情况下，应通过消除证书来证明消除的事实。

6.8.1.5 消除媒体的验证

消除媒体的验证目标是确保目标数据得到有效的消除。如果设备接口支持（例如ATA或SCSI硬盘驱动器或固态硬盘），通常通过完整读取所有可访问区域来验证消除的有效性（除非在实验室外）。如果时间和外部因素允许，应进行完整的验证。这种验证方式通常仅适用于在消除后设备处于可操作状态的情况，以便通过原生接口读取数据。

如果组织选择代表性抽样，则对电子媒体消除的验证有三个主要目标：
a) 使用新的种子为伪随机数发生器（PRNG）每次应用分析工具时在媒体上选择伪随机位置。这样可以减少只消除媒体的子集的消除工具在敏感数据仍存在的情况下导致验证成功的可能性。
b) 在可寻址空间中选择位置。例如，将媒体概念上分成大小相等的子节段。选择足够多的子节段，使媒体得到充分覆盖。实际子节段数取决于设备和寻址方案。利用逻辑块地址（LBA）寻址的硬盘驱动器建议的最小子节段数为一千。从每个子节段内至少选择两个不重叠的伪随机位置。例如，如果选择了一千个概念上的子节段，则至少会读取和验证媒体寻址空间的前一千分之一内的至少两个伪随机位置，然后会读取和验证媒体寻址空间的第二千分之一内的至少两个伪随机位置，以此类推。除了已确定的位置，还应包括存储设备上第一个和最后一个可寻址位置。
c) 每个连续的样本位置（除了第一个和最后一个可寻址位置）应该覆盖子节段的至少5％，并且不与子节段中的其他样本重叠。在得到两个不重叠的样本后，验证结果应覆盖至少10％的媒体。

受访问控制机制保护的设备有其他的验证考虑因素。无论这些设备是通过覆写、块擦除还是加密擦除（参见A.3）进行消除的，这些设备在消除前后都需要可访问，以便启用验证过程。

加密擦除与其他操作不同，因为加密擦除后的内容可能是未知的，因此不能与给定的值进行比较。当使用加密擦除时，应尝试应用简单的检查，例如读取具有已知内容的存储位置（例如，文件系统元数据），以验证是否返回了预期的数据。如果由于任何原因（例如，执行加密擦除的人员没有读取访问权限）而无法实现，则可以跳过验证。

6.8.2 数据机密性

6.8.2.1 总则

在存储基础设施中，通常使用某种加密方法来维护数据的机密性。这些方法通常与在存储基础设施内传输数据时（有时称为在飞行中或运动中）或将数据存储在设备上或存储媒体上时（即静态存储）保护数据相关。

加密的过程是将加密算法（或密码）应用于明文数据，得到加密数据（或密文）。反之，解密将密文转换回其原始明文。与存储相关的许多重要密码的定义和规范可以在以下文档中找到：ISO/IEC 18033:2005、NIST FIPS 197、NIST Special Publication 800-67和IEEE 1619.2-2010。

对于某些类型的密码（例如n位块密码），可以使用多种方式（称为操作模式）将密码用于加密明文。常见操作模式的定义和规范可以在以下文档中找到：ISO/IEC 10116:2006、NIST Special Publication 800-38A、NIST Special Publication 800-38C、NIST Special Publication 800-38D、NIST Special Publication 800-38E和IEEE 1619-2007。

密码与密钥以及可能的其他密钥材料（例如，初始化向量）一起工作。在对称密码中，加密和解密算法使用相同的密钥。在非对称密码中，加密和解密使用不同但相关的密钥。密钥管理的管理和保护（称为密钥管理）在维护数据机密性方面至关重要。

密钥管理的目的是为处理对称或非对称加密机制使用的加密密钥材料提供程序。有关密钥管理不同方面的定义和规范可以在以下文档中找到：ISO/IEC 11770（第1部分和第2部分）和NIST Special Publication 800-57（第1部分和第2部分）。ISO/IEC 27002:2013，10.1.2还提供了有关密钥管理的相关指导。

为了提供适当的数据机密性功能，供应商应在其产品中实现6.8.2.2和6.8.2.3中描述的功能。

6.8.2.2 加密传输的数据

在存储基础设施中，对在两个点之间传输的信息进行数据机密性或完整性（数字签名或认证代码）保护可能是有意义的，特别是对于离开实体受控数据中心范围的数据。

诸如ESP_Header（见C.7.3）、IPsec、TLS或甚至基于计算机的加密技术等协议可以在数据传输时为信息提供额外的保护。这些方法通常与在传输过程中保护数据相关（有时称为在飞行中或在传输中）。

数据在传输中的保护通常是数据的临时保护，可能仅在数据被传输时存在。对于传输中的加密，发送方应用加密算法并发送密文。它还可以应用完整性算法并发送完整性值。相反，接收方应用解密算法将密文转换回其原始明文，并检查完整性值。有多种标准规范，包括光纤通道安全标准（见C.7.1）、IPsec RFC和TLS RFC，详细介绍了保护数据在传输中的替代方案。

对于某些协议，标准中存在多种操作模式或选项。此外，还有多种密码模式或数字签名（完整性）算法。常见操作模式的定义和规范可以在ISO/IEC 10116:2006中找到。
数据在传输中的保护与密钥建立或密钥协商过程或协议相结合。在维护数据传输中数据的机密性和完整性方面，对初始认证密钥的管理和保护至关重要。前面引用的标准详细说明了使用数据传输中数据保护方法时必须保护的关键安全参数的附加信息。

- 当需要数据在传输中的保护时，应提供端到端的保护。
- 数据在传输中的加密可能对通信实体造成重大的计算负担，因此应实施适当的补偿措施以最小化影响。
- 对于IPsec，应使用版本3和Internet Key Exchange（IKE）版本2（或更高版本）。
- 对于TLS，存储客户端应遵守Storage Networking Industry Association（SNIA）技术立场文件：存储系统的TLS规范v1.0（或最新版本）中的要求。

6.8.2.3 对静态数据进行加密

随着存储的敏感和受监管数据不断增加，组织需要采取措施确保这些数据以加密形式存储。尽管尽可能在数据产生和使用的地方进行加密是理想的情况，但在存储基础设施内对静态数据进行加密确实为防止由于媒体丢失（特别是磁带）而导致的数据泄露提供了基本级别的保护。因此，应使用存储设备（自加密驱动器以及基于控制器的技术）、交换机、专用设备、HBAs等中的加密机制。

实施数据加密需要更多工作，不仅仅是购买具有加密功能的设备并将其连接到现有的存储基础设施。需要选择加密机制的位置（加密点）来应对已确定的风险，并安排为该位置提供密钥材料。需要识别要处理的数据，并且在某些情况下可能需要更改其位置。此外，还需要创建适当的加密证明，通常以日志的形式，并将其集成到审计日志基础设施中。更多信息请参见7.5。

所有类型的存储加密都依赖于加密密钥的管理。不良的密钥管理可能会威胁数据的安全，无论加密的强度有多强。最终，由加密保护的信息的安全性直接取决于密钥的强度，与密钥相关的机制和协议的有效性以及为密钥提供的保护措施。所有密钥都需要受到修改的保护，对于对称加密而言，秘密密钥（Symmetric encryption）和对于非对称或公钥加密而言，私钥（Private key）需要受到未经授权的披露的保护。密钥管理为密钥的安全生成、存储、分发和销毁提供了基础。密钥管理的整体框架在ISO/IEC 11770中给出。此外，结构化信息标准推进组织（OASIS）的密钥管理互操作性协议（KMIP）规范和配置文件是存储基础设施内集中密钥管理的主要机制。

对于存储上的静态数据加密，应遵循以下步骤：
- 应使用专门为存储技术设计的加密算法和操作模式，例如用于HDD的XTS-AES（在IEEE 1619-2007中指定）和用于磁带

的Counter with Cipher block chaining Message authentication code（CCM）或Galois/Counter Mode（GCM）（在IEEE 1619.1-2007中描述）；如果没有存储特定的模式，可以使用合适的AES模式，如Cipher Block Chaining（CBC）（在ISO/IEC 10116:2006中指定）；

- 限制密钥以明文形式存在的时间，并防止人员查看明文密钥；
- 密钥只应用于一种目的，具体来说，不要使用密钥加密密钥（也称为密钥包装密钥）来加密数据，也不要使用数据加密密钥来加密其他密钥；
- 从整个密钥空间随机选择密钥；
- 检查并避免使用已知的弱密钥；
- 数据加密密钥应限制在有限的密码周期内（通常不超过2年）或限制在处理的最大数据量；
- 在可能的情况下，存储系统和基础设施应使用互操作性、集中化的密钥管理基础设施（例如，生成和存档加密密钥）；
- 存储系统和基础设施应使用经OASIS批准的、符合KMIP标准的客户端来访问和使用密钥管理基础设施（参见C.8）。

6.8.3 数据减少

作为常规业务的一部分，组织可能会尝试减少存储和传输的数据量，以降低成本。两种较常见的方法是数据压缩和数据去重。数据压缩通过使用已知算法对数据进行编码，产生一个比未编码表示使用更少存储位的数据表示。数据去重则试图用对共享副本的引用替换多个数据副本。这两种技术可以结合使用以最大化数据减少。

数据压缩通常与磁带存储结合使用，以减少备份等方面所需的磁带数量。此外，压缩可以成为远程复制中使用的网络网关的重要组成部分，以降低灾难恢复和业务连续性支持所需的带宽。数据压缩通常在硬件中执行，因此需要注意确保以后能够解码编码数据（例如，当一盘磁带被不同的磁带驱动器读取或接收到网络网关的压缩数据时）。

数据去重可以在存储基础设施的不同位置进行，包括在文件系统级别、在线到存储网络和存储设备上。

本身而言，数据减少技术并不代表安全机制。然而，它们的存在可能受到存储安全活动的影响。

- 当加密与压缩一起使用时，应先应用压缩再应用加密，因为密文不能有效地进行压缩；在另一端应使用相反的顺序（即解密后再展开）。
- 当加密与去重一起使用时，应先应用去重再应用加密，因为去重通常对密文不起作用；在数据需要解密时应使用相反的顺序。
- 当加密与压缩和去重一起使用时，应先使用去重和压缩，然后再加密；在数据需要解密时应使用相反的顺序。
- 压缩或去重可能会影响灾难恢复和业务连续性的实施，因此应将它们纳入灾难恢复和业务连续性解决方案的设计、文档编制和测试中。

7 设计和实施存储安全的指导方针

7.1 总则

尽管个人计算机和部门工作站的计算能力不断增强，但由于需要数据整合、数据一致性和数据质量，对于集中式数据中心仍然存在依赖。随着关键数据量的巨大增长，许多组织已经采用以存储为中心的架构来构建他们的信息通信技术基础设施。因此，存储安全在保护这些数据方面扮演着重要角色，并且在许多情况下，它充当了最后的防线。

设计和实施存储安全解决方案需要遵循核心的安全设计原则。此外，必须将第6条中描述的控制措施和指导方针整合到存储安全解决方案的设计和实施中，以应对存储安全威胁。数据的敏感性、重要性和价值也可以是设计中重要的考虑因素（请参阅附件B，特别是B.1.2节）。

与存储安全架构相关的常见风险领域包括由于设计不当或缺乏适当考虑业务连续性规划，或设计与当前或预期的威胁水平不符。设计应考虑存储系统中所描述的所有相关威胁和漏洞，如5.4节所示。

有关评估安全风险和相关威胁的信息也可以在ISO/IEC 27001、ISO/IEC 27002和ISO/IEC 27005中找到。第7条确定了作为存储安全架构的一部分需要考虑的一般设计问题。

7.2 存储安全设计原则

7.2.1 深度防御

组织需要从不同角度看待安全，而不仅仅是一个层面的观点，而是采用综合性的分层方法，贯穿于所有应用程序、系统、网络、存储和设备中。当这样的分层方法结合了策略、设计、管理和技术时，被视为深度防御。深度防御的追求程度对每个组织是不同的，取决于数据价值和敏感性、合规要求、对抗能力和活动等因素。

一个重要的深度防御原则是利用多种安全控制或安全技术来帮助减轻防御的一个组件被破坏或绕过的风险。例如，当环境中已经存在防火墙和服务器上的病毒防护时，可以在个人工作站上安装反病毒软件。

具体指导包括：
- 确保在三个主要方面（人员、技术和操作）上保持平衡的关注；
- 贯彻有效的信息保障政策和程序，分配角色和责任，投入资源，培训重要人员，并承担个人责任；

- 在多个位置部署保护机制以抵御所有类型的攻击；
- 在潜在对手和目标之间部署多个防御机制（分层）；
- 同时包含检测和保护机制；
- 部署健壮的密钥管理和公钥基础设施（PKI）框架，支持所有信息保障技术，并对攻击高度抵抗；
- 维护可见且最新的系统安全政策；
— 积极管理存储技术和保护机制的安全姿态（例如安装安全补丁和反病毒更新，维护访问控制列表等）；
— 定期进行安全威胁评估，以确定持续的安全状态；
— 监控并针对当前威胁做出反应。

基于分层方法的安全解决方案具有灵活性和可扩展性，并且能够适应组织的安全需求。

对于存储，分层方法意味着安全控制在整个存储基础设施中部署和使用，包括计算机中的HBA/CNA/NIC、存储网络交换机/路由器、存储设备、存储元素和存储设备。

7.2.2 安全域

安全域是基于不同敏感级别的系统资源（即不同的风险容忍值和威胁易感性）应该被放置在不同位置的概念上。这样可以确保系统只提供特定域的任务所需的数据。作为一个设计原则，体系结构应强制执行域分离，以确保实体拥有访问权限的资源不能被另一个实体访问或影响。

对于存储基础设施，一个安全域通常会以SAN的形式表示，特别是当敏感数据在存储系统内部存储和处理时。在数据敏感性较低的情况下，可以考虑使用分区和VLAN，但需要注意的是，这种通用能力不是诸如FC-SP分区（见C.7.5）之类的安全机制。

在ISO/IEC 27033-2中描述的隔离原则的基础上，应考虑以下存储安全设计规则：
- 在使用安全域时考虑数据敏感性
    - 不同敏感级别的存储和存储网络应位于不同的安全域；
    - 为外部网络（例如Internet）提供服务的设备和计算机系统应位于不同的域（非军事区或DMZ），而不是内部网络设备和计算机系统；
    - 关键资产应位于专用安全域；
    - 不受信任的设备和计算机系统应对存储资产具有有限或无访问权限。
- 在使用安全域时考虑目的
    - 用于不同目的（例如开发、生产、管理等）和使用不同技术（例如CIFS/NFS、iSCSI、CDMI等）的存储和存储网络应位于不同的安全域；
    - 存储网络应位于不同的安全域，而不是常规网络（例如公司LAN）；

- 存储设备和存储网络管理系统应位于专用安全域；
- 开发阶段的系统应位于不同的域，而不是生产系统。

- 可以允许位于单个安全域的存储设备，但用于多种目的或包含多个级别的敏感数据的，应进一步隔离（使用分区、VLAN和虚拟存储区域网络或VSAN），以最小化可能的交互作用。

7.2.3 设计弹性

存储安全设计应该包含多层冗余，以消除单点故障，并最大程度地提高存储基础设施的可用性。这包括使用冗余接口、备份模块、备用设备和拓扑冗余路径。此外，设计还应使用广泛的方法，使存储对攻击和网络故障更具弹性。

7.2.4 安全初始化

作为一个设计原则，存储系统的架构应支持安全初始化序列，以确保在施加上电或重置后从“关闭”状态过渡。在初始化阶段，外部可访问的进程和网络接口不应可用或拒绝访问，直到主体经过身份验证。软件和操作系统加载过程应从已知状态开始，该状态由系统管理员在系统最后一次运行时指定。

供应商应在其产品中实现7.2.4中描述的安全初始化功能。

7.3 数据可靠性、可用性和弹性

7.3.1 可靠性

在基本层面上，可靠性是设备在特定条件下在特定时间段内执行其所需功能的概率。可靠性可用以下方式量化：

- 对于可维修产品，是MTBF（平均故障间隔时间），即系统或组件连续故障之间的预期时间，有时被视为系统或组件在故障之间执行正常操作的平均时间（见图5）；
- 对于可维修产品，是MTTR（平均修复时间），即将故障的系统或组件恢复到正常运行所需的预期或观察到的持续时间，有时被视为修复故障组件的平均时间；
- 对于不可维修产品，是MTTF（平均故障时间），即系统或组件在执行正常操作直至发生故障的平均时间。

在存储的背景下，系统的受损和攻击可能会对MTBF、MTTR和MTTF产生负面影响。此外，包括安全功能（如恶意软件防护）、应用系统或应用程序补丁的应用，或者像6.4.5中描述的其他系统加固措施，也可能产生影响。例如，不正确地应用更新或使用来自未经批准或不受信任来源的更新可能会产生不良影响。

- 存储系统和基础设施的可靠性不应受到安全功能的不利影响；
- 应主动管理漏洞，以最小化其对系统可靠性的影响；
- 应评估控制措施，以确定它们是否能够确保数据的可靠性和安全性。

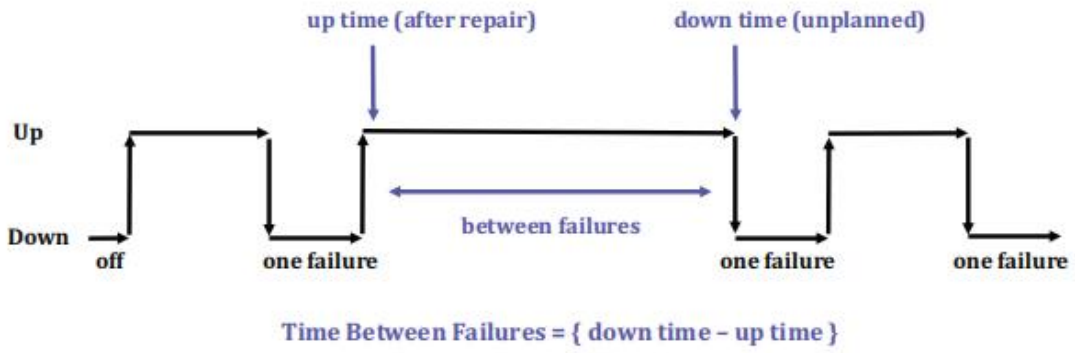


图5 — 可靠性的量化

Figure 5 — Quantification of reliability

7.3.2 可用性

在存储的背景下,数据可用性通常指的是以某种形式存储的数据在通过网络或外部存储介质进行远程存储时的可访问性。这个术语通常用于指涉几个不同的概念，主要包括数据可靠性（与试图访问数据的人的相关性），即“正常运行时间”，以及访问数据的速度。

可用性通常被测量为某物在需要时可用的概率(即系统处于工作状态的时间占总时间的比例），可以通过(a)系统在给定时间段内能够使用的总时间与(b)时间段的长度的比率来计算。例如，一个存储阵列在一年中大约有5分钟的停机时间，假设是24x7运行，它的可用性为0.99999（99.999%）。

为了实现数据的高可用性,在现代存储系统和存储基础设施中实施了大量的硬件和软件冗余（例如自动I/O路径故障转移、冗余组件、RAID保护、全局热备用和带有电池备份的镜像数据缓存）。此外，通常使用数据冗余机制（如镜像和复制）以及数据保护机制（如备份和CDP）来确保在发生故障时能够快速恢复数据。

- 由于可用性的重要性，存储安全的设计和实施应努力将对可用性的影响降到最低（例如，最小化单点故障）。
- 应管理数据加密密钥，以避免在密钥不可用或意外销毁时导致数据可用性问题。
- 数据保护机制（如备份、复制等）应作为可用性设计的一部分，以防止由于系统故障而导致的重大停机。

7.3.3 备份和复制

由于对数据可用性和完整性的依赖增加，许多组织采用各种数据保护机制，如备份和复制，以增加数据的弹性。不幸的是，通常关注的是创建备份和复制数据集，而不是能够利用它们来从问题中恢复。所有的数据保护解决方案都应该被视为数据恢复机制。

数据保护机制本身也需要一定程度的安全性，包括但不限于：
- 数据保护机制（如备份、复制等）应设计为快速恢复，而不仅仅是数据保存；
- 备份安全
  - 确保备份方法，尤其是对于业务/任务关键数据，与其相关的还原策略相一致；
  - 确保备份方法提供足够和适当的保护，防止未经授权的访问（例如，加密或用户验证）；
  - 建立一系列可信任的个人（和供应商），他们处理存储介质；
  - 实施备份验证，以证明符合还原要求。
- 复制安全
  - 确保复制方法，尤其是对于业务/任务关键数据，与其相关的可靠性、容错性或性能要求相一致；
  - 确保复制方法提供足够的保护，防止未经授权的访问（例如，数据传输加密）。
- CDP安全
  - 确保CDP方法（例如，连续、准连续、固定间隔等），尤其是对于业务/任务关键数据，与其相关的还原策略相一致；
  - 在高网络带宽场景下（例如，多媒体文件），采用限速技术，优先处理网络流量，以减少CDP对日常运行的影响；
  - 确保CDP方法提供足够的保护，防止未经授权的访问（例如，数据传输和数据静态加密）。

7.3.4 灾难恢复和业务连续性

ISO/PAS 22399:2007总结了业务连续性管理（BCM）的方法，包括预防、应对和恢复事件。BCM包括事故准备、运营连续性管理（IPOCM）、灾难恢复计划（DRP）和风险缓解，重点是提高组织的弹性，使其在预定的时间范围内有效地应对事件并恢复。

ISO/IEC 27031:2011描述了用于业务连续性的ICT准备性（IRBC）的概念和原则，并提供了一套方法和流程框架，以识别和规定提高组织ICT准备性的所有方面（如性能标准、设计和实施），以确保其ICT服务/基础设施在发生可能影响关键业务功能的新兴事件、事故和相关中断（包括安全性）时，能够支持业务运营。它适用于任何组织（私人、政府和非政府，无论规模大小）开发其ICT准备性计划，并要求其ICT服务/基础设施在发生紧急事件和事故时准备支持业务运营，并保证其IRBC的绩效参数能够以一致和认可的方式相互关联。

存储通常是组织IRBC计划或非正式DR/BC活动的关键要素，因此有必要：
- 确保将存储生态系统纳入DR/BC规划和实施；
- 为有限的中断事件（系统故障、对抗性攻击、操作员错误）做好准备；
- 识别和记录与存储生态系统相关的独特人员和设施要求；
- 进行持续规划和定期测试假设，这对于成功的DR/BC至关重要；DR/BC测试的结果应反馈到持续维护DR/BC计划中。

7.3.5 弹性

弹性是在面对故障（系统故障）和挑战（如攻击、事故或大规模自然灾害）时，提供和维持可接受水平的服务能力，通常与保持数据完整性和可用性相关联。由于其对数据整体可用性的影响，这种能力通常在存储系统和基础设施的部署中是一个重要考虑因素。

在考虑弹性时，个别组件的故障可能是可以接受的，只要服务仍在提供且服务的完整性仍然存在。在实际情况中，弹性是一种设计策略，旨在减少漏洞，通常通过缩短供应线路、提高关键区域的冗余性、增强本地能力并解决更深层次的依赖和失能问题来实现。

- 安全应是弹性战略的一个重要组成部分；要考虑存储和安全技术的单元故障和妥协情况。
- 应尽可能利用冗余性。
- 在可能的情况下，使用易于修复的多样化组件。
- 安全功能和功能（例如加密、集中身份验证等）应以不对存储系统或基础设施的弹性产生不利影响的方式实施。

7.4 数据保留

7.4.1 长期保留

由于传统存储组件的寿命较短且可靠性有限，随着媒体随着时间的推移逐渐退化，数据可能会损坏。这个问题对于从事长期保留数据（例如管理数据归档）的人员来说相对较为明确，它在以下适用于存储基础设施的标准中得到了解决：
- ISO/TR 10255:2009，文件管理应用 – 光盘存储技术、管理和标准
- ISO/TR 18492:2005，电子文档信息的长期保存
- ISO 16175-1:2010，信息与文献 – 电子办公环境中的记录的原理和功能要求 – 第1部分：概述和原则声明
- ISO 16175-2:2011，信息与文献 – 电子办公环境中的记录的原理和功能要求 – 第2部分：数字记录管理系统的指南和功能要求

- ISO 16175-3:2010，信息与文献 - 电子办公环境中的记录的原理和功能要求 - 第3部分：业务系统的记录的指南和功能要求

长期归档存储系统引入了不同于非归档存储系统的完整性、认证和隐私威胁。此外，数据的长寿命给攻击者提供了一个更大的窗口，在其中他们可以尝试攻击安全系统；在归档存储中，攻击者可能有数十年的时间进行攻击（缓慢攻击）。

- 归档存储假定具有一次写入、可能多次读取的访问模式，因此应定期主动检查系统中数据的完整性，而不是等到读取时才检查。
- 在将归档数据迁移到更新的存储技术时，引入可用的安全功能，以提供增强的安全措施，以更好地保护数据在新位置的安全性。
- 由于长期存档中的数据可能超过数据所有者的寿命，安全的归档存储系统应能够对新用户进行身份验证，并建立他们与附加到现有用户的资源的关系。
- 机密性机制（例如加密、秘密共享等）应在完全没有编写数据的用户的情况下运行（例如，给予具有读取数据权限的新用户应该同时具有解密数据的能力）。
- 安全日志记录应该足够完整且长期保存（以几十年为单位），以帮助检测缓慢攻击并维护攻击历史，以用于决策调整数据保护。
- 该系统应立即处理任何妥协情况，或保持妥协历史，以便智能安排纠正措施。
- 使用数据减少技术（例如压缩和去重）时，应以不损害数据完整性的方式使用（例如，考虑到可能与数据减少技术没有任何关联的副本）。

7.4.2 短期到中期的保留

许多组织被迫保留数据的时间段比传统存档短（少于10年）。通常，保留的原因是基于法律、监管或法定要求，其中也包括安全规定。不满足这些要求可能会导致组织面临重大责任。

为了确保在短期到中期保留期间成功保留数字信息，需要采用与保留的信息价值、从所有因素中损失的风险以及保留期内可接受的损失量相匹配的数据保护、灾难恢复和数字保护和维护实践。从存储角度来看，这些短期和中期数据保留方案通常涵盖一个或多个技术代的时间，并需要捕获和保留相关的元数据。以下内容适用于短期和中期保留：
- 创建和保存数据的多个物理或逻辑副本；副本需要尽可能地组织得独立（例如，地理位置、行政/管理和平台/操作系统），其数量应根据数据的价值和风险容忍度来选择。
- 在规定的时间表内进行审核，检查明显和潜在的故障（例如完整性检查）以及它们可能导致的损害；在损害蔓延之前，使用其他副本中的良好数据来修复损坏的数据。
- 将访问控制方案与所保存信息的法律和监管要求相匹配。
- 确保责任和可追溯性措施足够且有效；所有数据访问可能需要审计日志记录。
- 实施机制以证明数据的真实性、来源和保管链，特别是对于具有证据性质的数据。

- 如果使用加密，应将密钥和密钥材料存档/托管；在建议的加密周期内或当底层加密算法需要替换时重新生成数据的密钥。

7.5 数据保密性和完整性

在评估基于存储的加密解决方案时，需要考虑多个因素，包括但不限于以下内容：
- 加密可能会影响其他安全方面（例如，数据检查、反病毒等）；
- 虽然加密是必要的，但它可能使数据不可用，如果数据处理、数据转换、密钥管理或实际加密出现任何问题；
- 加密可能会对系统和存储元素造成重大开销或影响；
- 当加密与跨区域复制用于灾难恢复和业务连续性时，可能需要集中密钥管理；
- 加密可能会降低或抵消数据减少技术（例如压缩和去重）的效益；
- 加密的密码学质量（安全强度、经过验证等）会影响实际提供的保护水平。

并非所有数据都值得加密。风险评估可以帮助确定需要使用加密的敏感和高价值数据，并协助进行成本效益分析（即，风险减少是否值得成本）。
重要的是要注意，当数据被视为关键资产时，还有其他方法来保护信息的机密性。

如在6.8.2.3中所述，加密的点很重要，因为它代表了数据在ICT基础设施中必须经过的位置，然后才能解密并可用。常见的安全观点是尽可能接近源头处进行加密，因为这往往可以最大程度地提供保护，但在选择加密点时可能有许多选项（参见图6），包括：
- **应用级别**：在特定应用程序或数据库的控制下进行加密；具有最精细的控制粒度和对数据（类型、用户、敏感性）的最大了解。
- **文件系统级别**：在操作系统或操作系统级别应用程序的控制下进行加密；在文件级别进行控制，并对用户有深入了解。
- **网络级别**：在网络设备（如HBA、存储控制器或交换机）的控制下进行加密。
  - 基于文件的（NAS）：在共享/文件系统级别进行控制（可能是文件级别），并对用户有适度了解。
  - 基于块的：在逻辑卷级别进行控制，并对“用户群体”有有限的了解。
- **设备级别**：在最终设备（例如磁带驱动器、磁盘阵列、硬盘驱动器等）的控制下进行加密；在介质级别进行控制（可能在逻辑卷级别进行控制），并对“用户群体”有有限的了解。

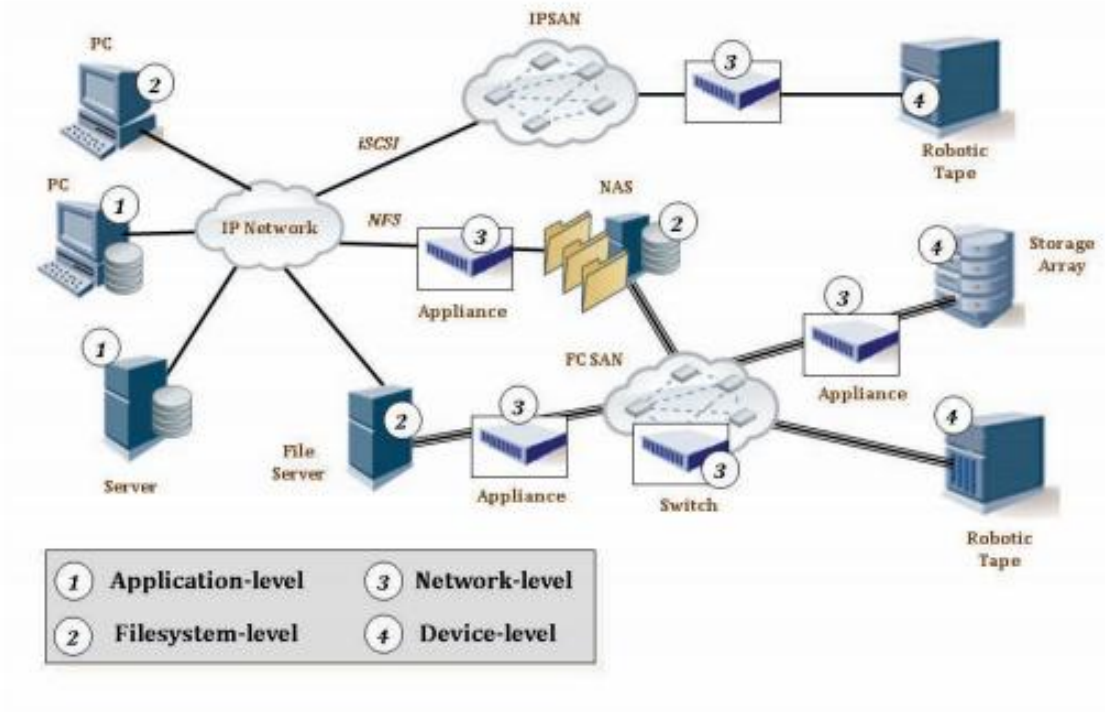


图6 — 加密示例点

Figure 6 — Sample points of encryption

当认为需要加密时，请考虑以下指导：

- 对于敏感数据，存储基于加密的加密不应是主要的加密形式；
- 在选择加密点时，应考虑灾难恢复和业务连续性、数据减少和数据保护等因素；
- 在选择和部署加密时，应考虑数据保留需求；
- 加密解决方案的安全强度应至少为112位，推荐最低安全强度为128位；
- 用于保护敏感或受管制数据的密码模块应使用认可的标准进行验证（例如，ISO/IEC 19790、ISO/IEC 15408、NIST FIPS 140-2等）；
- 可以使用多个加密步骤，例如，对于为了保护隐私而加密的数据，可以进一步通过自加密驱动进行安全加密。

与清除数据一样，重要的是组织保留数据加密的记录，以记录受保护的媒体以及何时和如何加密它们。当怀疑组织失去对包含敏感信息的存储媒体的控制时，这些记录或加密证明可以有助于证明没有发生数据泄漏，从而避免昂贵的数据泄漏通知和其他责任。以下内容应被视为加密的证据：

- 确保加密机制创建适当的审计日志条目（激活、验证、完整性检查、重新密钥等）；
- 预先商定哪些审计日志材料可以证明（对合规人员的满意程度）加密已正确执行；
- 定期进行经审计的检查，确保加密已正确执行，并考虑外部认证。

成功使用加密取决于遵守与密钥材料相关的基本原则以及实施密钥管理。随着存储系统和设备集成用于数据静止的加密，密钥管理变得重要，应解决以下问题：
- 利用集中的密钥管理；
- 尽可能完全自动化密钥管理；
- 少用寿命长的密钥（即接近最大建议的加密周期，通常不超过1-2年，取决于密钥类型）；
- 强制执行严格的访问控制，限制用户权限和分离职责约束（例如，安全角色），用于密钥的生成、更改和分发；
- 对于敏感或高价值数据，加密应该是端到端的（即数据在传输和静止时都要加密）。

数据完整性是大多数存储系统和基础设施的重要设计准则，它在重要性上仅次于数据可用性。为了解决数据完整性问题，通常在存储基础设施中部署各种技术，包括但不限于RAID、备份、复制和CDP。尽管重要，这些数据保护技术通常不被视为存储安全控制的一部分。

数据保留和合规要求通常包括以阻止记录删除或更改（即不可变性）为特点的存储数据的方式，同时要求进行完整性验证（例如，哈希）和明确的保留期限（例如，法定保留）。可以使用多种基于WORM（写一次、读多次）的存储来满足不可变性（不可编辑）要求。此外，许多CAS（参见6.7.3）实现将WORM与可用于执行明确完整性检查并执行数据到期的元数据相结合。

- 恶意软件是破坏数据、应用程序和操作系统完整性的常见威胁；存储系统应包括足够的恶意软件保护，以防范对数据的攻击（例如破坏、销毁等）；
- 应使用基于WORM的存储来满足不可变性要求；

厂商应在其产品中实现7.5节中描述的加密、密钥管理和完整性功能。

7.6 虚拟化

7.6.1 存储虚拟化

存储虚拟化将服务器和应用程序使用的逻辑存储抽象与存储信息的物理存储系统、设备或介质分离，使得逻辑与物理的关系随着时间变化，同时可以隐藏物理实体的细节。例如，在服务器或存储阵列中的逻辑卷管理器可以将多个物理磁盘驱动器的部分区域呈现为一个镜像的逻辑卷，并在原始驱动器中的一个故障后能够重建镜像卷以使用另一个磁盘驱动器。另一个例子是存储阵列中的自动分层功能可以根据访问模式的变化（例如，将更频繁访问的信息移动到性能更高的驱动器上）来改变信息存储的驱动器。

存储虚拟化的存在是控制设计和应用的重要考虑因素。控制可以应用于逻辑或物理存储实体。对于逻辑存储实体的控制不受信息的物理迁移的影响，但对于物理实体的控制应该应用于整个物理实体域（例如，存储系统、设备、介质），以避免信息的迁移导致控制被绕过。
当存储虚拟化可以在分布式实体域（例如，在多个存储系统中存储的信息并随时间迁移）上存储或迁移信息，并且正在使用存储网络时，适当的存储网络控制（见6.3）应该应用于整个域，因为将这样的控制应用于域的子集可能会导致信息迁移时绕过控制，或者新的受控信息存储在尚未应用该控制的实体上。

如果存储虚拟化暴露了虚拟化的物理存储实体（例如，由存储阵列虚拟化的外部存储），则应该应用控制来限制或防止直接访问非虚拟化的物理元素，因为这样的访问与访问虚拟化存储不等同。

当存储被虚拟化时，物理存储实体上的数据清除控制（见6.8.1）和数据静止加密控制（见6.8.2）应该假设受控存储实体（例如，系统、设备和介质）可能包含在其上存储的最敏感信息。例如，如果使用加密来控制存储在从存储阵列中移除的磁盘驱动器上的数据的机密性（例如，因为驱动器发生故障），并且该存储阵列实现了存储虚拟化，则加密算法应该适用于保护存储阵列可能存储的最敏感数据。

其他虚拟化方面的考虑包括：
- 确保虚拟存储的适当服务级别目标，包括：
  - 将存储基础设施的可用性目标与应用程序要求相匹配；
  - 将存储基础设施的机密性和隐私要求与存储的信息类型相匹配。
- 根据需要解决多租户问题（参见7.7.4）。

7.6.2 用于虚拟化系统的存储

服务器虚拟化将典型操作系统的共享资源访问扩展到一种模型，其中虚拟化软件提供了超过一个计算机、硬盘驱动器、打印机等的幻觉。物理服务器通常运行一个负责创建、释放和管理“客户”操作系统或虚拟机（VM）资源的虚拟化软件。这些客户操作系统被分配了物理服务器资源的一部分，通常以使客户不知道除了虚拟化软件分配给它的资源外的任何其他物理资源。

当使用存储系统和基础设施来支持虚拟化服务器时，通常需要额外的注意，以确保数据可用，但不会过度暴露于潜在的数据泄漏风险。

以下是相关的虚拟化存储指南，应该遵循：
- VM对存储网络的访问应通过服务器虚拟化（hypervisor）软件中的访问控制进行控制；

– 应适当地利用N_Port_ID虚拟化（NPIV）来限制虚拟机对存储目标的访问（有关NPIV的详细信息，请参见C.6），包括：

– 使用虚拟机特定的世界范围端口名（WWPN）配置FC SAN区域和呈现LUN，以便LUN只对该虚拟服务器可见，而不对任何其他虚拟服务器可见；

– 避免由于资源限制（例如，服务器、网络结构和存储中的状态相关信息）导致的扩展问题，通过限制NPIV的使用仅创建必要的N_Port_ID，以在较大的域（例如，单个组织或服务提供商的单个租户的VM集合）之间提供隔离。

– 控制基础设施中物理服务器之间的虚拟机迁移/移动，以避免产生意外的安全后果，例如：

– 将虚拟机从风险较低（更受信任）的域移动到风险较高（较不受信任）的域可能会暴露服务器包含或允许处理的敏感信息，除非其配置得到适当加固；

– 相反，当虚拟机从风险较高（较不受信任）的域移动到风险较低（更受信任）的域时，其加固配置可能会干扰正常操作，除非与适用于较低安全性域的配置相匹配；

– 虚拟机可能会移动到受损的虚拟化服务器，从而使数据处于风险之中。

7.7 设计和实施考虑因素

7.7.1 加密和密钥管理问题

使用加密技术引入了一些不可忽视的挑战。这些挑战可能包括严格的规定，管制技术的进口/出口，以及在某些故障条件下导致灾难性损失。

以下是相关的加密和密钥管理指南，应该遵循：

– 遵守进口/出口管制，包括：

– 了解和遵守与加密和密钥管理相关的政府进口规定；

– 了解和遵守与加密和密钥管理相关的政府出口规定；

– 遵守企业或政府的密钥托管要求；以及

– 了解和遵守为企业官员、执法机构等提供加密密钥的企业或政府要求，以便访问和恢复加密数据。

– 问题计划：

– 在密钥泄漏事件发生时拥有恢复计划；

— 确保存在密钥备份计划，以确保对加密的业务/任务关键信息持续访问。

— 其他问题领域

— 在处理/访问相同数据的存储设备之间安全地分发密钥材料。例如，数据在一个节点上进行加密，但在第二个节点上进行解密；

— 需要了解加密对去重和压缩技术的影响，并在设计和实施中加以考虑；

— 需要了解不能对加密数据应用病毒扫描等安全技术的情况，并通过其他机制加以缓解。

7.7.2 对齐存储和策略

ISO/IEC 27002:2013第5.1条指出，“应该定义一组信息安全政策，并经过管理层批准，发布并向员工和相关外部方通报。”政策的存在与否在确保安全和合规性方面起着重要作用。

— 将存储纳入政策中

— 确定最敏感（个人可识别信息、知识产权、商业机密等）和业务/任务关键数据类别，以及相应的保护要求；

— 将存储专用政策与其他政策整合（即避免为存储生态系统创建单独的政策文件）；

— 解决数据保留和保护问题（例如写入一次读取多次或WORM、真实性、访问控制等）；

— 解决数据销毁和媒体清除问题。

— 遵守政策

— 确保存储生态系统的所有要素符合政策（例如，ISO/IEC 27001:2013第5.2条和ISO/IEC 27002:2013第5条）；

— 对最敏感/最关键的数据给予优先考虑。

7.7.3 合规性

遵守法律和监管要求已成为全球范围内一个重要问题,这种合规性正推动许多组织的安全议程和战略。除了ISO/IEC 27002:2013第18条中的相关合规性指南外，以下元素是与信息系统审计员相关的存储系统和基础设施合规性方面的关键因素。

— 可追溯性

— 确保记录的事件/事务数据包含足够的应用程序或系统细节，以清楚地识别来源；

— 确保用户信息可以追溯到特定个人；

— 在适当的情况下，将日志记录视为证据（链式监管、不可否认性、真实性等）。

— 检测、监控和评估

— 确保存储层参与外部审计日志措施；

— 监控审计日志事件并发出适当的警报。

— 信息保留和清除

— 实施适当的数据保留措施；

— 实施适当的数据完整性和真实性措施；

— 在硬件删除、重新利用或停用时正确地进行数据清除；

— 在生命周期结束时正确地进行虚拟服务器镜像及其副本的数据清除。

— 隐私

— 实施适当的数据访问控制措施以控制对数据和元数据（例如，搜索结果）的访问；尽可能采用最小权限策略；

— 实施适当的数据保密措施以防止未经授权的披露。

— 法律
— 确保数据去重使用不与数据真实性要求冲突；
— 确保数据和媒体清除机制不违反保存令；
— 确保处理证据数据（例如，审计日志、元数据、镜像、时间点副本等）时遵循适当的监管程序。
注意：附录B可以是审计存储系统和基础设施时有用的资源。

7.7.4 安全的多租户

多租户，根据Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014的定义，侧重于“分配物理和虚拟资源，使得多个租户及其计算和数据与其他租户隔离且无法访问彼此。”安全的多租户在此概念基础上增加了安全控制，明确防范数据泄露，并允许验证这些控制状态（例如，它们处于活动状态）和验证控制的有效性（即确保它们起作用）。
在考虑安全的多租户时，包括租户（包括其管理员）的视角非常重要。因此，安全的多租户解决方案需要具备以下能力，既能提供安全隔离，同时又能提供共享资源的管理和灵活性优势，确保：
— 没有租户能确定其他任何租户的存在或身份；
— 没有租户能访问其他任何租户的数据在传输中（网络）；
— 没有租户能访问其他任何租户的数据静态（存储）；
— 没有租户能执行影响其他租户操作的操作；
— 没有租户能执行可能导致拒绝服务的操作；
— 每个租户的配置与其他租户的存在和配置独立（例如在命名或寻址方面）；
— 当从租户处注销资源（计算、存储或网络）时，该资源应被清除所有数据和配置信息；
— 可在租户级别提供问责和可追溯性措施。
在用于部分或整体用于安全的多租户解决方案的存储系统和基础设施中，应使用以下附加安全措施：
— 与租户对资源使用方式相匹配的加密存储；
— 强大的对称加密（即至少128位的安全强度）来保护静态数据；
— 安全快速的去配置化（请参阅附录A中的介质清除，包括加密擦除）；
— 受信任的第三方数据存储管理（例如，SNMPv3，带有TLS的SMI-S30等）；
— 自动化的密钥管理提供租户控制的密钥管理（使用符合KMIP标准的服务器）；
— 安全的数据复制（例如，数据在传输中和静态数据的加密）；
— 保护数据免受管理员的影响（例如，强制执行最小权限访问模型，管理员不能访问密钥材料等）；
— 高度可用的存储网络设备（多路径和多样路径）；
— 集中且安全的审计日志记录（例如，TLS上的syslog）；

— 密码模块和其他安全措施（例如，介质清除，访问控制等）的验证和认证（例如，公共标准标准）。
厂商应在其产品中实现7.7.4中描述的安全多租户功能。

7.7.5 安全的自主数据移动

许多存储系统和基础架构具备在不同存储设备和存储元素之间移动数据的能力（例如，层级存储），在数据中心之间进行数据复制（例如，同步和异步数据复制），传输至数据归档设施，或备份至数据保护系统（例如，磁带机器人或虚拟磁带）等。在信息生命周期管理（ILM）和数据生命周期管理（DLM）解决方案中，还存在更复杂的场景。然而，所有这些情况都假设：
- 数据移动是基于策略的；
- 没有必要要求操作员或计算机在整个过程中进行介入或干预。

由于自主数据移动具有多种形式，其安全需求可能会有很大的差异，可能包括以下部分或全部内容：
- 账户与追踪
  - 配置数据移动策略应限制为经过身份验证和授权的特权用户；
  - 建立配置的个人应熟悉源和目的地的安全属性；
  - 实施或终止自主数据移动的配置更改应在审计日志中反映；
  - 所有自主数据移动事务应在执行数据移动的系统的审计日志中反映；
- 完整性、真实性和不可变性
  - 作为自主数据移动事务的一部分，应验证数据的完整性（最好使用加密散列函数）；
  - 自主数据移动事务不应影响数据的真实性（例如，原始系统元数据如创建日期、最后访问时间等在移动后的数据中应正确表示）；
  - 自主数据移动事务不应破坏不可变性或其他数据保护控制（例如，支持法定保留）。
- 保密性
  - 自主数据移动事务不应削弱或消除与数据相关的加密控制；
  - 跨系统的自主数据移动事务应包含敏感和高价值数据的数据传输加密。
- 消除
  - 作为自主数据移动事务的一部分，应适当地对源数据或存储介质进行消除（参见6.8.1.2和6.8.1.3），然后才能重新使用；
  - 在进行自主数据移动时执行消除操作时，还应进行验证（参见6.8.1.5），并提供某种形式的消除证明（参见6.8.1.4）。
- 可信度与物理安全性

- 自主数据移动事务不应使数据跨越安全域（例如，从生产环境移动到开发环境）；
- 自主数据移动事务不应将数据移动到没有足够认证和授权的系统；
- 自主数据移动事务不应将数据移动到物理安全性不足的系统。

厂商应在其产品中实现7.7.5中描述的安全自主数据移动功能。

附录 A（规范性附录）

媒体消除

A.1 媒体消除的方法

媒体消除可以使用多种不同的方法，其中最常见的三种方法如下：

— **清除（Clear）**- 一种媒体消除方法是使用软件或硬件产品，将媒体上的存储空间覆盖为非敏感数据。此过程可以通过接口覆写，或者使用适当的ATA/SCSI固件命令覆写逻辑可寻址和逻辑不可寻址的物理媒体。通过接口覆写应包括覆盖文件的逻辑存储位置（例如，文件分配表），也可以包括所有可寻址的位置。覆盖的安全目标是用固定或随机数据替换所有先前写入的数据。覆盖不能用于已损坏或不可重写的媒体。媒体类型和大小也可能影响覆盖是否适用作为媒体消除的方法。

— **清洗（Purge）**- 消除的方法包括退磁、密码擦除（见A.3）以及执行适当的ATA/SCSI固件命令，对逻辑可寻址和逻辑不可寻址的物理媒体使用块擦除操作。退磁不适用于含有非磁性介质（例如SSD或SSHD）的设备。

— 消磁（Degaussing）是将磁介质暴露于强磁场，以干扰记录的磁区域。磁场消磁器是用于消除磁性媒体的设备。磁场消磁器根据它们可以擦除的磁性媒体类型（即低能量或高能量）进行评级。磁场消磁器使用强永磁体或电磁线圈。退磁可以是一种有效的方法，用于消除受损或无法工作的媒体，用于消除存储容量异常大的媒体，或用于快速消除软盘。

— 加密擦除（Cryptographic Erase）利用目标数据的加密，从而使目标数据的加密密钥得到消除。这样，在媒体上只剩下密文数据，实现了数据的消除。

— **销毁（Destruct）**- 有许多不同类型、技术和程序可用于媒体销毁。如果由于信息的高安全分类而决定进行销毁，那么在销毁之后，媒体应该能够抵抗实验室攻击。

— 分解（Disintegrate）：这是一种设计用于完全破坏媒体的消除方法，通过将其打碎或分解（例如，用酸溶解）成构成元素、部件或小颗粒。

— 焚烧（Incinerate）：这是一种设计用于完全破坏媒体的消除方法，通过将其烧成灰烬。

— 熔化（Melt）：这是一种设计用于完全破坏媒体的消除方法，通常通过施加热源将其熔化。

— 粉碎（Pulverize）：这是一种设计用于完全破坏媒体的消除方法，通过将其研磨成粉末或尘埃形式。

— 撕毁（Shred）：可以使用碎纸机来销毁柔性媒体，例如软盘，一旦将媒体从其外部容器中取出。垃圾的碎纸尺寸应足够小，以合理地确保数据的保密性，使数据无法被重建。

— **硬拷贝（Hard Copy）**：硬拷贝媒体是信息的物理表现形式，通常与纸质打印件相关。然而，打印机和传真机的色带、鼓片和印版都是硬拷贝媒体的例子。与产生纸质打印件有关的耗材通常是最不受控制的。包含敏感数据的硬拷贝材料如果在没有有效消除的情

况下离开组织，会给“垃圾桶翻找者”和过于好奇的员工带来严重的漏洞风险，从而可能发生意外泄露。表A.1提供了此类媒体的指导。

— **电子（或软）拷贝（Electronic or Soft Copy）：**电子媒体是包含位和字节的设备，例如硬盘驱动器（HDD）、随机访问存储器（RAM）、只读存储器（ROM）、磁盘、存储设备、手机、移动计算设备、网络设备、办公设备等多种类型。表A.2、A.3、A.4、A.5、A.6、A.7、A.8和A.9提供了常见电子媒体的指导。

表A.1 – 硬拷贝存储消毒

消毒方法	说明
纸张和缩微胶卷	
清除/清洗：	不适用，请参阅"摧毁"。
销毁：	使用可产生1 x 5毫米大小(或更小)颗粒的横撕碎纸机销毁纸张，或使用装有1.5毫米安全筛网的分解装置粉碎/分解纸张材料。 通过焚烧销毁缩微胶片(缩微胶片、缩微胶片或其他缩小图像的照片底片)。材料燃烧后，残留物会变成白色灰烬。

表A.2 – 网络设备消毒

消毒方法	说明
路由器和交换机(家庭、家庭办公室、企业)	
清除：	执行完整的制造商重置，将路由器或交换机重置为出厂默认设置。
清洗：	请参阅"销毁"。大多数路由器和交换机只提供清除(而非清洗)数据内容的功能。路由器或交换机可能提供清除功能，但这些功能与设备的硬件和固件有关，应用时应谨慎。请咨询设备制造商，以确定设备是否具有应用介质相关技术(如重写或块擦除)的清除功能，以确保数据恢复不可行，而且设备不会简单地删除文件指针。
销毁：	将设备撕毁、分解、粉碎，或在有许可证的焚烧炉中焚烧。
对于 "清除" 和 "清洗" (如适用)，有关正确消毒程序的更多信息，请咨询制造商。 网络设备可能包含可移动存储。应使用特定媒体技术移除可移动媒体并对其进行消毒。	

表 A.3 – 移动设备消毒

消毒方法	说明
苹果iPhone和iPad	
清除/清洗：	选择完全清除选项。如果支持加密擦除，则清除操作可能只需几分钟；如果设备应用了依赖介质的非加密清除技术，即利用覆盖技术，则清除操作可能需要几个小时(取决于介质大小)。
销毁：	将设备撕毁、分解、粉碎，或在有许可证的焚烧炉中焚烧。
黑莓	
清除/清洗：	选择完全消毒选项，确保选择所有子类别的数据类型进行消毒。根据介质大小，消毒操作可能需要几个小时。
销毁：	将设备撕毁、分解、粉碎，或在有许可证的焚烧炉中焚烧。
运行谷歌安卓操作系统的设备	
清除：	选择完全消毒选项。
清洗：	安卓设置和功能可能会被设备供应商或服务提供商修改，因此不应假设出厂数据重置所提供的保证程度。某些版本的Android支持加密，并可能支持加密擦除。请咨询设备制造商(如果适用，也可能咨询服务提供商)，以确定设备是否具有应用介质相关技术(如重写或块擦除)或加密擦除的"清除"功能，以确保数据恢复不可行，并且设备不会简单地删除文件指针。
销毁：	将设备撕毁、分解、粉碎，或在有许可证的焚烧炉中焚烧。
所有其他移动设备这包括手机、智能手机、个人数字助理、平板电脑，以及上述移动设备类别未涵盖的其他设备。	
清除：	手动删除所有信息，然后执行完整的制造商重置，将移动设备重置为出厂状态。
清洗：	请参阅"销毁"。许多移动设备只提供清除(而非清洗)数据内容的功能。移动设备可能提供清除功能，但这些功能是设备硬件和软件的特定功能，应用时应谨慎。应向设备制造商咨询，以确定设备是否具有应用介质相关技术(如重写或块擦除)或加密擦除的清除功能，以确保数据恢复不可行，而且设备不会简单地删除文件指针。
销毁：	将设备撕毁、分解、粉碎，或在获得许可的焚烧炉中焚烧。

可能需要拆卸电池和显示屏。执行"清除"或(如适用)"清理"操作后，手动导航到设备的多个区域(如通话记录、浏览器历史记录、文件、照片等)，以验证设备上未保留任何个人信息。对于"清除"和"清洗"(如适用)，请向制造商咨询正确的消毒程序。有关正确消毒程序的更多信息，以及设备版本和操作系统版本之间的实施差异详情，请咨询制造商。使用指南进行正确的初始配置有助于确保数据保护和清除保证级别尽可能强大。如果设备包含可移动存储介质，请确保使用适当的介质相关程序对介质进行清除。

表 A.4 – 设备消毒

消毒方法	说明
办公设备 包括复印机、打印机、传真机和多功能机	
清除:	执行完整的制造商重置，将办公设备重置为出厂默认设置。
清洗:	请参阅 "销毁"。大多数办公设备只提供清除(而非清除)数据内容的功能。办公设备可 能提供清除功能，但这些功能是特定的 设备的硬件和固件，应谨慎使用。请向设备制造商咨询，以确定设备是否具有应 用介质相关技术(如重写或块擦除)或加密擦除的 "清除 "功能，以确保数据恢复 不可行，而且设备不会简单地删除文件指针。办公设备可能有可移动存储介质，如果 有，则可对相关存储设备应用依赖于介质的清除技术。
销毁:	将设备撕毁、分解、粉碎，或在获得许可的焚烧炉中焚烧。
对于 "清除 "和 "清理" (如适用)，请手动导航到设备的多个区域(如存储的传真号码、网络配置信息等)，以验证设备上没有保留任何个人信息。 对于 "清除 "和 " 清理" (如适用)，应根据适用的法律、环境和健康考虑，移除并销毁或处理墨水、墨粉 和相关耗材(鼓、熔断器等)。其中一些耗材可能会保留机器打印的数据印记，因此可能会造成数据暴 露的风险，应进行相应处理。如果设备功能正常，降低相关风险的一种方法是打印空白页，然后打印全 黑页，再打印空白页。对于带有专用彩色组件(如青色、品红色和黄色墨粉及相关耗材)的设备，也应 在空白页之间打印每种颜色的一页。打印出来的纸张应在办公设备保密(消毒前)的情况下处理。请注意，这些程序不适用于一次性使用的墨水/碳粉等耗材，因为它们通常不会再次使用，因此不会通过设备 发送更多页面来处理。办公设备耗材也可能对健康造成危害，应使用适当的程序进行处理，以尽量减少 与打印组件和墨粉的接触。 对于 "清除 "和 " 清洗" (如适用)，有关正确消毒程序的更多信息，请咨询制造商。	

表 A.5 – 磁性介质消毒

消毒方法	说明
软盘	
清除:	使用组织批准的软件覆盖介质，并验证覆盖的数据。清除程序应至少包括一次写入固定 数据值(如全部为零)的过程。也可选择使用多次写入或更复杂的值。
清洗:	在组织认可的消磁器中进行消磁。
销毁:	焚烧软盘和磁盘，可在有许可证的焚化炉中焚烧或粉碎。
可移动柔性或刚性磁盘 包括 、 Floptical、 Jaz、 SyQuest、 LS-120 等。	
清除:	使用组织批准的软件覆盖介质，并验证覆盖的数据。清除程序应至少包括一次写入固定 数据值(如全部为零)的过程。也可选择使用多次写入或更复杂的值。
清洗:	在组织认可的消磁器中进行消磁。
销毁:	焚化磁盘和软盘的方法是在获得许可的焚化炉中焚烧或粉碎。
卷式和盒式磁带 还包括8 毫米、DDS DAT、DLT、QIC 等。	
清洗:	有四种选择: a)如果支持，应用SANITIZE命令。可以使用以下一个或两个选项: 1)OVERWRITE服务操作。利用反相选项，对伪随机模式总共进行三次传递，以便第二次传递是指定模式的反相版本。2)如果设备支持加密，则可使用CRYPTOGRAPHIC ERASE服务操作。可选：在对设备成功应用加密擦除后，使用OVERWRITE服务操作(如果支持)在介质上写入一次零或伪随机图案。如果不支持"擦写"服务操作，则可使用"清除"程序。 b)通过TCG Opal SSC或Enterprise SSC接口进行加密擦除，根据需要发出命令，使所有MEK发生变化(不支持部分清除)。更多信息，请参阅TCG和出货TCG Opal或Enterprise存储设备的供应商。 可选：在对设备成功应用加密擦除后，使用OVERWRITE服务操作(如果支持)在介质上写入一次零或伪随机图案。如果不支持"擦写"服务操作，则可使用"清除"程序。 c)如果前两个选项都不支持，则可使用本地读写接口至少写入一次固定数据值(如全部为零)。也可以使用多次传递或更复杂的值。 d)使用组织认可的自动消磁器进行消磁，或拆卸硬盘驱动器，并使用组织认可的消磁棒清除封闭的盘片。在使用SANITIZE命令和OVERWRITE服务操作时，如果使用了三次遍历和反转(也称为补充)选项，验证过程将只搜索原始模式(在第三次遍历中再次写入)。虽然人们普遍认为一次覆写就足以清除数据，

	但如果有一个包含反转数据模式功能的专用命令，就可以采用一种高效、有效的方法，降低与不同设备制造商磁记录功能实施差异相关的任何残余风险。
销毁：	将设备撕毁、分解、粉碎，或在有许可证的焚烧炉中焚烧。
SCSI硬盘/SSHD,包括并行SCSI、串行连接SCSI(SAS)、光纤通道、USB附加存储、SCSI Express等。	
清除：	使用组织批准和验证的覆写技术/方法/工具覆写介质。清除程序应至少包括一次写入固定 数据值(如全部为零)的过程。也可选择使用多次写入或更复杂的值。
清洗：	有四种选择： a)如果支持，应用SANITIZE命令。可以使用以下一个或两个选项： 1)OVERWRITE服务操作。利用反相选项，对伪随机模式总共进行三次传递，以便第二次传递是指定模式的反相版本。 2)如果设备支持加密，则可使用CRYPTOGRAPHIC ERASE服务操作。 可选：在对设备成功应用加密擦除后，使用OVERWRITE服务操作(如果支持)在介质上写入一次零或伪随机图案。如果不支持"擦写"服务操作，则可使用"清除"程序。 b)通过TCG Opal SSC或Enterprise SSC接口进行加密擦除，根据需要发出命令，使所有MEK发生变化(不支持部分清除)。更多信息，请参阅TCG和出货TCG Opal或Enterprise存储设备的供应商。 可选：在对设备成功应用加密擦除后，使用OVERWRITE服务操作(如果支持)在介质上写入一次零或伪随机图案。如果不支持"擦写"服务操作，则可使用"清除"程序。 c)如果前两个选项都不支持，则可使用本地读写接口至少写入一次固定数据值(如全部为零)。也可以使用多次传递或更复杂的值。 d)使用组织认可的自动消磁器进行消磁，或拆卸硬盘驱动器，并使用组织认可的消磁棒清除封闭的盘片。 在使用SANITIZE命令和OVERWRITE服务操作时，如果使用了三次遍历和反转(也称为补充)选项，验证过程将只搜索原始模式(在第三次遍历中再次写入)。虽然人们普遍认为一次覆写就足以清除数据，但如果有一个包含反转数据模式功能的专用命令，就可以采用一种高效、有效的方法，降低与不同设备制造商磁记录功能实施差异 相关的任何残余风险。
销毁：	将设备撕毁、分解、粉碎，或在有许可证的焚烧炉中焚烧。
6.8.1.5所述的"清除和清洗"中的每种技术都必须进行验证，但消磁除外。消磁所提供的保证取决于选择有效的消磁器、适当地使用消磁器和定期抽查消磁结果，以确保消磁器按预期工作。 存储设备可支持人为限制媒体部分访问能力的配置功能，例如	

—SCSI模式参数块描述符的逻辑块数(NUMBER OF LOGICAL BLOCKS)字段(可通过MODE SENSE和MODE SELECT命令访问)。
—主机保护区(HPA)、设备配置覆盖(DCO)或可访问最大地址(均在ATA标准中定义)
即使专用的ATA/SCSI清洗命令处理了这些区域，如果保留这些区域，也可能会影响可靠验证清洗程序有效性的能力。任何限制访问存储介质整个可寻址区域的配置选项都应在应用清除技术之前重置。
应用加密擦除时，有必要在应用其他清除技术(如适用)(如在加密擦除后应用清除或清除技术)之前执行验证，以确保加密操作成功完成。在加密擦除后应用任何附加技术后，还应执行6.8.1.5中所述的快速抽样验证。
并非所有加密实现都适合依赖加密擦除作为清除机制。决定是否使用加密擦除取决于对本指南和A.3中先前确定的属性的验证。
本指南仅适用于磁性介质，在消毒前核实介质类型至关重要。请注意，新出现的介质类型(如HAMR介质或混合硬盘)可能不容易通过标签识别。有关存储设备中介质类型的详细信息，请咨询制造商。
对存储设备中的介质消磁通常会导致设备无法使用。
对于焚烧以外的销毁技术，介质在销毁前应进行适当的消磁处理，所产生的碎片应小于12毫米的网
格。

表 A.6 – 外围连接存储设备消毒

消毒方法	说明
外部本地连接硬盘 包括USB、Firewire 等(将eSATA 视为ATA 硬盘) 。	
清除:	使用组织批准和验证的覆写技术/方法/工具覆写介质。清除程序应至少包括一次写入固定 数据值(如全部为零)的过程。也可选择使用多次写入或更复杂的值。
清洗:	请参阅 "销毁"。外部本地连接硬盘的执行方式在不同型号和供应商之间存在很大差异， 因此 向设备发出任何特定命令都可能无法合理、一致地确保所需的清除结果。 当外部硬盘托架包含 ATA 或 SCSI 硬盘驱动器时，如果命令可直接传递到设备，则可根据 相关的特定介质指南对设备进行消毒。但是，硬盘可能会以特定于供应商的方式进行配置 ，从而在从机箱中取出时无法进行消毒。此外，如果应用了消毒技术，硬盘在重新安 装到机壳中时可能无法按预期运行。 请咨询设备制造商，以确定设备是否具有应用介质相关技术(如重写、块擦除、加 密擦除等)的 "清除 "功能，以确保数据恢复不可行，而且设备不会简单地删除文件 指针。
销毁:	将设备撕毁、分解、粉碎，或在获得许可的焚烧炉中焚烧。
6.8.1.5 中所述的验证应在清除和清理中对每种技术进行。 某些外置本地连接硬盘，特别是具有安全或加密功能的硬盘，还可能具有隐藏的存储区域，即使将硬盘从 机箱中取出也可能无法处理。设备供应商可能会利用专有命令与安全子系统交互。请向制造商咨询， 以确定介质上是否存在任何保留区域，以及如果存在，是否有任何工具可用于移除或清除这些区域。 对于焚烧以外的销毁技术，介质在销毁前应进行适当的消磁处理，所产生的碎片应小于 12 毫米的网 格。	

表 A.7 – 消毒光学介质

消毒方法	说明
CD, DVD, BD	
清除/清洗：	不适用，请参阅 "摧毁"。
销毁：	按建议顺序销毁： a)使用商用光盘研磨设备去除CD介质的信息承载层。请注意，这仅适用于CD，而不适用于DVD或BD介质 b)使用许可设备焚烧光盘介质（减少为灰）。使用光盘介质碎纸机或崩解装置减少为标称边缘尺寸为点5毫米（.5 mm）和点表面积为25平方毫米（.25 mm2）或更小的颗粒。对于在闪存存储上焚烧以外的破坏技术，产生的碎片应该小于2毫米的网格。

表 A.8 – 基于闪存的存储设备消毒

消毒方法	说明
ATA SSD包括PATA、SATA、eSATA、CF、CFast等。	
清除：	a)使用组织批准和验证的覆写技术/方法/工具覆写介质。清除程序应至少包括一次写入固定数据值(如全部为零)的过程。也可选择使用多次写入或更复杂的值。 值得注意的是，对闪存介质进行覆盖可能会大大降低介质的有效寿命，而且可能无法清除未映射物理介质中的数据(即旧数据可能会保留)。 b)如果支持，请使用SECURITY ERASE UNIT命令。 鉴于SECURITY ERASE UNIT命令的执行方式多种多样，建议在未咨询制造商以确认存 储设备的特定型号执行方式符合组织需求的情况下使用该命令。
清洗：	有三种选择： a)如果支持，使用ATA"消毒设备"功能集命令之一执行"消毒"操作。可使用以下一个或两个选项： 1)BLOCK ERASE EXT命令。 可选：在对设备成功应用BLOCK ERASE EXT后，在存储介质的用户可寻址区域写入二进制1，然后执行第二次BLOCK ERASE EXT。 2)如果设备支持加密，则可使用CRYPTO SCRAMBLE EXT命令。 可选：在对设备成功应用加密擦除后，使用BLOCK ERASE EXT命令(如果支持)来阻止擦除介质。如果不支持BLOCK ERASE EXT命令，则可使用ATA安全功能集SECURITY ERASE UNIT命令或清除程序。
	b)如果支持，在增强擦除模式下使用SECURITY ERASE UNIT命令。与SECURITY ERASE UNIT命令相比，ATA Sanitize Device功能集命令更受欢迎。 c)通过TCG Opal SSC或Enterprise SSC接口进行加密擦除，根据需要发出命令，以更改所有MEK。有关详细信息，请参阅TCG和TCG Opal或Enterprise存储设备出货厂商。可选：在对设备成功应用加密擦除后，使用块擦除命令(如果支持)对介质进行块擦除。如果不支持BLOCK ERASE EXT，则可使用清除程序。 对于磁性介质来说，SECURITY ERASE UNIT命令是一种清除机制，但对于闪存来说，它只是一种清除机制，因为在执行过程中存在变数，而且敏感数据有可能残留在备用 单元等已轮换停用的区域。
销毁：	将设备撕毁、分解、粉碎，或在获得许可的焚烧炉中焚烧。

SCSI固态硬盘包括并行SCSI、串行附加SCSI(SAS)、光纤通道、USB附加存储、SCSI Express等。	
清除：	使用组织批准和验证的覆写技术/方法/工具覆写介质。清除程序应至少包括一次写入固定 数据值(如全部为零)的过程。也可选择使用多次写入或更复杂的值。 值得注意的是，对闪存介质进行覆盖可能会大大降低介质的有 效 寿命，而且可能无法 清除未映射物理介质中的数据(即旧数据可能会保留)。
清洗：	有两种选择： a)如果支持，应用SANITIZE命令。可以使用以下一个或两个选项： 1)BLOCK ERASE服务操作。 2)如果设备支持加密，则可使用CRYPTOGRAPHIC ERASE服务操作。 可选：在对设备成功应用加密擦除后，使用BLOCK ERASE服务操作（如果支持）来阻止擦除介质。如果不支持BLOCK ERASE服务操作，则可使用清除程序。 b)通过TCG Opal SSC或Enterprise SSC接口进行加密擦除，根据需要发出命令，以更改所有MEK。更多信息，请参阅TCG和供应商提供的TCG Opal或Enterprise存储设备。可选：在对设备成功应用加密擦除后，使用BLOCK ERASE服务操作（如果支持）来阻止擦除介质。如果不支持BLOCK ERASE服务操作，则可使用清除程序。
销毁：	将设备撕毁、分解、粉碎，或在获得许可的焚烧炉中焚烧。
NVM Express 固态硬盘	
清除：	使用组织批准和验证的覆写技术/方法/工具覆写介质。清除程序应至少包括一次写入固定数据值（如全部为零）的过程。也可选择使用多次写入或更复杂的值。
清洗：	有 两种选择： a) 如果支持，应用 NVM Express 格式化命令。可使用以下一个或两个选项： 1) 用户数据擦除命令。 2) 如果设备支持加密，则使用加密擦除命令。 可选：在对设备成功应用加密擦除后，使用用户数据擦除命令（如果支持）擦除介质。如 果不支持用户数据擦除命令，也可以使用清除程序。 b) 通过 TCG Opal SSC 或 Enterprise SSC 接口进行加密擦除，根据需要发出命令， 以更改所有 MEK。更多信息，请参阅 TCG 和供应商提供的 TCG Opal 或 Enterprise 存储 设备。

	可选：加密擦除成功应用到设备后，使用用户数据擦除命令（如果支持）擦除介质。如 果不支持用户数据擦除命令，则可使用清除程序。
销毁：	将设备撕毁、分解、粉碎，或在获得许可的焚烧炉中焚烧。
USB 可移动媒体，包括笔式驱动器、拇指驱动器、闪存盘、记忆棒等。	
清除：	使用组织批准和验证的覆写技术/方法/工具覆写介质。清除程序应包括至少两遍写入，第一遍写入模式，第二遍写入补码。可使用额外的写入程序。
清洗：	大多数USB可移动媒体不支持消毒命令，或者即使支持，这些设备也不支持标准化的接口。请参考制造商以了解可用消毒功能和命令的可用性和功能详情。在大多数需要清除的情况下，应销毁USB可移动媒体。
销毁：	将设备撕毁、分解、粉碎，或在获得许可的焚烧炉中焚烧。
存储卡，包括 SD、SDHC、MMC、Compact Flash、Microdrive、MemoryStick 等。	
清除：	使用组织批准和验证的覆写技术/方法/工具覆写介质。清除程序应包括至少两遍写入，第一遍写入模式，第二遍写入补码。可使用额外的写入程序。
清洗：	不适用，请参阅"摧毁"。
销毁：	将设备撕毁、分解、粉碎，或在有许可证的焚烧炉中焚烧。
板卡和设备上的嵌入式闪存，这包括主板和外设卡，如网络适配器或任何其他包含非易失性闪存的适配器。	
清除：	如果设备支持，请将状态重置为原始出厂设置
清洗：	不适用，请参阅"摧毁"。如果可以很容易地识别闪存并将其从电路板上移除，则闪存的销毁可以与包含闪存的电路板的处理分开进行。否则，应销毁整个电路板。
销毁：	撕毁、分解、粉碎或焚烧，在获得许可的焚烧炉中焚烧该装置。
如6.8.1.5所述，必须对清除和清理中的每种技术进行验证。 存储设备可支持人为限制媒体部分访问能力的配置功能，例如 —SCSI模式参数块描述符的逻辑块数（NUMBER OF LOGICAL BLOCKS）字段（可通过MODE SENSE和MODE SELECT命令访问）。 —主机保护区(HPA)、设备配置覆盖(DCO)或可访问最大地址（均在ATA标准中定义）即使专用的ATA/SCSI清洗命令处理了这些区域，如果保留这些区域，也可能会影响可靠验证清洗程序有效性的能力。任何限制访问存储介质整个可寻址区域的配置选项都应在应用清除技术之前重置。 应用加密擦除时，有必要在应用其他清除技术（如适用）（如在加密擦除后应用清除或清除技术）之前执行验证，以确保加密操作成功完成。在加密擦除后应用任何附加技术	

后，还应执行6.8.1.5中所述的快速抽样验证。 并非所有加密实现都适合依赖加密擦除作为清除机制。决定是否使用加密擦除取决于对本指南和A.3中先前确定的属性的验证。 在基于闪存的存储设备或包含非易失性闪存存储介质的混合设备上，不要完全依赖消磁作为一种消毒技术。在存在非易失性闪存介质时，如果使用介质相关技术对闪存组件进行了消毒，则可以使用消磁技术。 虽然嵌入式闪存历来没有在介质消毒指南中专门提及，但系统的复杂性和闪存的相关使用增加了存在敏感数据的可能性。例如，集成到现代主板中的远程管理功能可能需要存储IP地址、主机名、用户名和密码、证书或其他可能被视为敏感的数据。因此，对于清除来说，可能需要与多个界面交互才能完全重置设备状态。将此概念应用于示例时，可能包括BIOS/UEFI界面和远程管理界面。与其他类型的介质一样，消毒技术的选择基于特定环境的考虑。虽然可以选择既不清除也不清理嵌入式闪存，但重要的是要认识到并接受潜在的风险，并随着环境的变化不断重新评估风险。对于闪存上除焚烧以外的销毁技术，所产生的碎片应小于2毫米的网格。

表 A.9 – 基于 RAM 和 ROM 的存储设备消毒

消毒方法	说明
动态随机存取存储器(DRAM)	
清除/清洗：	关闭包含DRAM的设备电源，从电源上取下设备，并取出电池(如果有电池支持)。或者，从设备中取出DRAM。 无论哪种情况，DRAM都应保持断电状态至少5分钟。
销毁：	撕毁、瓦解或粉碎。
电子可更改PROM(EAPROM)	
清除/清理：	按照制造商的数据表进行全面的芯片清洗。
销毁：	撕毁、瓦解或粉碎。
电子可擦除PROM(EEPROM)	
清除/清洗：	使用组织批准和验证的覆写技术/方法/工具覆写介质。
销毁：	将设备撕毁、分解、粉碎，或在获得许可的焚烧炉中焚烧。

未来，组织将使用本国际标准未明确涉及的媒体类型。本国际标准描述的流程应该引导媒体消除的决策，不论所使用的媒体类型是什么。

A.3 加密擦除设备指南

加密擦除利用目标数据的加密密钥来进行消除。这将只留下媒体上的密文，有效地进行了数据消除。如果没有用于加密目标数据的加密密钥，那么数据将无法恢复。解密此信息所需的工作量将取决于以下两者中较小的那一个：

- 用于加密数据的加密算法的强度（包括操作模式）；
- 目标数据的加密的熵级别。

因此，数据的消除变成了消除用于加密数据的加密密钥。通过加密擦除，数据的消除可以在很短的时间内进行高可靠性的执行，比其他消除技术要快得多。加密本身就是对数据进行了消除。

通常，加密擦除可以在几秒钟内完成。这对于存储设备变得越来越大导致其他消除方法需要更多时间的情况尤为重要。加密擦除也可以作为其他消除方法的补充或附加方法。

如果满足以下条件之一，不应仅依赖于加密擦除来清除设备上的媒体：

- 敏感数据在未消除的情况下存储在设备上后才启用加密；

– 不知道是否在加密之前未消除的情况下存储了敏感数据，则不应仅依赖于加密擦除作为清除机制。

如果打算使用加密擦除来清除媒体（包括自加密驱动器、移动设备和其他设备），则保证级别取决于以下因素：
– 在存储在设备上之前对所有数据进行加密擦除（包括数据和虚拟副本）；
– 在媒体上存储数据加密密钥的位置（包括目标数据的加密密钥或相关的包装密钥）可通过适当的媒体特定消除技术直接访问以进行消除(确保实际存储密钥的位置得到处理）；
– 消除用于加密目标数据的所有加密密钥的所有副本；
– 如果目标数据的加密密钥本身使用一个或多个包装密钥进行了加密，可以通过消除相应的包装密钥来执行加密擦除；
– 用户能够清楚地识别设备提供的命令以执行加密擦除操作。

其他加密擦除的考虑：
– 如果加密密钥（或在加密擦除期间进行消除的密钥级别或更低级别的密钥）存在于存储设备之外（通常是由于抵押或注入），则有可能将来使用该密钥恢复存储在加密媒体上的数据。
– 不应该信任使用加密擦除进行设备的备份或抵押（ESCROW）密钥的设备，除非组织对密钥的存储和管理方式有很高的信心，并在设备外部进行了处理。这样的备份或抵押密钥的副本应该是单独设备消除政策的对象。该政策应该涵盖在实际存储它们的设备范围内的备份或抵押副本。

是否利用加密擦除取决于组织对清除的要求，以及最终用户是否能够确定实施是否提供了足够的保证防止将来恢复数据。保证级别在很大程度上取决于表A.10中描述的因素。

表 A.10 – 加密擦除注意事项

地区	考虑因素
密钥生成	随机数源的熵水平和应用于随机数据的白化程序的质量。这适用于加密密钥，也可能适用于受加密擦除操作影响的封装密钥。
媒体加密	用于保护目标数据的加密算法/模式的安全强度和实施有效性。
密钥级别和缠绕	被清除的密钥可能不是媒体加密密钥，而是用于封装(即加密)媒体加密密钥或另一密钥的密钥。在这种情况下，所使用的封装技术的安全强度和保证级别应与加密擦除操作的强度级别相称

用户在考虑使用加密擦除技术时，应在依赖加密擦除进行介质清除之前，确定存储设备实现这些领域的机制。以下是需要确定的内容：

- **厂商/型号/版本/介质类型**：适用于哪种产品和版本，以及设备使用的介质类型（如磁性介质、固态硬盘、混合介质等）。
- **密钥生成**：确定是否使用了确定性随机比特生成器，比如SP800-90中列出的生成器，并对其进行了验证。
- 介质加密：标识算法、密钥强度、操作模式以及任何适用的验证。
- **密钥级别和封装**：标识MEK（可包装或不包装）是否直接进行清除，或者是否对MEK进行包装（KEK）并对其进行清除。仅在需要清除KEK（而不是MEK）时才提供包装细节。若提供包装细节，应包括使用的算法、强度和（如果适用）操作模式。
- **数据区域**：描述哪些区域是加密的，哪些区域不加密。对于任何未加密区域，描述如何进行清除。
- **密钥生命周期管理**：设备上的密钥可能在设备的生命周期内多次进行封装活动（封装、解封和重新封装）。标识在加密擦除操作之外直接处理要清除的密钥的封装活动方式。例如，用户可能已经收到一台始终进行加密的自加密驱动器（SED），只需启用身份验证接口。标识在使用用户的身份验证凭据封装前的MEK的上一实例如何进行清除。
- **密钥清除技术**：描述用于清除要清除的密钥的介质相关清除方法。例如，如果介质是磁性介质，可能会采用三次反转覆盖方法；对于固态硬盘，可能会采用块擦除方法；对于其他类型的介质，可能会采用其他特定于介质的技术。
- **密钥托管或注入**：标识设备是否支持密钥托管或注入。标识设备是否支持发现在设备之外是否托管了任何密钥。如果MEK加密密钥是直接进行清除，而只有KEK可以进行托管，请明确标识此事实。
- **错误条件处理**：标识设备在遇到阻止加密擦除操作完全完成的错误条件时的处理方式，例如，是否遇到一个存储要清除的密钥实例的缺陷。例如，如果无法清除存储密钥的位置，加密擦除操作是否向用户报告成功或失败。
- **接口明确性**：标识哪些接口命令支持该声明中描述的功能。如果设备支持使用多个MEK，请标识是否使用可用的接口命令更改所有MEK以及确保更改所有MEK所需的任何额外命令或操作。

实施者选择应用加密擦除技术时，应寻求对这些保证领域的独立验证，或要求供应商标识用于确保这些关注领域已得到解决的机制。应使用通常被接受并（如果适用）标准化的机制。例如，加密模块的安全要求规定在ISO/IEC 19790:2006中，而加密模块的测试要求规定在ISO/IEC 24759:2008中。这些要求和测试涵盖了某些（但不是所有）关注领域。

关于是否依赖加密擦除，还应考虑介质加密密钥是否已被托管或注入，以及如果是这样，密钥在存储设备之外如何受到保护。如果介质加密密钥（或在加密擦除期间进行清除的任何密钥）存在于存储设备之外，则有可能在未来使用该密钥来恢复存储在加密介质上的数据。

附录 B（信息性附录）

选择适当的存储安全控制

B.1 选择控制的标准

B.1.1 概述

根据本国际标准的内容，存储安全指南可能看起来是一组同等重要或需要全部实施的控制措施。实际上，这两种说法都不正确，组织可以从采用一组对其特定环境和需求最相关的控制措施中获益。选择的实际控制措施可以根据监管要求、已知的威胁和漏洞、组织政策、行业或地区指南以及适用的标准，通过添加和删除控制措施而与这些指南有所不同。

这个信息性附录B提供了所有存储安全控制（见B.2）的摘要，以及基于以下标准的选择依据：
- 数据敏感级别类别 - 以数据为中心的焦点，利用两个类别，适用于已对基本数据进行分类的组织；
- 安全优先级代码 - 提供信息，以帮助基于机密性、完整性和可用性安全方面的相对重要性，进行控制措施的分阶段或排序决策。

组织应该将这些标准和指南视为选择存储安全控制措施的起点（另见ISO/IEC 27002:2013, 8.2）。它们还可以帮助组织根据风险评估（见ISO/IEC 27005）采用存储安全控制措施的分阶段方法。

在信息安全管理体系的规划和实施中，使用附录B中列出的一组存储安全控制措施作为特定优先级或数据敏感级别的强制要求是不恰当的，应该进行安全控制的选择。此外，附录B中的安全优先级和数据敏感性标准不应被用作评估或评分存储系统或基础设施的安全性的依据。

B.1.2 数据敏感级别类别

B.1.2.1 总则

已对数据敏感性或关键性进行基本分类的组织，可以利用这些分类来帮助确定与其环境最相关的存储安全控制措施。为了帮助这种努力，定义了两个通用的数据敏感级别类别或级别：低（见B.1.2.2）和高（见B.1.2.3）。

作为起点，组织需要将其具体的数据分类映射到附录B中定义的两个数据敏感级别类别之一。然后可以参考附录B.2中列出的表格中的控制摘要，以确定相关的存储安全控制措施；在这些表格中，“L”的数据敏感级别对应“低”，“H”的数据敏感级别对应“高”。

B.1.2.2 低数据敏感级别

此类数据通常易于访问，并在更大的组织或机构内部用于内部使用（例如，商业实体、政府机构等）。此外，这些数据被认为是不太敏感的（例如，没有规定的保密或隐私要求），其价值有限，且不被视为业务/任务关键。

尽管如此，仍需要最低限度的保护控制，因为未经授权的披露或传播可能会导致以下情况：
- 对业务造成有限的负面影响，但不会违反合同或法律协议；
- 对政府造成有限的负面影响；
- 在社会和经济方面对个人产生有限的影响。

B.1.2.3 高数据敏感级别

此类数据通常仅限于单个人或小型已知人员组或高度安全的组织单位（例如，商业群体/项目、政府部门/群体等）。此外，这些数据被认为是敏感的（例如，受到规定的保密或隐私要求）或非常敏感的（例如，受到规定的保密或隐私要求），其价值显著至非常高，并且被视为业务/任务关键（例如，商业机密）。

由于未经授权的披露或传播可能会导致以下情况，因此必须采取严格的保护控制：
- 对业务造成显著且可能危及生存的负面影响，并可能违反合同或法律协议；
- 违反政府安全性，暴露机密或可能的秘密数据；
- 对个人在社会和经济方面产生显著影响；在极端情况下，危及个人的健康、生命或人身自由。

B.1.3 安全优先级代码

组织可以确定和优先选择与其环境最相关的存储安全控制。这可以通过首先进行信息安全风险评估（见ISO/IEC 27005）来实现，该评估有助于确定数据机密性、完整性和可用性需求以及这些安全方面的相对重要性。

如果组织已经了解数据机密性、完整性和可用性的优先级，那么可以利用这些信息来帮助确定相关的存储安全控制，使用B.2中的表格。此外，还可以采用分阶段的方法来解决这些控制，从风险评估中确定的优先级最高的控制措施开始。

为了帮助这种努力，将第6和第7条中的存储安全控制摘要列在B.2中的表格中。每个控制都显示了安全方面（机密性、完整性和可用性）的一组优先级值，以及系统级的指示器（即三个安全方面的优先级代码相同）。在B.2表格中，“C”的优先级指示器对应“机密性”，“I”对应“完整性”，“A”对应“可用性”，“S”对应“系统级”，而表格中使用的优先级值范围从0到5，其中5表示最高优先级，0表示最低优先级；“系统级”标记用“X”表示。

为了演示组织如何使用优先级代码数据，考虑一个情况，风险评估已确定数据机密性是主要的问题领域。通过将机密性安全方面作为重点，组织可以审查安全控制，并确定具有“C”优先级代码最高值的控制。具有值为5的优先级代码的控制很可能是适用的。因此，组织可以开始实施优先级代码为5的控制，然后按阶段进行，接下来处理优先级代码为4的控制，然后是优先级代码为3的控制，依此类推。

B.2 存储安全控制摘要

B.2.1 支持存储安全的控制措施

表格B.1、B.2、B.3、B.4、B.5、B.6和B.7总结了第6条中包含的安全控制和指导，同时显示了它们与不同数据敏感级别（见B.1.2）和优先级代码（见B.1.3）的相关性。

表 B.1 – 直接连接存储 (6.2)

控制装置	优先事项 (5为最高)				数据 敏感性	
	S	C	I	A	L	H
应确保DAS的物理安全		5	3	5	X	X
对于DAS上的敏感数据和高价值数据，应使用某种形式的加密(SED、FDE、基于计算机的加密或基于应用程序的加密)来保护静态数据		5	3	0		X
应在所有涉及敏感和高价值数据的DAS上使用介质消毒技术		5	1	0		X
如有可能，应使用FC-SP-2 AUTH-A Authentication等身份验证，以防止未经授权访问敏感和高价值数据		5	3	0		X
为防止意外或故意丢失或损坏数据，应定期备份DAS内容		0	5	0	X	X

表 B.2 – 存储联网(6.3)

控制装置	优先事项 (5 为最高)				数据 敏感性	
	S	C	I	A	L	H
存储区域网络 (6.3.2)						
尽可能避免班级之间的网络连接(如生产或开发)		5	3	0	X	X
将存储设备与其他数据中心设备物理隔离	X	2	2	2		X
从逻辑上隔离存储流量和正常服务器流量	X	4	4	4		X
将存储管理流量与所有其他流量隔离开来		2	3	1	X	X
确保网络网关的配置保持适当的网络隔离		3	3	4	X	X
对于FC，使用ACL、绑定列表、FC-SP-2 Fabric策略等技术限制服务器对交换机的访问。		4	3	3		X
对于FC，使用启用NPIV的HBA为虚拟服务器分配单独的N_Port_ID		5	3	2		X
对于FC，使用ACL、绑定列表、FC-SP-2 Fabric策略等技术限制交换机互连		4	3	2		X
FC SAN Fabric中应优先使用硬分区		4	3	3	X	X
对于FC，确定基本分区对于目标环境是否是足够强大的安全措施，如果不是，则在供应商支持的情况下使用更强大的技术，如FC-SP分区		4	3	3		X
对于 FC，禁用未使用的交换机端口		3	4	1	X	X
对于 FC，请谨慎使用默认区段和区段集(假设采用最小权限态势)		3	3	1	X	X
对于 FC，配置交换机、扩展器、路由器和网关时应尽量减少访问量		4	4	2	X	X
避免将 iSCSI 接口连接到通用局域网；为安全和性能进行隔离	X	5	5	5	X	X
对于 iSCSI，如果无法使用物理隔离的局域网，则应使用 VLAN	X	5	5	5	X	X
建立 FCIP 实体之间的对等关系		5	3	5	X	X
在可能的情况下， FCIP 实体应专门使用专用 IP 网络		5	3	5		X
对于 FCIP ，至少使用IPsec 进行加密验证和数据完整性验证		3	4	3		X
对于 FCIP,使用 IPsec 通过适当的保密措施保护敏感数据		5	4	3		X

对于 FCoE，利用光纤通道安全机制		5	3	2	X	X
对于 FCoE，防止以太网广播风暴(如分配足够的输入缓冲区)导致吞吐量和超时问题		0	1	3	X	X
应使用 ACL 控制 FCoE 网络访问(例如，禁止特定计算机访问不必要或不需要的流量)		5	4	1	X	X
在无法使用物理隔离局域网时，使用 FCoE VLAN	X	5	5	5	X	X
网络附加存储 (6.3.3)						
当 NFSv3 用于敏感数据或高价值数据时，应格外小心		4	3	1		X
仅在需要时启用 NFS		3	3	1	X	X
尽可能使用 NFSv4 (或更高版本)，限制使用 NFSv3		3	3	1	X	X
对于 NFS，按 IP 地址过滤客户端和管理访问，以提高安全性		2	3	4	X	X
对于 NFS ，必要时加密客户端数据访问(如 IPsec		5	5	2		X
使用较新版本的 SMB 协议		3	4	5	X	X
对于 SMB/CIFS，关闭低安全性会话协商协议，如 NTLM v1、LanMan 和明文，改用 NTLM v2 或 Kerberos	X	5	5	5	X	X
保持最新的补丁级别	X	4	4	4	X	X
使用 SMB 签名		5	5	0	X	X
安全维护活动目录 (AD) 服务		3	3	5	X	X
尽可能使用从叶域到父域的单向信任		5	5	2	X	X
仅在需要时启用 SMB/CIFS		3	3	1	X	X
对于 SMB/CIFS，必要时对客户端数据访问进行加密(如 IPsec)		4	3	0		X

表 B.3 – 存储管理(6.4)

控制装置	优先事项 (5 为最高)				数据敏感性	
	S	C	I	A	L	H
身份验证和授权(6.4.2)						
所有用户都应有一个供个人使用的唯一 ID		5	5	0	X	X
应选择合适的身份验证技术(强密码、强身份验证或多因素身份验证)来证实用户所声称的身份		5	5	0	X	X
对于所有远程访问，使用强身份验证或多因素身份验证以及安全通道		5	5	0	X	X
在可能的情况下，使用集中式身份验证解决方案来改进监控		4	4	0	X	X
在管理敏感和高价值数据时使用多因素身份验证		4	4	0		X
禁止登录 root 账户。远程记录所有权限升级操作		3	3	0	X	X
在可能的情况下，在 TLS 和IPsec 连接以及存储协议中使用实体验证		3	3	0		X
在存储系统中实施和使用安全管理员、存储管理员、安全审计员和存储审计员等一般角色		3	3	0	X	X
确保管理接口的安全(6.4.3)						
限制对管理界面的物理访问	X	5	5	5	X	X
不使用时禁用和断开串行管理端口		2	2	1	X	X
将用于管理的局域网接口与其他局域网流量隔离，注意最好是物理隔离，但至少应使用逻辑隔离(如 VLAN		3	2	1	X	X
使用防火墙和 TCP 封装器，限制授权系统和协议访问管理网络		4	4	5	X	X
使用实体认证在存储系统和管理系统之间建立信任关系(例如，使用FC-SP-2 AUTH-A 对执行带内管理的实体进行认证)		3	3	4		X
利用 IDS 和 IPS 机制识别异常行为并加以防范	X	4	4	4	X	X
使用信息和通信技术基础设施(DNS、 SLP、NTP)，并采取适当的安全控制措施，以避免间接攻击	X	3	3	3	X	X
采用适当的特权用户控制，包括身份验证、 授权和安全	X	5	5	5	X	X

审计/监控						
在存储管理方面，确保操作系统和应用程序是最新的，并经过充分加固，可抵御攻击		5	5	3		X
对于远程存储管理，所有远程访问都要使用安全通道(VPN、TLS、SSH、HTTPS)	X	5	5	5	X	X
对于远程存储管理，请使用强身份验证或多因素身份验证	X	5	5	5	X	X
对于远程存储管理，将权限限制在所需的最低限度(即最低权限)		4	4	2		X
制定组织和技术控制措施,限制用于远程(非本地)供应商维护会话的管理界面		3	2	2	X	X
技术控制应将通信流量(即系统、端口和协议)限制在远程供应商维护操作所需的最低限度内		3	3	5	X	X
在访问方(供应商维护人员)获得授权后，应在访问点设计额外的控制措施，以授权供应商维护会话，包括接受、请求批准或拒绝所请求的会话		3	3	5		X
应生成包含供应商行动审计记录的适当日志。	X	4	4	4	X	X
组织应将拨号接入线路限制在授权接入方范围内，执行调制解调器回拨协议，并在供应商请求维护会话并获得组织授权之前，禁止建立连接		2	3	2	X	X
安全审计、会计和监控(6.4.4)						
将存储系统和基础设施纳入日志记录策略(收集内容、保留/保存、时间同步等)。	X	4	4	4	X	X
在政策中，确定并处理对存储日志的证据要求	X	5	5	5	X	X
采用外部和集中式事件日志记录，将事件记录到可信的远程来源	X	5	5	5	X	X
在整个存储系统和基础设施中建立并使用通用、准确的时间源	X	5	5	5	X	X
将事件记录到一个(最好是多个)外部日志服务器上	X	4	4	4	X	X
使用支持可靠传输和安全传输的标准日志协议，如syslog	X	3	3	3	X	X
出于合规、问责或安全目的，事件发生时应及时记录(无缓冲)。	X	4	4	4	X	X
实施分析协议，关联各事件源的审计日志记录，以确定可提供安全事件迹象的重大安全事件	X	3	3	3	X	X
在部署SIEM技术时，确保将存储日志记录考虑到SIEM解决方案中	X	3	3	3		X

记录所有发生的最低安全事件，并提供必要的数据	X	5	5	5	X	X
应正确处理可能具有证据价值的审计日志数据(例如，保持监管链、可验证的完整性和真实性等)。	X	5	5	5	X	X
有特定保留要求的审计日志数据(例如，为遵守法规)应通过组织的数据保留解决方案进行保留	X	5	5	5	X	X
采取适当措施，保持日志完整性，防止日志被修改或销毁	X	5	5	5		X
当审计日志条目包含敏感信息时，应使用适当的保密机制保护审计日志数据	X	5	5	5		X
对于特殊的审计日志要求(如大容量、特殊保存、事件签名等)，应使用专用的、经过特别加固和配置的系统	X	4	4	4		X
利用日志中继和日志过滤功能，最大限度地降低专门存储要求(WORM)的影响	X	3	3	3		X
系统加固 (6.4.5)						
所有操作系统、管理程序和应用程序都应根据存储系统的使用情况进行加固	X	3	3	3	X	X
删除不需要/不使用的软件		2	3	3	X	X
删除不必要的账户	X	3	3	3	X	X
消除、禁用或更改预定义或默认账户的密码	X	4	4	4	X	X
只打开需要的网络端口		1	1	3	X	X
从可信来源安装最新补丁	X	4	4	4	X	X
从可信来源更新固件	X	4	4	4	X	X
安装和维护恶意软件保护	X	5	5	5	X	X

表 B.4 – 基于数据块的存储 (6.5)

控制装置	优先事项 (5为最高)				数据敏感性	
	S	C	I	A	L	H
光纤通道存储(6.5.1)						
应使用LUN屏蔽和映射(WWN过滤)以及其他访问控制机制来限制对存储的访问		4	4	1	X	X
所有服务器和交换机都应使用FC-SP-2 AUTH-A相互验证；尽可能利用集中验证服务		2	2	5	X	X
如果可能，应使用ESP_Header对离开保护区的光纤通道连接进行加密。		4	3	1		X
敏感数据和高价值数据应在FC存储设备或介质上加密		5	3	1		X
应在可能接触敏感数据或受监管数据的FC存储设备中实施加密，以方便快速消毒		5	3	1		X
对于FC存储，敏感数据和受监管数据应使用介质对齐消毒技术		5	3	1		X
逻辑清除应用于清除虚拟化FC存储，尤其是在无法确定实际存储设备		5	3	1		X
和介质的情况下						
IP存储(6.5.2)						
根据源IP地址和协议进行过滤，控制iSCSI启动程序的访问		5	3	5	X	X
在所有iSCSI实施中，启动程序和目标都应使用双向CHAP身份验证，并使用随机挑战(即不重复)。	X	5	5	5	X	X
当敏感数据或高价值数据可能暴露时，应使用IPsec确保通信通道的安全		5	3	2		X
使用iSNS、SLP、DNS基础设施时应采取适当的安全控制措施，以避免间接攻击	X	3	3	3	X	X
敏感数据和高价值数据应在IP存储设备或媒体上加密		5	3	1		X
应在可能接触敏感数据或受监管数据的IP存储设备中实施加密，以方便快速消毒		5	3	1		X
对于IP存储，应针对敏感数据和受监管数据使用介质对齐消毒技术		5	3	1		X

逻辑清除应用于清除虚拟化IP存储，特别是在无法确定实际存储设备和介质的情况下		5	3	1		X

表 B.5 – 基于文件的存储（6.6）

控制装置	优先事项 (5为最高)				数据 敏感性	
	S	C	I	A	L	H
基于NFS的NAS(6.6.1)						
尽可能采用用户级身份验证(例如，使用Kerberos V5的NFSv4)	X	5	5	5	X	X
配置NFS服务器，为授权用户明确导出文件系统		3	2	1	X	X
配置NFS服务器，以最低所需权限导出文件系统		3	2	1	X	X
避免授予"root"或"管理员"访问网络文件系统上文件的权限		5	5	3	X	X
确保正确分配NFSv4 ACL		4	4	2	X	X
为NFSv3使用Kerberos验证	X	3	3	3	X	X
考虑使用Kerberos安全和专用模式对NFS流量进行签名和加密		4	4	2	X	X
尽可能过滤客户端对NFS共享的访问	X	3	3	3	X	X
不允许NFS客户端在导出文件系统上运行suid和sgid程序		3	3	5	X	X
导出的文件系统应放在自己的分区中，以防止攻击者在导出文件系统写满之前写入文件导致系统降级	X	4	4	4	X	X
对于NFS，必要时对静态数据进行加密		3	3	1		X
不允许NFS导出管理文件系统(如/etc)	X	3	3	3	X	X
对于NFS，防范恶意软件(如病毒、蠕虫、rootkit等)。	X	5	5	5	X	X
持续监控NFS共享中的内容和相关访问控制		4	1	2		X
基于SMB/CIFS的NAS(6.6.2)						
禁用对CIFS共享和NAS设备的未验证访问(即限制匿名访问)		5	3	4	X	X
禁止"访客"和"每个人"访问所有CIFS共享		4	4	2	X	X
对于SMB/CIFS，通过集中机制(RADIUS、LDAP)实施身份验证和访问控制	X	5	5	5		X
为客户端和NAS设备启用SMB签名		3	5	3		X
尽可能启用CIFS审计		3	3	1		X
持续审查CIFS共享中的内容和相关访问控制		4	1	2		X

对于SMB/CIFS，必要时对静态数据进行加密		3	3	1		X
对于SMB/CIFS，防范恶意软件(如病毒、蠕虫、rootkit等)	X	5	5	5		X
使用强身份验证(NTLMv2、Kerberos)实施CIFS		4	4	1	X	X
基于NFS的并行NAS(6.6.3)						
控制和控制机制应一致地应用于各个群集(包括对称和非对称群集)		3	5	3	X	X
安全保证属性不应依赖于客户端访问特定的文件服务器	X	3	3	3	X	X
对于非对称群集，控制措施的实施应使其在不同协议中保持一致	X	4	4	4	X	X
安全控制不应依赖于跨服务器文件系统名称空间的路径遍历		2	2	4	X	X

表 B.6 – 基于对象的存储 (6.7)

控制装置	优先事项 (5为最高)				数据敏感性	
	S	C	I	A	L	H
云计算存储(6.7.1)						
对于云存储，确保所有交易都使用IPsec或TLS等传输安全措施		5	4	2	X	X
当敏感数据存储在第三方云环境中时，应使用静态数据加密(和适当的密钥管理流程)来防止未授权方(如云服务提供商人员、其他租户、对手等)访问。		5	2	2		X
对于云存储，应确保用户注册的安全性，并使用强大的密码验证功能来保护对数据的访问		5	4	3	X	X
对于云存储，应采用访问控制，防止其他租户未经授权的访问，同时为获准访问数据的用户提供适当的访问权限		4	4	2	X	X
使用所提供的清除功能，清除云计算存储中的敏感数据		4	2	2		X
使用CDMI时，确保所有交易都使用TLS	X	4	4	4	X	X
查询云服务提供商CDMI实施的安全功能，并根据风险判定所提供的安全性是否充分	X	5	5	5	X	X
验证CDMI实体(服务器的证书和客户端的HTTP基本验证)	X	5	5	5	X	X
使用CDMI域为外部身份验证提供商的身份验证映射提供位置		4	4	1		X
启用CDMI安全日志，并定期、及时地从相应的日志队列中检索安全事件数据		3	3	1		X
使自动删除功能(CDMI删除)与机构的数据保留政策保持一致	X	3	3	3		X
在使用CDMI Holds之前，了解解除CDMI Hold的流程和机制	X	4	4	4		X
使用数据静态加密措施保护敏感数据和高价值数据		4	1	1		X
对于加密功能，应始终验证实施是否使用了所请求的CDMI能力(受支持的操作)，而不是其他功能		4	1	1		X
使用CDMI清洗功能清除云服务提供商存储中的敏感数据	X	3	3	3		X
基于对象的存储设备(6.7.2)						

就OSD而言，在不安全网络上涉及敏感数据的所有交易都应使用IPsec		5	5	0		X
对于OSD，对象存储应在执行操作前验证能力的真实性	X	5	5	5	X	X
OSD和安全管理器之间的时钟同步应使用安全协议来实现	X	4	4	4	X	X
对于OSD来说，能力过期时间应有限制，以最大限度地减少受损能力的使用时间	X	3	3	3	X	X
对于OSD，工作密钥(用于生成能力密钥)应经常刷新	X	3	3	3		X
内容寻址存储(6.7.3)						
在允许访问CAS系统之前，应先对用户和应用程序进行身份验证和授权。	X	5	5	5	X	X
计算机辅助服务系统应确保内容在其整个生命周期内的可读性和可访问性。		0	5	5	X	X
CAS系统应采用稳健的散列机制		0	4	4	X	X

表 B.7 – 存储安全服务(6.8)

控制装置	优先事项(5为最高)				数据敏感性	
	S	C	I	A	L	H
数据清除(6.8.1)						
组织和个人应对其信息进行分类，评估记录信息的介质的性质，评估保密风险，并确定介质的未来计划(例如重复使用)。		5	5	1	X	X
应根据成本、环境影响等因素对所选的消毒类型进行评估，并作出最能降低保密风险和最能满足对流程施加的其他限制的决定。		5	3	1	X	X
只有在信息披露不会对组织任务造成影响、不会导致组织资产受损、不会造成财务损失或对任何个人造成伤害的情况下，才可考虑在不进行消毒处理的情况下处置存储设备或存储元件。		5	0	1	X	X
当消毒是合规的一个要素时，应审查具体要求和相关规范，以确定它们是否规定了特定的覆写技术、消毒证明文件等。		5	3	1	X	X
清除操作的级别应与风险谨慎平衡，尤其要注意PII和电子病历以及业务或关键任务数据(如商业秘密、知识产权等)。		5	3	1	X	X
当存储介质被转移、过时、不再使用或不再为信息系统所需时，应清除残留的磁性、光学、电气或其他数据表示形式。		5	0	1	X	X
应使用附件A确定建议对特定培养基进行的消毒。		5	0	1	X	X
并非所有类型的可用介质都在本国际准则中作了规定，对于未包括在内的介质，各组织应确定并使用可实现清除、清理或销毁其介质意图的流程。		5	0	1	X	X
即使使用加密方法，也建议在使用结束时对介质进行消毒。		3	0	1	X	X
如果逻辑存储是可写的，则应使用覆盖或加密擦除技术进行清除，以清除逻辑存储使用的底层存储介质部分；成功应用加密擦除进行清除的前提是，在逻辑存储上记录数据之前，加密已激活。		2	0	1	X	X

数据保护技术(可包括复制、备份和CDP存储)通常与逻辑存储结合使用，因此应在与数据保护机制相关的存储上执行单独的清除操作，以消除敏感数据或高价值数据。		2	0	1		X
各组织应保存消毒活动记录，以记录消毒了哪些介质、时间、消毒方式以及介质的最终处置。	X	4	4	4	X	X
应出具消毒证书，并包含适当的详细信息	X	4	4	4	X	X
与清理相关的审计跟踪应记录带有时间戳的交易和进度。	X	4	4	4	X	X
如果时间和外部因素允许，应进行全面的消毒验证。	X	4	4	4	X	X
如果使用加密擦除进行清除，则应进行适当的验证。	X	4	4	4	X	X
数据保密(6.8.2)						
需要对移动中的数据进行加密时，应提供端到端保护		3	3	1		X
对运动中的数据进行加密会给通信实体带来巨大的计算负担，因此应实施适当的补偿措施，以尽量减少影响		4	4	5		X
对于IPsec，应使用版本3和IKE版本2(或更高版本)。	X	5	5	5		X
对于TLS，存储客户端应遵守SNIA技术立场中的要求：存储系统TLS规范v1.0(或最新版本)	X	5	5	5		X
为了提供基本的保护，防止因失去对介质的控制而造成数据泄露，应使用存储设备、交换机、专用设备、HBA等内部的加密机制		5	2	2		X
对于静态加密，应使用专为存储技术设计的算法和操作模式	X	5	5	5		X
限制密钥以明文形式存在的时间，防止人类查看明文密钥		5	3	3		X
加密密钥只能用于一个目的，具体来说，不要使用密钥加密密钥来加密数据，也不要使用数据加密密钥来加密其他密钥	X	5	5	5		X
从整个密钥空间中随机选择密钥		4	3	3		X
检查并避免使用已知的弱密钥	X	3	3	3		X
数据加密密钥应限于有限的加密期(一般不超过2年)或处理的最大数据量		4	3	3		X
在可能的情况下，存储系统和基础设施应使用可互操作的集中式密钥管理基础设施(例如，生成和存档加密密钥)	X	3	3	3		X

存储系统和基础设施应使用经认可的OASIS、符合KMIP标准的客户端可访问和使用密钥管理基础设施	X	3	3	3		X
减少数据(6.8.3)						
当加密与压缩同时使用时，应在加密前进行压缩	X	4	4	4	X	X
当加密与重复数据删除同时使用时，重复数据删除应在加密之前应用	X	4	4	4	X	X
当压缩和重复数据删除与加密同时使用时，使用顺序应为重复数据删除和压缩或组合和重复数据删除，然后是加密	X	4	4	4	X	X
压缩或重复数据删除会影响灾难恢复和业务连续性实施，因此在设计、记录和测试灾难恢复和业务连续性解决方案时应考虑到这一点	X	5	5	5	X	X

B.2.2 存储安全设计与实施指导

表格B.8、B.9、B.10、B.11、B.12和B.13总结了第7条中包含的安全控制和指导，同时显示了它们与不同数据敏感级别（见B.1.2）和优先级代码（见B.1.3）的相关性。

表 B.8 – 存储安全设计原则（7.2）

控制装置	优先事项 (5为最高)				数据 敏感性	
	S	C	I	A	L	H
纵深防御(7.2.1)						
确保均衡地关注三大要素：人员、技术和运营	X	5	5	5	X	X
通过有效的信息保证政策和程序、角色和责任的分配、资源的承诺、关键人员的培训以及个人问责制来贯彻执行	X	4	4	4	X	X
在多个地点部署保护机制，抵御各类攻击	X	3	3	3	X	X
在潜在广告和目标之间部署多重防御机制(分层	X	3	3	3	X	X
包括检测和保护机制	X	3	3	3	X	X
部署强大的密钥管理和PKI，支持所有信息保障技术，并具有很强的抗攻击能力	X	4	4	4		X
维护可见的最新系统安全政策	X	3	3	3	X	X
积极管理存储技术和保护机制的安全状况(如安装安全补丁和病毒更新、维护ACL等)	X	3	3	3	X	X
定期进行安全威胁评估，以确定持续的安全准备状态	X	3	3	3	X	X
监测并应对当前的威胁	X	4	4	4	X	X
安全域(7.2.2)						
不同敏感度的存储和存储网络应位于不同的安全域中		4	4	3		X
为外部网络提供服务的设备和计算机系统应位于与内部网络设备和计算机系统不同的域中		3	3	2	X	X
战略资产应位于专门的安全域内		5	3	2		X

不受信任的设备和计算机系统对存储资产的访问应受到限制或根本无法访问	X	5	5	5	X	
用于不同目的(如开发、生产、管理等)和使用不同技术(如CIFS/NFS、iSCSI、CDMI等)的存储和存储网络应位于不同的安全域中		3	2	1		X
存储网络应与普通网络(如企业局域网)处于不同的安全域中		2	4	2	X	X
存储设备和存储网络管理系统应位于专用安全域中		1	3	1	X	X
开发阶段的系统应与生产系统位于不同的领域		5	3	3	X	X
应进一步隔离(使用分区、VLAN和VSAN)可能被允许驻留在单个安全域但用于多种用途或持有多级敏感数据的存储设备，以最大限度地减少可能的交互作用		4	4	1		X
设计复原力(7.2.3)						
存储安全设计应包含多层冗余，以消除单点故障，最大限度地提高存储基础设施的可用性。	X	5	5	5	X	X
这些设计还应采用多种方法，使存储设备更能抵御攻击和网络故障	X	4	4	4	X	X
安全初始化(7.2.4)						
作为一项设计原则，存储系统的架构应支持安全初始化序列，以确保在通电或复位后从"停机"状态过渡。	X	4	4	4	X	X
在初始化阶段，外部可访问的进程和网络接口应不可用，或至少拒绝访问，直到主体通过验证。	X	4	4	4	X	X
软件和操作系统加载过程应从已知状态开始，并在系统最后一次运行时由系统管理员指定安全值。	X	3	3	3	X	X

表 B.9 – 数据可靠性、可用性和复原力 （7.3）

控制装置	优先事项 (5为最高)				数据敏感性	
	S	C	I	A	L	H
可靠性(7.3.1)						
存储系统和基础设施的可靠性不应受到安全功能的不利影响		1	4	4	X	X
应积极主动地管理漏洞，将其对系统可靠性的影响降至最低		1	4	4	X	X
应评估控制措施，以确定它们是否能够确保数据的可靠性和安全性	X	3	3	3	X	X
可用性(7.3.2)						
由于可用性的重要性，存储安全设计和实施应努力将对可用性的影响降至最低		1	1	5	X	X
应管理数据加密密钥，以避免在密钥不可用或不慎损毁时出现数据可用性问题		1	1	5	X	X
数据保护机制应成为可用性设计的一部分，以防止因系统故障造成		1	3	4	X	X
重大故障						
备份和复制(7.3.3)						
数据保护机制(如备份、复制等)的设计应考虑到快速恢复，而不仅仅是保存数据		1	4	5	X	X
确保备份方法，特别是业务/关键任务数据的备份方法，与相关的还原策略保持一致		1	4	5	X	X
确保备份方法提供充分保护，防止未经授权的访问(如加密)		4	4	1		X
建立处理存储介质的可信个人(和供应商)链	X	5	5	5		X
实施备份验证，"证明"恢复要求已得到满足		0	5	5		X
确保复制方法，尤其是业务/任务关键数据的复制方法，符合相关的可靠性、容错性或性能要求	X	5	5	5		X
确保复制方法提供足够的保护，防止未经授权的访问(如移动加密)		5	0	3		X

确保CDP方法(如连续、接近连续、固定间隔等)，特别是对于业务/任务关键数据，与相关的恢复战略保持一致		0	3	3	X	X
在网络带宽较高的情况下(如多媒体文件)，采用优先处理网络流量的节流技术，以减少CDP对日常运行的影响		0	2	2		X
确保CDP方法提供足够的保护，防止未经授权的访问(如移动数据和静态数据加密)		4	3	2		X
灾难恢复和业务连续性(7.3.4)						
确保在灾难恢复/灾难备份规划和实施中考虑到存储生态系统的因素	X	5	5	5	X	X
为有限的中断事件(系统故障、恶意攻击、操作员失误)做好准备	X	4	4	4	X	X
确定并记录与存储生态系统相关的独特人员和设施要求	X	3	3	3	X	X
对假设进行持续规划和定期测试，这对成功的灾难恢复/灾后恢复至关重要；应将灾难恢复/灾后恢复测试结果反馈到灾难恢复/灾后恢复计划的持续维护中	X	3	3	3	X	X
复原力(7.3.5)						
安全应是复原力战略不可分割的一部分；计划应对存储和安全技术的单元故障和损害	X	5	5	5	X	X
应尽可能利用冗余		0	5	5	X	X
应尽可能使用易于维修的各种部件		2	2	4	X	X
安全特性和功能的实施不应对存储系统或基础设施的恢复能力造成不利影响	X	4	4	4	X	X

表 B.10 – 数据保留(7.4)

控制装置	优先事项 (5为最高)				数据 敏感性	
	S	C	I	A	L	H
长期保留(7.4.1)						
定期检查系统中数据的完整性，而不是等到读取数据时才进行检查		1	4	4	X	X
在将存档数据迁移到较新的存储技术时，引入可用的安全功能，提供更强的安全措施，以更好地保护数据在新位置的安全	X	2	2	2		X
确保档案存储系统能够对新用户进行身份验证，并建立他们与现有用户所附资源的关系		4	1	1		X
确保保密机制在写入数据的用户完全不在场的情况下发挥作用		5	0	0		X
确保安全日志足够完整和持久，以帮助检测缓慢的攻击，并保持攻击历史记录，用于做出调整数据保护的决策	X	4	4	4		X
系统应立即处理任何漏洞，或保留漏洞历史记录，以便智能地安排纠正措施	X	5	5	5		X
在使用数据缩减技术(如压缩和重复数据复制)时，应避免损害数据完整性		1	4	1		X
中短期留用(7.4.2)						
应创建和保存数据的多个物理或逻辑副本；副本的组织应尽可能独立(如地理、行政/管理和平台/操作系统)，并根据数据的价值和风险承受能力选择副本的数量		0	5	5	X	X
按照规定的时间表，审计明显和潜在的故障(如完整性检查)及其造成的损害；在损害扩大之前，使用其他副本中的良好数据修复损坏的数据		0	4	2	X	X
将访问控制计划与保存信息的法律法规要求相匹配	X	5	5	5	X	X
确保问责制和可追溯性措施充分有效；所有数据访问都可能需要审计日志条目	X	4	4	4	X	X
实施证明数据真实性、来源和保管链的机制，特别是对证据性质的数据而言		4	5	0	X	X

如果使用加密技术，则对密钥和密钥材料进行存档/回收；在建议的加密周期内或需要更换底层加密算法时，重新为数据配制密钥		5	5	3	X	X

表 B.11 – 数据的保密性和完整性 (7.5)

控制装置	优先事项 (5为最高)				数据敏感性	
	S	C	I	A	L	H
基于存储的加密不应成为敏感数据的主要加密形式		4	3	2		X
加密点的选择应受到灾难恢复、业务连续性、数据缩减和数据保护等因素的影响	X	4	4	4	X	X
选择和部署加密时应考虑数据保留需求	X	3	3	3	X	X
加密解决方案的安全强度至少应为112位，建议最低为128位		4	4	1	X	X
用于保护敏感数据或受监管数据的加密模块应采用公认的标准进行验证	X	5	5	5		X
可使用多个加密步骤，例如，为隐私目的加密的数据由加密硬盘为安全目的进一步加密	X	3	3	3		X
确保加密机制创建适当的审计日志条目(激活、验证、完整性检查、重新密钥等)。	X	4	4	4	X	X
事先商定哪些审计日志材料可以证明(令合规人员满意的)加密已正确执行	X	4	4	4	X	X
对加密是否正确进行定期审计检查，并考虑外部认证	X	3	3	3	X	X
利用集中式密钥管理	X	3	3	3	X	X
尽可能实现密钥管理的完全自动化	X	3	3	3	X	X
少用寿命长的密钥(即接近建议的最长加密周期，一般不超过1-2年，取决于密钥类型)	X	4	4	4		X
对密钥的生成、更改和分发实施严格的访问控制，以限制用户能力和职责分离约束(如安全角色	X	5	5	5		X
对于敏感数据或高价值数据，应进行端到端加密(即移动中的数据和静态数据)。	X	3	3	3		X

为保护数据完整性，存储系统应包含足够的恶意软件保护，以防止对数据的攻击	X	4	4	4	X	X
应使用基于WORM的存储来帮助满足不变性要求		2	4	2	X	X

表 B.12 – 虚拟化（7.6）

控制装置	优先事项 (5为最高)				数据 敏感性	
	S	C	I	A	L	H
存储虚拟化(7.6.1)						
对物理存储实体的控制应适用于整个域，以便在重新配置信息时不会绕过控制。	X	4	4	4	X	X
适当的存储联网控制应适用于整个域，因为当信息被重新定位或受控制的新信息被存储在未应用控制的实体上时，对域的子集应用此类控制可能会导致绕过控制	X	4	4	4	X	X
确保虚拟存储达到适当的服务级别目标	X	4	4	4	X	X
将存储基础架构的可用性目标与应用需求相匹配		0	0	5	X	X
将存储基础结构的保密和隐私要求与所存储的信息类型相匹配		5	0	0		X
酌情处理多租户问题		3	3	2	X	X
虚拟化系统的存储(7.6.2)						
应通过使用服务器虚拟化(管理程序)软件中的访问控制来控制虚拟机对存储网络的访问		0	3	3	X	X
应适当利用NPIV限制虚拟机访问存储目标	X	3	3	3	X	X
应谨慎控制基础设施中物理服务器之间的虚拟机迁移/移动，以避免产生意想不到的安全后果	X	3	3	3	X	X

表 B.13 – 设计和实施方面的考虑因素 (7.7)

控制装置	优先事项 (5为最高)				数据敏感性	
	S	C	I	A	L	H
加密和密钥管理问题(7.7.1)						
了解并遵守与加密和密钥管理相关的政府进口法规		3	0	0	X	X
了解并遵守与加密和密钥管理相关的政府出口法规		4	0	0	X	X
遵守企业或政府的密钥托管要求		5	3	2	X	X
制定关键设备受损时的恢复计划	X	5	5	5		X
制定密钥备份计划，确保持续访问加密的业务/关键任务信息	X	5	5	5		X
在处理/访问相同数据的存储设备之间安全分发关键材料		5	5	3		X
应了解加密对重复数据删除和压缩技术的影响，并在设计和实施中将其考虑在内	X	4	4	4		X
应理解无法在加密数据上应用病毒扫描等安全技术的问题，并通过其他机制加以解决	X	4	4	4		X
调整存储和政策(7.7.2)						
确定最敏感(个人身份信息、知识产权、商业秘密等)和业务/任务关键数据类别以及保护要求		5	2	1		X
将特定于存储的政策与其他政策相结合(即避免为存储生态系统创建单独的政策文件)	X	2	2	2	X	X
解决数据保留和保护问题(如一写多读或WORM、真实性、访问控制等)		3	4	2		X
解决数据销毁和介质消毒问题		4	1	1		X
确保存储生态系统的所有要素都符合政策要求(如ISO/IEC27001/27002)	X	3	3	3	X	X
优先处理最敏感/最关键的数据	X	4	4	4		X
合规性(7.7.3)						

确保用户，尤其是特权用户，拥有唯一的用户名(即无共享账户)		5	0	0	X	X
在可能的情况下，根据角色授予权利和特权	X	3	3	3	X	X
记录所有尝试(成功和不成功)的管理事件和事务	X	4	4	4	X	X
确保记录的事件/交易数据包含足够的应用程序或系统细节，以清楚地识别来源	X	3	3	3	X	X
确保用户信息可追溯到特定个人	X	3	3	3	X	X
适当时，将日志记录视为证据(保管链、不可抵赖性、真实性等)。	X	4	4	4	X	X
确保存储层参与外部审计记录措施	X	4	4	4	X	X
监控审计日志事件并发出相应警报	X	5	5	5	X	X
实施适当的数据保留措施		0	4	0	X	X
实施适当的数据完整性和真实性措施		4	5	0	X	X
在删除、重新使用或停用硬件时正确清除数据		4	0	0	X	X
在生命周期结束时正确消毒虚拟服务器映像及其副本	X	1	1	1	X	X
实施适当的数据访问控制措施，控制对数据和元数据(如搜索结果)的访问；尽可能采取权限最小的态势		3	0	1	X	X
采取适当的数据保密措施，防止未经授权的披露		5	0	0		X
确保重复数据删除的使用不与数据真实性要求相冲突		3	4	0		X
确保数据和媒体消毒机制不违反保全命令	X	5	5	5		X

确保在处理证据数据(如审计日志、元数据、镜像、时间点副本等)时遵循适当的监管链程序		5	5	0	X	X
安全多租户(7.7.4)						
在提供共享资源的管理和灵活性优势的同时，提供安全隔离，确保任何租户都无法确定任何其他租户的存在或身份，无法访问任何其他租户的移动数据(网络)，无法访问任何其他租户的静态数据(存储)，无法执行影响其他租户执行的操作，或者无法执行可能拒绝为其他租户提供服务的操作，并确保每个租户都能拥有独立于其他租户的存在和配置的配置	X	4	4	4	X	X
当资源(计算、存储或网络)从租户退役时，应清除资源中的所有数据和配置信息	X	4	4	4	X	X
在租户层面采取问责和可追溯措施	X	4	4	4	X	X
根据租户对资源的使用情况使用加密存储		4	4	0	X	X
使用强大的对称加密(即至少128位的安全强度)来保护静态数据		5	3	0	X	X
使用安全快速的删除配置(介质消毒，包括加密擦除)		5	0	0	X	X
使用可信的第三方数据存储管理(如SNMPv3、带TLS的SMI-S等)	X	4	4	4	X	X
使用自动密钥管理，提供由租户控制的密钥管理(利用符合KMIP标准的服务器)	X	3	3	3	X	X
使用安全的数据复制(如运动中和静止时的数据加密)		5	0	0	X	X
保护数据不受管理员侵犯(例如，执行最小权限访问模式，管理员无权访问密钥材料等)		4	0	0	X	X
使用高度可用的存储网络结构(多路径和不同路径)		0	0	4	X	X
使用集中、安全的审计日志(如通过TLS的系统日志)		4	4	0	X	X

加密模块和其他安全措施(如媒体消毒、访问控制等)的验证和认证(如通用标准)	X	1	1	1	X	X
确保自主数据移动安全(7.7.5)						
配置数据移动策略应仅限于经授权和授权的特权用户	X	2	2	2	X	X
建立配置的人员应熟悉来源地和目的地的安全属性	X	3	3	3	X	X
实施或终止自主数据移动的配置更改应反映在审计日志中	X	2	2	2	X	X
所有自主数据移动事务都应反映在进行数据移动的系统的审计日志中	X	2	2	2	X	X
作为自主数据移动交易的一部分，移动数据的完整性应得到验证(最好使用加密哈希)。		0	3	0	X	X
自主数据移动事务不应影响数据的真实性(例如，原始系统元数据，如创建日期、最后访问时间等，在移动数据中得到正确体现)		0	4	2	X	X
自主数据移动交易不应否定不变性或其他数据保存控制措施(如支持法律保留)。		0	4	0	X	X
自主数据移动交易不应取消或削弱与数据相关的加密控制		4	0	0		X
跨系统的自主数据移动交易应包括敏感和高价值数据的移动中数据加密		4	0	0		X
作为自主数据移动交易的一部分，源数据或存储介质在释放供重新使用之前，应适当进行消毒处理		4	0	0		X

附录 C（信息性附录）

重要的安全概念

C.1 认证

在基本层面上，认证是通过验证所提供的信息（即验证声明的身份）来验证用户或实体的声称身份的过程。认证是系统和协议设计中常见的安全问题，有各种可用的认证技术。常见问题是如何选择技术或在给定技术的各种基本相似实现中选择哪种。
认证可以是单向的或互通的（双向的）。对于单向认证，通常只有客户端（用户或实体）被验证为系统（或服务器）。对于互通认证，双方通信的各方都进行相互验证。认证也可以涉及多于两方的情况。在三方认证中，信任的第三方是双方进行认证过程的中间人。
认证要素是用于安全目的认证或验证用户或实体身份的信息。通常认可的三个认证要素是：
a) 认证方所知的东西，例如秘密或密码。
b) 认证方所持有的东西，例如物理硬件令牌或钥匙卡。
c) 认证方的身份特征（例如指纹、视网膜图案）、认证方所做的事情（例如签名）或认证方所在的位置。

当系统要求至少使用上述认证要素中的两个时，称其为采用了双因素认证（或多因素认证）。这与传统密码认证不同，传统密码认证只需要一个认证要素（例如密码知识）即可访问系统。最佳认证机制结合了这些要素中的两个或更多个。
ISO/IEC 27002:2013, 13.3.1 提供了有关使用秘密认证信息的适用指南，可以总结为：
— 保持秘密认证信息的机密性，不要共享它；
— 避免记录秘密认证信息；
— 一旦有任何可能被泄露的迹象，即更改秘密认证信息；
— 当使用作为秘密认证信息的密码时，选择高质量密码（最小长度、复杂组合、不容易猜测，不包含字典中的单词，没有相同的连续字符等）。

认证实现可以采用多种形式，包括：

— 本地认证 – 需要认证服务的系统也是认证器（即做出认证决策的实体）。无法轻松同步用于验证的凭据数据库，因此其在较大组织内的可用性有限。
— 外部认证 – 认证器位于需要进行认证决策的系统的控制和影响范围之外；而且，认证器是值得信任的权威来源。

— 集中认证 – 这种形式的外部认证旨在支持许多系统（通常是异构的），它通常包括冗余、使用标准协议，并提供附加有用信息（例如角色标识符）。不尝试使后续认证透明化（即通常需要进行多次认证）。
— 单一登录（SSO） – 这种形式的集中认证使用一组凭据，然后透明地代表用户执行后续认证。此外，通常与集中授权系统密切结合，以确保一致的权限。

许多企业已经将身份管理(目录服务、NIS、NIS+)和认证服务(例如RADIUS、PKI、Kerberos、LDAP等)集中，因此自然希望利用这个基础设施和为填充身份数据所做的投资来帮助解决认证和授权问题。

C.2 授权和访问控制

授权是确定经过身份验证的一方是否有权访问特定资源或服务的过程。虽然紧密相关，但认证和授权是两个独立的机制。也许由于这种紧密耦合，有时会错误地认为认证意味着授权。认证只是验证一方的身份；授权则确定他们是否可以执行某种操作。确保适当地授予或限制对资源和服务的访问的方法通常作为访问控制机制的一部分实施。

自20世纪70年代初以来，已经开发了许多访问控制模型和系统（例如Bell-LaPadula、Cark-Wilson等）。几乎所有这些访问控制模型都可以使用以下概念及其关系来形式化地描述：
— 用户 – 与系统进行接口的人；重点是人而不是凭据
— 主体 – 代表用户执行操作的计算机进程；它们可以发起请求执行对象上的操作或一系列操作
— 对象 – 计算机系统上可访问的任何资源；被动实体，包含或接收信息
— 操作 – 由主体调用的主动过程
— 权限（或特权） – 执行系统上某些操作的授权；通常涉及对象和操作的某种组合

这些概念已被纳入各种访问控制策略（规则）和机制中，包括以下内容：
— 自主访问控制（DAC） – 策略允许授予和撤销访问权限由各个用户自行决定
— 强制访问控制（MAC） – 策略由安全策略管理员集中控制；用户无法覆盖策略
— 基于角色的访问控制（RBAC） – 将权限分配给特定角色，并将角色分配给用户；管理个人用户权限只需将适当的角色分配给用户

授权和访问控制机制的实现可以采用许多形式，并具有不同的复杂程度。较简单的实现可能对经过身份验证的用户(即授予对系统资源无限制访问)施加少量或不施加任何控制。更复杂的实现可能会根据用户所属的组或所持有的特定角色来对用户施加控制。后一种方法通常使用基于角色的访问控制（RBAC）机制来实现，并且是推荐的实现技术。

访问控制列表（ACL）是实施访问控制矩阵的一种方式，它指定用户或主体允许对对象执行的操作。在典型的ACL中，列表中的每个条目都指定了一个主体和一个操作；如C.1表中所示，ACL中的条目（Alice，Delete）表示Alice有权删除文件XYZ。

表格 C.1 — 文件“XYZ”的访问控制列表（ACL）

用户/子等	操作
Alice	删除
Joe	读、写
Jan	执行

在基于ACL（访问控制列表）的安全模型中，系统首先检查列表以决定是否允许用户（主体）请求的操作。该列表通常是一个数据结构，通常是一个表，其中包含指定各个用户或组对特定系统对象（例如程序、进程或文件）的权限条目。这些条目有时被称为访问控制条目（ACE）。每个可访问的对象都包含一个指向其ACL的标识符。特权或权限确定特定的访问权限，例如用户是否可以读取、写入或执行对象。在某些实现中，ACE可以控制用户或用户组是否可以更改对象上的ACL。

还可以将用户（主体）分组，使ACL包含组的名称而不是个别用户。这样可以更轻松地管理ACL，因为撤销用户的权限将涉及将其从组的成员资格中删除，而不是修改ACL本身。

保护位机制与ACL类似；但是，位与对象关联，而不是与用户和操作条目关联。保护位机制通常在UNIX操作系统中实现，并用于将用户划分为不同的类别，通常是用户（自身）、组和其他。访问控制系统通过将读（r）、写（w）或执行（x）操作与每个用户类别关联来控制对文件的访问。

作为访问控制机制，保护位机制存在一系列问题，包括：
- 创建文件的用户默认为所有者。
- 文件的所有者通常是唯一可以修改保护位的人（除了超级用户或管理员）。
- 每个文件只有一个可用的组。
- 系统管理员控制组成员资格；随着组内成员资格的变化，用户访问文件的权限也会随之变化。
- 系统无法以个别方式授予对象访问权限。

访问控制决策通常由个人用户作为组织成员承担的角色决定。这包括指定职责、责任和资格。例如，与医院相关联的个人可以担任医生、护士、临床医生和药剂师等角色。在银行中的角色包括出纳员、贷款办事员和会计师。角色还可以应用于军事系统；例如，战术系统中的常见角色包括目标分析师、态势分析师和通信分析师。

C.3 自加密硬盘（SED）

许多存储器制造商推出了集成加密和访问控制功能的存储设备,也称为自加密硬盘(SED)。具备始终开启加密功能的SED可以大大降低未加密数据被误留在设备上的可能性。终端用户无法关闭加密功能（因此，所有先前在指定区域的数据都是加密的）。SED通常会加密大部分或全部用户可寻址区域，可能会有一些例外，例如专门用于存储预启动应用程序和相关数据的明确标识的区域。

SED的一个重要附加优势是可以紧密耦合控制器和存储介质，使设备能够直接寻址存储密钥的位置,而仅依赖软件的抽象用户访问接口的解决方案可能无法直接访问这些区域。

SED也非常适合执行一种特殊形式的清除操作，称为加密擦除（见A.3），这种清除操作的可靠性比其他清除技术要高得多。通常，加密擦除可以在几秒钟内完成（而其他备选的媒体清除操作可能需要数小时或数天）。随着存储设备变得更大，当采用非加密方法时，清除变得更加繁琐和耗时，因此加密擦除非常重要。

C.4 清除操作

信息和通信技术（ICT）系统使用各种媒体捕获、处理和存储信息。这些信息不仅位于预期的存储媒体上，还位于用于创建、处理或传输此信息的设备上。这些媒体可能需要特殊处理，以降低未经授权的信息披露风险并确保其机密性。对于从始建到处置阶段，高效有效地管理ICT系统创建、处理和存储的信息是ICT系统所有者和数据保管者的主要关注点。

随着越来越复杂的加密技术的使用,希望获取组织敏感信息的攻击者被迫在系统本身之外寻找这些信息。攻击的一个途径是从媒体中恢复被删除的数据。这些残留数据可能使未经授权的个人重建数据，从而获得对敏感信息的访问权限。通过确保已删除的数据不易恢复，清除操作可以用于阻止这种攻击。

当存储媒体转移、过时或不再可用或不再被信息系统需要时，重要的是确保已删除的数据的残留磁性、光学、电气或其他表示不易被恢复。清除操作是指从存储媒体中删除数据的一般过程，以合理确保数据不易被检索和重构。

对于包含遗留磁性媒体的存储设备，使用固定模式（例如零）的单次覆写通常可以防止即使使用最先进的实验室技术，数据也无法被恢复。仅依赖于用于执行覆写过程的本地读写接口的主要缺点在于，不会处理当前未映射到活动逻辑块寻址（LBA）地址的区域（例如缺陷区域和当前未分配空间）。专用的清除命令更有效地支持处理这些区域。使用这些命令会产生一种权衡，因为虽然它们应更彻底地处理媒体的所有区域，但使用这些命令还需要从供应商那里获得信任和保证，即命令已按预期实

施。

习惯于在磁性媒体上依赖覆写技术，并且在媒体类型发展（例如转向闪存设备）的过程中继续应用这些技术的用户，可能将其数据暴露给意外披露的风险。尽管具有不同基础媒体类型的设备可能具有相同（或非常相似）的主机接口（例如ATA或SCSI），但是必须将清除操作技术仔细匹配到媒体上。

对于某些媒体类型的破坏性技术在未来可能变得更加困难或不可能。传统技术（例如对磁性媒体的去磁）在磁性媒体发展的过程中变得更加复杂，因为某些新兴的磁记录技术变体采用了更高的磁化强度（磁力）。因此，现有的去磁器可能没有足够的磁力有效去磁这些媒体。

对非磁性存储媒体（如闪存）应用破坏性技术也越来越具有挑战性，因为常用的研磨技术所需的颗粒大小与闪存存储密度的任何增加成比例下降。闪存芯片已经因其组件材料的硬度而在研磨机中偶尔损坏，而随着研磨机试图将芯片研磨成更小的碎片，这个问题将变得更加严重。

基于加密的清除功能（见A.3）是一种可以在时间和可靠性方面提供显著优势的清除技术，根据支持的几乎所有主要存储供应商的支持，这种功能很可能会在不久的将来广泛可用。加密擦除（如果定义得当）可能具有重要价值，具体体现在：
- 有助于快速清除敏感数据（仅需几秒，而不是几小时或几天）；
- 减少对存储设备的磨损（因此可能延长设备的使用寿命）；
- 减少执行清除操作所需的人工时间；
- 处理可能不适合使用传统去磁和销毁技术的媒体类型。

对于所有支持加密且意图使用加密擦除来清除媒体的设备（包括SED、移动设备和其他设备），其可靠性（在很大程度上）取决于以下因素：
a) 所有目标数据是否已加密或（对于未加密的任何目标数据）是否能够使用特定于媒体的技术进行有效清除。
b) MEK的熵水平。
c) 如果在加密擦除过程中被清除的密钥是用于包装MEK的密钥（而不是MEK本身），则包装机制的强度和待清除的包装密钥的熵水平。
d) 用于加密数据的加密算法的强度，包括操作模式和正确实施的保证。
e) 在擦除后检索MEK的难度，以及解开密钥的任何努力（如果密钥被存储在另一个值的包装下）。
注意：在某些情况下，媒体加密密钥可能已明文存储，因为媒体加密的唯一目的可能是支持加密擦除。

移动设备（和其他非SED设备）也可以支持强加密功能。是否依赖于加密擦除来清

除设备上的媒体取决于设备上是否已对所有敏感数据进行了加密。如果敏感数据在存储设备加密之前存储在设备上，或者不确定在加密之前是否在设备上存储了敏感数据，则加密擦除可能不适合作为清除机制（见A.3）。

在加密擦除中，确保所有加密密钥的所有副本都已销毁是一个重要问题。SED通过在内部生成密钥并永不暴露它们来保证这一点。擦除是通过密钥更改请求操作执行的。SED可能包含多个分区，每个分区都有一个唯一的密钥，因此可能需要多个密钥更改请求。

C.5 日志记录

在存储系统和基础设施中，有各种各样的交易或事件可能会导致生成事件日志条目（消息）。此外，这些事件日志条目必须以某种方式记录以进行事件日志记录。从安全或合规性的角度来看，捕获那些需要证明操作的事件日志条目（例如加密和保留），执行责任和可追溯性，满足证据要求，以及对系统进行充分监视是非常重要的。这个常用的一小部分日志记录称为审计日志。

并不是所有的事件日志条目都是相同的，因为有些可能只用于调试目的，提供系统健康状态，警告小的配置问题等。从审计日志的角度来看，管理事件（即人类的操作）总是有兴趣的，数据访问事件通常有限的兴趣（除非需要严密监控关键文件和目录），控制事件通常兴趣最小（它们在事件发生后的根本原因分析中可能提供有用的信息）。

此外，审计日志通常要求将感兴趣的事件条目与设备生成的大多数其他事件日志条目分别处理。这种特殊处理可以通过使设备将审计日志条目发送到特殊的日志基础设施来完成，或者可以通过从通用日志流中删除这些事件条目来实现（这是一种更具挑战性的方法，因为它要求预先知道所有感兴趣的事件条目）。这种特殊处理的另一个方面是，组织通常必须证明它正在监视（例如对异常事件生成警报）和报告；这些操作通常需要某种形式的集中日志记录基础设施，而不仅仅是简单的收集器。

C.6 N_Port_ID虚拟化（NPIV）

作为起点，光纤通道（Fibre Channel，FC）端口是一个硬件路径，用于在FC链路（有时称为通道）上执行数据通信。FC定义了许多不同类型的端口，但以下端口与NPIV相关：
- N端口：用于将节点连接到FC交换机的网络或节点端口。这可以是服务器中的HBA（主机总线适配器）或存储阵列上的目标端口。
- F端口：用于将FC交换机与节点（N端口）连接在一起，通常是服务器的HBA或存储阵列的目标端口。

- E端口：用于将（级联）FC交换机连接在一起；两个E端口之间的连接形成互联交换链路（Inter-Switch Link，ISL）。

通常，N端口将与一个N_Port_ID关联。这个N_Port_ID是由光纤通道交换机在Fabric登录（FLOGI）过程中分配的24位地址，该过程在链路运行后发生。

注意：N_Port_ID与全局端口名（World Wide Port Name，WWPN）不同，尽管通常WWPN和N_Port_ID之间存在一对一的关系。因此，对于给定的物理N端口，会有一个WWPN和一个N_Port_ID与之关联。

NPIV使得单个物理N端口可以具有多个WWPN，因此可以与多个N_Port_ID相关联。在正常的FLOGI过程之后，启用了NPIV的物理N端口可以随后发出额外的命令来注册更多的WWPN，并接收更多的N_Port_ID（每个WWPN一个）。光纤通道交换机也需要支持NPIV，因为链接另一端的F端口会“看到”来自服务器的多个WWPN和多个N_Port_ID，并且需要知道如何处理这种行为。

一旦注册了所有适用的WWPN，每个WWPN都可以用于SAN分区或LUN展示。物理WWPN和虚拟WWPN之间没有区别；它们都表现出完全相同的方式，并且可以以完全相同的方式使用。

NPIV创建的每个N_Port_ID都会消耗与该N_Port_ID相关的服务器、网络和存储资源。在具有大量虚拟服务器的环境中，为每个虚拟服务器创建N_Port_ID可能会导致资源限制而引起扩展问题。对于这样的环境，可以将NPIV的使用限制为仅创建必要的N_Port_ID，以在更大的域之间提供隔离(例如为单个组织或服务提供商的单个租户的虚拟服务器集合）。

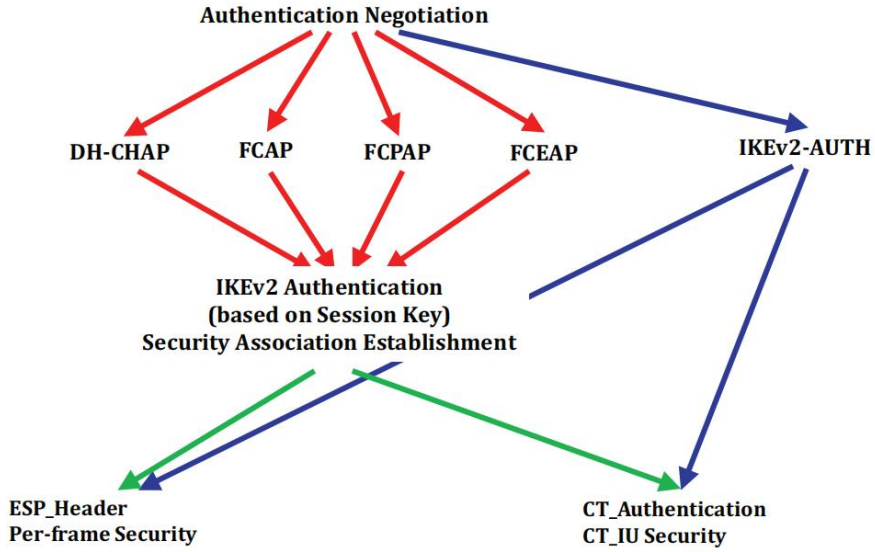
C.7 光纤通道安全

C.7.1 概述

光纤通道布局可能跨越多个远距离分散的站点，因此确保安全服务可用以确保一致的配置和适当的访问控制至关重要。
ANSI INCITS 496-2012《信息技术 - 光纤通道 - 安全协议 - 2》（FC-SP-2）定义了用于认证光纤通道实体、建立会话密钥、协商参数以确保逐帧完整性和机密性，并在光纤通道布局中定义和分发策略的协议。要声称符合FC-SP-2，实现必须支持FC-SP-2标准附录A（具体而言是A.2.1）中描述的AUTH-A合规要素。
FC-SP-2定义的安全架构包括以下组件：
a）认证基础设施 - 针对几种认证基础设施定义了布局安全架构：基于密钥、基于证书、基于密码和基于预共享密钥的认证。

b）认证 – 定义了认证协议，允许实体确保通信实体的身份。两个实体可以协商是否需要认证以及可以使用哪种认证协议。认证适用于交换机到交换机、节点到交换机和节点到节点，使用以下协议之一：
– Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP)：强制性使用（见C.7.2）；
– 光纤通道证书认证协议 (FCAP)；
– 光纤通道密码认证协议 (FCPAP)；
– 光纤通道可扩展认证协议 (FCEAP)；
– 安全关联管理协议 (IKEv2-AUTH)。
c）安全关联 – 定义了适用于光纤通道的IKEv2协议子集（即安全关联管理协议），以建立实体之间的安全关联。有两种机制可用于保护特定类型的流量：ESP_Header用于保护光纤通道帧，CT_Authentication用于保护通用传输信息单元。
d）加密完整性和机密性 – 通过使用ESP_Header（见C.7.3）逐帧实现加密完整性和机密性、重播保护和流量源认证。CT_Authentication（见C.7.4）可用于提供通用传输信息单元的加密完整性和机密性、重播保护和流量源认证。ESP_Header处理和CT_Authentication处理是相互独立的。
e）授权（访问控制） – 布局策略提供基本的授权控制，以Access Control Lists (ACLs)的形式存在，并定义了以下两种基本类型的策略：
– 包含布局范围数据的策略，分发到布局的每个交换机；
– 包含每个交换机数据的策略，发送到单个交换机。
布局策略可用于控制哪些交换机被允许组成布局，哪些节点被允许连接到布局。策略还可进一步用于指定布局环境内的拓扑限制（例如，哪些交换机可以连接到哪些其他交换机或哪些节点可以连接到哪些交换机）。
布局策略还提供控制对布局的管理访问的机制，并具有控制认证选择和指定布局实体（例如，节点和交换机）的安全属性的能力。对布局的管理访问可以受控于通用传输或IP访问。

图C.1是FC-SP-2标准第4.5条中的图示，显示了认证协议和安全关联之间的关系。定义的认证协议能够进行可选共享密钥建立的相互认证。在认证事务结束时计算出的共享密钥可用于建立安全关联。



图C.1 — FC-SP-2认证协议与安全关联之间的关系

C.7.2 DH-CHAP 认证

DH-CHAP是一种基于密钥的认证和密钥管理协议，它使用了CHAP算法并增加了可选的Diffie-Hellmann算法。DH-CHAP可在认证发起方和认证响应方之间提供单向或双向认证。当协议的Diffie-Hellmann部分未被使用时，DH-CHAP将其操作简化为CHAP协议的操作，称为带有NULL DH算法的DH-CHAP。所有符合FC-SP-2的实现都必须支持带有NULL DH算法的DH-CHAP。要声称符合FC-SP-2，实现必须支持AUTH-A合规要素（FC-SP-2附录A中描述的要素），其中包括2048位DH算法。

除了识别认证算法，FC-SP-2还指定认证适用于交换机到交换机、设备到交换机和设备到设备实体，并且这些协议能够支持相互认证。因此，符合或合规的产品在适用时还必须实现以下每个内容：

- **交换机到交换机**：包含这些实体之间的认证的产品必须能够对交换机进行认证，并能够被交换机进行认证。
- **设备到交换机**：包含这些实体之间的认证的产品必须能够从设备的角度对交换机进行认证，并能够被交换机进行认证；或者能够从交换机的角度对设备进行认证，并能够被设备进行认证。
- **设备到设备**：包含这些实体之间的认证的产品必须能够对设备进行认证，并能够被设备进行认证。此外，每个设备在执行此认证之前必须完成适当的设备到交换机认证。

符合要求的产品还必须实现重新认证功能，使得产品可以在任何时候被其他实体重新认证。

C.7.3 ESP_Header

ANSI INCITS 470 - 2011，信息技术 — 光纤通道 — 帧和信令-3 (FC-FS-3)定义了可用于光纤通道帧内的可选头部。其中，ESP_Header和ESP_Trailer在安全方面扮演重要角色，因为它们是支持帧负载加密的机制。

ESP_Header和CT_Authentication协议的安全关联由光纤通道安全关联管理协议（在FC-SP-2中定义）进行协商。该协议是IKEv2协议的修改子集，执行相同的核心操作，并使用光纤通道AUTH协议来传输IKEv2消息。IETF RFC 4595《在光纤通道安全关联管理协议中使用IKEv2》提供了关于光纤通道使用IKEv2的其他信息。

注意由于光纤通道数据流量与控制流量的分离，任何FC安全关联只适用于ESP_Header或CT_Authentication协议中的一个。

封装安全负载（ESP）在RFC 4303中定义，是一种通用机制，用于为IP数据包提供机密性、数据来源认证和防重放保护。FC-SP-2定义了如何在光纤通道中使用ESP，包括任何协商过程、附加的加密或认证算法和处理要求。

FC-FS-3规定：“对于在传输模式下的FC帧，应用端到端的ESP_Header处理（参见RFC 4303）；对于在隧道模式下的FC帧，应用逐跳的ESP_Header处理（参见RFC 4303）。身份验证选项应被使用，机密性可以由两个通信的FC_Ports进行协商（参见FC-SP-2）。”

注意，逐跳的ESP_Header处理的一种预期应用是在Fabric内或Fabrics之间安全地保护连接，而不需要每个Nx_Port都使用ESP。

C.7.5 FC-SP Zoning

为了保持与现有区域定义和实现的向后兼容性，FC-SP-2描述了增强型区域模型的变体，该模型由ANSI INCITS 461 - 2010《信息技术 — 光纤通道 - 交换机结构 - 5 (FC-SW-5)》和ANSI INCITS 463 - 2010《信息技术 — 光纤通道 — 通用服务 — 6 (FC-GS-6)》定义，遵循策略模型的一般概念，但将区域管理和执行与其他策略管理和执行完全分离。这种区域的变体被称为FC-SP区域。

Fabric策略和区域策略允许在整个Fabric中对策略信息进行非对称分布，并定义了三种类型的交换机：

a) 服务器交换机：保留所有策略对象和所有节点之间的（区域）信息。

b) 自主交换机：保留其自己的每个交换机策略对象、所有Fabric范围的策略对象和所有节点之间的（区域）信息。
c) 客户端交换机：保留其每个交换机的策略对象、所有Fabric范围的策略对象以及对其操作相关的节点之间的（区域）信息子集，当需要时从服务器交换机获取。此外，它们维护Fabric的区域集合数据库散列值和活动区域集合散列值。

C.8 OASIS密钥管理互操作性协议（KMIP）

在存储安全环境中应用信息保护通常涉及使用加密密钥，因此需要密钥的生命周期管理（生成、更新、分发、跟踪使用、生命周期策略，包括状态、存档和销毁）、密钥共享以及加密密钥的长期可用性。

OASIS密钥管理互操作性协议（KMIP）是一个开放的、供应商中立的规范，定义了用于应用程序、设备或系统与管理加密密钥的系统之间进行通信的网络协议。

KMIP支持由客户端或服务器进行的加密密钥生成。密钥管理生命周期在KMIP中定义了所有受管加密对象的状态和状态转换。

KMIP定义的密钥管理协议包括以下组件：

a) 传输安全 – 客户端和服务器之间通过相互认证的TLS会话来确保通信的安全性和完整性。支持推荐的TLS版本（即版本1.2）。

b) 请求和响应消息 – KMIP基本上是一个无状态的请求/响应协议，密钥管理客户端发送请求消息到密钥管理服务器，服务器回复响应消息。

c) 认证 – 提供分层认证选项，包括零个或多个凭据（除了基于TLS会话的相互认证）：
— 验证凭据
— 设备凭证（可选密码）
— 用户名和密码

d) 受管对象 – KMIP支持以下类型的受管加密对象：
— 证书
— 私钥
— 公钥
— 机密数据
— 分割密钥
— 对称密钥

e) 操作 – 支持完整密钥管理生命周期的各种操作，包括：
— 激活
— 添加属性
— 存档
— 取消
— 认证
— 检查
— 创建
— 创建密钥对
— 删除属性
— 销毁
— 发现版本
— 获取
— 获取属性列表
— 获取属性
— 获取使用配额
— 定位
— 修改属性
— 通知
— 获得租约
— 轮询
— 放置
— 查询
— 重新认证
— 恢复
— 注册
— 重新加密
— 重新加密密钥对
— 撤销

f) 批量操作 – 每个请求/响应消息可以包含多个操作，在批处理项目中链接，以执行对受管对象进行事务安全系列的密钥管理操作。

g) 属性 – 每个受管对象都有一组相关属性，以提供受管对象的详细信息以支持生命周期管理，包括以下内容：
— 激活日期
— 应用程序特定信息

— 存档日期
— 证书标识符
— 证书颁发者
— 证书长度
— 证书主题
— 证书类型
— 受损日期
— 受损发生日期
— 联系信息
— 密码算法
— 密码域参数
— 密码长度
— 密码参数
— 密码使用掩码
— 自定义属性
— 停用日期
— 销毁日期
— 摘要
— 数字签名算法
— 新鲜
— 初始日期
— 最后更改日期
— 租约时间
— 链接
— 名称
— 对象组
— 对象类型
— 操作策略名称
— 进程开始日期
— 保护停止日期
— 撤销原因
— 状态
— 唯一标识符
— 使用限制
— X.509证书标识符
— X.509证书颁发者
— X.509证书主题

除了主要规范外，KMIP配置文件定义了针对特定

场景（例如在存储环境中创建的保险柜密钥）的功能集。KMIP配置文件还定义了需要使用的认证，以确保消息的保密性和完整性。遵循这些KMIP配置文件是确保KMIP客户端和服务器之间互操作性的主要机制。

参考文献
Bibliography

[1] ISO Guide 73:2009, *Risk management — Vocabulary*

[2] ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[3] ISO 16609:2004, *Banking — Requirements for message authentication using symmetric techniques*

[4] ISO/PAS 22399:2007, *Societal security - Guideline for incident preparedness and operational continuity management*

[5] ISO/IEC 10116:2006, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

[6] ISO/TR 10255:2009, *Document management applications — Optical disk storage technology, management and standards*

[7] ISO/TR 18492:2005, *Long-term preservation of electronic document-based information*

[8] ISO 16175-1:2010, *Information and documentation — Principles and functional requirements for records in electronic office environments — Part 1: Overview and statement of principles*

[9] ISO 16175-2:2011, *Information and documentation — Principles and functional requirements for records in electronic office environments — Part 2: Guidelines and functional requirements for digital records management systems*

[10] ISO 16175-3:2010, *Information and documentation — Principles and functional requirements for records in electronic office environments — Part 3: Guidelines and functional requirements for records in business systems*

[11] ISO/IEC 11770 (all parts), *Information technology — Security techniques — Key management*

[12] ISO/IEC 17826:2012, *Information technology — Cloud Data Management Interface (CDMI)*

[13] ISO/IEC 19790:2006, *Information technology — Security techniques — Security requirements for cryptographic modules*

[14] ISO/IEC 24759:2008, *Information technology — Security techniques — Test requirements for cryptographic modules*

[15] ISO/IEC 24775, *Information technology — Storage management*

[16] ISO/IEC 27003:2010, *Information technology — Security techniques — Information security management system implementation guidance*

[17] ISO/IEC 27031:2011, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[18] ISO/IEC 27033-1:2009, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[19] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[20] ISO/IEC 27033-3:2010, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[21] ISO/IEC 27037:2012, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[22] ISO/IEC/IEEE 24765:2010, *Systems and software engineering — Vocabulary*

[23] IEEE 1619-2007, *IEEE Standard for Wide-Block Encryption for Shared Storage Media*

[24] IEEE 1619.1-2007, *IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices*

[25] IEEE 1619.2-2010, *IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices*

[26] IETF RFC 1813 *NFS Version 3 Protocol Specification*

[27] IETF RFC 3195 *Reliable Delivery for syslog*

[28] IETF RFC 3530 *Network File System (NFS) version 4 Protocol*

[29] IETF RFC 3720 *Internet Small Computer Systems Interface (iSCSI)*

[30] IETF RFC 3723 *Securing Block Storage Protocols over IP*

[31] IETF RFC 3821 *Fibre Channel Over TCP/IP (FCIP)*

[32] IETF RFC 4303 *IP Encapsulating Security Payload (ESP)*

[33] IETF RFC 4595 *Use of IKEv2 in the Fibre Channel Security Association Management Protocol*

[34] IETF RFC 5246 *The Transport Layer Security (TLS) Protocol Version 1.2*

[35] IETF RFC 5424 *The Syslog Protocol*

[36] IETF RFC 5425 *TLS Transport Mapping for Syslog*

[37] IETF RFC 5426 *Transmission of Syslog Messages over UDP*

[38] IETF RFC 5427 *Textual Conventions for Syslog Management*

[39] IETF RFC 5661 *Network File System (NFS) Version 4 Minor Version 1 Protocol*

[40] IETF RFC 5663 *Parallel NFS (pNFS) Block/Volume Layout*

[41] IETF RFC 5848 *Signed Syslog Messages*

[42] IETF RFC 6012 *Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog*

[43] IETF RFC 6071 *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*

[44] IETF RFC 6587 *Transmission of Syslog Messages over TCP*

[45] IETF RFC 7146, *Securing Block Storage Protocols over IP: RFC 3723 Requirements Update for IPsec v3*

[46] ANSI INCITS 400–2004, *Information technology — SCSI Object-based Storage Device Commands (OSD)*

[47] ANSI INCITS 458–2011, *Information technology — SCSI Object-Based Storage Device Commands – 2 (OSD-2)*

[48] ANSI INCITS 461–2010, *Fibre Channel — Switch Fabric — 5 (FC-SW-5)*

[49] ANSI INCITS 462–2010, *Information Technology — Fibre Channel - Backbone — 5 (FC-BB-5)*

[50] ANSI INCITS 463–2010, *Fibre Channel — Generic Services — 6 (FC-GS-6)*

[51] ANSI INCITS 470–2011, *Fibre Channel — Framing and Signaling-3 (FC-FS-3)*

[52] ANSI INCITS 482–2012, *Information Technology — ATA/ATAPI Command Set — 2 (ACS-2)*

[53] ANSI INCITS 496–2012, *Information Technology — Fibre Channel — Security Protocols — 2 (FC-SP-2)*

[54] ANSI INCITS 512–2013, *Information Technology — SCSI Block Commands — 3 (SBC-3)*

[55] NIST FIPS 140–2, *Security Requirements for Cryptographic Modules*

[56] NIST FIPS 197, *Advanced Encryption Standard*

[57] NIST Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*

[58] NIST Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*

[59] NIST Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

[60] NIST Special Publication 800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*

[61] NIST Special Publication 800-57 Part 1, *Recommendation for Key Management: Part 1: General (Revision 3)*

[62] NIST Special Publication 800-57 Part 2, *Recommendation for Key Management: Part 2: Best Practices for Key Management Organization*

[63] NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*

[64] NIST Special Publication 800-88 Revision 1 (draft), *Media Sanitization*

[65] Storage Networking Industry Association (SNIA). *Storage Management Initiative – Specification (SMI-S), Version 1.5, Architecture Book*, http://www.snia.org/tech_activities/standards/curr_standards/smi

[66] Storage Networking Industry Association (SNIA). SNIA Technical Position: *TLS Specification for Storage Systems* v1.0, http://snia.org/tech_activities/standards/curr_standards/tls

[67] Trusted Computing Group, *Storage Architecture Core Specification*, Version 2.0, November 2011

[68] Trusted Computing Group, *Storage Security Subsystem Class: Enterprise*, Version 1.0, January 2011

[69] Trusted Computing Group, *Storage Security Subsystem Class: Opal*, Version 2.0, February 2012

[70] OASIS, *Key Management Interoperability Protocol Specification (*Version 1.2 or later)

[71] OASIS, *Key Management Interoperability Protocol Profiles (*Version 1.2 or later)

[72] Recommendation ITU-T X. 1601 (2013), *Security framework for cloud computing*

[73] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[74] ISO/IEC 14776-372:2011, *Information technology — Small Computer System Interface (SCSI) — Part 372: SCSI Enclosure Services–2 (SES-2)*

[75] ISO/IEC 11179-1:2004, *Information technology — Metadata registries (MDR) — Part 1: Framework*