数据存储安全管理体系技术规范

文件编号：DNI-GZ-JS-68

技术规范编号：CTS DNI-DSC-2026

文档版本：A/0

编制：技术部　　日期：2026.04.28

审核：杨舒　　日期：2026.04.28

批准：杨舒　　日期：2026.04.28

受控状态：受控文件

发布日期：2026年04月28日　　实施日期：2026年04月28日

发布单位：数网信认证服务（北京）有限公同

变更履历

日期	变更描述	版本/版次	审核	批准
2026.04.28	初始发布	A/0	杨舒	杨舒

数据存储安全管理体系技术规范

1 范围

本技术规范适用于所有类型和规模的组织用于规划、设计、记录和实施数据存储安全，本技术规范基于ISO/IEC 27040:2024转换为对数据存储安全提出了信息安全控制要求，是我机构开展数据存储安全管理体系认证的认证依据。

本技术规范特别要求组织已依据GB/T 22080-2025/ISO/IEC27001:2022建立信息安全管理体系并运行，以使达到管理体系的基本特性。

存储安全适用于保护存储在信息和通信技术(ICT)系统中的数据以及在与存储相关的通信链路上传输的数据。存储安全包括设备和介质的安全、与设备和介质相关的管理活动、应用程序和服务，以及在设备和介质的生命周期内以及停用或报废后对用户活动的控制或监控。

存储安全与所有参与数据存储设备、介质和网络的拥有、操作或使用的人员都息息相关。这包括高级管理人员、存储产品和服务的采购人员以及其他非技术管理人员或用户，此外还包括对信息或存储安全、存储操作负有特定责任的管理人员和管理员，以及负责组织整体安全计划和安全策略制定的人员。它也与参与规划的人员息息相关，存储网络安全架构方面的设计和实现。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于 本文件。

GB/T 22080-2025/ISO/IEC 27001:2022 信息安全、网络安全和隐私保护 信息安全管理体系 要求

ISO/IEC 27000 信息技术—安全技术—信息安全管理体系—概述和词汇

ISO/IEC 27002:2022 信息安全 网络安全和隐私保护—信息安全控制

ISO/IEC 27040:2024 信息技术-安全技术-存储安全

3 术语和定义

ISO/IEC 27040:2024中的术语和定义适用。

4 符号和缩写术语

ISO/IEC 27040:2024中的符号和缩写术语适用。

5 本技术规范的结构

5.1概述

本文档的基本结构首先在第6条介绍了存储安全，然后列出了组织控制（第7条）、人员控制（第8条）、物理控制（第9条）和技术控制（第10条），为正文内容。

5.2 控制措施

ISO/IEC 27001和ISO/IEC 27002的控制措施通常适用于存储生态系统以及采购、管理和运行这些生态系统的组织。本技术规范提供了对这些标准的补充要求，故特别要求组织已依据GB/T

22080-2025/ISO/IEC27001:2022建立信息安全管理体系并运行，以使达到管理体系的基本特性。

6 概述和概念

6.1总则

数据存储或信息存储（通常称为存储）是指以持久（即非易失性）形式保存数字数据的系统组件、存储设备和存储介质。虽然存储形式既有易失性形式也有非易失性形式，但本文档主要关注的是非易失性存储。存储是信息通信技术 (ICT) 系统的核心功能和基本组成部分。

为了确保存储基础设施的安全，必须清晰地了解存储技术和概念。此外，了解安全控制的类型以及它们如何影响存储技术并与之交互也至关重要。最后，任何旨在降低存储基础设施或单个存储系统风险的措施，都必须考虑该基础设施面临的威胁以及这些威胁带来的主要风险。

6.2 存储概念

最简单的存储形式可以是连接到信息通信技术(ICT)系统的硬盘驱动器(HDD)、固态驱动器(SSD)或磁带驱动器，用于存储数据。这种方法通常称为直接连接存储(DAS)，目前仍在企业数据中心以及小型办公室/家庭办公室环境中使用。随着网络技术的集成，存储系统和生态系统可以发展成为高度复杂的技术，提供用于管理、连接、保护（即确保安全）、共享和优化数据存储的解决方案。随着存储技术从非智能的内部和外部DAS发展到智能化，这些解决方案变得更加可行且经济高效。智能网络存储。在这些解决方案中使用网络会增加这些解决方案的攻击面，因此需要格外注意以降低相关风险。

现代存储解决方案包含以下部分或全部要素：

—存储设备和介质，由磁性、固态等材料构成，数据可以记录或访问于其上；

—基于块的存储，这是最基本、最根本的持久性数字数据存储形式，它以块序列（每个块由一系列字节或比特组成）的形式排列，并使用偏移量来表示各个数据块的位置；

—基于文件的存储，它将数据组织成文件系统上的文件和目录，同时抽象化底层硬件，以便本地用户访问或通过网络访问，通常以网络附加存储(NAS)的形式实现。NAS可以使多个计算机系统平等地访问存储的内容，而无需考虑它们的操作系统；

—存储接口，包括特定的存储直接连接接口以及存储网络接口；

—对象存储，是一种将数据集存储并随后检索为单个、唯一标识的不可分割项或对象的集合的方法。它适用于任何可以封装并作为对象进行管理的数据形式；

—云计算存储，可作为数据存储即服务(DSaaS)的一部分，如ISO/IEC 22123-1定义，并在ISO/IEC 22123-2中描述。云存储可以包括最基本的文件或原始二进制数据块存储、关系数据库和高级大数据平台，并提供自动备份、灾难恢复、地理冗余、高级故障转移和其他更复杂的功能；

—数据保护系统，用于创建生产数据的一个或多个副本，以便在发生灾难性事件后恢复系统或其数据；

—持久性存储器，是一种密度大于或等于动态随机存取存储器(DRAM)的非易失性存储器，驻留在内存总线上，并以与DRAM几乎相同的速度和延迟访问数据，同时具有NAND闪存的非易失性。

在企业级和中端计算环境中，存储已成为信息通信技术基础设施中一个重要且独立的层。这些环境的需求通常超出简单的数据存储能力。推动新型存储技术出现的应用和功能示例包括：

—通过网络在多个系统之间共享海量存储资源（以PB、EB和YB为单位）；

—需要更高的速度（更低的延迟）；

一增加存储容量；

—扩展存储客户端访问（例如移动设备和物联网）；

—支持分布式ICT架构（例如边缘计算）；

—支持虚拟化环境；

—无需使用局域网(LAN)即可备份数据的数据保护系统；

—关键任务数据的远程、容错、在线镜像；

—将容错应用程序和相关系统围绕单个数据副本进行集群；

—长期保存敏感或高价值的商业信息；

—分布式数据库和文件系统；

一支持遵守监管和法律要求；

一支持集中式数据存储库，以便快速恢复（例如备份）和归档；

—抵御网络攻击。

6.3存储安全简介

存储安全侧重于降低与存储系统和基础设施相关的风险，如6.2和中所述，通过采取安全措施和应对措施（即控制措施）来实现。这些控制措施根据ISO/IEC 27002:2022 4.2 进行分类。

存储安全可能还需要引入专门的控制措施来应对以下技术：

—系统安全加固；

—存储清理；

—虚拟化安全；

—自加密存储设备和数据加密软件；

—密钥管理服务；

—数据真实性和完整性服务；

—传输中数据的保护（加密和数据缩减）；

—目录服务和其他用户管理系统；

一数据保留和保存；

一数据保护和恢复。

了解存储技术的使用方式和原因有助于更好理解存储安全问题及其影响。首先，应考虑以下几点：

—存储系统可以作为存储网络的节点，这些网络可以基于但不限于传输控制协议/互联网协议(TCP/IP)、光纤通道 (FC)、InfiniBand(IB)等技术。潜在威胁会因网络技术及其拓扑结构的不同而显著变化。

一存储时，数据通常以块或文件/对象的形式表示和访问，这两种存储方式之间存在显著差异。同样，相关的安全性也不同。各项措施可能存在根本差异，尤其是在访问控制、加密和数据完整性方面。

—作为正常存储操作的一部分，许多存储设备类型的内部介质容量都大于通过接口暴露的容量。

固态硬盘 (SSD) 通常会进行介质超配，允许数据在物理介质区域之间内部移动，以改善写入延迟并均匀分配写入活动。机械硬盘 (HDD) 通常包含备用区域，当出现访问问题时，数据可以在这些备用区域中在物理介质区域之间内部移动。即使通过接口对设备进行后续写入，用户数据仍可能保留在超配区域或备用区域中。此类数据无法通过接口覆盖写入来清除。

—存储管理既是存储基础架构的一个组成部分，也是对该基础架构执行的操作。通常，该基础架构允许特权用户应用配置更改、配置存储、调优、监控等。某些管理操作可以远程执行，并且可能涉及第三方，例如供应商支持人员。

—数据可用性和完整性是组织存储架构的关键因素，因此，安全措施必须与高可用性措施相辅相成，而不是相互冲突，并且不能通过引入瓶颈和单点故障来抵消高可用性措施的效果。

—许多组织实施了复杂的数据弹性策略,这些策略是其业务连续性管理(BCM)计划不可或缺的一部分。如果实施不当，诸如静态数据加密之类的安全机制可能会对这些弹性策略产生负面影响。

—存储虚拟化可以采用多种形式，并在存储基础架构的不同位置实施。这种虚拟化可以掩盖与存储呈现相关的物理细节（例如，向服务器呈现的逻辑单元（见下文注释）或文件系统），掩盖设备的真实容量，执行策略驱动的自主数据移动（即分层存储），或完全抽象存储基础架构（即云计算存储）。平衡安全措施和虚拟化以确保它们能够互操作，需要仔细规划并选择合适的技术。

注释：在计算机存储中，逻辑单元是由SCSI协议或封装SCSI的协议（例如光纤通道或iSCSI）寻址的设备。逻辑单元号(LUN)是用于标识逻辑单元的编号。LUN可用于任何支持读/写操作的设备，例如磁带驱动器，但最常用于指代在SAN上创建的逻辑存储。虽然技术上并不完全准确，但术语LUN也经常被使用。指逻辑存储本身。

一某些组织的数据增长率正在推动数据存储技术的使用量增加。作为获取额外存储空间的替代方案，组织正在采用压缩和去重等数据缩减技术。然而，这些数据缩减技术可能会受到数据保留加密机制的影响，进而可能在业务连续性管理 (BCM) 操作期间引入数据完整性问题。

—数据保护策略的副产品可能包括数据副本，例如在系统和站点之间复制数据（参见10.14.3）、备份（参见10.14.2）和快照（参见10.14.4）。此类数据副本和残留数据与原始数据具有相同的敏感性考虑。

—敏感和高价值数据通常在系统之间和系统内部传输（例如，动态数据），增加了数据保护的考虑（参见10.5.4）。

一许多组织正在实施静态数据加密（参见10.5.5）以保护敏感和高价值数据。具体的加密机制和加密时机是实际数据保护以及满足合规性要求的重要因素。

-加密的成功使用通常取决于密钥材料在其整个生命周期中的正确管理（参见10.5.2）。这包括正确生成密钥、安全存储和传输密钥材料、作为确保数据可用性的常规策略的一部分复制密钥，以及在不再需要密钥材料时对其进行妥善处置。待保护数据的敏感性和重要性也会影响密钥管理方法。

确保存储在当前和新兴存储技术上以及访问的数据具有足够的机密性、完整性和可用性，需要在信息通信技术(ICT)的这一层面上做出共同努力。许多此类安全措施侧重于：

一保护存储管理（操作和接口）；

一确保充分的凭证和信任管理；

一保护数据备份和恢复资源；

一传输中数据保护；

一静态数据保护；

一数据可用性保护；

一BCM支持；

—对存储介质进行适当的清理和处置；

一安全的自主数据传输；

—安全的多租户。

6.4 存储安全风险

6.4.1背景

存储安全风险是由组织使用特定存储系统或基础设施而产生的。存储安全风险源于：

—针对存储系统和基础设施所处理数据的威胁；

一漏洞（包括技术漏洞和非技术漏洞）；

—威胁成功利用漏洞的可能性；

—威胁成功利用漏洞的影响。

风险管理是信息安全的关键概念。ISO/IEC 27005中提出的信息安全风险管理流程包括：建立环境、风险评估、风险处理、风险接受、风险沟通、以及风险监控和审查。

存储系统和基础设施面临的威胁可能包括：

—未经授权使用存储资源；

—未经授权的访问；

—因违反监管规定而承担的责任；

—对存储或网络的拒绝服务(DoS)和分布式拒绝服务(DDoS)攻击；

一数据损坏/修改和销毁，包括备份或恢复副本；

一未经授权的披露，可能构成数据泄露；

一存储介质被盗或意外丢失；

一恶意软件攻击或恶意代码植入（例如勒索软件）；

—使用完毕后未进行适当的清理或处置。

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而言；主要担忧包括数据泄露、数据损坏或销毁、暂时或永久性丧失访问权限/可用性以及未能满足法定、监管或法律要求所带来的风险。

6.4.2数据泄露

本文档将数据泄露定义为安全漏洞，导致受保护的传输、存储或以其他方式处理的数据遭到意外或非法销毁、丢失、更改、未经授权的披露或访问。此定义远超那些侧重于未经授权访问或披露特定类型数据的简单数据泄露定义。

根据所涉数据的数量和类型以及适用的法律法规，数据泄露可能使组织面临重大风险，这些风险包括调查数据泄露的成本、向受影响个人发出必要通知的成本、诉讼费用、监管罚款和其他法律处罚，以及公众舆论造成的品牌损害。披露数据泄露事件。

丢失自身或其他方的受保护信息会给实体带来经济和安全风险。此类信息可能包括：

—知识产权或其他敏感商业信息；

—个人身份信息 (PII)；

—财务账户或记录信息；

—个人身份识别健康记录信息。

寻求此类信息的不受信任或未经授权的实体可能资金雄厚，且动机各异。

表1总结了可能存在的基于存储的安全威胁，并列出了这些安全漏洞可能导致的数据泄露形式。

表1——面向存储的数据泄露

安全威胁	潜在的数据泄露形式
存储设备或存储介质被盗或丢失	非法或未经授权的披露、数据丢失或数据销毁
意外的配置更改（例如，存储管理、存储/网络资源和不正确的补丁管理）由授权人员执行	意外访问、意外泄露、意外数据销毁、意外数据更改或移除/拒绝访问
外部或内部攻击者恶意更改配置（存储管理、存储/网络资源和应用程序篡改）	非法访问、非法泄露、非法数据销毁、非法数据更改
授权用户滥用特权（例如，不当的数据窥探）	非法/未经授权的访问或泄露
外部或内部攻击者恶意篡改数据	非法数据销毁或更改
拒绝服务攻击	合法用户失去访问权限和系统不可用存储和数据
恶意监控网络流量	非法/未经授权的披露

6.4.3 数据损坏或销毁

数据损坏是指由于用户、硬件或软件错误导致的数据劣化或损坏（即对原始数据的非预期更改）。它可能发生在写入、读取、保留、传输或处理过程中。及早发现数据损坏可能在适当条件下恢复数据或元数据。如果未被发现或纠正，且根本原因持续存在，则数据损坏可能导致永久性数据丢失。另一方面，数据销毁会导致数据丢失，如果未采用备份等数据保护机制，则数据丢失可能是永久性的。数据损坏和数据销毁可能是意外事件或故意事件的结果，在后一种情况下，它们可能是进一步分为恶意和非恶意。

火灾、洪水、停电和用户操作失误等事件都是造成数据损坏和丢失的常见、非故意原因。背景辐射、硬盘磁头碰撞以及存储介质的老化或磨损是其他更偏向存储本身的问题来源。存储设备或存储介质故障导致的数据损坏通常可以通过校验和检测，并且通常可以使用纠错码进行纠正，但如果存储管理不当，这些静默纠正可能会导致其他问题（例如，随着存储设备或介质的劣化，暂时可纠正的错误可能会变成永久性错误）。

恶意攻击可能由外部人员或内部人员发起，目的是使部分或全部受影响的数据无法使用或被销毁。在此上下文中，“无法使用”可能意味着数据已被未经授权的修改、怀疑数据已被修改，或者数据可能使用未知密钥或机制加密（或者最初用于加密数据的密钥可能已被销毁）。非恶意事件通常是由于粗心大意、缺乏知识或出于完成工作等原因而故意规避安全措施造成的。然而，非恶意事件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维护数据完整性的重要方法。同样，检测数据丢失并使用数据保护机制恢复数据可以防止数据丢失。

6.4.4暂时或永久性访问/可用性丧失

可用性是指确保授权用户和系统在指定时间范围内以所需的性能水平访问数据。即使是暂时的访问中断，也可能对组织造成重大损害。此外，访问性能下降（例如，未达到最低性能阈值）同样会对组织造成损害。

访问中断或可用性丧失可能是由于存储设备、存储网络元件、存储数据、数据流、服务和应用程序的故障或问题，以及攻击造成的。通常，数据可用性是通过冗余来实现的。

6.4.5未能满足法定、监管或法律要求

组织若不遵守法规、条例或法律要求，可能承担重大责任并受到处罚。对于跨国组织而言，各国的具体法律法规对信息安全要求有着重要影响。

常见的合规问题包括：

—违反特定国家/地区的隐私要求；

—非法传输数据（例如，将受限数据移出特定司法管辖区）；

—违反保密义务；

—不符合组织政策（例如，数据清理）；

—数据保留和保护不足；

—安全证据不足（例如，审计日志和加密/清理证明）。

这些不合规问题可能导致代价高昂的制裁和补救措施（例如，违规通知）。

7 存储的组织控制

7.1总则

用户按照ISO/IEC 27002:2022第5条中列出的详尽的组织控制。其中一些或全部控制与存储系统和存储相关生态系统。

7.2 协调存储和策略

策略的存在与否在确保安全性和合规性方面起着至关重要的作用。

以下策略指南和要求适用。

a) OC-PLCY-G01 将存储纳入策略，应将存储纳入策略，以便：

—识别最敏感（个人身份信息、知识产权、商业秘密等）和业务/任务关键型数据类别以及保护要求；

—将特定于存储的策略与其他策略集成（即，避免为存储生态系统创建单独的策略文档）；

—处理数据保留和保护（例如，WORM、真实性和访问控制）；

—处理数据销毁和存储介质清理。

b)OC-PLCY-G02 确保存储符合策略，符合策略应：

—确保存储生态系统的所有元素均符合策略（例如，ISO/IEC 27001:2022 5.2 和 ISO/IEC 27002:2022 5.1）；

一优先处理最敏感/最关键的数据。

c) OC-PLCY-R01 将存储纳入日志策略，将存储纳入日志策略，使日志策略应：

—明确规定存储系统和设备参与审计日志记录；

—识别需要收集的重要存储相关事件；

—识别存储相关事件日志的保存要求；

—识别存储相关事件日志的保留和归档要求；

一指定存储相关事件日志的时间同步和使用要求；

—包括证据要求（真实性、监管链等）。

7.3 业务连续性管理

ISO 22301规定了实施和维护业务连续性管理体系的结构和要求，该体系旨在根据组织在中断后所承受的影响程度和类型，制定相应的业务连续性计划。ISO 22301中规定的要求是通用的，旨在适用于所有组织或其任何部分，无论组织的类型、规模和性质如何。这些要求的适用范围取决于组织的运营环境和复杂性。ISO 22301中规定的要求涵盖组织环境、领导力、规划、支持、运营、绩效评估和改进等方面。

ISO/IEC 27002:2022 5.30强调了信息通信技术(ICT)业务连续性准备(IRBC)的重要性，以确保组织的信息和其他相关资产在中断期间的可用性。ISO/IEC 27031描述了IRBC的概念和原则。它还提供了一个方法和流程框架，用于识别和明确所有方面（例如性能标准、设计和实施），以提高组织的信息通信技术准备度，从而确保业务连续性。该框架适用于任何正在制定信息通信技术业务连续性准备计划的组织（无论规模大小，包括私营、政府和非政府组织），并要求其信息通信技术服务/基础设施做好准备，以便在发生中断时支持业务运营。新兴事件和事故以及可能影响关键业务功能连续性（包括安全性）的相关中断。它还使组织能够以一致且公认的方式衡量与其内部风险连续性(IRBC)相关的绩效参数。

存储通常是组织内部风险连续性计划或非正式业务连续性管理(BCM)活动的关键要素。与BCM相关的控制措施如下：

a) OC-IRBC-G01将存储生态系统纳入BCM规划和实施

组织应确保将存储生态系统纳入BCM规划和实施。

b) OC-IRBC-G02为有限中断事件做好准备

组织应为有限中断事件（系统故障、对抗性攻击、操作员错误）做好准备。

c) OC-IRBC-G03识别并记录独特的人员配备和设施要求

各组织应识别并记录与存储生态系统相关的独特人员配备和设施需求。

d) OC-IRBC-G04持续进行业务连续性管理(BCM)的规划和测试

各组织应持续进行业务连续性管理(BCM)的规划和定期测试，这对成功的BCM至关重要。BCM测试结果应反馈到BCM计划的持续维护中。

7.4 合规性

遵守法律法规要求的重要性是许多组织安全议程和战略的重要组成部分。以下要素是信息系统(IS) 审计员关注的存储系统和基础设施的关键合规性方面。

与合规性相关的控制措施如下：

a) OC-CPLC-R01确保存储满足用户责任义务

通过确保以下事项来确保满足用户责任义务：

一用户，尤其是特权用户，应拥有唯一的用户ID（即，不得共享帐户）；

一应根据用户的职责（例如角色）并遵循最小权限原则（即，仅授予用户执行其功能所需的最低系统资源和授权）明确授予用户的权利和特权；

一所有尝试的（成功和失败的）管理事件和事务都应被记录。

b)OC-CPLC-G01确保存储满足用户可追溯性义务 确保存储满足用户可追溯性义务，具体如下：

- 已记录的事件/事务数据应包含足够的应用程序或系统详细信息，以便清晰地识别来源；

一用户信息应可追溯到特定个人；

一在适当情况下，日志记录应作为证据（监管链、不可否认性、真实性等）。

c) OC-CPLC-G02确保存储满足用户监控义务 确保存储满足用户监控义务，具体如下：

—存储层应参与外部审计日志记录措施；

一应监控审计日志记录事件，并在适当情况下发出警报。

d)OC-CPLC-G03确保存储满足数据保留和清理义务确保存储满足数据保留和清理义务，以便：

—应实施适当的数据保留措施；

—应实施适当的数据完整性和真实性措施；

— 在硬件重新利用或停用之前，应实施正确的数据清理；

—应在虚拟服务器映像及其副本的生命周期结束时，实施正确的数据清理。

e) OC-CPLC-G04确保存储符合隐私义务

确保存储符合隐私义务（参见 ISO/IEC 27701），具体如下：

—应实施基于最小权限原则的适当数据访问控制，以控制对数据和元数据（例如搜索结果）的访问；

一应实施适当的数据保密措施，以防止未经授权的披露。

f) OC-CPLC-G05考虑法律义务的存储 法律义务可能适用于存储，具体如下：

—使用数据去重不应与数据真实性要求相冲突；

一数据和存储介质清理机制的使用不应违反保存要求；

一处理证据数据（例如审计日志、元数据、镜像和时间点副本）时，应遵循正确的监管链程序。

8 存储人员控制措施

用户按照ISO/IEC 27002:2022 第 6 条中列出的详尽的人员控制措施。其中部分或全部控制措施与存储系统和存储生态系统相关。

ISO/IEC 27002:2022 第6.3条规定，组织应识别、制定并实施适当的培训计划，以培训那些需要特定技能和专业知识的技术团队。对于负责存储安全各个方面的人员，其技能和专业知识可能高度专业化，正如本文档所示。

与专业知识相关的控制措施如下：

a) SC-XPTS-G01确保具备足够的存储保护专业知识

存储团队和管理人员应了解与基于存储的数据保护技术相关的技术和实践（参见10.14）。此外，这种理解还应包括数据保护在组织中的适用性。

b) SC-XPTS-G02确保具备足够的存储安全专业知识

存储团队和管理人员应了解用于保护存储设备、系统和生态系统的技术和实践，以及如何利用基于存储的安全控制措施。

9 存储的物理控制措施

9.1 总则

用户按照ISO/IEC 27002:2022第7条中列出的广泛的物理控制措施。其中一些或全部控制措施与存储系统和存储生态系统相关。

9.2 物理安全存储

存储系统和生态系统特别容易受到物理威胁。除非在不使用或无人看管时进行保护，否则它们可能会遭受盗窃、破坏和未经授权的访问。存储介质、设备和系统的大小差异很大，因此保护它们的方法也可能有所不同。

与物理保护存储相关的控制措施如下：

a) PC-PHYS-G01物理保护存储介质

所有存储有记录数据的存储介质都应根据其信息分类，存放在安全可靠的环境中，并按照制造商的规范，保护其免受环境威胁（例如高温、潮湿、电磁场或老化）。

b) PC-PHYS-G02物理保护存储设备

根据存储设备的大小和位置，应采取物理保护措施：

一办公环境中的小型存储单元可以固定在家具或墙壁上，不用时也可以存放在上锁的柜子或保险箱中；或者大型存储单元可以安装在机架上，并放置在实验室或数据中心，从而受益于设施的安全措施（例如，上锁的盖板或笼子）。

9.3 保护存储的物理接口

保护管理接口免受未经授权的访问和侦察至关重要。由于未能实施适当的控制措施而导致的对管理接口的未经授权访问，可能导致数据销毁、损坏或拒绝访问。

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、局域网、调制解调器，甚至数据路径所使用的技术（例如光纤通道）。混合接口（例如插入控制台集中器的串行端口，该集中器提供局域网接口）也相对常见。

保护物理存储接口的相关控制措施如下：

PC-PHYS-R01保护物理接口，为保护这些物理接口，组织应：

—限制对管理接口的物理访问；

—不使用时禁用并断开串行管理端口；

— 将用于管理的LAN接口与其他LAN流量隔离，注意物理隔离是首选，但逻辑隔离（例如VLAN）被认为是最佳实践；

—不需要时禁用调制解调器端口。

9.4 存储系统的隔离

存储设备的物理隔离和逻辑隔离（例如，在SAN内部）也发挥着重要作用。与存储隔离相关的控制措施如下：

a) PC-PHYS-G03物理隔离存储系统，物理隔离应用于：

- 将生产系统与其他系统类别（例如，质量保证、开发）隔离，包括：

一尽可能避免不同类别之间的网络连接（例如，生产服务器连接到（包括生产网络和开发网络）。

—在适当情况下按类别隔离网络和存储；

—将每个类别中的系统进行物理隔离；

—如果可行，将存储设备与其他数据中心设备隔离。

b) PC-PHYS-G04存储系统的逻辑隔离，逻辑隔离应用于：

—使用以下方法将存储流量与正常服务器流量隔离：

—使用可用的网络控制在公共物理基础架构上创建独立的逻辑域；

—使用信任和访问控制来管理逻辑域的成员资格；

一将存储管理流量与其他所有流量隔离；

—配置网络网关以实现适当的网络隔离。

10 存储技术控制

10.1 总则

用户按照ISO/IEC 27002:2022第8条中列出的详尽的物理控制措施。其中一些或全部控制措施与存储系统和存储生态系统相关。

10.2 存储安全的设计与实施

10.2.1 总则

随着关键数据量的爆炸式增长，许多组织在其ICT基础设施中采用了以存储为中心的架构。因此，存储安全在保护这些数据方面发挥着重要作用，并且在许多情况下，它是最后一道防线。存储安全的有效性通常受设计因素的影响。

与存储设计和实施相关的控制措施如下：如下：

a)TC-DSGN-G01 遵循核心安全设计原则

设计和实施存储安全解决方案需要遵循核心安全设计原则。此外，应将第 7、8和9条中描述的控制措施和指南整合到存储安全解决方案的设计和实施中，以应对适用的威胁。数据敏感性、关键性和

价值也是设计中需要考虑的重要因素（参见10.2.2）

b) TC-DSGN-G02 在设计中考虑相关威胁

存储安全架构的常见风险领域包括：由于设计缺陷、缺乏对业务连续性管理计划的适当考虑，或与当前或预期威胁级别不符而导致的设计缺陷。设计应考虑存储系统中所有相关的威胁和漏洞，如6.4 节所述。

有关评估安全风险和相关威胁的信息，也可参阅 ISO/IEC 27001、ISO/IEC 27002 和 ISO/IEC 27005。

10.2.2 存储安全设计原则

10.2.2.1纵深防御

越来越多的组织开始采用一种覆盖所有应用程序、系统、网络、存储和设备的全面分层方法来考虑安全性。采用这种分层方法被认为是纵深防御，尤其是在结合以下因素时：策略、设计、管理和技术。每个组织采取纵深防御的程度各不相同，取决于数据价值和敏感性、合规性要求、对手能力和活动等因素。

纵深防御的一个重要原则是利用多种安全控制或安全技术来帮助降低防御体系中某个组件被攻破或绕过的风险。例如，在同一环境中，如果防火墙和服务器上已经安装了病毒防护软件，则在各个工作站上安装防病毒软件也是一种纵深防御。

与纵深防御相关的控制措施如下：

TC-DSGN-G03 部署纵深防御，存储系统和解决方案应：

—确保平衡关注三个主要要素：人员、技术和运营；

—遵循有效的信息保障政策和程序、角色分配和

责任、资源承诺、关键人员培训以及个人责任；

—在多个地点部署保护机制，抵御多种类型的攻击；

—在潜在对手和目标之间部署多层防御机制；

一包括侦查机制和保护机制；

—利用集中管理和监控的稳健（例如支持许多用例和容量）和高度抗攻击（例如零信任架构）安全基础设施（例如密钥管理、公钥基础设施和身份管理）；

—维护可见且最新的系统安全策略；

—主动管理存储技术和保护机制的安全态势（例如安装安全补丁、防病毒更新和维护ACL）；

—定期进行安全威胁评估，以评估安全准备情况；

—监控当前威胁并做出反应。

对于存储而言，多层防御机制意味着在整个存储基础设施中部署和使用安全控制，包括主机中的融合网络适配器（CNA）、存储网络交换机/路由器、存储设备和存储设备。

注：CNA是单一网络接口设备，提供FC主机总线适配器(HBA)和TCP/IP以太网网络接口卡的功能。

10.2.2.2安全域

安全域基于这样的概念：将不同敏感级别（即不同的风险容忍值和威胁易感性）的系统资源进行

隔离。这确保了系统仅提供执行特定域任务所需的数据。作为一项设计原则，该架构强制执行域隔离，以确保一个实体有权访问的资源不会受到其他域的访问或影响。

对于存储基础设施，安全域通常表示为SAN，尤其是在存储系统中存储和处理敏感数据时。在数据敏感性较低的情况下，使用分区和VLAN是可以接受的，但需要注意的是，这种通用功能并非安全机制，例如 FC-SP-2 分区]

基于ISO/IEC 27033-2中描述的隔离原则，以下存储安全设计建议适用：

a) TC-DSGN-G04 将数据敏感性纳入考虑安全域设计

数据敏感性应纳入安全域设计考量，具体如下：

-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（例如互联网）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（非军事区）；

—战略资产应位于专用安全域；

—不受信任的设备和计算机系统应限制或禁止访问存储资产。

b) TC-DSGN-G05 将用途纳入安全域设计

用途应纳入安全域设计考量，具体如下：

一用于不同用途（例如开发、生产和管理）且采用不同技术（例如 SMB、NFS、iSCSI和CDMI）的存储和存储网络应位于不同的安全域中；

一存储网络应与使用相同技术的常规网络位于不同的安全域中（例如，承载iSCSI 流量的IP网络应与普通的企业LAN隔离）；

一 存储设备和存储网络管理系统应位于专用的安全域中；

—开发系统应与生产系统位于不同的域中。

c) TC-DSGN-G06 在安全域内进一步隔离

允许驻留在单个安全域内，但用于多种用途或存储多层敏感数据的存储设备，应进一步隔离，以最大程度地减少可能的交互。

10.2.2.3设计弹性

与设计弹性相关的控制措施如下：

TC-DSGN-G07 在设计中纳入弹性

存储安全设计应包含多层冗余，以消除单点故障并最大限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，设计还应采用广泛的冗余机制。旨在增强存储系统抵御攻击和网络故障能力的一系列方法。

10.2.2.4安全初始化

与安全初始化相关的控制措施如下：

TC-DSGN-G08 支持安全初始化序列

作为设计原则，该体系结构应在从停机状态到运行状态的转换期间（例如，上电或重置后）支持安全初始化序列。在初始化阶段，外部可访问的进程和网络接口应被拒绝访问或在主体经过身份验证

之前不可用。软件和操作系统加载进程应从系统上次运行时系统管理员指定的安全值的已知状态开始。

10.2.3 存储系统质量属性

10.2.3.1可靠性

ISO/IEC 27000 将可靠性定义为一致的预期行为和结果的属性。对于存储，可靠性通常被认为是设备在规定条件下、特定时间段内执行其所需功能的概率，并量化为：

—MTBF（平均故障间隔时间）对于可修复产品来说，是系统或组件中连续故障之间的预期时间，有时被认为是系统或组件在故障之间执行正常操作的平均可用时间（参见图1）；

—MTTR（平均修复时间）对于可修复产品来说，是指使故障系统或组件恢复正常运行的预期或观察到的持续时间，有时被认为是修复故障组件的平均时间；

—MTTF（平均故障时间）对于不可修复的产品，这是的平均可用时间

系统或组件执行其正常操作，直到发生故障。

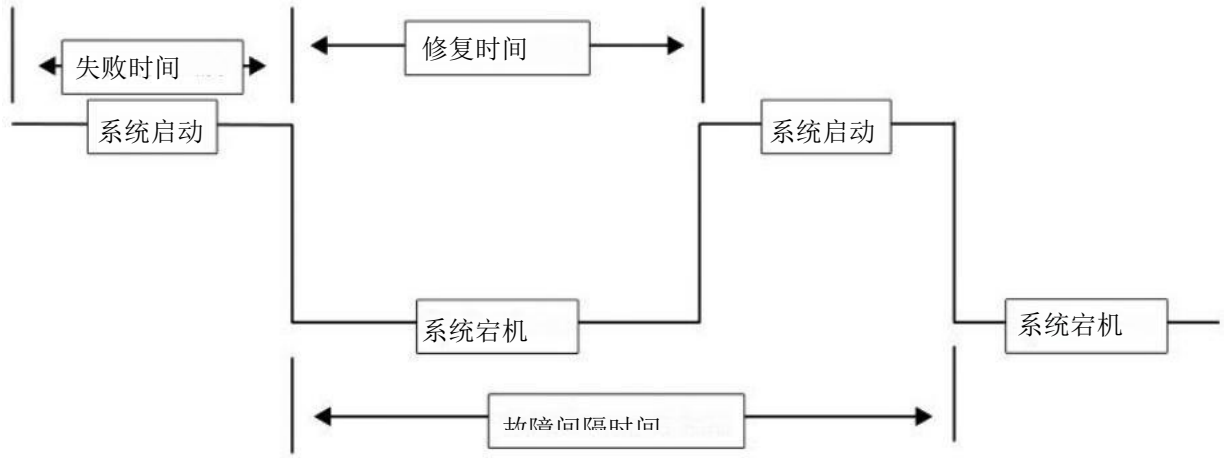

图 1——可靠性量化

在存储领域，系统受损和攻击（例如 DDoS 攻击）会对平均故障间隔时间 (MTBF)、平均修复时间 (MTTR)（例如，MTTR 也可能涉及攻击后的恢复操作）和平均故障间隔时间 (MTTF) 产生负面影响。此外，安全功能的引入、系统或应用程序补丁的应用，或其他系统加固措施（例如10.3.1中所述的措施）也会产生影响。例如，错误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利影响。

与可靠性相关的控制措施如下：

TC-DSGN-G09 最大程度地减少对存储可靠性的影响

具体的可靠性指导包括：

一存储系统和基础设施的可靠性不应因安全功能的加入而受到不利影响；

一应主动管理存储漏洞，以最大限度地减少其对系统可靠性的影响；

一应评估各项控制措施，以确定它们是否能够确保数据的可靠性和安全性。

10.2.3.2可用性

在存储领域，数据可用性通常指的是数据以某种形式存储时的可访问性，通常是指通过网络或外部存储介质进行远程存储的数据。该术语通常用于指代几个不同的概念，主要包括授权用户访问数据的可靠性（以正常运行时间为衡量标准）以及访问数据的速度。

可用性是指在满足特定性能保证（例如，检索信息所需时间不超过 5 毫秒）的前提下，授权用户能够访问某项内容的时间比例。例如，假设一个存储阵列每周 7 天、每天 24 小时运行，且一年内停机时间约为 5 分钟，则其可用性为 0.99999（99.999%）。

为了实现数据的高可用性，现代存储系统及其基础设施中都实施了大量的硬件和软件冗余（例如，自动输入/输出路径故障转移、冗余组件、全局热备件和带电池备份的镜像数据缓存）。此外，通常还会使用数据冗余机制（例如镜像和复制）以及数据保护机制（例如备份）来确保在发生故障时能够快速恢复数据。

与可用性相关的控制措施如下：如下：

TC-DSGN-G10 最大限度减少对数据可用性的影响

由于可用性至关重要，应最大限度减少以下原因对数据可用性的影响：

—存储安全设计和实施不足（例如，最大限度减少单点故障）；

—数据加密密钥管理不足，当密钥在需要时不可用或被意外销毁时，可能导致问题；

—数据恢复机制不足，无法防止重大数据丢失或存储中断。

10.2.3.3弹性

弹性是指在面对故障（系统故障）和正常操作挑战（例如攻击、事故或大规模自然灾害）时提供和维持可接受水平的服务的能力，通常与保持数据完整性和可用性相关。这种能力通常是存储系统和基础设施部署中的重要考虑因素，因为它会影响数据的整体可用性。

在考虑弹性时，如果服务仍在交付并且该服务的完整性仍然存在，则单个组件的故障是可以接受的。但是，存储系统或存储基础设施的弹性通常由系统中弹性最差的组件决定，并且成本/性能或其他因素可能会限制弹性可能或实用的程度。

与弹性相关的控制如下：

TC-DSGN-G11 尽量减少对存储弹性的影响 应尽量减少对弹性的影响，因为：

—未能将安全性作为弹性策略的一个组成部分，该策略解释了存储和安全技术的单元故障、攻击和妥协；

——冗余存储组件不足；

——未充分使用易于维修的各种组件；

——安全特性和功能的不恰当实现（例如加密和集中化）

身份验证），这降低了存储系统及其基础设施的整体弹性。

10.2.3.4完整性

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，其重要性仅次于数据可用性，对存储人员而言至关重要。存储在存储设备上或响应存储请求而通过网络传输的数据可能因硬件或软件故障

而损坏。硬件故障也可能引发软件异常行为，从而导致存储数据严重受损。软件中的错误，例如设备驱动程序中的错误，也可能导致数据意外修改。不可靠的网络可能会损坏通过网络传输的数据。

此外，重要信息可能被恶意程序、恶意用户或故障的系统组件篡改。例如，病毒代码可能被插入二进制可执行文件中，从而导致系统上存储的所有数据丢失。允许访问原始磁盘的操作系统可能会无意中帮助攻击者绕过文件系统中的安全检查，从而损坏存储的数据。

用户错误可能会在应用程序级别损害数据完整性。例如，意外删除关键数据。文件（例如数据库模式文件）损坏可能导致数据损坏。

与完整性相关的控制措施如下：

TC-DSGN-G12 最大程度减少对数据完整性的影响

为解决数据完整性问题，组织应采用常见的完整性保证技术，包括数据复制或镜像、RAID 奇偶校验或校验和。还应使用能够执行预防措施以避免特定类型完整性违规（例如只读存储和日志文件系统）或在检测到问题后能够从损坏中恢复的完整性保证机制。

10.2.4 数据的保留、保存和处置

保留是指根据记录要求保存记录，以作为业务功能、活动或交易的证据，并用于记录流程，包括记录的保存方式和保存期限。另一方面，保存是指采取措施维护记录的可用性、真实性、可靠性和完整性。术语“保留”和“保存”经常被互换使用，导致对同一信息的维护方式、保存期限以及是否以及如何保护和安全等方面存在不同的、相互冲突的记录要求。

与数据保留、保存和处置相关的控制措施如下：

a) TC-DSGN-G13 确保数据保留和保存

负有数据保留和保存义务的组织应以阻止记录销毁或更改（即不可更改）的方式存储数据，并进行完整性验证（例如哈希）和强制执行。明确的保留期限（例如法律保留期限）。为了满足不可篡改性（不可编辑）要求，组织应使用基于一次写入多次读取(WORM)的存储或基于对象的存储（参见10.12）实现，这些实现将 WORM 与可用于执行显式完整性检查以及强制执行数据过期的元数据相结合。

b)TC-DSGN-G14 确保妥善处置数据

在常见的记录和信息管理框架中（参见下文注释 1），处置是记录生命周期的最后阶段。在这些框架中，处置并不一定意味着销毁记录，而是转移到档案馆（参见10.15）。在后一种情况下，这可以简单地延迟大多数记录的销毁时间（政府以外的记录应尽量减少保留）。

无限期地）。当不再需要记录（数据）时，数据销毁就成为有效数据治理计划中至关重要且通常必不可少的组成部分。组织应采用数据销毁流程，以某种方式删除信息，使纸质记录无法读取，或使数字记录无法恢复（参见下文注2）。在后一种情况下，通常会使用存储清理技术（参见10.6）。

注1：ISO 15489-1 是用于规划和实施记录管理计划的众多框架之一。

注2：在数字世界中，使数据无法恢复需要付出一定的努力检索它。

10.3 存储系统安全

10.3.1 系统加固

所有操作系统、虚拟机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。除了 ISO/IEC

27002:2022 8.8 中的技术漏洞管理指南外，还有许多针对各种操作系统的现有最佳实践可供参考。

在存储系统中，操作系统存在于多种类型的设备中[例如，存储阵列、SAN 交换机、虚拟化设备、备份和归档设备]。其他底层设备（例如，主机总线适配器、存储控制器、网络适配器）也需要定期进行软件和固件更新。某些存储操作系统安全功能默认情况下未启用，例行维护和更新可能会重置存储系统先前执行的加固操作。

管理员与系统加固相关的控制措施如下：

a) TC-HARD-G01 执行基本操作系统加固

作为存储系统安全卫生的一部分，组织应：—移除不需要/未使用的软件、服务和协议；

—移除不必要的帐户；

—尽可能重命名或禁用预定义或默认帐户，并更改所有默认密码；

—仅打开所需的网络端口；

—从可信来源安装最新补丁；

—从可信来源更新固件；

—安装并维护恶意软件防护（参见 ISO/IEC 27002:2022,8.7）；

—应用供应商推荐的安全配置。

b) TC-HARD-G02 使用来自可信来源的软件更新和补丁

当存储基础架构的组件收到更新（例如固件）或补丁时，应确保所应用的软件来自可信来源。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、僵尸网络或其他恶意软件。

10.3.2 S安全审计、统计和监控

合规性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记账是满足这些要求的关键功能。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，因为它既可以实时使用，也可以作为事件调查的一部分。

在存储系统和基础设施中，各种各样的事务或事件都可能导致生成事件日志条目（消息），这些条目可以通过某种事件日志记录方式进行记录。从安全或合规性的角度来看，捕获那些对于证明操作（例如加密和保留）、强制执行问责制和可追溯性、满足证据要求以及对系统进行充分监控至关重要的事件日志条目。这部分通用事件日志通常被称为审计日志。

并非所有事件日志条目都具有相同的价值，有些条目仅用于调试、提供系统运行状况、警告轻微的配置问题等。从审计日志的角度来看，管理事件（即用户执行的操作）始终是重要的，数据访问事件通常意义有限（除非关键文件和目录受到严密监控），而控制事件通常最不重要（尽管它们可以在事件发生后的根本原因分析期间提供有用的信息）。

此外，审计日志记录通常要求对感兴趣的事件条目进行区别对待，并将其与设备生成的大多数其他事件日志条目分开处理。这种特殊处理可以通过让设备将审计日志条目发送到专用日志基础设施来实现，也可以使用日志过滤机制从通用日志流中筛选出来（这种方法更具挑战性，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，组织通常需要证明其正在进行监控（例

如，针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式日志基础设施，而不仅仅是简单的收集器。

以下安全审计、统计和监控要求及指南适用于存储系统：

a) TC-HARD-R01 对存储执行日志记录 对存储执行日志记录，以便：

—应尽可能在存储系统和设备上启用日志记录；

一存储系统和设备应使用外部或集中式事件日志记录，并可使用本地日志记录；

- 整个环境中应使用通用、准确的时间源，以确保来自不同来源的事件记录可以关联；

- 存储系统和设备应尽可能使用支持可靠交付和安全传输（例如 TLS）的标准日志记录协议（例如 syslog）原生记录事件；

注1：Syslog 在 IETF RFC 5424[47] 中定义，更多细节包含在 IETF RFC 3195[41] IETF RFC中。5425,48]IETF RFC 5426,49 IETF RFC5427,50]IETF RFC 5848,51 ETF RFC6012,5Z1 和 IETF RFC 6587.54]

—外部或集中式事件日志记录应与可信的远程源一起使用；

注 2：可信的外部事件日志源是指位于专用安全区域或域中的 ICT 安全管理产品，并假定其能够正确执行安全功能。

一应避免将设备日志用于系统健康监控和调试以外的任何用途，因为设备驻留日志更容易被篡改或销毁，日志存储空间有限，并且会妨碍集中式自动化分析、警报和归档的使用；

—存储系统和设备应使用多个外部日志服务器；

注 3：某些日志协议使用不可靠的网络协议，例如用户数据报协议 (UDP)[391]，因此日志消息可能会因网络或服务器性能问题而丢失。将消息发送到多个日志目标可以降低意外丢失的风险。

—当审计日志记录的主要驱动因素是合规性、问责制或安全性时，应将存储系统和设备配置为在事件发生时立即记录事件（即不使用缓冲）。

b)TC-HARD-G03 确保存储审计日志记录的完整性

实用性事件日志记录的完整性在一定程度上取决于所捕获的信息（例如时间戳、来源、事件类型等）。对于存储系统，确保审计日志条目的完整性包括：

一一旦确定了要记录的事件类型，则应始终如一地记录这些事件的所有发生情况（无论是带内还是带外）；

—以下类型的事件应被记录（最基本的安全事件集）：

—登录尝试失败和成功；

—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、区域划分更改）；

—安全服务器使用情况的变更（例如，syslog、网络时间协议 (NTP)、域名系统 (DNS)、身份验证）；

—系统关机和重启；

—特权操作（即管理员发起的更改）；

—敏感工具的使用（例如，权限提升命令）；

—访问关键数据文件；

一虚拟服务器在物理服务器之间的移动。

-每条日志条目应包含：

—时间戳（日期和时间）；

一严重级别；

—日志条目的来源（区分名称、IP 地址等）；

一 事件 ID 以及文本描述（用于启用事件的本地化/国际化，其中事件 ID 保持不变，但文本描述可以翻译成不同的语言）；

一事件描述。

c)TC-HARD-G04 实施适当的存储监控 实施适当的监控，以便：

一存储系统和审计日志基础架构应谨慎使用符合日志策略的过滤（例如，基于严重性等字段）；

一应实施分析协议，以关联跨事件源的审计日志记录，从而识别能够指示安全事件的重大安全事件；

-部署安全信息和事件管理 (ISEM) 技术时，应将存储日志记录纳入 ISEM 解决方案；

—部署信息安全持续监控 (ISCM) 技术时，应将存储系统和设备纳入 ISEM 解决方案。

d)TC-HARD-G05 使用日志保留和保护进行存储 实施适当的保留和保护措施，以便：

-应正确处理具有证据价值的审计日志数据（即，维护监管链，并确保其完整性和真实性可验证）；

一具有特定保留要求（例如，出于法规遵从性）的审计日志数据应使用组织的数据保留解决方案进行保存；

一 应采取适当措施来维护日志完整性，并防止其被修改或销毁（无论是恶意还是意外）；

一 当审计日志条目包含敏感信息时，应使用适当的保密机制来保护审计日志数据；

注4：某些日志条目可能会泄露密码等信息（例如，用户输入密码而不是用户 ID 时），但也可能存在更隐蔽的问题（例如，搜索命令会泄露特定名称和运行状况问题）。

—针对特殊的审计日志记录要求（例如，高容量、特殊保存和事件签名）

应使用专用且经过特殊加固和配置的系统；

—应利用日志中继和日志过滤来最大限度地减少特殊存储要求（例如，一次写入只读或 WORM）的影响。

10.3.3 存储漏洞管理

ISO/IEC 27002:2022 8.8强调了管理技术漏洞的重要性，并提供了具体指导。本规范阐述了技术漏洞的识别、评估和修复。

与存储漏洞管理相关的控制措施如下：

TC-HARD-G06 将存储纳入漏洞管理计划

由于存储技术的特殊性，存储系统并非总是包含在组织的漏洞管理计划中。此外，许多用于识别

漏洞的工具并未全面覆盖存储操作系统，并且应用程序。组织应将存储系统纳入其漏洞管理计划。

10.4 存储管理

10.4.1 背景

存储网络和基础设施元素是复杂的架构，会对管理员提出严格的管理要求。为了满足这些要求，组织会实施存储基础设施管理工具和流程，以确保所有存储设备的可用性和性能、更高的数据保护和安全性、集中式审计以及满足合规性要求。

存储系统可以使用带内或带外机制进行管理（参见图 2）。在此上下文中，带内管理通常是指通过用户数据传输路径来管理存储系统。存储管理命令通过输入/输出连接发送，例如串行连接SCSI、光纤通道或互联网 SCSI、PCIExpress® 等。另一方面，带外管理使用与用户数据流量不同的备用路径来访问存储系统的管理接口。带外管理通过网络连接或边带接口发送命令。即使存储系统同时支持这两种存储管理方式，它们的管理功能和安全注意事项也可能存在显著差异。

10.4.2 认证和授权

10.4.2.1身份验证

管理存储系统和基础设施的人员通常是特权用户。不当使用系统管理权限（信息系统的任何功能或工具，允许用户覆盖系统或应用程序控制）可能是导致系统故障或安全漏洞的主要因素。为了帮助降低这些风险，可以使用 ISO/IEC 27002:2022 8.5中描述的安全登录程序，并根据需要采取额外的身份验证措施。

与身份验证相关的控制措施如下：

a) TC-MGMT-R01 最低用户身份验证措施

存储管理通常涉及特权操作，这些操作由具有最低身份验证级别的用户执行，其中包括：

—所有用户应用户应拥有仅供其个人使用的唯一标识符（用户ID）；

—为证实用户所声称的身份，应使用以下合适的身份验证技术之一：

一足够复杂且保密的密码，攻击者难以猜测或以其他方式破解；

一强身份验证（例如，挑战-响应协议）；或

一多因素身份验证，例如生物特征数据（例如，指纹验证或视网膜扫描）和使用硬件令牌（例如，智能卡）。

一所有远程访问均应使用强身份验证或多因素身份验证以及安全通道。

b)TC-MGMT-G01 使用集中式身份验证解决方案

应使用集中式身份验证解决方案，例如远程身份验证拨入用户服务(RADIUS)、单点登录、开放授权 (OAuth)、安全断言标记语言 (SAML) 等，以改进监控和控制。

c) TC-MGMT-G02 使用多因素身份验证

在管理敏感和高价值数据时，应使用多因素身份验证。

d) TC-MGMT-G03 禁用 root 或 admin 帐户登录 应禁用 root 或 admin 帐户登录。

e] TC-MGMT-G04远程记录所有权限提升操作 应远程记录所有权限提升操作。

f)TC-MGMT-G05使用实体身份验证机制

除了用户身份验证之外，存储系统有时还会采用实体身份验证。实体身份验证是指分布式系统中的代理对通信伙伴身份的信任过程。这种实体身份验证可以在传输层安全协议 (TLS) 和 IPsec 连接中进行，也可以在存储协议中进行，例如 iSCSI 中的质询握手身份验证协议 (CHAP)、FCP 中的 Diffie-Hellman 质询握手身份验证协议 (DH-CHAP) 等。应尽可能使用这些实体身份验证机制。

10.4.2.2授权和访问控制

在金融服务和医疗保健等市场领域，通过利用特定角色，使授权和访问控制符合最小权限原则的趋势正在兴起。

与授权和访问控制相关的控制措施如下：

TC-MGMT-G06分离安全角色和非安全角色

存储技术中应实现和使用以下角色：

—安全管理员。此角色拥有只读/查看和修改权限，可以建立和管理帐户，创建和关联角色/权限，配置审计日志及其内容（审计日志事件条目不可更改），与 IT 基础架构建立信任关系（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，以及设置访问控制；

—存储管理员。此角色拥有存储系统所有方面的查看和修改权限，但安全相关元素或数据（即安全管理员负责的元素或数据）除外；

—安全审计员。此角色拥有查看权限，允许进行授权审查、验证安全参数和配置以及检查审计日志。无权访问存储、配置或数据；

—存储审计员。此角色拥有查看权限，允许验证存储参数和配置以及检查运行状况/故障日志。无权访问安全相关元素或数据。

每个存储管理事务都应与一个安全角色或存储角色关联。这些角色是确保管理能力职责分离的重要控制措施。

10.4.3 保护管理接口

除了物理接口（参见9.3）之外，存储系统还采用各种软件和固件来实现存储系统的管理。这些软件接口可以包括简单的命令行界面(CLI)、基于 Web 的界面（包括图形用户界面或 REST 应用程序编程接口 (API)）、对简单网络管理协议 (SNMP) 的支持，以及处理带内管理（即通过数据路径）的基于服务器的代理。

与保护管理接口相关的控制措施如下：

a)TC-MGMT-G07保护管理软件/固件的网络接口

存储管理软件/固件接口通常使用以下措施进行保护：

—应使用防火墙和 TCP 包装器来限制对管理网络的访问，仅允许授权的系统和协议访问；

—应使用实体认证来建立存储系统和管理系统之间的信任关系（例如，使用 FC-SP-2 AUTH-A[61]）以对执行带内管理的实体进行认证）；

管理”）；

—应利用入侵检测系统和入侵防御系统机制来识别异常行为并加以防范；

—ICT 基础设施，例如域名系统 (DNS)、服务位置协议 (SLP) 或网络时间协议 (NTP)

NTP 应与适当的安全控制措施一起使用，以避免间接攻击；

— 适当的特权用户控制措施，包括身份验证（参见10.4.2.1）、授权（参见10.4.2.2)，以及安全的审计/监控（参见 10.3.2）应予以采用；

操作系统和应用程序应为最新版本，并具备足够的安全防护能力以抵御攻击（参见10.3.1）。

b) TC-MGMT-R02 确保远程管理安全

远程管理存储系统时，应采取以下附加安全措施：

使用安全通道，例如虚拟专用网络 (VPN)、TLS、安全外壳协议 (SSH) 或超文本传输 协议 (HTTPS)

所有远程访问均应使用安全传输协议 (HTTPS)；

—采用强身份验证或多因素身份验证；

—将权限限制在必要的最小范围内（即最小权限原则）。

组织应制定组织和技术控制措施，以限制用于远程（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）进行通信的个人执行的远程供应商维护操作

通过互联网等外部网络进行通信的个人会对可用性、完整性和机密性构成重大风险。

c) TC-MGMT-R03 限制供应商远程维护管理

技术控制措施应将通信流量（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。访问方通过身份验证后，应在接入点设计额外的控制措施来授权供应商维护会话。这些措施包括接受、请求批准或拒绝请求的会话。应生成包含供应商操作审计记录的相应日志。

d)TC-MGMT-R04 限制拨号访问的使用

组织应将拨号接入线路限制为仅限授权访问方。这包括强制执行调制解调器回拨协议，并在供应商请求维护会话且该请求获得组织授权之前禁用连接建立。

e] TC-MGMT-R05 安全 IPMI

某些存储系统包含基于硬件的平台管理系统，从而可以集中控制和监控系统，包括管理远程物理位置的服务器，而无需考虑已安装的操作系统。此软件无需存储系统操作系统的许可，因为它运行在连接到主板或服务器的独立硬件上。

在某些实现中，基板管理控制器(BMC)位于板载传感器和接口与带外通信接口（例如以太网）之间。智能平台管理接口 (IPMI) 可处理一系列接口（包括 BMC），这些接口提供对系统的底层访问，可以覆盖操作系统控制。IPMI 消息可以传输。 IPMI 2.0 中定义了一种额外的包格式（RCMP+）。该格式支持通过远程管理控制协议 (RMCP) 和 UDP 数据报（ASF-RMCP 的 UDP 目标端口为 623）与 BMC 进行通信。此功能也称为“基于 LAN 的 IPMI”。IPMI 还定义了 LAN 特定的配置设置，类似于 IP 地址的配置。RMCP+ 除了支持各种身份验证扩展外，还支持加密数据传输。

使用 IPMI 时，需要采取以下额外的安全措施：

默认配置应禁用 IPMI，仅在需要时临时启用；

—IPMI 流量（通常为 UDP 端口 623）应限制在受信任的内部网络，例如具有强网络控制的管理 VLAN 段；

—运行 IPMI 的设备上的 IPMI 服务应设置并使用强密码和唯一密码；

—如果可能，应在 IPMI 上启用加密（例如使用 RMCP 或 RMCP+ 协议）；

—“密码 0”〔在许多启用 IPMI 的设备上默认启用〕并且应禁用匿名登录，以

防止攻击者绕过身份验证并发送任意 IPMI 命令； —存储的密码应在系统生命周期结束时被清除。

10.5 数据保密性

10.5.1总则

在存储基础设施中，数据保密性通常使用某种加密方法来维护。这些方法最常用于保护在存储基础设施内传输（有时称为“传输中”或“动态”）的数据，以及在设备或存储介质上存储（或“静态”）的数据（有关存储系统和生态系统的加密和密钥管理的有用概述，请参阅参考文献和 [74）。

加密过程是将加密算法（或密码）应用于明文数据，从而生成加密数据（或密文）。相反，解密过程则是将密文还原为其原始数据。

明文。许多与存储相关的重要密码的定义和规范可以在ISO/IEC 18033 系列、NIST FIPS 197 和 IEEE 1619.2-2021 中找到。

对于某些类型的密码（例如 n 位分组密码），可以使用多种方式（称为操作模式）来加密明文。常见操作模式的定义和规范可在 ISO/IEC 10116、NIST 特别出版物 800-38A、NIST 特别出版物 800-38C、NIST 特别出版物 800-38D、NIST 特别出版物 800-38E、IEEE 1619-2018 中找到。

密码算法与密钥以及其他密钥材料（例如初始化向量）配合使用。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的但相关的密钥。密钥的管理和保护（称为密钥管理）对于维护数据机密性至关重要。

密钥管理的目的是提供处理用于对称或非对称密码机制的加密密钥材料的程序。密钥管理各个方面的定义和规范可在 ISO/IEC 11770 系列标准和 NIST 特别出版物 800-57 第 1 部分[69J和第 2 部分Z⁰中找到。ISO/IEC 27002:2022,8.24 也提供了有关密钥管理的指导。管理。

10.5.2 加密和密钥管理问题

使用加密技术会引入一些不容忽视的问题。未能解决这些问题可能会使组织面临监管处罚，并在某些情况下造成灾难性损失。

与加密和密钥管理相关的控制措施如下：

a) TC-CNFD-G01 遵守密码学进出口法规

加密技术的进出口可能受到严格的监管。为避免出现问题，各组织应：

一了解并遵守与加密和密钥管理相关的政府进口法规；

一了解并遵守与加密和密钥管理相关的政府出口法规。

b)TC-CNFD-G02 遵守密钥托管和披露要求

一些组织使用密钥托管服务来管理第三方对其系统某些部分的访问，包括强制性密钥披露。使用密钥托管服务时，假定组织将：

—遵守公司或政府的密钥托管要求；

— 理解并遵守公司或政府关于向公司官员、执法机构等提供加密密钥的任何要求，以便访问和恢复加密数据。

c) TC-CNFD-G03 密钥故障应对计划

加密密钥的丢失或损坏会导致数据无法使用，因此组织通常会采取措施来保护其加密密钥（例如，密钥管理服务器的密钥备份）。密钥备份通常在特定的加密/密钥管理解决方案中实施，其重点是为解决方案提供对用于加密解决方案内部数据的密钥的访问权限。

为确保密钥丢失或泄露得到充分保护，组织应具备：

—密钥丢失或泄露时的恢复计划；

—密钥备份计划，以确保持续访问加密的业务/关键任务数据。

d)TC-CNFD-G04 限制密码学对运营的影响

密码学（尤其是加密）的使用可能会对运营产生影响，进而影响信息通信技术 (ICT) 基础设施的有效性或效率。组织应尽量减少这些影响，包括：

—由于通信中使用端到端加密，导致基于网络的数据丢失防护技术有效性降低；

— 由于无法对密文应用数据缩减技术（重复数据删除和压缩技术），导致网络或存储利用率增加；

—无法对加密数据应用集中式恶意软件扫描。

10.5.3 存储加密

在评估基于存储的加密解决方案的部署时，需要考虑多个因素，包括但不限于：

-加密可能会影响其他安全方面（例如数据检查和防病毒）；

-如果数据处理、数据转换、密钥管理或实际加密过程中出现任何问题，加密都可能导致数据不可用；

—加密可能需要大量的计算资源；

- 加密可能需要集中式密钥管理，尤其是在将加密与跨区域复制结合用于业务连续性管理 (BCM) 时；

-加密可能会削弱或抵消数据缩减技术（例如压缩和去重）的优势，因为加密数据不易压缩；

-加密技术的质量（安全强度以及经过行业测试和认可的算法）会影响实际提供的保护。

并非所有数据都值得加密。风险评估可以帮助识别需要加密的敏感和高价值数据，并协助进行成本效益分析（即降低风险是否值得付出成本）。值得注意的是，当数据被视为关键资产时，还有其他机制可以保护数据的机密性。

保护传输中的数据通常涉及两个或多个通信实体建立用于传输数据的加密通道（参见 10.5.4）。此连接通常是短暂的，并且通常会在需要时协商安全性。

静态数据保护（参见10.5.5）通常涉及数据路径上的一个单一点（加密点），用于加密/解密数据。加密点至关重要，因为它代表了数据路径中数据加密（密文）和可用（明文）的位置。一种常见的安全策略是尽可能在数据源或使用点附近进行加密，因为这往往能最大限度地提高保护效果。但是，加密点的选择有很多种（参见图 3），包括：

一应用层，例如特定应用程序或数据库，可以提供最精细的控制粒度，并最大程度地了解数据（类

型、用户、敏感性）。

—文件系统级，例如操作系统或操作系统级应用程序，提供文件级控制，并可了解用户信息。

—网络级，例如主机总线适配器 (HBA)、阵列控制器或交换机，其中：

—基于文件的（NAS）提供共享/文件系统级（可能为文件级）控制，并可了解部分用户信息；

—基于块的，提供逻辑卷级控制，但对用户群体了解有限。

注1：具体的用户群体及其各自的访问权限未知。用户群体由有权访问各个逻辑卷的服务器定义。

—设备级控制，例如磁带驱动器、存储阵列和磁盘驱动器，可在存储介质级别（以及可能在逻辑卷级别）进行控制，但对用户群体的了解有限。

如果没有精心设计和持续监控存储生态系统的变化，可能会出现多个加密点被部署的情况。这种情况可能会产生负面影响，尤其是在信息通信技术人员不了解静态数据加密部署的情况下。

以下方法可用于使用静态数据加密保护存储中的数据（另见10.5.5）：

a) TC-CNFD-R01 使用至少 128 位安全强度的加密技术

应在整个过程中使用至少 128 位安全强度的加密技术。加密解决方案。b) TC-CNFD-G05 避免将存储加密作为敏感数据的主要保护措施

基于存储的加密不应作为敏感数据的主要保密保护措施。

注 2：存储加密通常仅在数据驻留在存储系统或介质上时才处于活动状态（即，一旦经过加密点，数据即为明文，而加密点会在每次访问数据时发生）。

c) TC-CNFD-G06 选择合适的加密点

加密点的选择和实施应与 BCM（参见 7.3）、数据缩减（参见 10.13）、数据保护（参见 10.14）和数据保密性（参见 10.5）要求兼容。

d) TC-CNFD-G07 使用与数据保留和保存要求相兼容的适当加密和密钥管理方案

加密和密钥管理解决方案应与数据保留和保存要求相兼容。

e) TC-CNFD-G08 对敏感或受监管数据使用经过验证的加密模块

用于保护敏感或受监管数据的加密模块应使用公认的标准（例如 ISO/IEC 19790、ISO/IEC 15408 系列和 NIST FIPS 140-3631）进行验证。

f)TC-CNFD-G09 生成和保留存储加密记录

与数据清理一样，组织维护其静态数据加密记录至关重要，组织需要记录受保护的存储介质，以及加密的时间和方式。当组织怀疑其存储介质（包含敏感数据）失去控制时，这些记录或加密证明可以有效证明未发生数据泄露，从而避免代价高昂的数据泄露通知和其他责任。加密证明应包含以下内容：

—确保加密机制生成适当的审计日志条目（激活、验证、完整性检查、重新密钥等）；

—定期进行审计检查，确保加密已正确执行，并考虑外部认证。

g) TC-CNFD-G10 遵循基本密钥管理原则

成功使用密码学取决于遵循与密钥材料和密钥管理相关的基本原则。集成静态数据加密和密钥管理的存储系统和设备可以通过以下方式进一步提高安全性：

—应使用集中式密钥管理进行密钥生命周期管理；

—应尽可能实现密钥管理自动化；

一生命周期较长的密钥（即接近建议的最大加密周期，通常不超过 1 到 2 年，具体取决于密钥类型）应谨慎使用；

一应使用严格的访问控制来限制用户权限，并对密钥的生成、更改和分发实施职责分离约束（例如安全角色）。

10.5.4 加密传输数据

10.5.4.1总则

在存储基础设施中，数据机密性或完整性（数字签名或认证码）

在两点之间传输的数据可能非常重要，特别是对于离开物理控制数据中心范围的数据。此外，存储系统内部的数据传输也值得关注。

诸如 FC ESP_Header;,60]I Psec 之类的协议（参见10.5.4.3)TLS（参见10.5.4.2），或甚至基于计算机的

加密技术可以在数据传输过程中提供额外的保护。这些方法最常用于保护移动中的数据（也称为飞行中或传输中）。

移动中数据保护通常是对数据的临时保护，仅在数据移动时存在。对于移动中数据加密，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。该算法将密文转换回其原始明文，接收方执行完整性检查。有多种标准规范，包括光纤通道安全标准、IPsec RFC 和 TLS RFC，详细说明了传输中数据安全保护的替代方案。

某些协议在标准中规定了多种操作模式或选项。此外，还存在多种加密模式或数字签名（完整性）算法。操作模式的定义和规范可在 ISO/IEC 10116 中找到。

传输中数据的保护与密钥建立或密钥协商过程或协议密切相关。初始认证密钥的管理和保护对于维护传输中数据的机密性和完整性至关重要。前面引用的标准详细说明了在使用传输中数据保护方法时应保护的关键安全参数的更多信息。

与加密传输数据相关的控制措施如下：

a) TC-CNFD-G11 为传输中数据提供端到端安全保护

当需要保护传输中数据时，应提供端到端保护（即一种确保通信安全的方法，可防止第三方在数据从一个终端系统或设备传输时访问数据）。 （到另一个）。

b) TC-CNFD-G12 补偿传输中数据加密的计算影响

传输中数据加密可能会给通信实体带来显著的计算负担，因此应实施适当的补偿措施以最大限度地减少这些影响。

10.5.4.2 传输层安全协议 (TLS)

TLS 是一种旨在促进互联网通信隐私和数据安全的安全协议。

TLS 协议版本 1.3 在 IETF RFC 8446.58 中进行了规定。与 TLS 相关的控制如下：

TC-CNFD-R02 TLS 最低要求

当 TLS 是用于运动数据保护，具体实现如下：

一应使用 TLS 进行存储管理，以便存储客户端和服务器符合

组织认可的 TLS 配置文件（例如 ISO/IEC 20648 或参考[71]）；一应使用 TLS 版本 1.358 或更高版本进行数据访问。

10.5.4.3IP 安全 (IPsec)

有多个 IETF RFC 与互联网协议安全 (IPsec) 规范相关。IETF RFC607153]p对 IPsec 和 IKE 相关的 RFC 进行了很好的概述。

IPsec 可能会对某些技术的使用产生不利影响，例如网络地址转换 (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帧的系统。是否依赖 IPsec 取决于具体情况。 IPsec 或其他动态数据保护协议的选择可能取决于权衡取舍——

其他技术的价值可能会因此而降低。

与 IPsec 相关的控制措施如下：

TC-CNFD-R03 IPsec 最低要求

当 IPsec 用于动态数据保护时，其实现应：

—支持 IPsec 版本 3；

—支持 IPsec 的隧道模式或透明模式；

—支持至少一个安全策略数据库 (SPD)（例如 IETF RFC 430144）。

—支持使用加密算法的 IPsec ESP（例如 RFC 4303[45]）；

—支持 Internet 密钥交换 (IKE) 版本 2（或更高版本）密钥交换算法；

一支持使用 IKEv2 加密有效负载；

—确保 IKE 协议使用符合预共享密钥方法（例如 IETF RFC 4945[461]）的 X.509v3 证书的 RSA/ECDSA 算法执行对等身份验证。

10.5.5 静态数据加密

随着越来越多的敏感和受监管数据被存储，各组织机构正在采取措施确保这些数据以加密形式存储。虽然在数据尽可能靠近其来源和使用位置进行加密是理想情况，但对存储基础设施中的静态数据进行加密也能提供基本的保护，防止因存储介质（尤其是磁带）失控而导致的数据泄露。因此，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、主机总线适配器 (HBA) 等内部的加密机制可以提供有效的保护。

与静态数据加密相关的控制措施如下：

a) TC-CNFD-G13 使用合适的加密点

实施数据加密远不止购买具有加密功能的设备并将其连接到现有存储基础设施那么简单。应根据已识别的风险选择加密机制（加密点）在基础设施中的位置，并做出相应的安排。为该位置提供密钥材料。应识别待处理的数据，在某些情况下，应更改其位置。

b) TC-CNFD-G14 创建适当的加密证明

此外，应创建充分的加密证明（通常以日志的形式），并将其集成到审计日志基础架构中。有关

更多信息，请参阅10.5.3。

c) TC-CNFD-R04 保护用于加密存储的密钥

所有类型的存储加密都依赖于加密密钥的管理。无论加密强度如何，糟糕的密钥管理都可能轻易导致数据泄露。最终，受密码学保护的数据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密钥所受到的保护。所有密钥都应防止被篡改。对称加密的秘密密钥和非对称加密或公钥加密的私钥都应防止未经授权的披露。密钥管理为密钥的安全生成、存储、分发和销毁提供了基础。密钥管理的总体框架在 ISO/IEC 11770 中给出。

密钥管理为密钥的安全生成、存储、分发和销毁提供了基础。密钥管理的总体框架在 ISO/IEC 11770 中给出。系列。

d) TC-CNFD-R05 使用适用于存储的加密算法和操作模式

应使用适用于存储技术的加密算法和操作模式，可以包括：

—对于 HDD 和 SSD，应使用 IEEE 1619-2018 中描述的 XTS 模式的 AES；[36]

—对于磁带，应使用 IEEE 1619.1-2018 中描述的带有计数器的 AES，以及带有密码块链接消息认证码 (CCM) 或 Galois/计数器模式 (GCM) 的模式。[37]

e) TC-CNFD-G15 限制明文密钥的明文暴露

应限制密钥以明文形式存在的时间，并应防止用户查看明文密钥。

f) TC-CNFD-R06 仅使用加密密钥用途

加密密钥只能用于一个用途。请勿使用密钥加密密钥（也称为密钥包装密钥）来加密数据，或使用数据加密密钥来加密其他密钥。

g) TC-CNFD-R07 使用整个密钥空间随机生成密钥 密钥应从整个密钥空间中随机生成。

最佳实践建议使用密码学安全的伪随机数生成器，该生成器确保在完全了解算法和输出序列的情况下，无法使用实际计算方法确定序列之前的数字或序列之后的数字。

h) TC-CNFD-R08 密钥使用限制在有限的加密周期或处理的最大数据量内。

如果适用，数据加密密钥的使用应限制在有限的加密周期内（通常不超过 2 年）或处理的最大数据量内。

注 1：并非所有密钥都可以替换（例如，可信平台模块中的静态背书密钥）。

i) TC-CNFD-G16 使用集中式密钥管理基础设施。

如果可能，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，生成和归档加密密钥）。

j〕TC-CNFD-G17 使用 OASIS KMIP 访问和使用集中式密钥管理基础设施

结构化信息标准促进组织 (OASIS) 密钥管理互操作性协议(KMIP)规范和概要文件定义了在存储基础设施中访问集中式密钥管理的主要机制。

注 2：OASIS KMIP 的规范见参考文献 [75]和 [76]。

存储系统和基础架构应使用符合 OASIS KMIP 2.0 版（或更高版本）标准的客户端来访问和使用密钥管理基础架构。

10.6 存储清理

10.6.1 概述

ISO/IEC 27002:2022 的 7.10 和 7.14 条款提供了关于存储介质处置和再利用的指导，以防止信息泄露。ISO/IEC 27002:2022 的 8.10 条款也提供了关于信息删除的相关指导。通常，存储介质上记录的敏感数据应在再利用或处置存储介质之前清除。

为了满足 ISO/IEC 27002 中关于处置和再利用的关键指导原则，可以采用与组织采用的数据分类方案相一致的存储清理程序。此类程序通常包括：

—规范最低可接受的清理方法（参见 10.6.2）；

—确定已执行清理的充分性所需的验证步骤（参见10.6.6）；

—识别满足合规义务所需的记录或证据（参见 10.6.7）。

存储清理是指使存储中先前记录的数据无法检索的一般过程，从而可以合理地保证数据无法轻易检索或重建。在存储中执行的存储清理可以采用逻辑清理（参见 10.6.4）或基于介质的清理（参见10.6.3）的形式。由于存储清理的重要性，可能需要承担额外的义务来验证清理操作的结果，并生成清理操作的记录（证据）（参见 10.6.7）。

与存储清理相关的控制措施如下：

a) TC-SNTZ-G01 将存储清理纳入数据治理

存储数据清理应是组织数据治理流程的一个组成部分。是否使用存储数据清理应基于组织的数据分类，重点关注被归类为敏感的数据。敏感数据的常见示例包括个人数据、个人身份信息(PII)和电子医疗记录，以及某些业务数据（例如商业秘密、知识产权、客户记录和财务记录）或关键任务数据（例如国家安全数据）。如果组织失去对存储设备或存储介质的控制权，则未能清理存储数据或未能妥善记录清理操作可能会触发数据泄露通知。

注意：此处的敏感数据是指，披露后可能对组织使命产生影响的数据，

可能导致组织资产受损，或导致组织或个人遭受经济损失或伤害的数据。

b)TC-SNTZ-R01 处置前清理存储数据

逻辑存储（see 10.6.4)或基于介质的存储（参见和 10.6.3)用于记录敏感数据，在处置或转移给组织外部方（即组织失去对存储的控制权）之前，应进行数据清理。当数据的敏感性需要保密保护（例如，合规义务或组织政策）时，在同一组织内部进行存储转移（例如，从人力资源部门转移到工程部门）之前，也应进行数据清理。

c) TC-SNTZ-R02 验证存储数据清理结果

当强制要求进行数据清理时，应在处置或转移存储之前验证存储数据清理结果，以确保组织风险已得到充分解决。

10.6.2 消毒方法的选择

可以使用多种清理方法，具体取决于存储（逻辑或基于介质），它们采用以下形式：

—清除：涉及使用软件或硬件用非敏感数据覆盖目标数据。

— 清除：涉及使用物理或逻辑技术使恢复变得不可行，使用最先进的实验室技术，同时将存储保

持在潜在可重复使用的状态。

一破坏：涉及物理技术的使用（例如分解、焚化、熔化、粉碎和粉碎）

销毁存储。此清理方法不适用于逻辑存储。

上述每种清理方法都提供了不同的保证，确保数据无法轻易检索或重建，并且它们基于对手为破坏保护而付出的努力程度。

从这个角度来看，当清理方法正确执行时，clear 方法提供的保证最少，而 destruct 方法提供的保证最多。

并非所有清理方法都适用于所有类型的逻辑存储（请参阅 10.6.4）或基于媒体的存储（请参阅 10.6.3）。

与选择存储消毒方法相关的控制措施如下：

a) TC-SNTZ-R03 选择最低可接受的存储消毒方法

所选择的存储消毒方法应指定为可接受的最低限度。应允许提供更强保证级别的消毒方法（例如，当使用破坏时，但清除是最低要求）。不应使用提供较弱保证级别的消毒方法。

b)TC-SNTZ-G02 考虑存储数据清除的成本和环境影响

应根据成本和环境影响等因素评估所选的存储数据清除类型，并做出能够最大程度降低机密性风险并最大程度满足流程其他约束条件的决策。

10.6.3 基于介质的数据清除

数据存储技术以及针对存储的攻击都在快速变化和发展。因此，与三种数据清除方法（参见 10.6.2）相关的特定数据清除技术会频繁更新，这些技术适用于各种类型的存储设备或存储介质。本文档不提供有关如何清除特定类型介质的详细信息，而是建议参考其他提供此类信息的资源。

与基于介质的数据清除相关的控制措施如下：如下：

a) TC-SNTZ-R04 按照可接受的标准对介质进行清理

当确定需要对存储设备或存储介质进行清理时，应根据所选的清理方法（清除、擦除或销毁）执行清理，并且清理方式应符合组织政策认可的标准（例如 IEEE 2883，该标准提供了有关选择合适的清理方法以及特定技术的清理技术的更多信息）。

当使用加密擦除的擦除方法时，请参阅10.6.5以了解其他注意事项或要求。

b) TC-SNTZ-R05 验证介质清理结果的充分性

验证（参见10.6.6）介质清理结果的充分性清理结果应在基于介质的存储上执行。

10.6.4 逻辑清理

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（参见10.16.1）。一个众所周知的例子是存储阵列上的逻辑单元，其大小可以远远超过单个存储设备的容量；云计算存储（参见 10.11）可以将这种虚拟化提升到更高的抽象级别。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 10.16.2）和 BCM（参见7.3）时，情况会变得更加复杂。对于这些情况，几乎不可能识别所有记录敏感数据的底层存储介质。此外，对所有物理介质进行清理通常既不合适也不可行，因为多个逻辑存储实例可以共存于共享的物理介质上。

与逻辑清理相关的控制措施如下：

TC-SNTZ-R06 按照可接受的标准清理逻辑存储

如果逻辑存储（例如逻辑单元、文件系统、对象存储或云计算存储）可写，则可以使用明文方法进行清理；或者，如果已正确使用加密，则可以使用加密擦除的清除方法进行清理（参见10.6.5）。当确定需要对逻辑存储进行清理时，应根据具体情况采用以下任一方式进行清理：

—通过提供的接口，覆盖（替换）所有可寻址的逻辑存储空间，进行清除，

使用已知的非敏感数据（通常为零）；或

—使用加密擦除进行清除，如10.6.5节所述。

b) TC-SNTZ-R07 验证逻辑存储清理结果的充分性

验证（参见10.6.6）逻辑存储的清理结果是否充分。

c) TC-SNTZ-G03 考虑针对数据保护机制的额外存储清理

数据保护技术（参见10.14），例如复制和备份，通常与逻辑存储结合使用，因此应针对与数据保护机制相关的存储执行单独的清理操作。

10.6.5 加密擦除

从根本上讲，加密擦除利用目标数据的加密，通过清理用于加密目标数据的加密密钥来实现。这样，存储上就只剩下密文，从而有效地清理了加密密钥。数据。

与加密擦除相关的控制如下：

a) TC-SNTZ-R08 在正确条件下使用加密擦除进行清除

要使用加密擦除作为清除方法，至少应满足以下条件：

—所有拟进行加密擦除的数据在记录到存储设备之前均应进行加密；

—用于加密目标数据的加密算法强度（包括操作模式）应至少为 128 位；

—熵的比特数应至少等于用于加密目标数据的加密密钥的比特数；

—所有用于加密目标数据的加密密钥副本均应进行清理；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加密，则可以通过清理相应的包装密钥来执行加密擦除。

注意E虽然将加密擦除与其他清理方法（例如明文）结合使用可能很诱人，但这种方法并不能提高安全性，反而会显著减慢清理操作，并可能妨碍对加密擦除的验证。采用这种方法的理由通常包括通过阻止访问密文来减少攻击面，但这恰恰表明加密擦除可能不适用于数据的敏感级别。

b) TC-SNTZ-G04 寻求对用于加密擦除的加密技术质量的保证

选择应用加密擦除的用户应寻求对以下保证领域的独立验证，或要求供应商说明用于确保解决这些问题的机制：

—密钥生成：随机密钥的熵水平随机数据白化程序的数量来源和质量。这适用于加密密钥，也可能适用于受加密擦除操作影响的包装密钥。

一介质加密：用于保护目标数据的加密算法/模式的安全强度和有效性。

一密钥级别和封装：对用于封装（即加密）介质加密密钥的密钥进行清理，或者

另一个密钥可以提高封装的安全强度和保证级别

所用技术（例如，与加密擦除操作的强度级别相匹配）。

应使用普遍接受的和（在适用情况下）标准化的机制。例如，

加密要求在 ISO/IEC 19790 中规定，加密模块的测试要求在 ISO/IEC 24759中规定。这些测试要求和测试涵盖了部分（但并非全部）关注领域。

c) TC-SNTZ-G05 确定已销毁的加密密钥是否可恢复

在决定是否依赖加密擦除时，还应考虑加密密钥是否可以从内部或外部恢复（例如，从密钥管理服务器或密钥托管服务注入）。如果加密密钥（或任何级别等于或低于加密擦除期间清除的密钥级别的密钥）存在于存储设备之外，则将来有可能使用该密钥来恢复存储在加密存储设备上的数据。

10.6.6 存储清除的验证

验证清除结果是存储清除程序的重要组成部分。确定存储数据清除的充分性或有效性是必要的。此验证因清除方法而异。对于清除或吹扫，使用设备界面检查清除操作的结果。对于销毁，则使用物理检查来检查清除结果。此验证至关重要，因为可能存在错误或异常情况，需要采取额外措施来完成清除，或者需要组织决定接受任何残留风险。

为了说明验证的重要性，可以考虑一个假设场景：使用粉碎技术对光盘（记录了个人身份信息）执行销毁清除方法。此外，粉碎后的碎片尺寸不得超过 3 毫米 x 3 毫米。然而，光盘粉碎后产生的碎片尺寸为 5 毫米 x 5 毫米。考虑到光盘上可能存在敏感的个人身份信息 (PII) 数据，该组织面临一个抉择：要么接受粉碎结果（即组织接受大尺寸碎片带来的风险），要么不接受粉碎结果，然后采用其他销毁方法（例如焚烧、熔化或粉碎）处理这些碎片。在本例中，该组织接受粉碎结果，但记录了与最大粉碎尺寸 3 毫米 x 3 毫米的偏差。

与存储介质销毁验证相关的控制措施如下：

a) TC-SNTZ-G06 验证清晰的销毁方法结果

对于清晰的销毁方法，应进行存储介质的代表性抽样以验证销毁效果。已执行。IEEE 2883确定了两种代表性的采样选项，包括对用户可寻址空间的百分比进行随机采样，以及将用户可寻址空间划分为预定义数量的频带，然后对这些频带进行随机采样的方法。

b)TC-SNTZ-G07验证清除清理方法的结果

对于清除清理方法，应执行对存储介质的全面验证。如果使用加密擦除执行清理，则可能无法执行验证，因为存储介质不可访问，或者存储介质上剩余的随机位模式不提供比较基础。

采用访问控制机制保护的存储设备需要考虑额外的验证因素；存储设备在数据清除前后均应可访问，以便进行验证。这可能会造成问题，因为某些清除操作可能导致存储设备上的目标数据无法访问。

c) TC-SNTZ-R09 销毁式数据清除方法结果的验证

当采用销毁式数据清除方法时，物理检查是唯一选择，因为存储设备（根据定义）已无法使用。当需要对基于销毁的数据清除方法进行验证时，应检查其结果，并将其与组织政策认可的标准进行比较，以确定其充分性（例如 IEEE）。

结果应进行检查，并与组织政策认可的标准进行比较，以确定其充分性（例如 IEEE）。 如果在审查与销毁结果相关的验证结果后，确定数据清除结果不足，则应重复基于销毁的数据清除操作，并

考虑使用其他销毁方式。

10.6.7 数据清除证明

组织应保存数据清除活动记录，以记录哪些存储介质被清除、清除的时间和方式以及存储介质的最终处置方式。通常，当组织被怀疑失去对其信息的控制时，是因为其存储介质数据清除记录保存不完整。

与数据清除证明相关的控制措施如下：

a) TC-SNTZ-G08 生成和保存存储数据清除记录

数据清除证明至少有两种形式：1) 审计日志跟踪和 2) 数据清除证书，用于记录数据清除过程。这些数据清除记录是组织出于合规/法律目的而应保留的证据，以防止受到制裁或收到代价高昂的数据泄露通知。此证明的重要性，以及与数据清除记录相关的来源或监管链要求，是促使将数据清除工作置于安全人员控制之下的主要原因。

b)TC-SNTZ-G09 数据清除认证的最低信息记录

为了生成数据清除证书，应尽可能在执行数据清除之前（例如，销毁硬盘驱动器）收集某些信息。数据清除证书记录的最低信息应包括：

制造商；型号；

一序列号；

—存储介质类型（例如，磁性、闪存和混合）；

一存储介质来源（即存储介质来自的用户或系统）；

一使用的清除方法（即，清除、清除或销毁）；

一 所用清除技术的描述（例如，消磁、覆盖、块擦除和加密擦除）；

—清理结果描述（例如成功/失败和错误/异常）；

—清理验证（清除或清除）：

—使用的工具（包括版本）；

—验证方法（例如完整验证和快速抽样）。

—清理和验证：

—人员姓名；

—人员职位/职称；

—完成日期和时间；—地点；

一联系信息（例如电话号码和电子邮件地址）；

—消毒人员签名栏。

除了与数据清除证书相关的详细信息外，审计跟踪还应记录与数 据清除相关的带时间戳的交易和进度。例如，应反映数据清除操作的启动和结束，以及中间的覆盖和验证进度。

10.7 直接连接存储

直接连接存储(DAS) 设备是一种直接连接到主机计算机的存储设备（例如 HDD、SSD和磁带），无需中间存储网络（即无需集线器、路由器或交换机等网络设备）。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），其中外部存储可以包括扩展器，用于增加可连接的驱动器数量。DAS还可以包括带有可移动介质（例如光盘、闪存盘、SD 卡）的存储设备，这些存储介质可以直接连接到主机。无需关闭存储设备或系统电源即可添加或移除DAS设备。虽然DAS设备通常专用于其所连接的系统，但如果它提供多个允许并发直接访问的接口（端口），则可以在多台计算机之间共享。

这些存储设备的数据访问和管理接口有限（后者通常为带内接口）。与DAS相关的控制措施如下：

a) TC-DASS-G01 保护DAS免受未经授权的访问

为避免未经授权访问DAS上的敏感或高价值数据，应使用某种形式的身份验证访问控制（驱动器锁定）和存储设备加密来保护静态数据。

b)TC-DASS-G02 重新利用或处置 DAS 前的数据清理

在重新利用或处置之前，应按如下方式清理存放敏感或高价值数据的DAS：

一使用存储设备中集成的存储清理功能（参见10.6.2）；

一使用基于计算机或应用程序的数据清理。

c) TC-DASS-G03 备份 DAS 以确保数据丢失后的恢复

为防止意外或故意的数据丢失或损坏，应定期备份 DAS 内容（参见10.14.2），并将其妥善保存在不同的位置。

10.8 存储网络

10.8.1 背景

网络在存储基础架构中扮演着重要角色，可以包括常见的网络技术（例如 LAN 和广域网）、使用这些技术的存储专用网络协议以及存储专用技术（例如光纤通道）。对于前者，ISO/IEC 27033系列标准中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。本文档将介绍特定于存储的网络协议和技术。

存储系统使用网络主要有三个目的：1)数据存储和检索；2)数据保护；3)存储系统管理。这些用途均不强制要求使用特定的网络技术或方法。例如，某些存储管理操作可以通过服务器访问数据时使用的同一光纤通道接口（即带内）以及与存储系统管理接口（带外）的TCP/IP连接来完成。

10.8.2 存储区域网络

10.8.2.1概述

存储区域SAN（存储区域网络）是一种专用的高速网络，可提供对存储的块级网络访问。SAN通常由服务器、交换机和存储设备组成，这些设备使用各种技术、拓扑结构和协议互连。SAN还可以跨越多个站点。

SAN通常用于提高应用程序可用性（例如，多条数据路径）、增强应用程序性能（例如，卸载存储功能和使用独立网络）、提高存储利用率和效率（例如，整合存储资源和分层存储）以及提高数据保护和安全性。此外，SAN 通常在组织的业务连续性管理 (BCM) 活动中发挥重要作用（参见7.3）。

图 4显示了一个地理分布的单个 SAN 示例。这样的 SAN 允许任一站点的计算机访问两个站点中的存储资源（例如，有利于本地化响应和故障转移）。此外，存储系统可以将数据复制到其他存储系

统，而无需考虑它们的位置。两个站点之间的互连机制可能会引入额外的安全隐患。

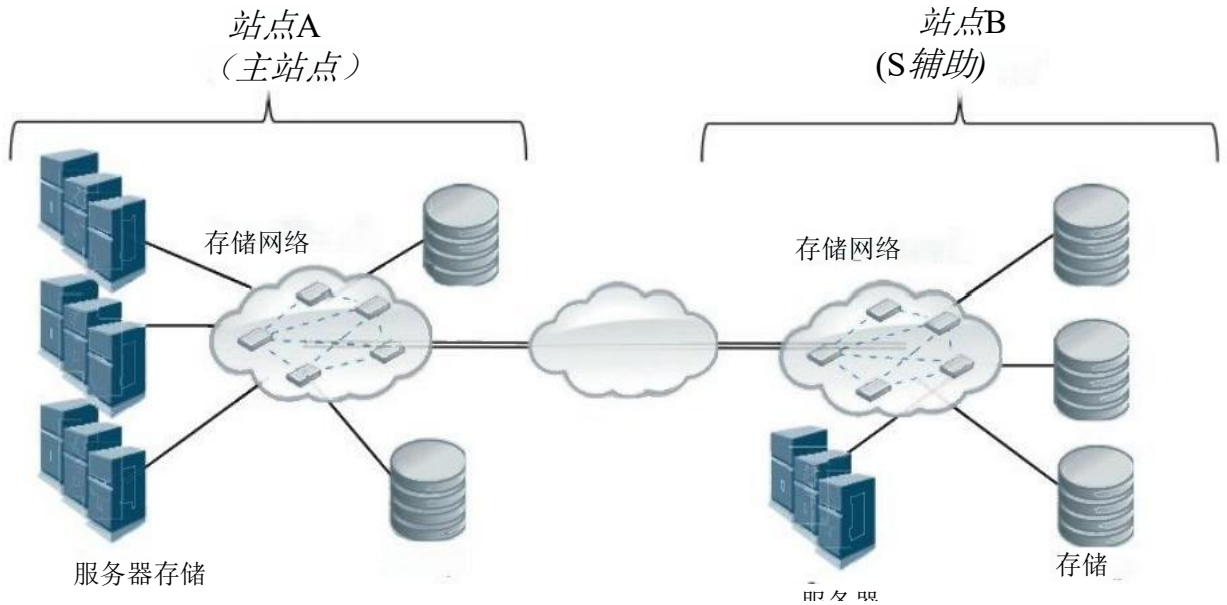

图 4—存储区域网络示例

SAN 将存储设备（例如磁盘阵列和磁带库）呈现给服务器操作系统，使服务器感觉存储设备就像是本地连接的。这种简化的存储呈现方式是通过不同类型的虚拟化技术实现的。

SAN 通常基于以下技术：

—光纤通道 (FC) 技术，它利用光纤通道协议 (FCP) 为开放系统提供 SCSI 接口，并为大型机提供专有变体；

— 互联网小型计算系统接口 (iSCSI)，通常用于中小型系统组织作为 FC 的一种更经济的替代方案；

—InfiniBand，常用于高性能计算环境；

—NVMe⑧3) over Fabric (NVMe-OFT⁴)，[Z8]使用不同的交换矩阵传输（参见 10.8.25），因其低延迟和高吞吐量的多任务处理能力而备受青睐；

—利用扩展器和交换机的互连也具备 SAN 的特性。

此外，还可以使用网络网关在不同的 SAN 技术之间移动数据（参见图图 5）。这种互连对于业务连续性管理支持至关重要。

站点 A站点 B

（主）（备用）

服务器存储服务器存储

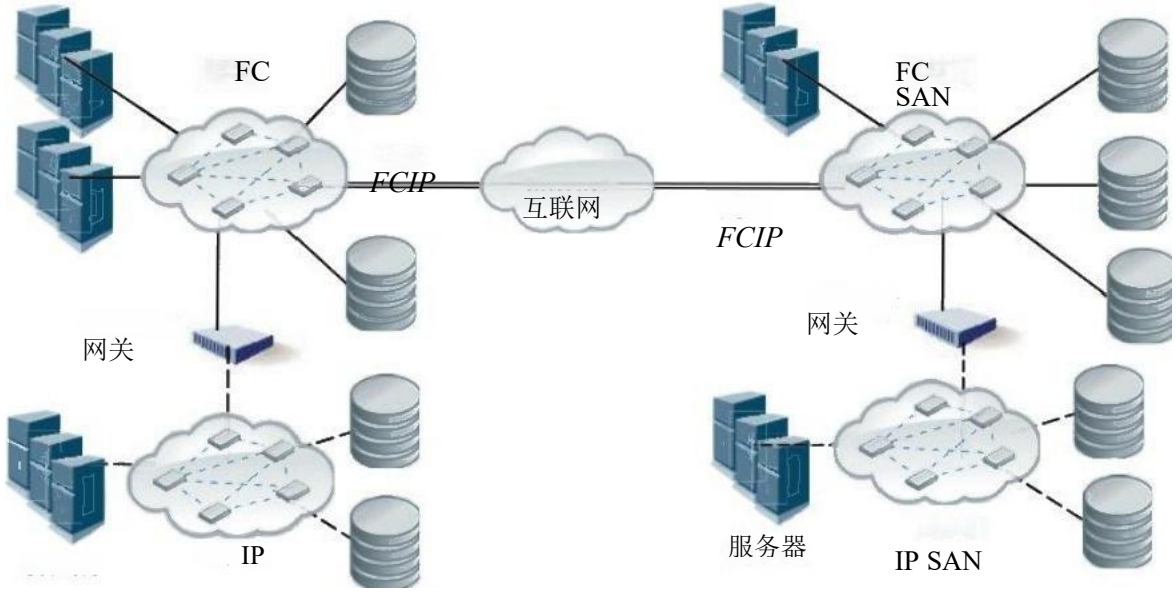

图 5 — 多站点和多种类型 SAN 的示例

纵深防御策略（参见10.2.2.1）有助于降低因单一安全机制失效而带来的风险控制（可能存在单点故障）会危及受保护的资产。

10.8.2.2光纤通道 SAN

光纤通道存储区域网络是一种用于块存储的多千兆级网络技术（参见10.9）。光纤通道有三种主要的拓扑结构，描述了多个端口的连接方式：点对点（两个设备直接连接）、仲裁环路和交换式结构。从安全角度来看，交换式结构拓扑以及光纤通道协议(FCP)（用于在此网络技术上传输 SCSI 流量的接口协议）更值得关注。

与光纤通道存储区域网络 (FC SAN) 相关的安全控制可分为访问控制、身份验证和加密（有关存储系统和生态系统中光纤通道安全性的有用概述，请参阅参考文献[73]）。

SAN 上的访问控制通过应用区域划分、逻辑单元号 (LUN) 掩码和端口绑定机制来实现：

—端口绑定：全局唯一标识符（称为光纤通道的全球名称 (WWN)）用于在 SAN 中进行标识。端口绑定是一种 SAN 安全机制，它将物理端口 ID 与端口绑定。

3) 提供此商标名称是出于公共利益或公共安全考虑。此信息仅为方便本文档用户而提供，并不构成 ISO 的认可。

4) 提供此商标名称是出于公共利益或公共安全考虑。此信息仅为方便本文档用户而提供，并不构成 ISO 的认可以及连接设备的 WWN。这种关联可以减轻潜在攻击者的窥探尝试。

—区域划分：SAN 结构可以划分为不同的区域，以限制 SAN 部分内容对特定服务器和存储设备的可见性。软区域划分基于限制 SAN 结构名称服务器对查询的响应，其假设是服务器请勿联系未通过名称服务器发现的存储设备。硬分区使用 SAN 交换机上的物理端口号来限制流量转发，是一种更安全的分区方法，因为它不依赖于服务器的正确行为，尤其不易受到服务器身份欺骗的影响。

一 LUN 掩码和映射：存储设备可以划分为不同的逻辑单元，这些单元由 LUN 标识。LUN 映射是指为 LUN 分配一个编号，它通常发生在存储阵列中，但也可能作为交换机、HBA 或 CNA 以及虚拟化层中的重定向（从初始地址到新地址）的一部分发生。LUN 掩码是指使 LUN 对某些服务器可见，而对其他服务器不可见。

对于SAN而言，交换机验证与其通信的SAN中其他交换机的身份至关重要。如果未实施交换机身份验证，恶意交换机可以加入SAN并可能危及SAN数据安全。同样，SAN中的节点（例如存储设备和服务器）也可以采用身份验证来限制对SAN数据的访问。

SAN上的数据机密性主要包含两个方面：传输中的数据和静态数据。对于SAN中的敏感和高价值数据，无论数据处于传输状态还是存储在存储设备上，都可以使用加密保护措施。这种保护可能需要使用专用硬件来加密发送到存储设备的数据。有关传输中数据保护的更多指导，请参阅10.5.4；有关静态数据保护的指导，请参阅10.5.5。其余部分。

与光纤通道 SAN 相关的控制措施如下：

a) TC-FCSS-G01控制 FCP节点访问

应通过使用访问控制列表 (ACL)、绑定列表和 FC-SP-261]f交换矩阵策略等技术来限制交换机上的服务器访问，从而控制 FCP 节点访问。

b) TC-FCSS-G02 使用基于 FC 交换机的控制措施 应实施基于交换机的控制措施，以：

—使用访问控制列表 (ACL)、绑定列表和 FC-SP-2 交换矩阵策略等技术来限制交换机互连； —建立用于 FC SAN 架构的区域划分，优先采用硬区域划分；

一确定基本区域划分是否足以作为目标环境的安全措施，如果

否，则在供应商支持的情况下，使用更强大的技术，例如 FC-SP-2 区域划分；—禁用未使用的端口；

—谨慎使用默认区域和区域集（遵循最小权限原则）。

c) TC-FCSS-G03配置 FC 设备以满足安全要求

配置交换机、扩展器、路由器和网关（例如FCIP）以互连存储网络时，配置应满足安全要求。

10.9.1提供了基于块的光纤通道存储的指南。

10.8.2.3IP SAN

互联网 SCSI 存储区域网络 (iSCSI)，在 IETF RFC7143 中有描述，[55]是一个基于 TCP 的面向连接的命令/响应协议，用于通过网络访问磁盘、磁带和其他设备。

与 IP SAN 相关的控制措施如下：

a) TC-IPSS-G01 使用 iSCSI 网络访问和协议iSCSI 网络访问和协议应通过以下方式进行控制：

一将 iSCSI 接口与通用 LAN 隔离，以提供安全性和更好的性能；

一当无法使用物理隔离的 LAN 时，使用虚拟局域网 (VLAN)。

基于 IP 的光纤通道 (FCIP)在 IETF RFC 3821,43 中定义，是一种纯光纤通道封装协议。它允许通过基于 IP 的网络互连光纤通道存储区域网络 (SAN) 的各个孤岛，从而形成统一的 SAN。

b) TC-IPSS-G02 使用 FCIP 网络访问和协议FCIP网络访问和协议应由以下方式控制：

—建立 FCIP 实体之间的对等关系，并确保安全策略的统一应用；

一尽可能使用仅供 FCIP 实体使用的私有 IP 网络。

c) TC-IPSS-G03 使用 IPsec 保护 FCIP

IPsec 安全措施（参见10.5.4.3）应与 FCIP 结合实施，具体如下：

—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[42]p提供了关于 iSCSI 和 FCIP 的其他有用信息。10.9.2提供了基于块的 IP 存储指南。此外，IETF RFC 714656]为 IETF RFC 3723 和 IETF RFC 3821 提供了重要的安全更新。

3723 和 IETF RFC 3821。43

10.8.2.4InfiniBand

InfiniBand 是一种低延迟、高带宽的互连技术，它所需的处理开销低，非常适合在单个连接上承载多种类型的流量（集群、通信、存储、管理）。InfiniBand 是一种基于交换机的点对点互连架构，它既可以在印刷电路板上作为组件对组件互连运行，也可以作为机箱对机箱互连运行。连接。

InfiniBand 架构定义了多个用于系统通信的设备：通道适配器（参见注释 1）、交换机、路由器和子网管理器（参见注释 2）。在子网内，InfiniBand 要求每个终端节点至少有一个通道适配器，并且需要一个子网管理器来建立和维护链路。此外，InfiniBand 还要求所有通道适配器和交换机都包含一个子网管理代理，用于处理与子网管理器的通信。

注释 1：通道适配器将 InfiniBand 连接到其他设备。通道适配器有两种类型：主机通道适配器和目标通道适配器。

注 2：子网管理器配置本地子网并确保其持续运行。InfiniBand 要求子网中至少存在一个子网管理器，用于管理所有交换机和路由器的设置，并在链路中断或新链路建立时进行子网重新配置。

与 InfiniBand SAN 相关的控制措施如下：

TC-IBSS-G01 保护 InfiniBand SAN应通过以下方式保护 InfiniBand SAN：

—确保连接到 IB 交换矩阵的所有 IB 主机的安全，因为 IB 交换矩阵的安全性取决于连接到它的安全性最低的 IB 主机；

一 维护物理安全，因为攻击者可以将恶意主机连接到 IB 交换机，从而破坏 IB 架构的安全。

10.8.2.5NVMe over Fabrics

NVM Express(NVMe) [78 由处理器用于通过 PCI Express (PCIe) 总线与非易失性存储器通信，80] 包括各种外形尺寸的 NVMe 固态硬盘 (SSD)。NVMe 旨在利用 SSD 和闪存等高速介质的低延迟和内部并行性。

NVMe over Fabric (NVMe-oFT)[78] 是一种通信协议，用于通过封装 NVMe 管理和输入/输出命令[79]，将远程系统中的 NVMe 目标暴露给客户端，这些命令通过各种称为“光纤通道”的传输方式进行访问。这些光纤通道可以是基于内存的传输方式，例如远程直接内存访问(RDMA)，也可以是基于消息的传输方式，例如 TCP和 FC。NVMe-oFT 指定了三种光纤通道系列：

— NVMe over Fibre Channel(NVMe/FC)；62]—基于 TCP 的 NVMe (NVMe/TCP)；81]

-基于 RDMA 的 NVMe (NVMe/RDMA),821包括：

—基于融合以太网的 RDMA NVMe (RoCE)；

—基于 InfiniBand 的 NVMe；

—基于 iWARP（基于传统以太网）的 NVMe。

与 NVMe-oF 相关的控制如下：

a) TC-NVSS-G01 使用 NVMe-oF 认证

NVMe-oF[Z8] 支持两种高级认证类型（交换矩阵安全通道和带内认证）。应使用其中一种或两种认证机制。

b)TC-NVSS-G02 使用 NVMe/FC 安全控制

NVMe/FC 的安全控制可以包括一些与 FC SAN 控制相同的控制（参见10.8.2.2）。对于 NVMe/FC，应使用以下措施：

—足够的物理安全措施，包括隔离网络；

—FC 分区以划分 FC 结构；

—存储上的 LUN 掩码以限制对特定 LUN 的访问；

-光纤通道设备的身份验证、安全密钥交换以及光纤通道设备之间的安全（即加密）通信。

注意：NVMe-oF[Z8]标准将 NVMe/FC 特有的安全问题交由 FC-SP-261] 技术处理。

该标准包含用于在多个方面增强光纤通道安全性的协议。

c) TC-NVSS-G03 使用NVMe/TCP安全控制

应使用NVMe/TCP的安全控制，包括：

一仅使用 DH-HMAC-CHAP 进行身份验证（需要配置身份验证密钥，每个实体一个）；

—安全通道与身份验证事务连接（其中身份验证事务会动态生成一个临时预共享密钥，供安全通道协议使用）；

单独的安全通道（需要为允许通信的每对实体提供预共享密钥）；

—与 NVMe-oF 解决方案采用适当的通信安全措施，具体如下：

一使用 TLS，不使用任何版本的安全套接字层 (SSL) 协议；

—基于 NVMe-oF 1.1 版的 NVMe-oF 解决方案不使用低于 1.2 版本的 TLS 协议；

一基于 NVMe Base 2.0 版规范[781] 和 NVMe over TCP 1.0 版规范[31] 的 NVMe-oF 解决方案不使用低于 1.3 版本的 TLS 协议。

d) TC-NVSS-G04 使用 NVMe/RDMA 安全控制

NVMe/RDMA 的安全控制应使用 DH-HMAC-CHAP 提供的带内身份验证。

10.8.3 网络附加存储协议

10.8.3.1概述

网络附加存储 (NAS) 是一种数据存储技术，它通过网络为异构客户端提供文件级访问。NAS 允许远程客户端计算机访问物理上位于一台服务器或设备上的文件系统，对用户而言，它就像一个本地文件系统。NAS 系统通常是专门为 NAS 用途设计和构建的，但也可以使用通用服务器计算机。

NAS 系统可以实现为独立的存储服务器，也可以实现为集群式存储系统。存储服务器通过在集群存储服务器上对数据和元数据进行切片或条带化，动态地分配客户端连接（参见图 6）。此外，NAS 系统可以使用一个或多个 SAN 将数据存储在本地或区域外（如图 6 中的 FC SAN-1 和 FC SAN-2 所示）。

服务器

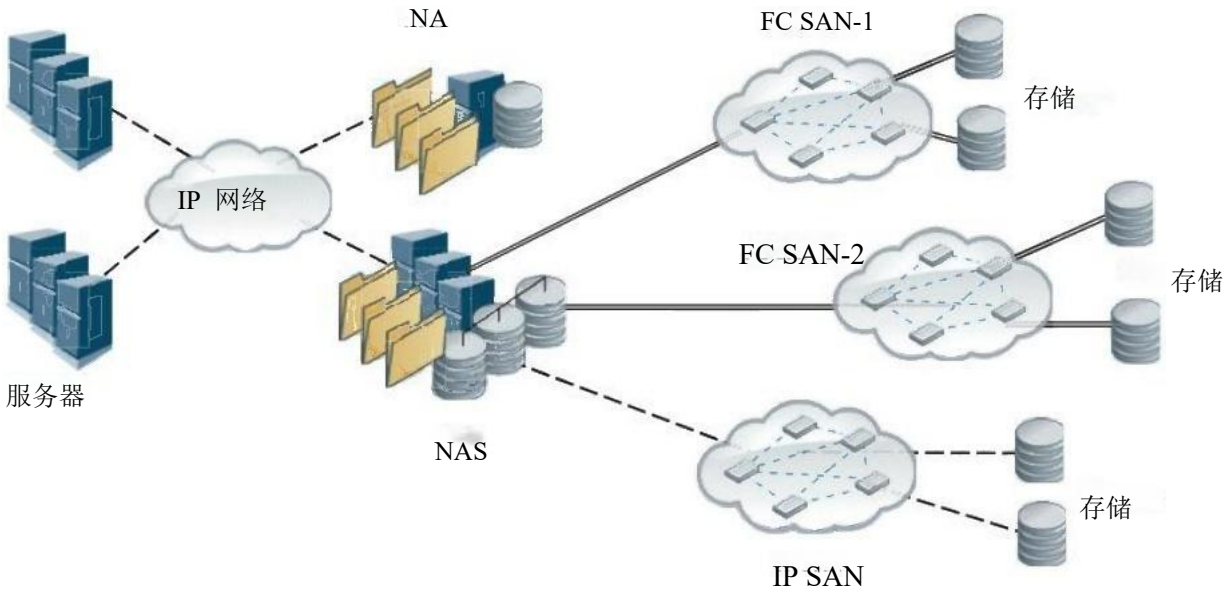

图 6—网络附加存储示例

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)通用互联网文件系统，以及其他技术，例如基于对象的存储和云计算存储。这些协议可以配置为帮助保护 NAS。

有关 NAS 和基于文件的存储的其他控制，请参阅10.10。

10.8.3.2网络文件系统

网络文件系统 (NFS) 是一种客户端/服务器应用程序，它使用基于远程过程调用的协议进行通信。NFS 有多个版本，包括 NFS 版本 3（在 IETF RFC 1813(401) 中指定）、NFS 版本 4（在 IETF RFC 7530 [5Z¹] 中指定）和 NFS 版本 4.1（在 IETF RFC中指定）。

888159). 从安全角度来看，NFS 版本 3 (NFSv3) 的安全性较低，在处理敏感或高价值数据时需要格外小心。

与 NFS 相关的控制措施如下：

a) TC-NASP-G01 使用 NFS 网络访问和协议 应通过以下方式控制 NFS 网络访问和协议：

—仅在必要时启用 NFS，以消除其作为潜在攻击途径的可能性；

—尽可能使用 NFSv4（或更高版本），并限制 NFSv3 的使用；

—通过 IP 地址过滤客户端和管理访问，以进一步保护安全。安全性。

b) TC-NASP-G02 使用加密保护 NFS

NFS 客户端数据访问应使用加密（例如 IPsec 或 TLS）。

10.8.3.3服务器消息块 (SMB)

SMB 3 是一种旨在为客户端系统提供开放的跨平台机制的协议，客户端系统可以通过网络向服务器系统请求文件服务。它基于标准 SMB 协议，该协议被广泛用于运行各种操作系统的个人计算机和工作站。

与 SMB 相关的控制措施如下：

TC-NASP-G03 使用 SMB 网络访问和协议

以下网络指南适用于基于 SMB 的 NAS，应予以遵循：

一使用更高版本的 SMB 协议；

—关闭低安全性的会话协商协议，改用 Kerberos；

—保持最新的补丁级别；

一使用 SMB 签名；

—安全地维护目录服务；

一尽可能使用从叶子域到父域的单向信任；

一通过以下方式控制 SMB 网络访问和协议：

—仅在必要时启用 SMB。这消除了它作为攻击者可能利用的攻击向量的可能性；

—必要时加密客户端数据访问。

10.9 基于块的存储

10.9.1 光纤通道 (FC) 存储

光纤通道存储系统使用专用网络（参见10.8.2.2）向计算机提供基于块的存储资源。这些资源通常以逻辑单元（逻辑存储）和磁带设备（包括虚拟磁带）的形式存在。

与 FC 存储相关的控制措施如下：

a)TC-BBFC-G01 使用 FC LUN 掩码和映射

应使用 LUN 掩码和映射（全球端口名称过滤）以及其他访问控制机制来限制对存储的访问。

b)TC-BBFC-G02 使用 FCP 进行 SCSI 安全措施 应使用 FCP 进行 SCSI 安全措施，包括：

一使用 FC-SP-2 AUTH-A61 对所有服务器和交换机进行相互认证，尽可能利用集中式认证服务；

- 使用 ESP_Header 加密离开受保护区域（例如，物理控制的数据中心）的光纤通道连接。

注1：可以使用 ESP_Header 可选标头来提供光纤通道帧完整性或机密性，

c) TC-BBFC-G03 使用静态数据加密进行 FC 存储

静态数据加密措施（参见10.5.5）应用于：

一保护记录在 FC 存储设备或介质上的敏感或高价值数据的机密性；

注 2：FC 存储生态系统内的加密提供介质级保护，可以作为安全网，保护通常由服务器、应用程序等加密的数据，这些数据通常作为主要保护形式。

— 使用加密擦除快速删除 FC 存储上的数据（参见10.6.5）。

d)TC-BBFC-G04 使用存储清理技术对 FC 存储进行清理存储清理措施（参见 10.6）的形式如下：

—介质对齐清理（参见10.6.3）应用于 FC 存储介质和存储敏感及受监管数据的存储设备；

—逻辑清理（参见 10.6.4）应用于虚拟化 FC 存储（参见 10.16.1），尤其是在无法确定实际存储设备和介质的情况下。

10.9.2 IP 存储

与 FC 存储不同，IP 存储使用 TCP/IP 网络（参见10.8.2.3），特别是iSCSI，向计算机提供基于块的存储资源。

与 IP 存储相关的控制如下：

a) TC-BBIP-G01 过滤 iSCSI 发起程序访问

应根据源 IP 地址和协议过滤 iSCSI 发起程序访问。

b)TC-BBIP-G02 使用 iSCSI 安全措施

应使用 iSCSI 安全措施，包括：

—双向 CHAP 认证，对发起方和目标方均使用随机挑战（即不重复）；

一当敏感或高价值数据可能暴露时，使用 IPsec 保护通信通道。

10.5.4.3)；

—互联网存储名称服务 (iSNS)、SLP、DNS 基础设施，并配备适当的安全控制措施，以避免间接攻击。

c) TC-BBIP-G03 对 IP 存储使用静态数据加密

静态数据加密措施（参见10.5.5）应用于：

—保护记录在 IP 存储设备或介质上的敏感或高价值数据的机密性；

注：FC 存储生态系统中的加密提供介质级保护，可作为数据安全网。通常情况下，服务器、应用程序等会对其进行加密，作为主要保护形式。

— 使用加密擦除（参见 10.6.5）快速清除 IP 存储上的数据。。

d)TC-BBIP-G04 使用存储清理技术进行 IP 存储 存储清理措施（参见10.6）的形式如下：

-介质对齐清理（参见10.6.3）应用于 IP 存储介质和存储敏感及受监管数据的存储设备；

-逻辑清理（参见10.6.4）应用于虚拟化 IP 存储（参见10.16.1），尤其是在无法确定实际存储设备和介质的情况下。

10.10 基于文件的存储

10.10.1 概述

与基于文件的存储（通常为 NAS）相关的安全控制分为以下几类：

一授权控制，例如 ACL，用于限制用户对 NAS 设备提供的文件和文件夹资源的访问；

—静态数据加密；

一、身份验证控制，例如 Kerberos，用于验证尝试访问 NAS数据的用户的身份。

10.10.2 基于 NFS 的 NAS

这种类型的存储本质上是一个连接到 LAN 的文件服务器，它使用网络协议 NFS 来提供文件（参见10.8.3.2）。它由一个实现文件服务的引擎和一个或多个存储设备组成，数据存储在这些设备上。NAS 系统也可以连接到节点，在这种情况下，NAS 系统就像 SAN 上的任何其他服务器一样（例如，

提供对存储的访问和无 LAN 备份）。基于 NFS 的 NAS 系统可以采用多种不同的形式（例如，从简单的 NAS 服务器到高度可扩展的集群），而且它们往往具有很高的可扩展性。针对大量并发文件访问进行了优化。

与基于 NFS 的 NAS 相关的控制如下：

a) TC-FBNF-R01 应用 NFS 访问控制

应将访问控制应用于 NFS 导出的文件系统，以：

—尽可能采用用户级身份验证（例如，使用 Kerberos V5 的 NFSv4）；

—配置 NFS 服务器，以便为授权用户显式导出文件系统；

一配置 NFS 服务器以最小所需权限导出文件系统；

一避免授予 root 或管理员对网络文件系统上文件的访问权限；

—确保正确分配 NFSv4 ACL（访问控制列表）；

一对 NFSv3 使用 Kerberos 身份验证；

一在适当情况下，使用 Kerberos 安全模式和私有模式对 NFS 流量进行签名和加密。

b)TC-FBNF-R02 限制 NFS 客户端行为

NFS 客户端行为应限制为：

—尽可能过滤客户端对 NFS 共享的访问；

一禁止 NFS 客户端在导出的文件系统上执行期间提供临时提升权限的程序。

c) TC-FBNF-G01 保护 NFS 服务器上的数据NFS 服务器上的数据应通过以下方式保护：

一确保导出的文件系统位于其自身的独立分区中，以防止攻击者对系统造成损害

写入导出的文件系统直至其已满；—必要时对静态数据进行加密；

—禁止将管理文件系统导出到 NFS；

一防范恶意软件（例如病毒、蠕虫和 rootkit）；

一持续监控放置在 NFS 共享中的内容以及相关的访问控制。

10.10.3 基于 SMB 的 NAS

与基于 NFS 的 NAS（参见10.10.2）类似，基于 SMB 的 NAS 是一种连接到 LAN 的文件服务器，用于提供文件服务，但两者有所不同

的区别在于它使用的网络协议 SMB（参见10.8.3.3）。与基于 SMB 的 NAS 相关的控制措施如下：

a) TC-FBSM-R01 最低可接受的 SMB 协议

对于基于 SMB 的 NAS,应使用 SMB 版本 3 或更高版本,并禁用所有以前的版本。b) TC-FBSM-R02 应用 SMB 访问控制

应将访问控制应用于 SMB 导出的文件系统，以：

—禁用对 SMB 共享和 NAS 设备的未经身份验证的访问（即限制匿名访问）；

—禁用 Guest 和 Everyone 对所有 SMB 共享的访问；

—通过集中式机制（RADIUS，轻量级目录访问协议）实现身份验证和访问控制。

c) TC-FBSM-R03 限制 SMB 客户端行为

应通过为客户端和 NAS 设备启用 SMB 签名来限制 SMB 客户端的行为。

d) TC-FBSM-G01 保护 SMB 服务器上的数据 应通过以下方式保护 SMB 服务器上的数据：

—启用 SMB 审计可能；

—持续审查 SMB 共享中的内容和相关的访问控制；—必要时对静态数据进行加密；

—防范恶意软件（例如病毒、蠕虫和 rootkit）；

—使用具有强身份验证（Kerberos）的 SMB。

10.11 云计算存储

10.11.1 云计算存储安全

云计算存储产品既有专有的，也有基于标准的，它们通常提供复制功能（例如，在系统上镜像部分或全部存储）、备份和恢复功能、长期保留功能（例如，归档）以及多系统同步功能（例如，允许用户在多个可能不同类型的设备上同步数据）。然而，除非确信相关的安全威胁和挑战已得到解决，否则个人和组织在将数据委托给云计算存储时会犹豫不决（有关云计算的有用概述，请参阅参考文献[77]）。安全威胁和挑战）。

部分云计算实现是基于对象的，并且通常依赖于HTTPS（基于 TLS 的 HTTP）来保护底层通信。可以指定其他安全功能，但实际实现的功能与最终使用的功能之间可能存在显著差异。

与保护云计算存储相关的控制措施如下：

a) TC-CCSS-G01 使用传输安全进行云事务处理

所有事务都应使用传输安全协议，例如 IPsec 或传输层安全协议 (TLS)（参见）

10.5.4)。

b) TC-CCSS-G02 使用静态数据加密保护云存储

应使用静态数据加密（以及适当的密钥管理流程）来防止未经授权的访问方（例如云服务提供商人员、其他租户和攻击者）。

c) TC-CCSS-G03 使用强身份验证来获取云存储访问权限

应确保用户注册安全，并使用强身份验证来保护数据访问。

d) TC-CCSS-G04 使用访问控制来保护云存储上的数据

建议使用访问控制来防止其他租户的未经授权访问，同时为获准访问数据的用户提供适当的访问权限。

e) TC-CCSS-G05 使用存储清理保护云存储

应使用提供的存储清理功能来消除敏感数据。来自云计算存储。

注意：在某些司法管辖区，诸如删除权或被遗忘权之类的隐私要求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 10.16中的指导也可能适用。

10.11.2 CDMI 安全性

基于ISO/IEC 17826 中包含的云数据管理接口(CDMI)规范的云计算存储是一种基于对象的存储技术，它使用RESTfulHTTP接口。CDMI中的安全措施可概括为传输安全,用户和实体身份验证、授权和访问控制、数据完整性、数据和介质清理、数据保留、恶意软件防护、静态数据加密以及安全能力查询。

除了传输安全和安全能力查询（用于确定支持哪些功能的机制）这两项必须实施（但使用始终是可选的）之外，其他安全措施在不同的实现中可能存在显著差异。

与CDMI安全相关的控制措施如下：

a) TC-CDMI-R01 所有CDMI事务均使用TLS

所有CDMI事务均应使用传输层安全协议(TLS)（参见10.5.4.2）。

b)TC-CDMI-R02 对所有 CDMI 实体进行相互认证

CDMI 实体（服务器证书和客户端 HTTP 基本认证）应进行认证。

c) TC-CDMI-G01 使用 CDMI 功能查询评估安全性

应使用 CDMI 功能查询来确定云服务提供商的 CDMI 实现的安全功能是否充分，以识别其提供的安全功能。

d)TC-CDMI-G02 使用 CDMI 域

应使用 CDMI 域来提供到外部身份验证提供商的身份验证映射。

e] TC-CDMI-G03 将 CDMI 日志记录集成到审计日志中

应启用 CDMI 安全日志记录，并将安全事件数据包含在相应的日志记录队列中。应定期及时地检索。

f) TC-CDMI-G04 配置 CDMI 保留策略以使自动删除与策略保持一致

自动删除功能（CDMI 删除）应与组织的数据保留策略保持一致。

g) TC-CDMI-G05 在使用 CDMI 保留功能之前，验证解除 CDMI 保留的能力

在使用 CDMI 保留功能之前，应了解解除 CDMI 保留的流程和机制。

h) TC-CDMI-G06 对 CDMI 存储使用静态数据加密

应使用静态数据加密措施来保护敏感和高价值数据。

i) TC-CDMI-G07 对 CDMI 存储使用存储清理

应使用提供的存储清理措施从云服务提供商的存储中清除敏感数据。

10.12 基于对象的存储

基于对象的存储是一种用于处理大量非结构化数据的数据存储架构。离散的数据单元（对象）存储在结构扁平的数据环境中。每个对象都是一个简单的、自包含的存储库，包含数据、元数据（与对象关联的描述性、可自定义信息）以及唯一的标识 ID 号（而不是文件名和文件路径）。应用程序可以使用元数据或 ID 来定位和访问对象。

对象存储系统中的对象（数据）通过 API 访问。对象存储的原生 API 通常是基于 HTTP 的 RESTful API（也称为 RESTful Web 服务）。

与基于对象的存储相关的控制如下：

a) TC-OBSS-G01 对基于对象的存储事务使用传输安全协议

所有基于对象的存储事务都应使用传输安全协议，例如 IPsec 或传输层安全协议 (TLS)（参见10.5.4）。

b) TC-OBSS-G02 对基于对象的存储使用静态数据加密

应使用静态数据加密（对象级或租户级）来防止未经授权的方（例如服务提供商人员和攻击者）访问。

c) TC-OBSS-G03 为基于对象的存储启用数据不可变性

应启用适当的数据不可变性保护措施来防止恶意意外删除或加密（例如勒索软件）。

d) TC-OBSS-G04 使安全机制与租户保持一致基于对象的存储

安全机制（例如身份验证和密钥管理）应与基于对象的存储上的租户保持一致。

e) TC-OBSS-G05 对基于对象的存储使用存储清理

提供的存储清理功能应用于从基于对象的存储中清除敏感数据。

10.13 数据缩减

作为日常业务，组织通常会尝试减少存储和传输的数据量，以降低成本。两种比较常见的方法是数据压缩和数据去重。数据压缩旨在通过使用已知算法对数据进行编码来减少数据量，从而生成比未编码表示占用更少存储空间的数据表示。另一方面，数据去重尝试用对共享副本的引用来替换数据的多个副本。这两种技术可以结合使用，以最大限度地减少数据量。

注意：压缩算法包括有损压缩（会丢失部分原始信息）和无损压缩（保留原始数据的全部内容），但在存储行业中，通常只使用无损算法。应用特定的压缩算法可能会影响数据量。如果初始条件（例如历史缓冲区）相同，对多个数据实例使用相同的压缩算法可能会导致编码/压缩后的数据完全相同。

数据压缩通常与磁带存储结合使用，以减少备份等操作所需的磁带数量。此外，压缩还可以作为远程复制中使用的网络网关的组成部分，以降低BCM支持所需的带宽。数据压缩通常在硬件中执行，因此需要格外注意，以确保编码后的数据可以稍后解码（例如，当磁带被不同的磁带驱动器读取或压缩数据被网络网关接收时）。

数据去重可以在存储基础架构中的各种不同位置进行，包括文件系统级别、存储网络内部以及存储设备级别。

数据缩减技术本身并不代表安全机制。但是，它们的存在可能需要对存储安全活动进行调整。

与数据缩减相关的控制措施如下：

a) TC-DRDC-G01 加密前使用压缩

当加密与压缩结合使用时，应在加密前应用压缩，因为密文压缩效果不佳；在另一端应使用相反的顺序（即先解密后解压缩）。

b) TC-DRDC-G02 加密前使用去重

当加密与去重一起使用时，应在记录数据之前先进行去重，因为去重通常对密文无效；读取数据时应使用相反的顺序。

c) TC-DRDC-G03 多次数据缩减和加密的正确顺序

当压缩和去重与加密一起使用时，使用顺序应为：

—记录数据之前先进行去重、压缩和加密（读取数据时使用相反的顺序）；或

— 记录数据之前先进行压缩、去重和加密（读取数据时使用相反的顺序）。

d)TC-DRDC-G04 使用与BCM兼容的数据缩减方法

压缩或去重可能会影响BCM的实施，因此应将其纳入BCM解决方案的设计、文档编写和测试中。

10.14 数据保护和恢复

10.14.1 总则

从存储角度来看，数据保护是指保护重要数据免遭损坏或丢失的过程。数据恢复是指恢复已丢失、意外删除、损坏或无法访问的数据的过程。采用数据保护机制和流程的组织通常会以能够快速完整地恢复数据的方式实施这些机制和流程（有关存储系统和生态系统中的数据保护的有用概述，请参阅参考文献[72]）。由于对数据可用性和完整性的依赖性日益增强，许多组织采用一系列数据保护机制，例如备份（参见和 10.14.2）和复制（参见10.14.3），以提高数据弹性。然而，遗憾的是，人们往往更关注备份和复制数据集的创建，而不是利用它们从问题中恢复的能力。所有数据保护解决方案都可以被视为数据恢复。机制。

TC-PROT-G01 设计用于快速恢复的数据保护机制

数据保护机制（例如备份和复制）的设计应以快速恢复为目标，而不仅仅是数据保存。这些设计中应包含具体的恢复时间目标 (RTO) 和恢复点目标 (RPO)。

10.14.2 存储备份

虽然由于硬件和软件的可靠性提高，技术故障导致的数据丢失已不那么常见，但病毒和勒索软件带来的威胁却越来越多。这种数据丢失的风险迫使组织使用一种称为存储备份的技术。这些备份通常采用以下形式：

—完整备份，将目录中的所有文件复制到存储介质，而不管之前的备份如何；

—增量备份，仅将目录中自上次备份（完整备份或增量备份）以来已更改的文件复制到存储介质；

—差异备份，即将目录中自上次完整备份以来所有已更改的文件复制到存储介质。

传统备份（完整备份、增量备份或差异备份）面临的主要挑战是，它们需要移动大量数据，例如TB级或PB级数据。移动大型数据集是一个耗时的过程，最终可能导致超出组织所需的恢复时间。

ISO/IEC 27002:2022 8.13 提供了有关信息备份的有用信息。

与存储备份相关的控制措施如下：

a) TC-PROT-G02 安全地使用数据备份措施和操作备份安全性应：

—确保备份方法（特别是针对业务/任务关键型数据）与其相关的恢复方法保持一致。策略；

—确保备份方法提供充分且适当的保护，防止未经授权的访问（例如加密或用户验证）；

—建立由受信任的个人（和供应商）组成的存储介质处理链；

—实施备份验证，以证明恢复要求得到满足。

TC-PROT-G03 使用网络攻击恢复备份

虽然许多组织出于灾难恢复和业务连续性（非恶意）目的实施备份，但一些组织也在执行特殊备份以协助应对网络攻击（例如勒索软件攻击）。除了常规备份安全措施外，网络攻击恢复备份还应：

—不应向普通 IT 人员开放，而应仅向经过特别授权的极少数人员开放；

—保留更长时间，以便进行调查并处理那些潜伏已久、直到很久以后才被触发的攻击；

—异地存储，并与生产存储备份的存储位置分开；

— 定期使用独立的完整备份副本（即不依赖于生产基线数据）；

—恢复到隔离的暂存（或物理隔离）环境中，而不是直接恢复到目标主机或应用程序；

—使用不可变存储。

10.14.3 存储复制

复制是指创建生产数据的副本，使其可以立即使用，无需进一步移动或更改。复制是一个复杂且成本高昂的过程，仅适用于有限的场景。由于复制可以实现零数据丢失，因此它已成为灾难恢复解决方案的领导者。然而；复制并不能防止数据被删除、损坏或遭受勒索软件攻击。因此，尽管复制效率很高，但它不能替代备份。

与存储复制相关的控制措施如下：

TC-PROT-G04 安全地使用数据复制措施和操作 复制安全应：

-确保复制方法（特别是针对业务/任务关键型数据）与其相关的可靠性、容错性或性能要求相符；

-确保复制方法提供足够的保护措施，防止未经授权的访问（例如，传输中的数据加密）。

10.14.4 存储快照

存储快照可以是存储卷、文件或数据库在特定时间点的状态。发生故障时，用户可以从故障发生前的最新快照（或之前保存的任何其他快照）恢复数据。与涉及数据副本的备份不同，快照维护指向数据的指针，并记录对数据的更改（删除、添加、移动等）。快照通常单个占用的存储空间不多，但其总容量可能会增长，尤其是在删除了大量数据块/文件的情况下，因此供应商通常会限制可保留的快照数量。

与存储快照相关的控制措施如下：

TC-PROT-G05 将快照与备份结合使用

应将快照与备份策略结合使用，以提供更频繁的保护（以分钟或小时为单位），而备份则用于日常保护。快照的间隔应基于从特定时间点恢复的粒度要求。快照保留期应允许进行一到两次备份。在此期间（即快照被删除之前）。

TC-PROT-G06 使用快照安全性

快照安全性应：

一确保快照方法（特别是对于业务/任务关键型数据）与其相关的恢复策略保持一致；

—确保快照受到保护，免受更改（例如，只读）；

一确保快照方法提供足够的保护，防止未经授权的访问（例如

加密）。

10.15 数据归档和存储库

10.15.1 总则

虽然有人认为数据归档只是数据存储库的一种特殊类型，但存储库和归档之间通常存在侧重点不同。两者都具备访问和保存功能，但存储库通常侧重于访问，而归档通常侧重于保存。从存储和安全角度来看，这种差异对保护数据所需的底层技术和控制措施有着重大影响。

10.15.2 数据归档

10.15.2.1 概述

ISO 14721 指出，“归档”一词已被用来指代各种各样的存储和保存功能及系统。此外，传统归档是指保存由政府机构、机构或公司生成或为其生成的记录，供公众或机构访问的设施或组织。私有社区。归档通过取得记录的所有权、确保访问社区能够理解这些记录，以及管理这些记录以维护其信息内容和真实性来完成这项任务。

归档是数据对象的集合，代表数据的正式工作副本，但与更活跃的生产数据分开管理，其目的是为了长期保存和降低成本。此外，归档通常用于存储具有特定合规性义务的数据集，并且通常用于审计或分析，而不是用于应用程序恢复。另外，保留期限可能有所不同（例如短期、中期和长期），但归档应确保适当的完整性、不可篡改性、真实性、机密性和来源。

ISO/TR 18492 将长期保存定义为电子文档信息作为可访问且真实的证据保存的时间段，范围从几年到几百年不等。保存期限通常由法规遵从性、法律要求和业务需求决定，因此不同组织的保存期限可能差异很大。

与存储档案相关的控制措施如下：

a)TC-DARS-G01 解决存储档案中的关键保存问题

组织在制定长期保存策略时，应考虑并解决 ISO/TR 18492 中包含的以下存储档案关键问题。

一可读的电子文档信息。构成电子文档信息的比特流应可在最初创建、当前存储和当前访问该信息的计算机系统或设备上访问。它可用于存储，或用于将来存储；介质过时和数据格式也是需要考虑的因素。

一 可理解的基于电子文档的信息。基于电子文档的信息的可理解性取决于比特流实际代表的内容以及处理软件基于此信息采取适当行动的能力。

一可识别的电子文档信息。文档信息应以用户和信息系统能够根据名称或 ID 号等唯一属性区分信息对象的方式进行组织、分类和描述。便于搜索和检索也是需要考虑的因素。

一 可检索的基于文档的信息。离散的信息对象（或其部分）可以被检索并显示。可检索性通常依赖于软件，因为它需要将信息对象的逻辑结构（例如数据字段或文本字符串）与其物理存储位置链接起来的键或指针。

一 可理解的基于文档的信息。向计算机和用户传达信息，超越文档内容本身，包括创建和使用上下文（即元数据）以及与其他文档之间的关系。

一真实的电子文档信息。确保信息与其声称的内容相符，即信息不会随着时间的推移而被更改、篡改或以其他方式损坏。

b) TC-DARS-G02 采用安全服务解决档案的证据性问题

具有潜在证据相关性的档案应解决数据真实性、来源和监管链方面的问题，包括保留、保护和维护大量元数据。组织应使用 ISO 14721 确定的以下安全服务来保护数据和元数据。

—身份/认证服务用于确认信息系统资源使用请求者的身份。此外，认证也适用于数据提供者。认证服务应在会话开始时或会话期间进行。

一 访问控制服务防止未经授权使用信息系统资源。此服务还防止以未经授权的方式使用资源。此服务应应用于对资源访问的各个方面（例如，对资源的通信访问、对信息/数据资源的读取、写入或删除、对处理资源的执行），或应用于对资源的所有访问。

一数据完整性服务确保数据不会被以未经授权的方式更改或销毁。此服务适用于永久数据存储中的数据和通信消息中的数据。

数据保密服务确保数据不会被提供给未经授权的个人或计算机进程。此服务可应用于允许用户与信息系统交互的设备。此外，此服务还可以确保无法观察通信资源的使用模式。

—不可否认服务确保参与信息交换的实体不能否认其参与其中。此服务可以采用以下两种形式中的一种或两种。首先，向数据接收方提供数据来源证明。这可以防止发送方试图否认发送数据或其内容。其次，向数据发送方提供数据交付证明。这可以防止接收方随后试图否认接收数据或其内容。

这些安全服务应在数据和元数据存储以及与档案库之间传输的过程中应用。同样重要的是，在调整/更换安全服务/控制措施时，应谨慎操作，以避免档案数据遭受攻击或泄露（即风险）。

在许多标准和出版物中，档案库的隐私问题通常没有被直接提及。然而，随着世界各地隐私（个人身份信息保护）法规的日益增多，这是一个需要重视的重要方面。

溯源性和真实性是大多数档案库的基本要素，这意味着需要妥善处理元数据。为了满足证据要求，监管链措施也可能必不可少，这可能会使所使用的档案解决方案的性质变得复杂（例如，基于云计算的存储可能无法提供所需的详细信息）。

许多归档系统都关注于使用完整性验证方法来“证明”数据未被更改（真实性）。另一种策略是采用不可变性措施（例如 WORM 存储）来防止更改。

10.15.2.2中短期归档

许多组织必须将数据保留的时间短于传统归档（少于 10 年）。通常，保留期限的驱动因素是基于法律、法规或法令要求，其中也包括安全条款。未能满足这些要求可能会给组织带来重大责任。

在中短期保留期内成功保留和保存数据可能需要采用数据保护、业务连续性管理以及数字保存和管理实践。具体措施通常与所保留数据的价值、各种因素造成的损失风险以及在保留期内可接受的损失量相匹配。从存储角度来看，这些中短期数据保留方案通常跨越一个或多个技术世代，并且需要捕获和保留相关的元数据。

与中短期归档相关的控制措施如下：

a) TC-DARS-G03 创建归档数据中的多个物理或逻辑副本

应创建并保存数据的多个物理或逻辑副本；归档数据不应依赖于生产或灾难恢复基线数据。副本的组织应尽可能独立（例如，地理位置、管理/运营和功能）。平台/操作系统），其数量根据数据的价值和风险承受能力而定。

注意：需要考虑的重要方面是数字归档流程的质量和特性，而不是副本的数量。

b)TC-DARS-G04 对归档中保留的数据进行定期完整性审计

应按照既定计划执行完整性审计，查找显性和隐性故障（例如完整性检查）及其造成的损害。应使用其他副本中的良好数据修复损坏的数据，以免损害扩散。

c) TC-DARS-G05 使归档中保留的数据访问控制符合法律和监管要求

作为履行与数据访问相关的法律和监管义务（例如保护个人身份信息）的一部分，访问控制方案应足够稳健，即使义务随时间变化，也能防止不当访问。

d) TC-DARS-G06 使用问责制和可追溯性措施对档案数据访问进行监管

应实施问责制和可追溯性措施，并定期检查其是否充分有效。所有对敏感或高价值数据的访问都应记录在审计日志条目中。

e) TC-DARS-G07 使用机制解决档案中保留的数据的真实性、来源和监管链问题

用于解决数据真实性、来源和监管链问题的机制，特别是对于证据数据自然规律应该得到贯彻执行。

f) TC-DARS-G08 确保归档数据密钥生命周期管理的适当性

如果使用加密，密钥和密钥材料应进行归档或托管。应在建议的加密周期内或底层加密算法更换时重新生成密钥。

10.15.2.3长期归档

由于传统存储组件的使用寿命较短且可靠性有限，数据会随着存储介质的老化而损坏。对于相关人员来说，这个问题已经得到了较为充分的理解。参与数据长期保存（例如，管理数据归档）的人员。以下标准对此进行了阐述，这些标准适用于存储基础设施：

—ISO/TR 10255;

—ISO/TR 18492;

—ISO 16175-1;

—ISO/TS 16175-2.

长期归档存储系统引入了非归档存储系统通常不存在的完整性、身份验证和隐私威胁。此外，数据的长期保存也为攻击者提供了更大的攻击窗口，使其能够尝试攻破安全系统。对于归档存储，攻击者可能有数十年的时间进行攻击（慢速攻击）。

与短期至中期归档相关的控制措施（参见 10.15.2.2）也适用于长期归档。其他针对长期归档的特定控制措施也可能适用。

与长期归档相关的控制措施如下：

a) TC-DARS-G09 主动检查长期归档存储的数据完整性

归档存储采用一次写入、有限读取的模式，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进行检查。

b) TC-DARS-G10 在长期归档存储技术更新期间升级安全性

将归档数据迁移到更新的存储技术时，也应升级提供增强安全措施的安全功能，以更好地保护新位置的数据。

c) TC-DARS-G11 管理长期归档存储的用户和访问权限

由于长期归档中的数据可能为了确保数据所有者去世后数据仍然有效，一个安全的归档存储系统应该能够验证新用户的身份，并建立他们与现有用户所关联的资源和数据之间的关系。

d)TC-DARS-G12 在长期归档存储中维护数据机密性措施

保密机制（例如加密和密钥共享）应在存储数据的用户完全不在场的情况下也能正常运行（例如，获得数据读取权限的新用户也应具备解密数据的能力）。

e) TC-DARS-G13 长期归档存储的安全日志保留

安全日志记录应足够完整且保存时间足够长（以数十年为单位），以便有助于检测缓慢攻击并维护攻击历史记录，从而用于制定调整数据保护措施的决策。

f) TC-DARS-G14 检测和处理长期归档存储的入侵事件

归档系统应立即处理任何入侵事件，或维护入侵事件历史记录，以便智能地安排纠正措施。

g) TC-DARS-G15 确保数据缩减技术不会影响长期归档存储的数据完整性归档存储

数据缩减技术（例如压缩和去重）的使用方式应避免损害数据完整性（例如，将其分解为与数据缩减技术无关的副本）。

10.15.3 数据存储库

随着数据对业务决策的重要性日益凸显，对能够收集、存储和分析数据的平台的需求也随之增长。数据存储库就是这样一种存储实体，它可以帮助整合和管理关键的企业数据。

这些数据存储库的常见形式包括数据仓库、数据湖、数据集市和数据立方体。数据存储库可能会引入额外的复杂性，包括：

—数据存储库通常包含异构组件，而这些组件并非从一开始就设计了单一的安全方案；

—数据存储库越来越多地涉及一个或多个流式数据源，这些数据源与静态数据结合使用，从而产生独特的安全和隐私场景；

-最初并非设计用于一起使用的多个数据源可能会损害隐私、安全或两者兼而有之；

—在数据存储库中，真实性、上下文、来源和管辖权问题可能会被大大放大；—数据的保存时间可能会超过旨在保护它的安全措施的生命周期；

—由数据存储库促成的跨境数据流可能会给组织带来合规性挑战，因为数据会跨越国界流动。

与数据存储库相关的控制措施如下：

TC-DARS-G16 数据存储库的安全控制措施

除10.15.2中的控制措施外，数据存储库还应采用以下措施：

— 不得向未经授权的个人、实体或流程提供或披露信息；—应在数据的整个生命周期内维护数据的准确性和完整性；

—应确保在授权实体提出要求时，能够访问和使用个人信息；

—个人信息的使用、保留和披露（包括转移）应限于为实现特定、明确和合法目的所必需的范围。

此外，信息库的目的应符合适用法律，并具有合法依据。个人信息的收集应在适用法律的范围内，且为实现特定目的所绝对必要。

大数据通常与数据存储库结合使用，因此 ISO/IEC 20547-4 中的安全和隐私指南可能适用。

10.16 虚拟化

10.16.1 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数据的物理存储系统、设备或介质分离，从而使这种逻辑到物理的关系能够随时间变化，并可以掩盖物理实体的细节。例如，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内容呈现为单个镜像逻辑卷，并且能够在其中一个原始驱动器发生故障后重建镜像卷以使用另一个磁盘驱动器。另一个例子是自动分层功能存储阵列可以根据访问模式的变化（例如，将访问频率更高的数据移动到性能更高的驱动器）来更改数据存储所在的驱动器。

存储虚拟化的存在是控制设计和应用中的一个重要考虑因素。控制可以应用于逻辑存储实体或物理存储实体。逻辑存储实体上的控制通常不受数据物理迁移的影响。而对物理实体应用控制则可能涉及所有可能存储数据的物理实体（例如，存储系统、设备、介质）。这种扩展的覆盖范围对于避免数据迁移导致控制失效的情况是必要的。

已绕过与存储虚拟化相关的控制措施如下：

a) TC-SVSS-G01 将存储网络控制措施应用于参与存储虚拟化的实体

当存储虚拟化在分布式实体域中存储或重新定位数据（例如，存储在多个存储系统之一上并随时间重新定位的数据）且使用存储网络时，应将适当的存储网络控制（参见和10.8）应用于整个域。如果网络控制仅应用于域的子集，则当数据重新定位或受该控制约束的新数据存储在未应用该控制的实体上时，网络控制可能会被绕过。

b) TC-SVSS-G02 限制或阻止对非虚拟化物理元素的直接访问

如果存储虚拟化暴露了已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），则应应用控制措施来限制或阻止对非虚拟化物理元素的直接访问，因为这种访问不等同于访问虚拟化存储。

c) TC-SVSS-G03 使用安全控制措施保护虚拟化存储中的数据

虚拟化存储及其底层物理存储实体（例如系统、设备和介质）应使用适当的控制措施来保护存储在其上的最敏感数据。这些控制措施应包括：

—存储清理（参见 10.6）；

—静态数据加密（参见 10.5.5）。

d) TC-SVSS-G04 满足虚拟化存储的可用性、机密性和隐私性服务级别目标

应满足虚拟化存储适当的面向安全的服务级别目标，包括：

—使存储基础架构的可用性目标与应用程序需求相匹配；

—使存储基础设施的机密性和隐私要求与存储的数据类型相匹配。

e) TC-SVSS-G05 确保虚拟化存储满足多租户安全要求 应酌情满足多租户安全要求（参见 10.17）。

10.16.2 虚拟化系统的存储

服务器虚拟化将典型操作系统的资源共享访问扩展到一种模型，在该模型中，虚拟化软件提供了多台计算机、硬盘驱动器、打印机等的假象。物理服务器通常运行一个虚拟机管理程序，该程序负责创建、释放和管理客户操作系统或虚拟机(VM) 的资源。这些客户操作系统被分配一部分物理服务器资源，通常情况下，客户操作系统除了虚拟机管理程序分配给它的资源外，不会感知到任何其他物理资源。

当使用存储系统和基础架构来支持虚拟化服务器时，通常需要格外注意，以确保数据可用，但又不会过度暴露于潜在的数据泄露风险中。

虚拟化系统存储相关的控制措施如下：

a) TC-SVSS-G06 控制虚拟机对存储网络的访问

应通过服务器虚拟化（虚拟机管理程序）软件中的访问控制来控制虚拟机对存储网络的访问。

b) TC-SVSS-G07 控制虚拟机在物理服务器之间的迁移/移动

应控制基础架构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：

一将虚拟机从低风险（更可信）域迁移到高风险（更不可信）域，可能会暴露服务器包含或允许处理的敏感数据，除非其配置已进行适当的加固；

一 相反，当虚拟机从高风险（更不可信）域迁移到低风险（更可信）域时，其加固配置可能会干扰正常运行，除非其配置已针对低安全域进行适当的更改；

一虚拟机可能会迁移到已被入侵的物理服务器，从而使数据面临风险。

10.17 安全的多租户

ISO/IEC 22123-1 中定义的多租户侧重于多租户对资源的使用，使得租户的计算和数据彼此隔离且无法访问。安全的多租户在此概念的基础上，增加了安全控制措施，以明确防止数据泄露，并允许验证这些控制措施的状态（例如，它们是否处于活动状态）以及验证这些控制措施（即，确保它们有效）。

与安全的多租户相关的控制措施如下：

a)TC-SMTS-G01为多租户提供安全隔离保证

在考虑安全的多租户时，必须考虑租户的视角。 （包括）

他们的管理员）。因此，一个安全的多租户解决方案应该在提供安全隔离保障的同时，还能提供共享资源的管理和灵活性优势，从而确保：

—任何租户都无法确定其他租户的存在或身份；

—任何租户都无法访问其他租户的动态数据（网络）；

—任何租户都无法访问其他租户的静态数据（存储）；

—任何租户都不能执行影响其他租户操作的操作；

—任何租户都不能执行可能导致其他租户无法获得服务的操作；

一每个租户都可以拥有独立于其他租户的存在和配置的配置（例如，命名或寻址）；

一当资源（计算机、存储或网络）从租户处停用时，该资源的所有数据和配置信息都将被清除；

—租户级别提供问责制和可追溯性措施。

b)TC-SMTS-G02 使用安全措施实现安全的多租户

在部分或全部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：

—与租户资源使用情况相匹配的加密存储；

一强对称加密（即至少128 位安全强度）保护静态数据；

—安全快速的取消配置（有关存储介质清理，包括加密擦除，请参见 10.6）；

—可信第三方数据存储管理（例如 SNMPv3）；

—自动化密钥管理，提供租户控制的密钥管理（利用 KMIP[Z51 兼容服务器]）；

—安全的数据复制（例如，传输中和静态数据加密）；

— 保护数据免受管理员访问（例如，强制执行最小权限访问模型，并且禁止访问密钥材料）；

—高可用性存储网络架构（多路径和多样化路径）；

—集中式且安全的审计日志记录（例如，基于TLS的syslog）；

一加密模块和其他安全措施（例如，存储介质清理和访问控制）的验证和认证（例如，通用准则）。

10.18 安全自主的数据移动

许多存储系统和基础设施可以将数据在不同的存储设备之间（例如，分层存储）、数据中心之间（例如，同步和异步数据复制）、数据归档设施以及数据保护系统之间（例如，磁带机或虚拟磁带上的备份）移动。信息生命周期管理和数据生命周期管理解决方案中存在更复杂的场景。但是，所有这些场景都假设：

—数据移动由策略驱动；

—整个过程中无需操作员或信息技术系统介入即可启动或干预。

由于自主数据移动的形式多种多样，其安全需求也可能差异很大。与安全自主数据移动相关的控制措施如下：

a) TC-SADM-G01 使用问责制和可追溯性实现安全自主数据移动

安全自主数据移动的问责制和可追溯性考虑因素包括：

—数据移动策略的配置应仅限于经过身份验证和授权的特权用户；

—配置人员应熟悉源和目标的安全属性；

一、为实现或终止自主数据传输而进行的配置更改应反映在审计日志中；

一所有自主数据移动事务都应反映在执行数据移动的系统的审计日志中。

b) TC-SADM-G02 使用完整性、真实性和不可篡改性实现安全的自主数据移动

安全的自主数据移动事务的完整性、真实性和不可篡改性考虑因素应包括：

一验证移动数据的完整性（最好使用签名加密哈希）；

一确保不影响数据的真实性（例如，原始系统元数据，如创建日期和上次访问日期，在移动数据中正确表示）；

一确保数据不可篡改性或其他数据保存控制（例如，支持法律保留）不被取消。

c) TC-SADM-G03 使用保密性实现安全自主数据传输

安全自主数据传输事务的保密性考虑因素应包括:—确保与数据相关的加密控制不被取消或削弱；

—确保在系统间传输敏感或高价值数据时使用传输中加密。d)TC-SADM-G04 将数据清理与安全自主数据移动结合使用

安全自主数据移动事务的数据清理注意事项应包括：

—确保在源数据或存储介质被释放以供重复使用之前，对其进行适当的数据清理（参见 10.6.3 和 10.6.4）。

-确保清理验证（见 10.6.6）并生成某种形式的清理证明（见 10.6.7）。

e) TC-SADM-G05 利用可信度和物理安全实现安全自主数据移动

安全自主数据移动事务的可信度和物理安全考虑因素应包括：

—确保数据不会跨越安全域（例如，从生产环境到开发环境）；

—确保数据不会移动到认证和认可不足的系统（例如，

ISO/IEC 19790、ISO/IEC 15408 系列和 NIST FIPS 140-3(621)；

—确保数据不会移动到物理安全不足的系统。

附录A

（资料性附录）

存储安全控制概要

A.1 总则

本附录概述了本文档中列出的存储安全控制。

本附录旨在帮助组织识别与其存储基础架构最相关的控制措施。本文档与前一版本 (ISO/IEC 27040:2015) 的一个重要区别在于纳入了存储要求（概述于 A.2中），这些要求很可能被视为一组基准控制措施。A.3条款规定基于每种控制类型（组织、人员、物理和技术）的要求和建议的摘要。

A.2 存储安全要求

表 A.1列出了与本文档中提供的要求或要求组相关的控制标签。

表 A.1—存储安全要求

控制类型	控制	条款编号
组织	OC-PLCY-R01 将存储纳入日志策略	7.2
组织	OC-CPLC-R01 确保存储满足用户责任义务	7.4
物理	PC-PHYS-R01 保护物理接口	9.3
技术	TC-HARD-R01 对存储执行日志记录	10.3.2
技术	TC-MGMT-R01 最低用户身份验证措施	10.4.2.1
技术	TC-MGMT-R02 确保远程管理安全	10.4.3
技术	TC-MGMT-R03 限制供应商远程管理	10.4.3
技术	TC-MGMT-R04 限制拨号访问使用	10.4.3
技术	TC-MGMT-R05 安全 IPMI	10.4.3
技术	TC-CNFD-R01 使用至少 128 位安全强度的加密技术	10.5.3
技术	TC-CNFD-R02 TLS 最低要求	10.5.4.2
技术	TC-CNFD-R03 IPsec 最低要求	10.5.4.3
技术	TC-CNFD-R04 保护用于加密存储的密钥	10.5.5
技术	TC-CNFD-R05 对存储使用合适的加密算法和操作模式	10.5.5
技术	TC-CNFD-R06 加密密钥仅用于单一用途	10.5.5
技术	TC-CNFD-R07 使用整个密钥空间随机生成密钥	10.5.5
技术	TC-CNFD-R08 密钥使用限制在有限的加密周期或处理的最大数据量内	10.5.5

技术	TC-SNTZ-R01 处置前对存储进行清理 c) TC-SNTZ-R02 验证存储清理结果。请确保此表与文本一致，并确认哪个版本正确。	10.6.1

表 A.1（续）

控制类型	控制	条款编号
技术	TC-SNTZ-R02 验证存储清除结果	10.6.1
技术	TC-SNTZ-R03 选择最低可接受的存储清除方法	10.6.2
技术	TC-SNTZ-R04 按照可接受的标准清除介质	10.6.3
技术	TC-SNTZ-R05 验证介质清除结果的充分性	10.6.3
技术	TC-SNTZ-R06 按照可接受的标准对逻辑存储进行清理	10.6.4
技术	TC-SNTZ-R07 验证逻辑存储清理结果的充分性	10.6.4
技术	TC-SNTZ-R08 在正确条件下使用加密擦除进行清除	10.6.5
技术	TC-SNTZ-R09 验证销毁清理方法的结果	10.6.6
技术	TC-FBNF-R01 应用 NFS 访问控制	10.10.2
技术	TC-FBNF-R02 限制 NFS 客户端行为	10.10.2
技术	TC-FBSM-R01 最低可接受的 SMB 协议	10.10.3
技术	TC-FBSM-R02 应用 SMB 访问控制	10.10.3
技术	TC-FBSM-R03 限制 SMB 客户端行为	10.10.3
技术	TC-CDMI-R01 对所有 CDMI 事务使用 TLS	10.11.2
技术	TC-CDMI-R02 对所有 CDMI 实体进行相互认证	10.11.2

A.3 存储安全控制

表 A.2列出了与第 7 条中提供的要求和建议或要求和建议组相关的控制标签。

表 A.2 — 存储安全组织控制

主题	控制	条款编号
策略	OC-PLCY-G01 将存储纳入策略	7.2
	OC-PLCY-G02 确保存储符合策略	7.2
	OC-PLCY-R01 将存储纳入日志策略	7.2
业务连续性管理	OC-IRBC-G01 将存储生态系统纳入业务连续性管理规划和实施	7.3
	OC-IRBC-G02 为有限中断事件做好准备	7.3
	OC-IRBC-G03 识别并记录独特的员工和设施要求	7.3
	OC-IRBC-G04 执行持续规划和BCM 测试	7.3
	OC-CPLC-R01 确保存储满足用户问责义务	7.4

合规性	OC-CPLC-G01 确保存储满足用户可追溯性义务	74
	OC-CPLC-G02 确保存储满足用户监控义务	7.4
	OC-CPLC-G03 确保存储满足数据保留和清理义务	7.4
	oC-CPLC-G04 确保存储符合隐私义务	7.4
	OC-CPLC-G05 考虑法律义务的存储	7.4

表 A.3 列出了与第 8 条中提供的要求和建议或要求和建议组相关的控制标签.

表 A.3 — 存储安全人员控制

主题	控制	条款编号
存储安全专业知识	SC-XPTS-G01 确保具备足够的存储保护专业知识	8
	SC-XPTS-G02 确保具备足够的存储安全专业知识	8

表 A.4 列出了与条款中提供的要求和建议或要求和建议组相关的控制标签。 9.

表 A.4—存储安全物理控制

主题	控制	条款编号
物理	PC-PHYS-G01 物理保护存储介质	9.2
	PC-PHYS-G02 物理保护存储设备	9.2
	PC-PHYS-R°1 保护物理接口	9.3
	PC-PHYS-G03 物理隔离存储系统	9.4
	PC-PHYS-G04逻辑隔离存储系统	9.4

表 A.5 列出了与要求和建议或集群相关的控制标签

第 10 条中提供了要求和建议。

表 A.5 — 存储安全技术控制

主题	控制	条款编号
设计与实施	TC-DSGN-G01 秉承核心安全设计原则	10.2.1
	TC-DSGN-G02 在设计中考虑相关威胁	10.2.1
	TC-DSGN-G03 部署纵深防御	10.2.2.1
	TC-DSGN-G04 将数据敏感性纳入安全域设计	10。2.2.2
	TC-DSGN-G05 将目的纳入安全域的设计	10.2.2.2
	TC-DSGN-G06 在安全域内使用进一步隔离	10.2.2.2
	TC-DSGN-G07 设计中包含弹性	10.2.2.3
	TC-DSGN-G08 支持安全初始化序列	10.2.2.4
	TC-DSGN-G09 最大限度地减少对存储可靠性的影响	10.2.3.1
	TC-DSGN-G10 最大限度地减少对数据可用性的影响	10.2.3.2
	TC-DSGN-G11 最大限度地减少对存储弹性的影响	10.2.3.3

	TC-DSGN-G12 最大限度地减少对数据完整性的影响	10.2.3.4
	TC-DSGN-G13 确保数据保留和保存	10.2.4
	TC-DSGN-G14 确保正确的数据处理	10.2.4
系统安全	TC-HARD-G01 执行基本操作系统强化	10.3.1
	TC-HARD-G02 使用来自可信来源的软件更新和补丁	10.3.1
	TC-HARD-R01 在存储上执行日志记录	10.3.2
	TC-HARD-G03 确保存储审核日志记录的完整性	10.3.2
	TC-HARD-G04 实施适当的存储监控	10.3.2
	TC-HARD-G05 使用日志保留和保护进行存储	10.3.2
	TC-HARD-G06 包括漏洞管理程序中的存储	10.3.3

A.5（续）

主题	控制	条款编号
存储管理	TC-MGMT-R01 最低用户身份验证措施	10.4.2.1
	TC-MGMT-G01 使用集中式身份验证解决方案	10.4.2.1
	TC-MGMT-G02 使用多因素身份验证身份验证	10.4.2.1
	TC-MGMT-G03 禁用 root 或 admin 帐户登录	10.4.2.1
	TC-MGMT-G04 远程记录所有权限提升操作	10.4.2.1
	TC-MGMT-G05 使用实体身份验证机制	10.4.2.1
	TC-MGMT-G06 分离安全角色和非安全角色	10.4.2.2
	TC-MGMT-G07 保护管理软件/固件的网络接口	10.4.3
	TC-MGMT-R02 保护远程管理	10.4.3
	TC-MGMT-R03 限制供应商远程管理	10.4.3
	TC-MGMT-R04 限制拨号访问使用	10.4.3
	TC-MGMT-R05 保护 IPMI	10.4.3

表 A.5（续）

主题	控制	条款编号
	TC-CNFD-G01 遵守密码学进出口法规	10.5.2
	TC-CNFD-G02 遵守密钥托管和披露要求	10.5.2
	TC-CNFD-G03 密钥故障应对计划	10.5.2
	TC-CNFD-G04 限制密码学对运行的影响	10.5.2

数据保密性	TC-CNFD-R01 使用至少 128 位安全强度的密码学	10.5.3
	TC-CNFD-G05 避免将存储加密作为敏感数据的主要保护措施	10.5.3
	TC-CNFD-G06 选择合适的加密点	10.5.3
	TC-CNFD-G07 使用与数据保留和保存要求兼容的适当加密和密钥管理方法	10.5.3
	TC-CNFD-G08 使用经过验证的加密模块处理敏感或受监管的数据	10.5.3
	TC-CNFD-G09 生成和保留存储加密记录	10.5.3
	TC-CNFD-G10 遵循基本密钥管理原则	10.5.3
	TC-CNFD-G11 为传输中的数据提供端到端安全保护	10.5.4.1
	TC-CNFD-G12 补偿传输中数据加密的计算影响	10.5.4.1
	TC-CNFD-R02 TLS 最低要求	10.5.4.2
	TC-CNFD-R03 IPsec 最低要求	10.5.4.3
	TC-CNFD-G13 使用合适的加密点	10.5.5
	TC-CNFD-G14 创建适当的加密证明	10.5.5
	TC-CNFD-R04 保护用于加密存储的密钥	10.5.5
	TC-CNFD-R05 使用适当的加密算法和操作模式进行存储	10.5.5
	TC-CNFD-G15 限制明文密钥的明文泄露	10.5.5
	TC-CNFD-R06 加密密钥仅用于单一用途	10.5.5
	TC-CNFD-R07 使用全部随机数生成密钥密钥空间	10.5.5
	TC-CNFD-R08 密钥使用仅限于有限的加密周期或处理的最大数据量	10.5.5
	TC-CNFD-G16 使用集中式密钥管理基础架构	10.5.5
	TC-CNFD-G17 使用 OASIS KMIP 访问和使用集中式密钥管理基础架构	10.5.5

A.5（续）

主题	控制	条款编号
	TC-SNTZ-G01 将存储清理纳入数据治理	10.6.1
	TC-SNTZ-R01 在以下情况下清理存储：处置	10.6.1
	TC-SNTZ-R02 验证存储消毒结果	10.6.1
	TC-SNTZ-R°3 选择最低可接受的存储消毒方法	10.6.2

存储清理	TC-SNTZ-G02 考虑存储消毒的成本和环境影响	10.6.2
	TC-SNTZ-R04 按照可接受的标准对培养基进行消毒	10.6.3
	TC-SNTZ-R05 验证培养基消毒结果的充分性	10.6.3
	TC-SNTZ-R06 按照可接受的标准对逻辑存储进行清理	10.6.4
	TC-SNTZ-R07 验证逻辑存储清理结果的充分性	10.6.4
	TC-SNTZ-G03 考虑为数据保护机制增加额外的存储清理	10.6.4
	TC-SNTZ-R08 在正确条件下使用加密擦除进行清除	10.6.5
	TC-SNTZ-G04 寻求对加密擦除所用加密技术的质量保证	10.6.5
	TC-SNTZ-G05 确定已销毁的加密密钥是否可恢复	10.6.5
	TC-SNTZ-G06 验证清除清理方法的结果	10.6.6
	TC-SNTZ-G07 验证清除清理方法的结果	10.6.6
	TC-SNTZ-R09 销毁清理方法结果验证	10.6.6
	TC-SNTZ-G08 生成和保留存储清除记录	10.6.7
	TC-SNTZ-G09 记录清除认证所需的最低信息	10.6.7
直连存储	TC-DASS-G01 保护 DAS 免受未经授权的访问	10.7
	TC-DASS-G02 在重新利用或处置 DAS 之前对其进行清除	10.7
	TC-DASS-G03 备份 DAS 以确保数据丢失后的恢复	10.7
FC SAN	TC-FCSS-G01 控制 FCP 节点访问	10.8.2.2
	TC-FCSS-G02 使用基于 FC 交换机的控制	10.8.2.2
	TC-FCSS-G03 配置 FC 设备以满足安全要求	10.8.2.2
IP SAN	TC-IPSS-G01 使用 iSCSI 网络访问和协议	10.8.2.3
	TC-IPSS-G02 使用 FCIP 网络访问和协议	10.8.2.3
	TC-IPSS-G03 使用 IPsec 保护 FCIP	10.8.2.3
InfiniBand SAN	TC-IBSS-G01 保护 InfiniBand SAN	10.8.2.4
NVMe-oF	TC-NVSS-G01 使用 NVMe-oF 身份验证	10.8.2.5
	TC-NVSS-G02 使用 NVMe/FC 安全控制	10.8.2.5
	TC-NVSS-G03 使用 NVMe/TCP 安全控制	10.8.2.5
	TC-NVSS-G04 使用 NVMe/RDMA 安全控制	10.8.2.5
NAS 协议	TC-NASP-G01 使用 NFS 网络访问和协议	10.8.3.2
	TC-NASP-G02 使用加密保护 NFS	10.8.3.2
	TC-NASP-G03 使用 SMB 网络访问和协议	10.8.3.3

A.5（续）

主题	控制	条款编号
基于块的 FC 存储	TC-BBFC-G01 使用 FC LUN 掩码和映射	10.9.1
	TC-BBFC-G02 使用 FCP 实现 SCSI 安全措施	10.9.1
	TC-BBFC-G03 使用 FC 存储的静态数据加密	10.9.1
	TC-BBFC-G04 使用存储清理FC 存储	10.9.1
基于块的 IP 存储	TC-BBIP-G01 过滤 iSCSI 发起程序访问	10.9.2
	TC-BBIP-G02 使用 iSCSI 安全措施	10.9.2
	TC-BBIP-G03 对 IP 存储使用静态数据加密	10.9.2
	TC-BBIP-G04 使用存储清理技术进行 IP 存储	10.9.2
基于文件的 NFS 存储	TC-FBNF-R01 应用 NFS 访问控制	10.10.2
	TC-FBNF-R02 限制 NFS 客户端行为	10.10.2
	TC-FBNF-G01 保护 NFS 服务器上的数据	10.10.2
基于文件的SMB存储	TC-FBSM-R01 最低可接受的 SMB 协议	10.10.3
	TC-FBSM-R02 应用 SMB 访问控制	10.10.3
	TC-FBSM-R03 限制 SMB 客户端行为	10.10.3
	TC-FBSM-G01 保护 SMB 服务器上的数据	10.10.3
云计算存储	TC-CCSS-G01 使用传输安全进行云事务处理	10.11.1
	TC-CCSS-G02 使用静态数据加密进行云存储处理	10.11.1
	TC-CCSS-G03 使用强身份验证访问云存储	10.11.1
	TC-CCSS-G04 使用访问控制保护云存储上的数据	10.11.1
	TC-CCSS-G05 使用云存储数据清理	10.11.1
CDMI	TC-CDMI-R01 对所有 CDMI 事务使用 TLS	10.11.2
	TC-CDMI-R02 对所有 CDMI 实体进行相互认证	10.11.2
	TC-CDMI-G01 使用 CDMI 能力查询评估安全性	10.11.2
	TC-CDMI-G02 使用 CDMI 域	10.11.2
	TC-CDMI-G03 将 CDMI 日志记录集成到审计日志中	10.11.2
	TC-CDMI-G04 配置 CDMI 保留策略以使自动删除与策略保持一致	10.11.2
	TC-CDMI-G05 在使用 CDMI 保留功能之前，验证解除保留的能力	10.11.2
	TC-CDMI-G06 对 CDMI 存储使用静态数据加密	10.11.2
	TC-CDMI-G07 对 CDMI 存储使用存储清理	10.11.2

基于对象的存储	TC-OBSS-G01 使用传输安全进行基于对象的存储事务处理	10.12
	TC-OBSS-G02 使用静态数据加密进行基于对象的存储	10.12
	TC-OBSS-G03 为基于对象的存储启用数据不可变性	10.12
	TC-OBSS-G04 使基于对象的存储上的安全机制与租户保持一致	10.12
	TC-OBSS-G05 使用存储清理进行基于对象的存储	10.12
数据缩减	TC-DRDC-G01 在加密前使用压缩	10.13
	TC-DRDC-G02 在加密前使用去重	10.13
	TC-DRDC-G03 使用正确的顺序进行多次数据缩减和加密	10.13
	TC-DRDC-G04 使用与BCM兼容的数据缩减	10.13

表 A.5（续）

主题	控制	条款编号
数据保护与恢复	TC-PROT-G01 设计用于快速恢复的数据保护机制	10.14.1
	TC-PROT-G02 安全地使用数据备份措施和操作	10.14.2
	TC-PROT-G03 使用网络攻击恢复备份	10.14.2
	TC-PROT-G04 安全地使用数据复制措施和操作	10.14.3
	TC-PROT-G05 将快照与备份结合使用	10.14.4
	TC-PROT-G06 使用快照安全性	10.14.4
数据归档和存储库	TC-DARS-G01 解决存储归档中的关键保存问题	10.15.2.1
	TC-DARS-G02 使用安全服务解决归档的证据方面问题	10.15.2.1
	TC-DARS-G03 创建归档中保留数据的多个物理或逻辑副本	10.15.2.2
	TC-DARS-G04 对存档数据进行定期完整性审计	10.15.2.2
	TC-DARS-G05 使存档数据的访问控制符合法律法规要求	10.15.2.2
	TC-DARS-G06 对存档数据的访问采取问责制和可追溯性措施	10.15.2.2
	TC-DARS-G07 使用机制解决存档数据的真实性、来源和监管链问题	10.15.2.2
	TC-DARS-G08 确保对归档数据进行适当的密钥生命周期管理	10.15.2.2
	TC-DARS-G09 主动检查长期归档存储的数据完整性	10.15.2.3
	TC-DARS-G10 在长期归档存储的技术更新期间升级安全性	10.15.2.3
	TC-DARS-G11 管理用户和对长期归档存储的访问	10.15.2.3
	TC-DARS-G12 在长期归档存储中维护数据机密性措施	10.15.2.3

	TC-DARS-G13 保留长期归档存储的安全日志	10.15.2.3
	TC-DARS-G14 检测和处理长期归档存储的漏洞	10.15.2.3
	TC-DARS-G15 确保数据缩减技术不会影响长期归档存储的数据完整性	10.15.2.3
	TC-DARS-G16 使用数据存储库的安全控制	10.15.2.3
存储虚拟化	TC-SVSS-G01 将存储网络控制应用于参与存储虚拟化的所有实体	10.16.1
	TC-SVSS-G02 限制或阻止对非虚拟化物理元素的直接访问	10.16.1
	TC-SVSS-G03 使用安全控制保护虚拟化存储中的数据	10.16.1
	TC-SVSS-G04 满足虚拟化存储的可用性、机密性和隐私性服务级别目标	10.16.1
	TC-SVSS-G05 确保虚拟化存储满足多租户安全要求	10.16.1
	TC-SVSS-G06 控制虚拟机对存储网络的访问	10.16.2
	TC-SVSS-G07 控制物理服务器之间的虚拟机迁移/移动	10.16.2

A.5（续）

主题	控制	条款编号
安全的多租户	TC-SMTS-G01 为多租户提供安全隔离保证	10.17
	TC-SMTS-G02 使用安全措施实现安全的多租户	10.17
安全的自治数据移动	TC-SADM-G01 利用问责制和可追溯性实现安全的自主数据移动	10.18
	TC-SADM-G02 利用完整性、真实性和不可篡改性实现安全的自主数据移动	10.18
	TC-SADM-G03 利用保密性实现安全的自主数据移动	10.18
	TC-SADM-G04 将数据清理与安全的自主数据移动结合使用	10.18
	TC-SADM-G05 利用可信度和物理安全实现安全的自主数据移动	10.18