ICS 35.030
CCS L80

中华人民共和国国家标准

GB/T 32916—XXXX/ISO/IEC TS 27008：2019
代替 GB/Z 32916-2016

信息安全技术
信息安全控制评估指南

Information security techniques -
Guidelines for the assessment of Information security Controls

(ISO/IEC TS 27008:2019,IDT)

征求意见稿 V1.2

2022-3-25

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/Z 32916-2016《信息技术 安全技术 信息安全控制措施审核员指南》。

与GB/Z 32916-2016相比，主要技术变化如下：

——评审方法中增加了抽样的介绍；

——对旧版附录B增加了事件管理的内容，在新版中该附录次序调整为附录A；

——对旧版附录A“关于技术符合性检查实践指南”中关于控制的陈述和指南的结构保留，新版本中所列出的控制和GB/T 22081-2016保持一致，在新版中该附录次序调整为附录B“技术性安全评估实践指南”；

——新版增加的附录C提供了基于ISO/IEC 27017：2015的云服务技术性安全评估指南。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件等同采用国际技术规范ISO/IEC TS 27008:2019《信息技术　安全技术　信息安全控制评估指南》（英文版）。根据GB/T 1.1—2020和GB/T 20000.2—2009的规定，做了如下一些编辑性修改：

a)　使用与ISO/IEC　27000:2018对应的GB/T 29246(见2）；

b)　增加了3.2缩略语（见3）；

c)　增加了资料性附录D（见附录D）；

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：北京赛西认证有限责任公司、中国电子技术标准化研究院、中国合格评定国家认可中心、北京时代新威信息技术有限公司、长扬科技（北京）有限公司、北京神州绿盟科技有限公司、深圳红途科技有限公司、华为技术有限公司、国家计算机网络应急技术处理协调中心、美的集团股份有限公司、西安交大捷普网络科技有限公司、北京天地和兴科技有限公司、杭州趣链科技有限公司、杭州安恒信息技术股份有限公司、浙江省电子信息产品检验研究院、远江盛邦（北京）网络安全科技股份有限公司、陕西省网络与信息安全测评中心、北京金山云网络技术有限公司、上海观安信息技术股份有限公司、北京邮电大学、杭州中正检测技术有限公司、马上消费金融股份有限公司、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、中国科学院信息工程研究所、智网安云（武汉）信息技术有限公司、启明星辰信息技术集团股份有限公司、国网新疆电力有限公司电力科学研究院、西安邮电大学等。

本文件主要起草人：韩硕祥、赵丽华、付志高、王惠莅、黄俊梅、刘峰松、周晓宇、李春琦、张世杰、贺创新、张杰、王凌、蔡北方、郑堃、阎若彤、俞政臣、赵华、叶建伟、黄鹏程、刘海军、王文磊、杨坤、何建锋、刘乐农、魏遵博、梁伟、尹肖栋、王晶、杭肖、于丽芳、谢江、王东滨、曹宇、刘志强、李松恬、韩冬旭、王燕青、王红亮、邹振婉、潘正泰等。

本文件所代替文件的历次版本发布情况为：

——2016年首次发布为GB/Z 32916-2016；

——本次为第一次修订。

引　言

本文件支持GB/T 22080-2016中所给出的信息安全风险管理过程，以及所确定的相关控制措施集。

信息安全控制措施宜适合于目的（即适用于当前的任务，能够缓解信息安全风险）、有效（如适宜地指定、设计、实现、使用、管理和维护）和高效（为组织提供收益）。本文件说明了如何评估组织的信息安全控制措施，以确认其确实适宜、有效且高效（提供信任），或识别变更（改进机会）需求。信息安全控制措施作为一个整体，最终目的是以合理的成本效益和与业务一致的方式，充分缓解组织认为不可接受和不可避免的信息安全风险。本文件为基于业务使命和目标、组织策略和要求、已知的新出现的威胁与脆弱性、运行考虑、对信息系统和平台的依赖性，以及组织的风险偏好定制必要的评审提供了所需的灵活性。

有关信息安全管理体系审核指南见GB/T 28450，有关信息安全管理体系审核和认证机构的要求见GB/T 25067。

信息安全技术 信息安全控制评估指南

1 范围

本文件为评审和评估信息安全控制措施的实施与运行提供指南，包括对信息系统控制的技术性评估，该评审和评估基于组织所建立的信息安全要求及技术性评估准则。

本文件在如何评审和评估由GB/T 22080-2016规定的信息安全管理体系所管理的信息安全控制措施方面提供指南。

本文件适用于各种类型和规模的组织开展信息安全评审和技术符合性检查。

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 29246-20** 信息安全技术 信息安全管理体系 概述和术语（ISO/IEC 27000:2018，IDT）

ISO/IEC 27017:2015 信息技术 安全技术 基于ISO/IEC 27002 云服务信息安全控制措施实践指南(Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services)

3 术语、定义和缩略语

3.1 术语和定义

GB/T 29246 界定的术语和定义适用于本文件。

3.2 缩略语

下列缩略语适用于本文件：

ACL:访问控制列表（Access Control List）

API:应用程序接口(Application Program Interface)

ASP: 应用服务提供者（Application Service Provider）

BSS:业务支持系统（Business support systems）

CD:光盘（Compact Disk）

CMDB:配置管理数据库（Configuration Management Database）

CPU: 中央处理单元 （Central Processing Unit）

DHCP:动态主机配置协议(Dynamic Host Configuration Protocol)

DLT: 数字线性磁带（Digital Linear Tape）

DNS:域名系统（Domain Name System）

DVD:数字视频光盘（Digital Video Disc）

FC:光纤通道（Fibre Channel）

FTP:文件传输协议（File Transfer Protocol）
HBA:主机总线适配器（Host Bus Adapter)
Hypervisor:虚拟机管理程序（Hypervisor）
I/O:输入/输出（Input/Output）
IaaS:基础设施即服务（Infrastructure as a Service）
IC:集成电路（Integrated Circuit）
IDS:入侵检测系统（Intrusion Detection Systems）
ID:身份标识（Identity document）
IIS:互联网信息服务（Internet Information Service）
IPSec:互联网协议安全（Internet Protocol Security）
IPS: 入侵防御系统（Intrusion Prevention System)
IT:信息技术（Information Technology）
LDev:逻辑设备（Logical Device）
NIC:网络接口控制器（network interface controller)
NTP:网络时间协议（Network Time Protocol）
OS:操作系统（Operating System）
OSS:运营支持系统（operational support systems）
PII:个人可识别信息（Personally Identifiable Information）
PIM: 特权身份管理（Privileged Identity Management）
RACF: 资源访问控制设施（Resource access control facility）
RAID:独立磁盘冗余阵列（Redundant Arrays of Independent Disks）
SaaS:软件即服务（Software as a Service）
SAML:安全断言标记语言（Security Assertion Markup Language）
SAN:存储区域网络（Storage Area Network)
SDN:软件定义网络（Software Defined Network）
SIEM:信息安全和事态管理（Security Information and Event Management）
SLA:服务级别协议（Service-Level Agreement）
SSH:安全外壳（Secure Shell）
SSL:安全套接层（Secure Sockets Layer）
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)
UEFI:统一的可扩展固件接口（Unified Extensible Firmware Interface）
URL:统一资源定位符（Uniform Resource Locator）
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）
VMM:虚拟机监视器（Virtual Machine Monitor)
VPN:虚拟专用网（Virtual Private Network）
WWW:万维网（World Wide Web）
iSCSI:互联网小型计算机系统接口（Internet Small Computer System Interface）

4 本文件的结构

本文件描述了信息安全控制措施评估过程，包括技术性评估。

第五章提供背景信息。

第六章提供信息安全控制措施评估的概述。

第七章介绍评审方法。

第八章介绍控制评估过程。

附录A指导初始信息收集。

附录B指导技术性评估。

附录C指导云服务技术性评估。

附录D给出了GB/T 22081—2016/ISO/IEC 27002:2013与ISO/IEC 27002:2022控制的对应关系。

5 背景

信息安全控制措施是处置不可接受的信息风险、使其处于组织可接受风险水平之内的主要手段。

组织的部分信息安全控制措施通常是通过采用技术性信息安全控制措施实现。

组织的技术性安全控制可根据信息安全技术标准来定义、记录、实施和维护。随着时间的推移，信息系统改进、安全功能配置和信息系统环境的变化等内部因素及攻击技能的提高等外部因素可能对信息安全控制措施的有效性产生不利影响，并最终影响组织信息安全水平。技术性评估是GB/T 22081中控制措施之一。技术性评估通常通过手动和/或借助自动化工具进行。技术性评估可以由不参与执行控制的角色实施，如：系统的所有者，或者具体控制的责任人，或者内部或外部的信息安全专家来执行。

技术性评估的输出反映了组织在技术上遵守信息安全实施标准的实际程度。当技术性控制措施符合信息安全标准时，该证据提供了保证，否则将作为改进的依据。评估报告链宜在评估开始时就明确建立，并宜保证报告过程的完备性。宜采取相应的步骤，以确保：

——从一开始就确定并确保具备适当的测试能力，见6.2；

——相关责任方直接从信息安全审核员处收到未改动的技术性评估报告副本；

——不适宜或未经授权方无法获得来自信息安全审核员的技术性评估报告副本；

——允许信息安全审核员在不违反职责分离原则的情况下开展工作。

信息安全控制措施评估，尤其是技术性评估，可以帮助组织：

——识别和理解组织在实施和运行信息安全控制措施、信息安全标准及相应的技术性信息安全控制措施方面的潜在问题或不足程度；

——识别和理解未充分消除的信息安全威胁和脆弱性对组织的潜在影响；

——确定经识别的降低信息安全风险活动的优先级；

——确认已识别的或突发的信息安全脆弱性和威胁已得到充分解决；

——支持与组织信息安全管理改进有关的投资过程中的预算决策和其他管理决策。

6 信息安全控制措施评估概述

6.1 评估过程

6.1.1 总则

评估前，所委派的信息安全审核员需要做好控制方面和测试方面的准备（如适用工具的操作、测试的技术目标）。各项评审工作可依据预知的风险来排列优先顺序，也可按照特定的业务流程或系统进行安排，或者简单地按照顺序覆盖评估范围的所有领域。

在评估单个信息安全控制措施时，信息安全审核员通常先收集初步信息，评审策划的工作范围，联络组织相关部门的管理者和其他联系人，开展风险评估，以编制用于指导实际评估工作的评估文件。支持性资料见附录A至C。

6.1.2 初步信息

初步信息可能来源于多个方面：

a） 书籍、互联网搜索、技术手册、技术安全标准和组织的策略，以及对该领域常见风险和控制的其他一般背景研究，会议、研讨会、培训或论坛；

b） 以往的评估、测试和审核的结果，无论其是部分符合还是完全符合本次评估范围，也无论其是否是由信息安全审核员实施的（例如，由信息安全专业人员进行的发布前安全测试，可以提供有关主要应用系统安全的丰富知识）；

c） 从IT服务台、IT变更管理、IT事件管理流程和类似来源所收集的与信息安全事件、事态、请求支持的问题和变更相关的信息；

d） 由在评估范围相关领域具有专业知识的信息安全审核员或信息安全专业人员编写的通用评估检查单和论文。

建议根据初步信息评审已策划的评估范围，尤其是在几个月之前就已经制定好的评估计划范围。例如，其他评估活动未囊括值得深入探讨的关注点，或者与之相反，在某些领域增加了保障从而允许当前工作关注其他方面。

在初期阶段，联络管理人员和评估联系人是一项重要活动。在评估过程结束时，需要了解评估发现，以便对评估报告做出积极回应。彼此理解、相互尊重和充分解释评估过程，能显著改进评估结果的质量和影响。

6.1.3 评估检查单

每个审核员将其工作形成文件的方式有所不同，许多评估活动利用工作文件模板来支持标准化的评估过程，例如评估检查单、内部控制调查问卷、测试计划、风险控制矩阵等。

评估检查单（或类似的文档）是一个关键文件，有以下几个原因：

a） 列出了评估工作已策划的范围，可详细到描述单个评估测试和预期/理想发现的程度；

b） 提供了评估工作的结构，有助于确保充分覆盖所策划的范围；

c） 必要的分析最初编写的检查单，可为信息安全审核员后续的现场评估做好准备。随着评估进展开始分析过程，逐步填写检查单，再根据分析过程生成评估报告；

d） 提供了记录评估前期工作和现场评估结果的框架，例如，检查单里可引用和评价收集到的评估证据；

e） 审核管理人员或其他信息安全审核员可以评审检查单，作为评估质量保障过程的一部分；

f） 检查单一旦完成，其连同评审证据一起构成了一个对评审工作和评审发现的、详略得当的历史记录，用于证实或支持评审报告，向管理层报告和/或帮助策划以后的评审。

信息安全审核员宜谨慎避免简单使用他人编写的通用评审检查单，这样也许会节省时间，但可能会丧失上面提到的几个好处。

6.1.4 现场评审

大部分的现场评审工作是由信息安全审核员实施的或其要求实施的一系列测试组成，以收集评审证据并对其评审。评审经常是通过与源自于相关合规义务、标准或获得广泛认可的良好实践的预期或期望结果进行比较来实现。例如，在信息安全审核中检查恶意软件控制的一个测试，可以检查是否所有适用的计算机平台都安装了适宜的杀毒软件。此类评审测试经常使用抽样技术，因为很少会有足够的评审资源来进行全面的测试。抽样因信息安全审核员和实际情况而异，可能包括随机选择、分层选择和其他更复杂的统计抽样技术（例如，为了证实控制存在不足的程度，在初始结果不令人满意时采取额外的抽样）。

通常来说，以电子的方式来收集和测试证据时可进行更全面的测试，例如对从系统和资产管理数据库中整理出的评审证据数据库使用SQL查询语句。评估的抽样方法，至少部分宜以所评估的运行区域的风险为导向。

评审过程中收集到的证据通常宜在评审工作文件中予以标注、引用或编制清单。在评审分析、发现、建议和报告的过程中，信息安全审核员须充分保护评审证据，特别是一些可能是非常敏感和/或有价值的证据。例如，从生产数据库中提取的用于评审的数据，宜通过访问控制、加密等手段使其得到和生产数据库相同程度的保护。自动化评审工具、查询、实用程序/数据提取程序等宜受到严格控制。同样，信息安全审核员打印的或提供给他们的打印资料，一般宜通过上锁等措施保护其物理安全，以防止未经授权的泄露或修改。对于特别敏感的评审，宜在评审的早期阶段识别风险和必要的信息安全控制措施，并做好准备。

在完成评审检查单、实施了一系列评审测试和与相关方的面谈，并充分收集了评审证据之后，信息安全审核员宜能够对证据进行审查，确定信息安全风险被处置的程度，并评审任一残余风险的潜在影响。在这个阶段，可以起草某种形式的评审报告，对评审工作的质量进行评审（评审过程的活动之一），以及与管理人员讨论，特别是直接接受评审的业务单元、部门、职能或团队的管理人员，也可能与组织的其他相关部门进行讨论。

宜公正地评审证据，以确定：

——有充分的评审证据来提供能支持所有评审发现的事实依据；

——所有发现和建议均与评审范围相关，无关事项已排除在外；

——与评审范围内的系统和控制有关的证据是最新和有效的。

如果对评审发现需要策划进一步的评审，宜在报告中注明。

6.1.5 分析过程

与评审策划一样，尽管在现场评审期间收集的证据能为分析提供有用的信息，分析过程本质上是基于风险的。简单的符合性评审通常会产生一系列相对简单的具有明确意见的符合/不符合的结果。信息安全评审通常会产生一些需要管理层在决定采取何种适宜的行动（如有）之前需考虑和讨论的事项。在某些情况下，管理层可以选择接受信息安全评审确定的某些风险；在另一些情况下，管理层有权决定不采纳评审的建议。但这需要承担相应的责任。从这个意义上说，审核员承担的是建议而非执行的角色，但他们具有重大影响力，并且有充分的评审实践和事实证据做支撑。

信息安全审核员宜向受审核组织就其信息安全活动（不是所有组织都实施管理体系）达到了既定目标的程度提供合理保证。评审宜提供实际情况与引用文件之间的差异说明。如果引用文件是内部策略，则策略宜足够清晰，可以作为引用文件。可参考附录A所列的准则来确保这一点。信息安全审核员宜在评审范围内考虑内部策略和规程。缺失的相关准则仍可能被非正式地应用于组织内。缺少应用已确定的关键准则可能会导致潜在的不符合。

6.2 资源和能力

评审信息安全控制措施，需要有客观分析和专业报告的技能。对于技术性评估，还需要额外的专业技能，这包括具备了解信息安全策略是如何在软件、硬件、通信链路及其相关技术过程中执行的具体技术知识。信息安全审核员宜具备：

——基于对信息系统框架概念的理解，了解信息系统风险和安全架构；

——信息安全良好实践的知识，例如 GB/T 22081 和其他安全标准，包括适用的特定行业安全标准给出的信息安全控制措施；

——深入检查复杂技术信息的能力，以识别任何重大的风险和改进的机会；

——了解信息安全评审和信息技术评审存在的局限性；

——对安全测试工具、操作系统、系统管理、通信协议以及应用程序安全和测试技术有广泛而深入

的了解；

——检查物理安全要求的能力；

——理解社会工程安全要求的能力。

建议：

——任何参与信息安全控制措施评估的人员，要熟悉基于 GB/T 19011 的审核专业基础知识，具备职业道德、独立性、客观性、保密性、责任心和判断力；了解访问记录授权的权限来源、职能、资产、人员和信息；具有处理与保护所获得的信息、评审发现与建议以及随之而来的后续过程等的责任。

——任何领导信息安全控制措施评估的人员，要有实施技术性信息安全评估的足够经验，比如至少有三年可证实的经验。

为达到评审目的，评审小组可由具有各种相关专业能力的信息安全审核员组成。当要求范围内实施评审的相关专业技术或能力尚未具备，宜安排技术专家（以内部或外部资源的形式）并考虑风险和利益。

信息安全审核员还宜核实组织和负责信息安全的人员：

——具有足够的信息安全及其具体任务方面的知识；

——拥有可支配的必要资源，例如时间。

7 评审方法

7.1 概述

评审控制的基本概念通常包括评审规程、评审报告和评审跟踪。评审规程的设计和内容包括评审目的和评审方法。

审核员在信息安全控制措施评审过程中可以采用以下四种评审方法：

——过程分析；

——检查；

——测试与确认；

——抽样。

第7.2至7.5节包含对每种评审方法的进一步考虑。

测试与确认可能需要占用大量资源的自动化工具。在计划使用这种工具时，同时宜考虑这种工具对操作的潜在影响，例如安排非高峰时段的评审。当评审的某部分依赖于这种工具时，审核员宜证明或者提供证据来说明这种工具提供可靠结果，从而确保工具的完整性。

如果以下控制措施被标记为“部分可操作”或“完全可操作”，则对于以下控制措施，宜强制进行测试与确认：

——B.2.5 访问控制

——B.2.6 密码；

——B.2.8中关于GB/T 22081-2016的12.4.2日志信息的保护；

——B.2.9中关于GB/T 22081-2016的13.1网络安全管理；

——B.2.10中关于GB/T 22081-2016的14.1.2公共网络上应用服务的安全保护；

——B.2.10中关于GB/T 22081-2016的14.1.3应用服务事务的保护。

可以根据评审的性质和所需的保证级别适当地组合使用评审方法。用这种方式定义的调查深度可以是：

a） 低度评估：

1） 过程分析。

b） 中度评估：

1） 过程分析；

2） 对代表性样品的检查或测试。

c） 高度评估：

1） 过程分析；
2） 对大量的或近乎全部的样本进行检查和测试。

7.2 过程分析

7.2.1 总则

直接评估信息安全控制措施（例如检查和测试）并不总是可能或足以确保其运行的有效性和适用性。但是通过分析相关流程或活动以获取证据确认其符合以下特征，从而推断控制措施的有效性和适用性可能更合适或更必要：

——理论上为提供期望的控制效果而设计；
——正确实施；
——按设计运行；
——被正确地执行，监视和管理；
——在实践中实际上提供了预期的控制效果。

操作和执行的流程或活动是在控制运行的范围内进行的，通常以记录、日志条目等形式提供控制运行的证据。特别是，由控制生成的和处理的记录，诸如警示、警报、事态和事件报告，通常表明控制可以正常工作，但是不足以确认控制是否可靠且完全有效。在实践中对相关流程和活动的分析（例如，检验程序，观察和/或访谈相关人员）提供了额外的保障，并通过测试确认了预期会触发控制的数据、标准或情形与实际情况一致。

GB/T 19011-2021 A.5具体说明了如何验证信息的指南。

GB/T 19011-2021 A.17具体说明了如何进行访谈的指南。

7.3 检查

7.3.1 总则

检查作为评审方法的一种形式，通过对一个或多个评审对象进行核查、检验、复核、观察、研究或分析来促进理解、进行澄清或获得证据。评审的目的在于支持确定控制的存在、功能、正确性、完整性以及随着时间的推移可能进行改进的可能性。

评审对象通常包括：

——机制（例如，在硬件、软件、固件、应用程序，数据库中实现的功能）；
——过程（例如，系统的操作、监管、管理、演练）。

信息安全审核员的典型操作可包括：

——观察系统备份操作并评审应急预案演练的结果；
——观察事件响应过程；
——核查、研究或观察信息系统的硬件/软件中信息技术机制的运行；
——核查、研究和观察与信息系统有关的变更管理和活动日志；
——核查、研究或观察与信息系统的操作有关的物理安全措施（例如，观察纸质废弃保密文件的安全运输和销毁记录）；
——复核、研究或观察信息系统的配置。

7.3.2 规程控制

通过观察各种流程而无需与它们进行最少的交互（或在这样做时），可以使审核员立即收到有关特定活动如何运行的证据。当需要观察罕见或特定事件时，可通过使用获取的相关文件化信息来完成。

7.3.3 技术控制

与评审对象进行交互（直接或通过合格的操作员）可以使审核员提取或直接检验其配置设置，从而在无需实际测试的情况下预测其行为。这对于处理可能被测试技术干扰或审核员没有机会进行交互的关键评审对象是可取的。

7.4 测试与确认

7.4.1 总则

测试与确认是评审的一种形式，是指在给定的条件下执行一个或多个评审对象以对比其预期行为与实际结果的过程。其结果可用于支持判定控制措施的存在性、有效性、功能性、正确性、完整性及持续改进的可能性。

测试须由有能力的专家执行，且需谨慎。测试对组织的运行可能造成的影响须在测试开始前得到考虑并经过管理层的批准，并且还要考虑选择在非运行窗口或低负荷的环境，甚至在复制的测试环境中进行测试。测试导致的系统故障或不可用可能会对组织的正常业务运行造成重大影响，可能会造成组织经济损失或影响其声誉。因此，在测试策划以及签约时需要特别注意（包括考虑法律方面的事宜）。

在给出任何结论之前，信息安全审核员必须仔细检查测试结果中存在的误报和漏报。

典型的评审对象包括机制（如硬件、软件、固件）和过程（如系统操作、实现、管理、演练）。

信息安全审核员的典型活动可包括：

——测试访问控制、身份鉴别、授权和评审机制；
——测试安全配置设置；
——测试物理访问控制设备；
——执行关键信息系统组件的渗透测试；
——测试信息系统的备份操作；
——测试事件响应能力；
——演习应急策划能力；
——测试安全系统入侵检测、报警和响应的能力；
——测试加密机制和哈希算法；
——测试用户标识和特权管理机制；
——测试授权机制；
——验证安全措施的级联恢复能力；
——验证监视记录和日志；
——验证应用开发或获取应用程序时的安全方面。

7.4.2 盲测

信息安全审核员事先未掌握评审对象可公开获取信息外的其它特性。评审对象已对评审有所准备，并事先了解评审的所有细节。盲测评审主要考验信息安全审核员的技能。盲测评审的广度和深度只能体现信息安全审核员适用知识和工作效率。因此，这种测试在安全评审中的应用有限，且宜避免使用。

7.4.3 双盲测试

信息安全审核员事先未掌握评审对象除可公开获取信息外的其它特性。评审对象在评审前，也未被告知评审的范围和使用的测试向量。双盲评审测试了评审对象对未知变量的准备情况。

7.4.4 灰盒测试

信息安全审核员对评审对象的防御能力和资产的了解有限，但对可用的测试向量完全掌握。评审对象已对评审有所准备，并事先了解评审的所有细节。灰盒评审考验了信息安全审核员的技能。这种测试的本质是效率。测试的广度和深度取决于测试前提供给信息安全审核员的信息的质量，以及信息安全审

核员的适用知识。因此，这种测试在安全评审中的应用有限，且宜避免使用。这种类型的测试常称为脆弱性测试，通常由自我评估活动的对象发起。

7.4.5 双灰盒测试

信息安全审核员对评审对象的防御能力和资产的了解有限，但对可用的测试向量完全掌握。审查对象已被提前告知评审的范围和时限，但测试向量是未知的。双灰盒评审测试了评审对象对未知变量的准备情况。测试的广度和深度取决于测试前提供给信息安全审核员和评审对象的信息的质量，以及信息安全审核员的适用知识。

7.4.6 串联测试

信息安全审核员和评审对象都已对评审有所准备，且都事先了解评审的所有细节。串联评审测试了对目标的保护和控制情况。但它不能测试目标对未知变量的准备情况。

当信息安全审核员对所有的测试以及响应有全面的见解，这种测试的本质是全面的。测试的广度和深度取决于测试前提供给信息安全审核员的信息的质量，以及信息安全审核员的适用知识。这种测试常用于内部评审，并且信息安全审核员通常在整个安全过程中起到积极的作用。

7.4.7 逆向测试

信息安全审核员对评审对象的过程和运行安全有充分了解，但是评审对象不知道信息安全审核员将测试什么、如何测试以及何时测试。这种测试的本质是评审目标对未知变量和矢量扰动的准备情况。测试的广度和深度取决于提供给信息安全审核员的信息的质量，以及信息安全审核员的适用知识和创造力。这常被称为红队演练。

7.5 抽样

7.5.1 总则

GB/T 19011-2021，A.6 规定了如何实施抽样的准则。

7.5.2 典型抽样

对评审对象代表性样本（类型和数量）的检查，提供了必要的覆盖率，以确定相关控制措施是否实施且无明显错误。

7.5.3 穷举抽样

对足够多的评审对象样本(类型和数量)和其他对实现评审目的起重要作用的特定评审对象的检查，提供了必要的覆盖率，以确定相关控制措施是否实施且无明显错误、是否能进一步证明控制措施正确实施且按预期持续一致地运行，且对控制措施的有效性提供持续改进的支持。

8 控制评估过程

8.1 准备工作

为获得可接受的结论，在评审前、评审中和评审后建立并保持一组适当的期望很重要。这意味着为管理层提供信息，使其能够针对如何最佳地实现和运行信息系统做出合理的、基于风险的决策。组织和信息安全审核员的充分准备是进行有效评审的重要环节。准备活动宜关注一系列与成本、进度、专业知识的可用性和评审绩效等相关的问题。

从组织的角度看，评审准备包括以下关键活动：

——确保具备覆盖评审的适当的策略，并且被组织所有的成员所理解；

——确保为实现控制所策划的所有步骤在评审之前已经成功完成，并接受适当的管理评审（仅适用于被标记为“全面运行”的控制，而不适用于在准备或实施阶段中的控制）；

——确保控制已分配给适当的组织实体进行开发和实现；

——建立评审的目的和范围（即评审的意图和内容）；

——通知组织的主要管理者即将进行的评审并分配实现评审所需的必要资源；

——在评审范围内的组织管理者中建立适当的沟通渠道；

——为有效地管理评审，建立组织所需要的评审时间框架和关键里程碑决策点；

——识别和选择一个有能力的信息安全审核员或审核小组负责实现评审，并考虑审核员的独立性；

——收集组织文件（例如，包括组织结构图、策略、规程、计划、规范、设计、记录、管理员/操作员手册、信息系统文档、互联协议、资产清单、以往评审结果等信息安全控制措施记录）并提供给审核员；

——在组织和信息安全审核员之间建立一种机制，最小化评审期间发现的控制实现或控制弱点/缺陷的歧义或误解；

——通过组织和信息安全审核员之间的机制最小化歧义，可以采取后续/跟踪文档的形式；

——显示（由组织)提交或(由审核员）要求的文件，以及跟踪文档中收到的文件的有效性。可以要求提供附加信息，并有可能对提供过程中的不合理延迟进行时间跟踪。

除了组织为准备评审而进行的策划活动外，信息安全审核员宜从以下方面为评审做准备：

——理解组织的总体运行（包括任务、职能和业务流程）和评审范围内的信息资产如何支持这些组织运行；

——了解信息资产总体结构（即系统架构）；

——充分了解所有被评审的控制；

——研究这些控制中所引用的相关出版物；

——识别负责开发和实施评审范围内支持信息安全控制措施的组织实体；

——建立实现评审所需的适当的组织联络点；

——获得评审所需的组织文件（例如，包括组织结构图、策略、规程、计划、规范、设计、记录、管理员/操作员手册、信息系统文档、互联协议、资产清单的信息安全控制措施记录）；

——获得以往的适用于再次评审的评审结果（例如，报告、评审、漏洞扫描、物理安全检查、开发测试和评价）；

——与组织中相关的管理者会面，确保对评审目的、建议的评审严格程度和范围达成一致；

——制定评审计划。

为信息安全控制措施评审做准备时，宜收集必要的背景信息供信息安全审核员使用。为支持特定评审，组织宜识别组织中相关的个人或小组，并安排对其的访问。这些个人或小组负责开发、编制、分发、评审、运行、保持、更新所有的安全控制、安全策略和有关实现符合性策略控制的规程。

必需文件的可用性、关键组织人员与被评审信息系统的可访问性对一个成功的信息安全控制措施评审来说是非常重要的。

8.2 策划评估

8.2.1 概述

制定评审控制计划的信息安全审核员宜确定控制评审的类型（例如，完整评审或部分评审），以及基于评审的范围和目的确定评审中将包含哪些控制/控制增强。信息安全审核员宜评估和降低风险，并在可能的情况下减少审核活动对组织正常运行的影响，并基于评审活动选择适当的评审程序：

——评审中所涉及的控制和控制增强；

——它们关联的深度和覆盖范围。

信息安全审核员宜根据信息系统风险水平和组织的实际运行环境来对所选择的评审规程进行裁剪。必要时，审核员还宜针对本文件中未覆盖的安全控制、控制增强和额外保障需求制定附加的评审规程。

评估策划宜记录在评估计划中，策划中宜考虑环境、在已确定的环境下形成期望行为的基线以及测试/评价规范和对环境评价中的发现进行确认的方法。

计划宜包括制定应用扩展评审规程（必要时优化评审规程）的策略，以减少重复工作并提供有成本效益的评审方案。之后，信息安全审核员宜最终确定评审计划，并获得必要的批准以实施计划。

8.2.2 评估范围

范围界定了评估的组织和技术边界，评估的范围宜以控制的选择为基础，例如所建立的连续监测计划、活动计划中的项目和适当的里程碑。宜对不稳定的控制实施更频繁的评审。

评估的范围需要由信息安全审核员与管理层结合组织文件确定。文件宜提供信息资产安全需求的概述，并描述为满足这些安全需求现有的或计划的控制。审核员以信息安全文档中所描述的控制为起点并考虑评审目的。评审可以是对组织内所有信息安全控制措施的完整评审或对信息资产保护措施的部分评审（例如：在连续监视期间，对信息资产中的控制子集进行持续评审）。对于部分评审，信息资产负责人宜与评审相关的组织管理者共同确定需要评审哪些控制。

8.2.3 评审规程

评审规程包含一组评审目的，每个评审规程都可能有一组关联的评审方法和评审对象。明确陈述评审目的，使其与控制内容（即控制功能）紧密关联，确保了评审结果可追溯至基本控制措施要求。评审规程应用于某一控制措施后产生评审发现。这些评审发现随后将有助于确定控制措施的整体有效性。评审对象表明了要评审的特定项，包括了规范的说明、机制、过程和人员。

附录B提供了技术性评估和控制措施增强评审规程的示例。附录B中的实践指南用于收集证据，这些证据将用来确定控制是否正确实现、按预期运行，并产生与满足信息资产安全需求相关的预期输出。对于评审中所包括的每一个控制和控制增强，审核员可参照附录B制定相应的评审规程。在不同的评审中，根据当时的评审目的选择不同评审规程（例如年度控制措施评审，连续监视）。附录B提供了一个基于特定的评审关注点选择适宜的评审规程的工作表。

可以通过下列方式裁剪评审规程：

a） 选择能够最有效做出适当判定并满足评审目的所需的评审方法和评审对象；
b） 根据被评审的控制的特征和需做出的具体判定来选择评审方法的深度和覆盖范围的特征值，以满足评审期望；
c） 如果某些控制已被其他评审过程充分评审，则可删除相应的评审规程；
d） 修订适用于特定的信息系统/平台和特定组织的评审规程，以便成功地实施评审；
e） 在评审结论中引用以往合适的评审结果；
f） 如需从供应商获得必要的评审证据，则适当调整评审规程；
g） 在确保满足实现评审目的情况下，选择的评审方法宜考虑其对组织的影响。

8.2.4 与对象有关的考虑

组织可以通过多种方式来描述、记录和配置他们的信息资产，因此现有评审证据的内容和适用性会有所不同。这可能需要对不同的评审对象应用不同的评审方法，以形成用于确定控制在应用中是否有效的评审证据。因此，每个评审规程提供的评审方法和评审对象列表，被称为“潜力”，为了反映这一点，需要为特定的评审选择最合适的方法和对象。选用的评审方法和对象是为产生评审证据所必须的。评审规程中的潜在方法和对象是作为一种资源协助选择适当的方法和对象，而不是为了限制选择。因此，在从潜在的评审方法中选择评审方法以及从已选方法相关的评审对象清单中选择评审对象时，审核员宜有自己的判断。

信息安全审核员宜只选择那些有助于最有效的做出与评审目的相关的决定的方法和对象。测量评审结论的质量是基于所提供的选择评审方法和对象理由的合理性，而不是所采用的特定的方法和对象本身。

在大多数情况下，没有必要为了达到理想的评审结果而对每一个评审对象使用各种评审方法。而对于特定和全面评审，使用目前未列入的潜在方法或者不采用已列入的方法都可能是适宜的。

8.2.5 以往的发现

8.2.5.1 概述

信息安全审核员宜利用现有的控制评审信息以促进更有效地评审。

宜将先前已接受或批准的信息系统评审结论的重用作为确定所有控制有效性证据的一部分。

当考虑再次使用以往的评审结论和这些结论对当前评审的价值时，审核员宜确定：

——证据的可信性；

——以往分析的合理性；

——证据对当前信息资产状况的适用性。

当考虑再次使用以往的评审结果时，在某些情况下可能有必要通过附加的评审活动对其进行补充，以完全满足评审目的。例如，如果一个信息技术产品的独立第三方评价没有测试某信息系统中组织所采用的某特定配置的设置，那么审核员可能需要通过附加的测试来覆盖这种配置的设置，以补充原有的测试结果。

在确认以往的评审结果能否在当前评审中再次使用时，宜考虑8.2.5.2至8.2.5.4章节。

8.2.5.2 环境变化

在以往的评审中被视为有效的控制可能由于与信息资产或者周围环境相关的条件改变而变得无效，因此之前被认为可以接受的评审结论可能不再提供可信的证据来确定控制的有效性，故需要一次新的评审。将之前的评审结论应用于当前的评审，需要识别自上次评审以来发生的任何变更和这些变更对以往评审结果的影响。例如，如果确定已识别的策略、规程和风险环境没有显著变化，就可重用之前的评审结果检查组织的安全策略和规程。

8.2.5.3 重用评审结果的可接受性

在控制评审中使用以往的评审结果是否可接受（在控制评审时是否可使用以往的评审结果），宜与评审结论的使用者协调并获得其批准。在确定使用之前的评审结果时，信息资产所有者有必要与相应的组织管理者（例如，首席信息官、首席信息安全官、任务/信息所有者）配合。决定重新使用评审结果的决定宜记录在评审计划和最终报告中。

只要符合以下条件，安全评审可以包括以往的安全评审发现：

a） 审核计划中明确允许；

b） 来自以往评审的与本次审核有关任何限制或问题都应记录，这包括目前正在进行的实施计划部分解决的问题；

c） 审核员有充分的理由相信审核发现仍然有效；

d） 当前评审对这些运用于控制和过程中的任何技术或者规程上的审核发现的改变给予了充分的安全考虑。

e） 审核报告中明确表述了使用以往的审核发现和使用这些审核发现对风险管理潜在的影响。

8.2.5.4 时效

一般情况下，随着当前和以往评审之间的时间间隔增加，以往评审结果的可信性/可用性就会下降。主要是因为信息资产或者信息资产运行的环境更可能随着时间的推移而改变，可能会使之前评审依据的原始条件或者设想失效。

8.2.6 工作分配

信息安全审核员的独立性在某些类型的评审中是关键因素，尤其是对中等和高风险的信息资产。每次评审需要的独立性程度宜保持一致。例如，在当前更高独立性的评审中，不适合重新使用以往未要求审核员独立性的自我评估的结论。

8.2.7 外部系统

为适应外部信息系统的评审，需适当调整附录B中的评审方法和规程。因为组织并不能总是直接控制外部信息系统中所使用的安全控制，或对这些控制的开发、实现和评审上并不总是充分的了解，因此可能有必要采用替代的评审方法，这可能需要裁剪附录B中描述的评审规程。信息系统所需要的保障或已协定的控制需被记录在合同或服务级别协议中。审核员宜评审这些合同或协议，并在适当的情况下调整评审规程来评审按这些协议提供的控制或控制评审结果。此外，对于运行外部信息系统对被评审的信息资产进行保护的组织，审核员宜对组织已进行或正在进行的评审予以考虑。宜将评审中认为可信的可用信息纳入报告中。

8.2.8 信息资产和组织

评审规程可做调整以适应系统/平台特定的或组织特定的依赖关系。在技术性信息安全控制措施（即访问控制、审核与责任追究、标识与鉴别、系统和通信保护）相关的评审规程中常有这种情况。如果这些测试方法提供较高透明度（例如，测试了什么、何时测试、如何测试），最近的测试结果也可能适用于当前的评审。基于标准的测试协议可为组织如何帮助达到这种程度的透明提供范例。

8.2.9 扩展的评审规程

在达到信息安全控制措施的保障要求时组织有很大的灵活性。例如，保障缺陷及时处理的要求，组织可以基于具体控制、控制类型、具体系统甚至组织级别来满足要求。

考虑到这种灵活性，扩展的评审规程要基于逐个评审的基础加以应用，通常依照组织选择如何对评审中信息资产实现保障的方式。应用的方法宜记录在评审计划中。此外，组织根据信息资产风险水平为扩展的评审规程选择适当的评审目的。扩展的评审规程的应用是为了补充其他评审规程，以增加对控制正确实现、按预期进行操作、对符合适用的信息安全需求产生所期望结果的信心。

8.2.10 优化

信息安全审核员可以有一定程度的灵活性来组织所需的评审计划。这是一种在获取安全控制有效性必要证据的同时降低整体评审成本的机会。

在设计一个满足组织需求的评审计划上有一定的灵活性。在评审期间，评审方法可多次应用于信息安全控制措施特定区域内的各种评审对象。

为节省时间、降低评审成本、并最大限度地提高评审结果的可用性，审核员在可能或可行的情况下，宜评审选定的控制领域的评审规程和联合或整合程序（或规程的一部分）。

例如，信息安全审核员可能希望合并与组织内负责处理各种信息安全相关主题的关键管理者的访谈。审核员可通过同时检查所有适用的安全策略和规程，或组织相关策略和规程组（可作为一个统一实体进行检查），获得重大合并和节约成本的机会。获取并检查相关信息系统内相似的硬件和软件组件的配置设置是另一个可明显提高评审效率的示例。

优化评审过程中，另外需要考虑的一个问题是评审安全控制的顺序。先对一些控制评审可能会提供一些有利于了解和评审其他控制的信息。例如，控制领域可能会对信息资产进行一般性描述。在评审过程的早期对这些安全控制进行的评审可提供对信息资产的基本了解以帮助评审其他安全控制。许多控制的附加指南同样能识别在组织评审规程中提供有用信息的相关控制。换句话说，评审实施的顺序可能有助于将一个控制的评审信息在评审其他相关控制中再利用。

8.2.11 定稿

选择评审规程（包括开发不包含在本文中的必要规程）后，根据信息特定资产和组织特定的条件调整规程，使规程在效率上最优化，在必要时应用扩展的评审规程，并解决可能影响评审的意外事件，评审计划的完成和进度表的建立包含评审过程的关键里程碑。

一旦完成评审计划，该计划将由适当的组织管理者要评审和认可，以确保计划是：

——完整的；

——符合组织的安全目的和组织的风险评审；

——为评审而分配的资源有成本效益。

如果评审可能干扰组织的正常运作（例如由于渗透测试阻碍了关键人员通信或可能的（临时）系统故障），评审计划需要突出显示这些干扰的程序和时间范围。

8.3 实施评审

组织批准评审计划后，审核员根据达成一致的里程碑和日程执行计划。

针对已选择的评审对象应用设定的评审方法，并收集/形成与每个评审目的决策相关的必要信息，以此实现评审目的。审核员实施评审规程中作出的每一个判定陈述，可能有以下发现之一：

——满足（S）；

——部分满足（P）；

——不满足（O）。

“满足”表明，对于由判定申明所涉及的部分控制，获得的评审信息（即评审证据）表明控制的评审目的已经达到并产生完全可以接受的结果（S）。

“部分满足”表明在评审时，针对其目的，部分控制并未完全达到，或控制的实现仍在进行中，且保证控制将达到一个满意的结果（P）。

“不满足”表明，对于判定申明所涉及的部分安全控制，获得的评审信息表明控制在操作或实现中有潜在的异常情况，可能需要组织解决相关问题（O）。如果发现为“不满足”，也可能表明审核员无法获得足够的信息来做出在判定申明中需要的特殊判定，理由在评审报告中说明。

信息安全审核员宜根据控制评审中的发现形成公正的、基于事实的评审发现（即所做的判定）。对于每个“不满足”，审核员宜说明安全控制的哪些部分受到影响（即，被认为不满足的或不能够进行评审的控制），并描述控制与计划和期待的状态有何不同。审核员也宜注意那些“不满足”的发现记录对保密性、完备性和可用性的潜在影响。如果评审发现了可能会给组织带来显著风险的严重不符合项（即那些严重偏离计划的状况、“不满足”的调查发现），审核员宜立即通知负责人和管理层，以便立即启动风险降低程序。

8.4 分析和报告结果

评审计划提供了评审目的和如何进行评审的详细引导。评审报告作为评审输出和最终评审结果，记录了基于已实现的信息安全控制措施的信息安全保障水平。报告内容包括审核员作出的判断所使用控制有效性的必要信息以及基于其发现所作出的组织在实施适当的控制时的整体有效性的信息。该报告是确定组织的业务运作（即，任务、职能）、组织资产、个人和其他组织的信息安全风险的一个重要因素。

评审结果宜按照组织策略规定的评审报告格式，以适宜的详细程度来记录。该报告的格式也宜与控制评审的类型相适应（如信息系统负责人的自我评估、独立的验证和确认、审核员实施的独立控制评审）。

信息系统的负责人依赖审核员的信息安全专业知识和技术判断对安全控制进行评审，并就如何纠正控制的弱点和缺陷以及减少或消除已识别的脆弱性提出具体的建议。

在安全评审报告初稿中，审核员将把评审有关的信息（既“满足”或者“不满足”的评审发现/关于部分未产生令人满意的安全控制的鉴定/对危及信息资产的潜在危害的描述）提供给管理层。信息资产负责人可以选择：

——在评审报告定稿前，如果有机会纠正控制的脆弱性；

——纠正/澄清对评审结果的误解和解释。

信息安全审核员宜在评审报告定稿前把在此过程中被修改过的、增强的或者新增的控制重新评审一遍。将最终报告提交给管理层意味着信息安全控制措施评审的正式结束。

因为评审结果最终影响信息安全控制措施的内容、行动计划和里程碑，信息资产负责人要核对信息安全审核员的发现，并与管理层共同确定改正评审中已确定的脆弱性的适当步骤。通过使用“满足”（S）、“部分满足”（P）和“不满足”（O）的标记，报告评审发现的形式为管理层提供了关于特定弱点和信息安全缺陷信息，有助于按照信息安全风险管理的规程采取制度化和结构化的方法来降低风险。

例如，信息资产负责人经与管理层协商可决定某些标记为不满足的评审发现是不重要的，并不会给组织带来重大的风险。反之，信息资产负责人和管理者可能决定某些标记为不满足的评审发现是重要的，需要立即采取补救措施。总之，组织核对审核员发现的不满足证据，并就评审发现的严重程度和重要性（即，对组织的业务、资产、个人或其他组织的潜在不利影响）进行判断，并判定该评审发现是否足以证明进一步调查或需要采取补救措施是合理的。高级管理层参与降低风险的过程可能是必要的，以确保组织资产按照组织优先级来分配。这可以通过将资源首先分配给组织中支持最多关键业务的信息资产，或者分配给纠正导致最大风险缺陷的信息资产。最后根据评审发现，由信息资产负责人与组织指定的负责人协商发起的降低风险的措施，使得信息安全风险管理过程和信息安全控制措施得以更新。于是，管理人员更新用于判定信息资产安全状态的关键文件以反映新的评审结果。

在预先确定的里程碑或评审后的固定周期，例如最终报告完成后的三个月，通常会进行一次跟踪评审，重点关注那些待解决的或没有定论的问题，包括验证对以往评审发现实施方案的有效性。组织也可选择在下次评审时执行跟踪评审，特别是针对那些非关键或不紧急的问题。

附 录 A
（资料性）
初始信息收集（除信息技术以外）

A.1 总则

A.1.1 人力资源和安全

a） 相关人员是否能对其行为负责或承担义务；
b） 相关人员是否具有信息和信息安全常识、并能解答相关问题，激励他人并提供必要的指导；
c） 申请策略和规程是否清晰、明确、可测量、可接受、可实现、有时限；
d） 已受聘雇员是否具备组织期望的运行知识；
e） 组织是否信任接触可能危及组织生存的信息和系统的相关人员；
f） 相关人员是否值得信任；
g） 信任是如何被组织进行定义和测量的；
h） 是否进行了背景调查。

A.1.2 策略

A.1.2.1 战略一致性:
a) 信息安全方针是否与组织业务目标和总体安全策略保持一致；
b) 如何使信息技术、人力资源和获取方针联系在一起。

A.1.2.2 综合:
a) 这些方针是否能够覆盖组织所有业务活动区域的信息安全（人力资源、物理环境、信息技术、销售、制造、研发和合同安全等）；
b) 这些方针是否被设计成能够完整涵盖组织战略、战术和运营。

A.1.2.3 规划：
a) 这些方针是直接使用了 GB/T 22081 的相关内容，还是针对特定的背景对控制目标和控制进行了剪裁：
b) 这些方针是否以书面形式明确了执行者的职责？
c) 在一个策略中有一个期望活动，或者有一套考虑谁、何时、为什么、什么、哪里、如何等的基础性问题的规程：
   1） 如果没有明确执行活动的责任人(谁)，由谁来负责达成这组目标；
   2） 如果没有定义执行活动的时间（何时），是否能保证其按时启动和完成；
   3） 如果没有定义活动的目的和目标（为什么），活动是否会被正确理解，其重要性是否会被充分考虑到；
   4） 如果没有定义活动的内容（什么），如何知道该做什么；
   5） 如果一个活动没有定义对象、执行地点、操作规程和信息资产（哪里），或者没有定义其效果控制，如何使它有效；
   6） 一个规程中的活动如果没有明确定义如何被完成（如何），如何保证其能被正确执行；
   7） 如果一个活动没有定义指标和控制点，以验证其是否正确包含并且达到其既定目标，如何确保或能够达成组织目标；
d) 是否有控制和检测环境，以鉴定组织策略声明强制执行、实现和可达成既定目标；
e) 在策略声明中的目标陈述宜考虑明确、可测量、可接受、可实现、有时限准则，否则：
   1） 没有明确目标则不容易被清晰地辨识，并且未达成目标的责任也无法落实到人；
   2） 如果目标不可测量，组织一般无法验证目标的达成程度；

3） 如果目标没有在组织内进行充分沟通并达成共识，则可能造成对控制的被误解、被规避或被中断；
4） 如果组织不是根据自身的实际能力来确定目标，很可能因不切合实际而不能达到；
5） 如果组织没有确认实现方针目标的预期起始和结束时间点，就很可能无法确保组织能够采取实际的行动，达成目标也难以实现。

A.1.3 组织

a) 是否在考虑了在组织的特定环境和限制条件的情况下对组织人员角色和职责进行充分且必要定义和分配，以满足组织的业务目标；
b) 是否与外部机构保持联系；
c) 组织是否对自身没有能力承担的安全管理责任进行了外包；
d) 合同是否阐述信息安全的相关要求。

A.2 物理和环境安全

A.2.1 工作场所能否保证信息安全

a) 区域：
   1) 业务区与公众访问区是否充分隔离；
   2) 是否在定义了敏感信息处置的范围（通过人员或信息通信技术系统）；
   3) 这些安全区域是否被恰当地隔离，以避免其相互间的敏感信息交换。
b) 位置：
   1) 不同安全级别的区域是否被明确标识，并合理部署；
   2) 是否清晰地定义了边界（墙，天花板，地板等）以及其稳固性是否适合保护所包含的资产；
   3) 位置是否贴有适当的标识且关键位置是否对外部人员不可见。
c) 出入口：
   1) 当边界内的门窗或其它开口处于关闭状态时，能否提供与边界相当的防护能力；
   2) 是否对这些区域位置的进出采取适当的访问控制；
   3) 是否有防入侵系统；
   4) 是否有允许信息、人员和设备充分移动的紧急出口。
d) 走廊和通道：
   1) 能否识别去往固定区域或位置的通道，即人员的通道和线缆（信息传输通道）；
   2) 是否有可替代的通道；
   3) 这些通道是否受到保护和监控。
e) 监控：
   1) 监控设备能否在不被发现的情况下正常工作；
   2) 监控设备能否发现远处的入侵；
   3) 监控何时启动；
   4) 监控记录保存在哪里以及如何进行分析。
f) 装置：
   1) 是否适合于信息存储；
   2) 是否正确摆放；
   3) 实际运行是否和预期的结果一致。

A.2.2 工作场所能否保证信息通信技术的安全（环境方面）

a) 电力设施：
   1) 是否足够/适当；
   2) 是否有备用。
b) 空调设施：
   1) 是否足够/适当；
   2) 是否有备用。
c) 防火设施：
   1) 是否足够/适当；
   2) 是否有备用。

A.2.3 工作场所能否保证人员安全

a) 是否有紧急出口（并且采取了适当的控制）；
b) 电、水、气体、液体的泄漏是否对人员构成潜在危险；
c) 温度、湿度、材料和震动是否对人员构成潜在危险；
d) 设备的位置是否防止人员受伤；
e) 门的安装和操作是否防止人员受伤；
f) 装置的安装和维护是否防止人员受伤。

A.3 事件管理

a) 是否定义了信息安全事件；
b) 是否有响应信息安全事件的能力：
   1) 是否有指南或手册；
   2) 是否分配了角色和职责。

附 录 B
（资料性）
技术性安全评估实践指南

B.1 总则

本附录使用GB/T 22081-2016中描述的典型技术性控制措施为技术性评估提供一套实践指南。本附录中的每项控制措施基本上按照以下陈述和指南的结构来组织。GB/T 22080不要求只能从GB/T 22081中选择组织使用的控制措施。其他控制措施，如GB/T 32920和ISO/IEC 27017等标准中的行业特定控制措施可能是必要的。此外，组织可以设计自己的控制。本附录旨在说明可以使用的各种技术性评估的方法，使用GB/T 22081中的示例已足够。

B.2.1至B.2.14为GB/T 22081-2016中的每项控制提供了一个表格（见表B.1至表B.35），其内容按以下表述分组。

“技术控制”（带“附加技术信息”）

1 安全实施标准（带“安全实施标准技术注解”）

1.1 实践指南，设想的证据，方法

1.2 实践指南，设想的证据，方法

2 安全实施标准（带“安全实施标准技术注解”）

2.1 实践指南，设想的证据，方法

2.2 实践指南，设想的证据，方法

每个技术控制都有附加的技术信息，以便为信息安全审核员提供进一步的支持。它基本上由一系列“安全实施标准”组成，组织宜定期评审这些标准，以验证适用的标准是否得到适当的实现和运行。

每个“安全实施标准”都有一个补充的“安全实施标准技术注解”，为评审过程提供进一步的技术信息。它还提供了一系列的“实践指南”、“设想的证据”和“方法”。

“实践指南”提供了适用于安全实施标准的符合性检查规程。“设想的证据”列举了一些在符合性检查规程中可以接受为“证据”的系统、文件、文档或其他项目的例子。请注意，证据的名称可能因组织而异。然而，本附录中使用的名称可被认为在技术性评估领域普遍接受的。“方法”根据上述实践指南提供了一种适当的技术性评估方法。

本附录并未提供全部的技术性评估实践指南，但仍将尽最大可能帮助各类组织评审安全实施标准是否得到适当实施和运行。

B.2 GB/T 22081-2016 中控制的评估

B.2.1 信息安全策略

表 B.1

GB/T 22081-2016，5.1 信息安全管理指导		
	控制	**GB/T 22081-2016，5.1.1 信息安全策略** 信息安全策略集宜被定义，由管理者批准，并发布、传达给所有员工和外部相关方。
	控制	**GB/T 22081-2016，5.1.2 信息安全策略的评审** 宜按计划的时间间隔或当重大变化发生时进行信息安全策略评审，以确保其持续的适宜性、充分性和有效性。

B.2.2 信息安全组织

表 B.2

GB/T 22081-2016，6.1 内部组织		
	控制	**GB/T 22081-2016，6.1.1 信息安全的角色和责任** 所有的信息安全责任宜予以定义和分配。
	控制	**GB/T 22081-2016，6.1.2 职责分离** 宜分离可发生冲突的职责及其责任范围，以减少未授权或无意的修改或者不当使用组织资产的机会。
	控制	**GB/T 22081-2016，6.1.3 与职能机构的联系** 宜维护与相关职能机构的适当联系。
	控制	**GB/T 22081-2016，6.1.4 与特定相关方的联系** 宜维护与相关部门的适当联系。
	控制	**GB/T 22081-2016，6.1.5 项目管理中的信息安全** 宜关注项目管理中的信息安全问题，无论何种类型的项目。

表 B.3

GB/T 22081-2016， 6.2 移动设备和远程工作		
	控制	**GB/T 22081-2016，6.2.1 移动设备策略** 宜采用相应的策略及其支持性的安全措施以管理由于使用移动设备所带来的风险。
	控制	**GB/T 22081-2016，6.2.2 远程工作** 宜实现相应的策略及其支持性的安全措施以保护在远程工作地点上所访问的、处理的或存储的信息。

B.2.3 人力资源安全

表 B.4

GB/T 22081-2016，7.1 任用前		
	控制	**GB/T 22081-2016，7.1.1 审查** 宜按照相关法律法规和道德规范，对所有任用候选者的背景进行验证核查，并与业务要求、访问信息的等级和察觉的风险相适宜。
	控制	**GB/T 22081-2016，7.1.2 任用条款及条件** 宜在员工和合同方的合同协议中声明他们和组织对信息安全的责任。

表 B.5

GB/T 22081-2016，7.2 任用中		
	控制	**GB/T 22081-2016，7.2.1 管理责任** 管理者宜要求所有员工和合同方按照组织已建立的策略和规程应用信息安全。
	控制	**GB/T 22081-2016，7.2.2 信息安全意识、教育和培训** 组织所有员工和相关的合同方，宜按其工作职能，接受适当的意识教育和培训，及组织策略及规程的定期更新的信息。

表 B.5（续）

GB/T 22081-2016，7.2 任用中		
	控制	**GB/T 22081-2016，7.2.3 违规处理过程** 宜有正式的、且已被传达的违规处理过程以对信息安全违规的员工采取措施。

表 B.6

GB/T 22081-2016，7.3 任用的终止和变更		
	控制	**GB/T 22081-2016，7.3.1 任用终止或变更的责任** 宜确定任用终止或变更后仍有效的信息安全责任及其职责，传达至员工或合同方并执行。

B.2.4 资产管理

表 B.7

GB/T 22081-2016， 8.1 有关资产的责任		
	控制	**GB/T 22081-2016，8.1.1 资产清单** 宜识别信息，以及与信息和信息处理设施相关的其他资产，并编制和维护这些资产的清单。
	控制	**GB/T 22081-2016，8.1.2 资产的所属关系** 宜维护资产清单中资产的所属关系。
	控制	**GB/T 22081-2016，8.1.3 资产的可接受使用** 宜识别可接受的信息使用规则，以及与信息和信息处理设施有关的资产的可接受的使用规则，形成文件并加以实现。
	控制	**GB/T 22081-2016，8.1.4 资产归还** 所有员工和外部用户在任用、合同或协议终止时，宜归还其占用的所有组织资产。

表 B.8

GB/T 22081-2016，8.2 信息分级		
	控制	**GB/T 22081-2016，8.2.1 信息的分级** 信息宜按照法律要求、价值、重要性及其对未授权泄露或修改的敏感性进行分级。
	控制	**GB/T 22081-2016，8.2.2 信息的标记** 宜按照组织采用的信息分级方案，制定并实现一组适当的信息标记规程。
	控制	**GB/T 22081-2016，8.2.3 资产的处理** 宜按照组织采用的信息分级方案，制定并实现资产处理规程。

表 B.9

GB/T 22081-2016，8.3 介质处理		
	控制	**GB/T 22081-2016，8.3.1 移动介质的管理** 宜按照组织采用的分级方案，实现移动介质管理规程。
	控制	**GB/T 22081-2016，8.3.2 介质的处置** 宜使用正式的规程安全地处置不再需要的介质。

表 B.9（续）

GB/T 22081-2016，8.3 介质处理		
	控制	**GB/T 22081-2016，8.3.3 物理介质的转移** 包含信息的介质在运送中宜受到保护，以防止未授权访问、不当使用或毁坏。

B.2.5 访问控制

表 B.10

GB/T 22081-2016，9.1 访问控制的业务要求			
	控制	**GB/T 22081-2016，9.1.1 访问控制策略** 宜基于业务和信息安全要求，建立访问控制策略，形成文件并进行评审。	
	控制的附加技术信息	访问控制规则宜得到正式规程和明确责任的支持。基于角色的访问控制是许多组织成功使用的一种方法，用于将访问权限与业务角色联系起来。	
1	安全实施标准	访问控制可通过许多不同方法实现，包括： ——PIM； ——电子锁系统； ——门卫服务； ——SIEM; 注：其中有些方法有局限性。例如，SIEM 只能分析和存储当使用某种形式的访问控制时发生的日志。电子锁系统可用来控制对资源的物理访问。PIM 可用来管理身份及其访问权限。	
	安全实施标准技术注解	访问控制的复杂性随其所保护的资产、攻击的威胁和成功攻击的影响而增加。	
	1.1	实践指南	检查是否只有授权人员才能访问资源。
		设想的证据	——访问日志； ——对访问控制机制的访问。
		方法	测试与确认
	1.2	实践指南	检查访问权限是否将在不再需要时被清除。
		设想的证据	——撤销测试身份； ——访问日志； ——用户管理访问。
		方法	测试与确认
	1.3	实践指南	检查在没有特权帐户的情况下是否可以绕过访问请求过程。
		设想的证据	——访问日志； ——无访问权限的身份； ——用于比较的特权身份； ——对访问控制机制的访问。
		方法	测试与确认

表 B.10（续 1）

GB/T 22081-2016，9.1 访问控制的业务要求			
	1.4	实践指南	检查是否记录了所有访问事件，并可对其进行取证目的的分析，以便于取证。
		设想的证据	——日志文件； ——日志的业务需求。
		方法	测试与确认
	1.5	实践指南	检查是否有可能升级访问资源的特权
		设想的证据	——访问日志； ——无访问权限的身份； ——对访问控制机制的访问。
		方法	测试与确认
	1.6	实践指南	检查是否不可能绕过访问控制。
		设想的证据	——访问日志； ——无访问权限的身份； ——对访问控制机制的访问。
		方法	测试与确认
	1.7	实践指南	检查访问权限是黑名单还是白名单，并检查是否缺少任何资产。
		设想的证据	——业务要求； ——访问控制的业务要求； ——对访问控制管理界面的访问。
		方法	测试与确认
	1.8	实践指南	检查是否无法克隆或复制访问令牌或假扮其他人。
		设想的证据	——无访问权限的身份； ——具有要模仿的访问权限的身份； ——对访问控制机制的访问。
		方法	测试与确认
	控制	**GB/T 22081-2016，9.1.2 网络和网络服务的访问** 宜仅向用户提供他们已获专门授权使用的网络和网络服务的访问。	
	对控制的附加技术信息	未经授权和不安全的网络服务连接会影响整个组织。这个控制对于敏感或关键业务应用程序，或处于高风险位置（例如，组织信息安全管理和控制之外的公共或外部区域）的用户的网络连接尤为重要。	
1	安全实施标准	宜制定有关使用网络和网络服务的策略。	
	安全实施标准技术注解	该策略宜包括： a） 允许访问的网络和网络服务； b） 确定允许谁访问哪些网络和网络服务的授权程序； c） 对网络连接和网络服务访问的控制进行保护的管理控制和规程； d） 用于访问网络和网络服务的方式（例如，使用 VPN 或无线网络）；	

表 B.10（续 2）

GB/T 22081-2016，9.1 访问控制的业务要求			
		e） 访问各种网络服务的用户认证要求； f） 监控网络服务的使用。 使用网络服务的策略宜与组织的访问控制策略保持一致。	
	1.1	实践指南	适用时，使用网络嗅探来识别从网络服务响应或请求发出的协议。例如，网络基本输入/输出系统协议、地址解析协议、开放式最短路径优先协议等。
		设想的证据	对网络流量的访问。
		方法	测试与确认
	1.2	实践指南	验证所有目标的广播请求和响应是否与网络图和其他文件一致。
		设想的证据	——访问网络图； ——访问网络流量。
		方法	测试与确认
	13	实践指南	通过运行端口扫描发现并识别授权网络中所有打开的端口和服务。为发现的 TCP 和 UDP 端口请求所有服务标语（标志）。验证发现的服务是否基于用户权限和系统功能进行了调整。
		设想的证据	——对系统规范的访问； ——允许在目标网络中进行的端口扫描。
		方法	测试与确认
	1.4	实践指南	通过地址冒用在网络或其他网络中检测访问服务的措施。
		设想的证据	可以在测试或非关键环境中进行的地址欺骗。
		方法	测试与确认
	1.5	实践指南	通过多个网卡枚举和识别在其他受限网络中具有支点的所有系统。试图破坏这些入口点，以进入受限制的网络。
		设想的证据	完整的网络图。
		方法	测试与确认
	1.6	实践指南	枚举并标识可用于访问授权网络外部系统的所有远程桌面服务。试图通过远程桌面获得未经授权的访问，以进入受限制的网络。
		设想的证据	——完整的网络图； ——可连接到授权网络之外系统的远程桌面服务。
		方法	测试与确认
	1.7	实践指南	检查并验证防火墙规则，以确保仅向网络和网络服务授予预期的访问权限。
		设想的证据	——对防火墙规则的访问； ——对防火墙日志的访问。
		方法	测试与确认

表 B.11

GB/T 22081-2016，9.2 用户访问管理		
	控制	**GB/T 22081-2016，9.2.1 用户注册与注销**

表 B.11（续 1）

GB/T 22081-2016，9.2 用户访问管理			
		宜实现正式的用户注册及注销过程，以便可分配访问权。	
	控制的附加技术信息	宜利用正式过程分配、限制和控制特权用户对网络、服务和资源的访问。	
1	安全实施标准	宜记录并实施下列过程： ——用户注册和注销； ——用户访问设置； ——特权访问权的管理； ——用户秘密鉴别信息管理； ——评审用户访问权限； ——删除或调整访问权限。	
	安全实施标准技术注解	特权访问权的分配宜根据相关访问控制策略，通过正式授权过程进行控制。	
	1.1	实践指南	验证所有用户 ID 都是唯一的和个人特定的。通过抽查确认以前雇员的账户不再有效。检查是否有不正常的长时间未使用的用户 ID。
		设想的证据	——对用户管理部门的访问； ——对正式雇员或用户 ID 列表的访问。
		方法	测试与确认
	1.2	实践指南	确保口令的复杂性增加猜测口令难度，并且用户名不是公开信息，如电子邮件地址或社会安全号码。
		设想的证据	——访问口令策略； ——基于用户名和口令的授权。
		方法	测试与确认
	1.3	实践指南	确保在重置口令之前，用户必须对秘密答案、秘密问题或其他预定信息做出响应。
		设想的证据	——访问口令策略； ——基于用户名和口令的授权； ——访问口令重置功能； ——授权测试帐户。
		方法	测试与确认
	1.4	实践指南	当输入错误口令超过特定次数时，确保用户帐户被锁定一段时间。
		设想的证据	——授权测试帐户； ——基于用户名和口令的授权。
		方法	测试与确认
	1.5	实践指南	枚举目标上默认帐户的情况，通过最适宜和可用的破解技术测试对身份鉴别访问点的访问。
		设想的证据	基于用户名和口令的授权。
		方法	测试与确认

表 B.11（续 2）

GB/T 22081-2016，9.2 用户访问管理			
	控制	**GB/T 22081-2016，9.2.2 用户访问供给** 宜实现一个正式的用户访问设置过程，为所有系统和服务分配或撤销所有用户类型的访问权限。	
	控制	**GB/T 22081-2016， 9.2.3, 特许访问权管理** 宜限制并控制特许访问权的分配和使用。	
	附加技术信息	特权管理非常重要，因为特权的不当使用会对系统造成重大影响。 特权分配的状态宜在定义特权的文档（特权定义文档）中描述。因为与每个系统产品（操作系统、数据库管理系统和每个应用程序）相关联的访问特权是不同的。 特权类型示例如下： ——根目录（UNIX、Linux）； ——管理员（Windows）； ——备份操作员（Windows）； ——超级用户（Windows）； ——系统管理员（数据库管理系统）； ——数据库管理员（数据库管理系统）。 特权的分配宜在必须使用的基础上达到最低限度，且不需要经常分配。 系统中特权管理的方法是不同的。基于系统的特权管理示例如下： ——在操作系统中，ACL 定义了特权； ——在数据库管理系统中，定义了各种默认特权， ——在应用程序中，可以为应用程序的管理功能定义各种默认特权，因此信息安全审核员宜事先确定检查级别； ——在安全操作系统中，它具有强制访问控制的功能。	
1	安全实施标准	宜确定与每个系统产品（如操作系统、数据库管理系统和每个应用程序）相关联的访问特权，以及需要向其分配的用户。	
	安全实施标准技术注解	由于特权使用不当会对系统造成重大影响，因此宜对特权用户活动进行监控。如果系统结构不同，检测特权不当使用的方法也不同。 注：典型的系统架构包括： ——Mainframe； ——Windows； ——UNIX、Linux； ——安全操作系统。	
	1.1	实践指南	检查特权定义文档中所描述的特权分配。
		设想的证据	特权定义文档。
		方法	检查/观察
	1.2	实践指南	检查系统配置的设置是否如定义特权的文档中所述。特权操作的检查方法依系统架构不同而不同。 特权操作检查方法的示例如下： 1）（对于 Mainframe）通过检查 RACF 来检查特权的使用状态是否适当； 2）（对于 UNIX、Linux 或 Windows）通过调查显示特权使用情况的日志，检

表 B.11（续 3）

GB/T 22081-2016，9.2 用户访问管理			
			查特权使用的状态是否适宜。 注： 1） RACF 是一种主机安全管理中间件； 2） 在 UNIX 或 Linux 中，只检查 root 登录以调查 root 的不适当使用是危险的。原因是普通用户在 UNIX 或 Linux 上登录后，可能会使用 su 命令成为 root 用户。
		设想的证据	——特权定义文档； ——访问控制列表； ——RACF 报告。
		方法	检查/观察
2	安全实施标准	权限宜分配给区别于正常业务使用的用户 ID。	
	安全实施标准技术注解	在特权访问的情况下，存在未经授权操作的可能性，这种使用特权的情况经常成为未授权访问的温床。 如果操作不需要特权，用户宜使用他们的常规 ID。如果允许使用“root”特权限登录，则无法从日志中识别登录到系统的用户。	
	2.1	实践指南	通过观察系统的 ACL，检查特权用户是否有特权 ID 之外的正常用户 ID。
		设想的证据	访问控制列表
		方法	检查/观察
	2.2	实践指南	通过观察日志文件，检查特权用户是否为正常业务使用不同的用户 ID。 如果是 UNIX 或 Linux，检查系统配置，确保系统拒绝“root”登录。 注：当日志表明特权用户仅使用特权 ID 时，信息安全审核员宜尝试面谈检查特权用户是否使用不同用户 ID 用于正常业务用途。
		设想的证据	——日志文件； ——用“root”登录的系统配置。
		方法	检查/观察
	控制	**GB/T 22081-2016，9.2.4 用户的秘密鉴别信息管理** 宜通过正式的管理过程控制秘密鉴别信息的分配	
	控制	**GB/T 22081-2016，9.2.5, 用户访问权评审** 资产拥有者宜定期对用户的访问权进行评审。	
	控制	**GB/T 22081-2016，9.2.6, 访问权的移除或调整** 所有员工和外部用户对信息和信息处理设施的访问权在任用、合同或协议终止时，宜予以移除，或在变更时予以调整。	

表 B.12

GB/T 22081-2016， 9.3 用户责任		
	控制	**GB/T 22081-2016，9.3.1 秘密鉴别信息的使用** 应要求用户遵循组织在使用秘密鉴别信息时的惯例。

表 B.12（续）

GB/T 22081-2016， 9.3 用户责任			
	控制的附加技术信息	宜使用秘密身份验证信息的主要方法是直接使用用户的生物特征、使用包含秘密身份验证信息的设备（如 IC 卡）和使用口令。三种方法中的口令管理都需要对用户进行技术性评估。为了防止未经授权访问计算机资源，应创建口令并对不允许访问的人保密。 口令验证是一种由多种资源，如操作系统、程序、数据库、网络或网站，使用的用户验证方法。口令的质量取决于字符的长度和类型，如字母数字字符和标记。 用户可以为某些操作系统，如 Windows，配置口令策略的参数。另一方面，应用程序开发人员可以开发身份验证功能来配置口令策略。 审核员宜评估带有口令的授权功能是否有效地放置在计算机资源中，并且这些功能是否正常工作。	
1	安全实施标准	选择具有足够最小长度的高复杂度，这些口令是： 1） 易于记忆； 2） 不基于任何其他人易于猜出或获得的个人相关信息（如姓名，电话号码，出生日期等）； 3） 不易受到字典攻击（即不包含字典中包含的单词）； 4） 没有连续的、相同的、全数字的或全字母的字符； 5） 不同于以前的口令（考虑 n 代）。	
	安全实施标准技术注解	其他用户容易记住的口令通常是脆弱的。	
	1.1	实践指南	检查组织的口令策略中是否描述了口令选择规则。
		设想的证据	组织的口令策略
		方法	检查/评审
	1.2	实践指南	检查系统配置（系统口令策略）的设置是否如组织的口令策略中所述。
		设想的证据	——系统配置（系统口令策略）； ——组织的口令策略。
		方法	检查/观察
	1.3	实践指南	检查日志文件是否显示用户已更改口令。
		设想的证据	日志文件。
		方法	检查/观察

表 B.13

GB/T 22081-2016, 9.4 系统和应用访问控制		
	控制	**GB/T 22081-2016，9.4.1 信息访问限制** 宜按照访问控制策略限制对信息和应用系统功能的访问。
	控制	**GB/T 22081-2016， 9.4.2 安全登录规程** 当访问控制策略要求时，宜通过安全登录规程控制对系统和应用的访问。
	控制	**GB/T 22081-2016，9.4.3 口令管理系统** 口令管理系统应是交互式的，并宜确保优质的口令。

表 B.13（续）

GB/T 22081-2016, 9.4 系统和应用访问控制		
	控制	**GB/T 22081-2016，9.4.4 特权实用程序的使用** 对于可能超越系统和应用控制的实用程序的使用宜予以限制并严格控制。
	控制	**GB/T 22081-2016，9.4.5 程序源代码的访问控制** 宜限制对程序配置文件的访问，并宜对配置文件进行加密。

B.2.6 密码

表 B.14

GB/T 22081-2016，10.1 密码控制			
	控制	**GB/T 22081-2016，10.1.1，密码控制的使用策略** 宜开发和实现用于保护信息的密码控制使用策略。	
	有关控制的其他技术信息	密码学是一种保护计算系统和通信中的信息的工具。密码系统是标准协议，尤其是 TLS 协议的组成部分，可以轻松地将强大的密码功能集成到各种应用程序中。 这些密码控制可用于实现不同的信息安全目标，包括： ——保密性：使用信息加密以保护存储或传输中的敏感或关键信息； ——完整性：使用杂凑函数以验证信息的完整性； ——可鉴别性：使用密码协议以鉴别用户和系统对资源访问请求； ——真实性：使用诸如签名算法之类的密码技术来实现对通信或信息的不可否认性。 为了保护信息，宜确定通过使用密码学来防范威胁。	
1	安全实施标准	密码算法具有固有的复杂性，对密码控制的安全使用带来难度。在实施这些控制时，必须确保： ——使用足够的密钥长度； ——使用公认的强协议； ——使用公认的强密码算法； ——使用经过测试且能被安全地实现； ——持续评价。	
	安全实施标准技术注解	密码控制的实现应使用经过测试且强密码算法。不建议使用自行设计的密码算法。	
	1.1	实践指南	检查已实施密码控制的网络服务是否具有足够的密钥长度，并且不使用弱算法。
		设想的证据	——合法加密方法； ——访问加密服务。
		方法	测试与确认
	1.2	实践指南	检查所使用的密码控制实现是否安全。
		设想的证据	——密码控制的实现； ——所使用的版本控制机制。

表 B.14（续）

GB/T 22081-2016，10.1 密码控制			
		方法	测试与确认
	1.3	实践指南	检查移动设备和移动介质是否受强算法和足够的密钥长度的密码控制保护。
		设想的证据	——合法加密方法； ——访问移动媒体设备。
		方法	测试与确认
	1.4	实践指南	检查所有加密密钥是否安全可靠地存储，并且只能由授权人员访问。
		设想的证据	——加密密钥的访问控制方法； ——存储密钥的过程。
		方法	测试与确认
	1.5	实践指南	检查已实施密码控制的通信服务具有足够的密钥长度，并且不使用弱算法。
		设想的证据	——合法加密方法； ——访问加密服务； ——访问加密通信信息（例如证书）
		方法	测试与确认
	控制	**GB/T 22081-2016，10.1.2，密钥管理** 宜制定和实现贯穿其全生命周期的密钥使用、保护和生存期策略。	

B.2.7 物理和环境安全

表 B.15

GB/T 22081-2016,，11.1 安全区域		
	控制	**GB/T 22081-2016，11.1.1 物理安全边界** 宜定义和使用安全边界来保护包含敏感或关键信息和信息处理设施的区域。
	控制	**GB/T 22081-2016，11.1.2 物理入口控制** 安全区域宜由适合的入口控制所保护，以确保只有授权的人员才允许访问。
	控制	**GB/T 22081-2016，11.1.3 办公室、房间和设施的安全保护** 宜为办公室、房间和设施设计并采取物理安全措施。
	控制	**GB/T 22081-2016，11.1.4 外部和环境威胁的安全防护** 宜设计和应用物理保护以防自然灾害、恶意攻击和意外。
	控制	**GB/T 22081-2016，11.1.5 在安全区域工作** 宜设计和应用安全区域工作规程。
	控制	**GB/T 22081-2016，11.1.6 交接区** 访问点（例如交接区）和未授权人员可进入的其他点宜加以控制，如果可能，宜与信息处理设施隔离，以避免未授权访问。

表 B.16

GB/T 22081-2016，11.2　设备		
	控制	**GB/T 22081-2016，11.2.1 设备安置和保护** 宜安置或保护设备，以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会。
	控制	**GB/T 22081-2016，11.2.2 支持性设施** 宜保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断。
	控制	**GB/T 22081-2016，11.2.3 布缆安全** 宜保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听、干扰或损坏。
	控制	**GB/T 22081-2016，11.2.4 设备维护** 设备宜予以正确地维护，以确保其持续的可用性和完整性。
	控制	**GB/T 22081-2016，11.2.5 资产的移动** 设备、信息或软件在授权之前不宜带出组织场所。
	控制	**GB/T 22081-2016,11.2.6 组织场所外的设备与资产安全** 宜对组织场所外的资产采取安全措施，要考虑工作在组织场所外的不同风险。
	控制	**GB/T 22081-2016，11.2.7 设备的安全处置或再利用** 包含储存介质的设备的所有部分宜进行核查，以确保在处置或再利用之前，任何敏感信息和注册软件已被删除或安全的重写。
	控制	**GB/T 22081-2016，11.2.8 无人值守的用户设备** 用户宜确保无人值守的用户设备有适当的保护。
	控制	**GB/T 22081-2016，11.2.9 清理桌面和屏幕策略** 宜针对纸质和可移动存储介质，采取清理桌面策略；宜针对信息处理设施，采用清理屏幕策略。

B.2.8　运行安全

表 B.17

GB/T 22081-2016，12.1　运行规程和责任		
	控制	**GB/T 22081-2016，12.1.1 文件化的操作规程** 操作规程宜形成文件，并对所需用户可用。
	控制	**GB/T 22081-2016,12.1.2 变更管理** 宜控制影响信息安全的变更，包括组织、业务过程、信息处理设施和系统变更。
	控制	**GB/T 22081-2016，12.1.3 容量管理** 宜对资源的使用进行监视，调整和预测未来的容量需求，以确保所需的系统性能。
	控制	**GB/T 22081-2016，12.1.4 开发、测试和运行环境的分离** 宜分离开发、测试和运行环境，以降低对运行环境未授权访问或变更的风险。开发和测试环境宜使用匿名数据，以降低对运营数据产生影响的风险。

表 B.18

GB/T 22081-2016，12.2 恶意软件防范			
	控制	**GB/T 22081-2016,12.2.1 恶意软件的控制** 宜实现检测、预防和恢复控制以防范恶意软件，并结合适当的用户意识教育。	
	其他技术信息	恶意软件是一个通用术语，用来指包括软件，程序，脚本在内的，旨在通过窃取信息、欺诈、间谍、破坏和毁坏行为来损坏计算机系统的代码。 当恶意软件被植入计算机系统后，可能会损坏系统或窃取系统信息。这种行为也可能会危害其他系统。 恶意软件包括计算机病毒，蠕虫，特洛伊木马，僵尸程序，间谍软件，欺诈广告以及其他恶意和非期望的软件。 在组织网络接入互联网的情况下，信息安全审核员宜评审恶意软件的检测/预防功能全面有效地部署于互联网边界，且这些功能运行正常。 特别是，为了评审检测/预防功能是否正常运行，信息安全审核员必须确认用于检测恶意软件的样本文件或特征码是否已更新。 其中一些检测/预防系统被设计为使用样本文件或特征码来检测恶意软件，另一些被设计为不使用任何样本文件或特征码的系统来检测计算机系统的异常行为。 由于存在一些连接互联网的模式，例如通过网关将组织网络连接到互联网或将每台个人计算机直接连接到互联网，因此信息安全审核员宜确保检测/预防系统在每种情况下均正常工作。 注：信息安全审核员宜注意，对于未知恶意软件（例如零日攻击），检测/预防系统的能力是有限的。	
1	安全实施标准	作为预防性或例行控制措施，安装和定期更新恶意软件检测和修复软件以扫描计算机和介质文件，实施的检查宜包括： ——使用前检查所有电子或光学媒体上的任何文件以及通过网络接收的文件； ——使用前检查电子邮件附件和下载文件，检查宜在不同地方进行，如在电子邮件服务器、台式计算机上以及接入组织网络时； ——检查网页。	
	安全实施标准技术注解	在组织网络入口的网关处，恶意软件的检测/预防系统宜适配多种网络服务或协议，例如 WWW、邮件和 FTP。	
	1.1	实践指南	以下实践指南分别适用于“安全实施标准”的 1），2）和 3）： a） 通过评审系统规范或网络图，检查对所有电子或光学介质文件以及通过网络接收的文件全面有效部署恶意代码检测和修复系统： 1） 信息安全审核员宜通过评审系统规范或网络图来检查检测/预防系统全面是否有效部署。 b） 通过评审系统规范或网络图（包括电子邮件服务器，台式计算机和网关），检查对所有电子邮件附件和下载文件全面有效部署恶意代码检测和修复系统： 1） 系统规范中有时将恶意代码检测和修复系统明确描述为独立设备，但是，信息安全审核员同样关注未在系统规范中明确描述的部署在旨在提供一些其他功能/服务（WWW， 邮件和 FTP）的服务器中恶意代码检测和修复系统； 2） 对于桌面式个人计算机，信息安全审核员关注系统规范中没有明确描述的恶意代码检测和修复系统。 1)

表 B.18（续 1）

GB/T 22081-2016，12.2 恶意软件防范			
			c） 通过评审包含 Web 服务器的系统规范或网络图，检查对 Web 页面全面有效部署恶意代码检测和修复系统： 2） 对于用于审阅或浏览网页的桌面式个人计算机，信息安全审核员关注原本在系统规范中没有清楚说明的恶意代码检测和修复系统，在这种情况下，恶意代码检测和修复系统可能固化在浏览器中； 对于 Web 服务器，恶意代码检测和修复系统作为专用设备有时在系统规范中被清楚描述，然而，信息安全审核员宜关注安装在 Web 服务器中并未在系统规范中清楚描述的这些设备。
		设想的证据	——合同文件； ——网络服务设计文档； ——系统规范； ——网络图。
		方法	检查/评审
	1.2	实践指南	以下实践指南分别适用于“安全实施标准”的 1），2）和 3）。 a） 通过观察信息处理设施，检查用于检测所有电子或光学介质文件以及通过网络接收的文件的恶意软件检测和修复系统已部署且正常运行： 1） 恶意软件检测和修复系统在一个集成系统中管理的情况下，检查管理软件是否在集成系统中正常运行。 b） 通过观察信息处理设施，检查用于检测电子邮件服务器、抽样台式机、网关上的任何电子邮件附件和下载文件的恶意软件检测和修复系统已部署且正常运行： 1） 对于电子邮件，请检查检测系统不仅适用于附件文件，还适用于 html 邮件中的恶意软件。 c） 通过观察信息处理设施，检查用于检测任意网页的恶意软件检测和修复系统已部署且正常运行： 1） 对于用于查看或浏览网页的桌面式个人计算机，检查检测系统适用于未经授权的 Active X 控件，脚本等； 2) 对于 Web 服务器，检查检测系统不仅适用于 html 文件，还适用于 apache、IIS 等 Web 服务中的恶意软件。
		设想的证据	恶意软件检测和修复系统设施已部署，例如： ——文件服务器； ——电子邮件服务器； ——桌面式个人计算机样机； ——移动计算机； ——独立部署在网关位置（组织内网和互联网之间）的恶意软件检测和修复系统； ——Web 服务器； ——代理服务器； ——Web 浏览器； ——其他（阻止 USB 物理插入的设备）；

表 B.18（续 2）

GB/T 22081-2016，12.2 恶意软件防范			
		方法	检查/观察
	1.3	实践指南	从检测和修复系统收集日志文件，并检查日志记录以证明当检测出恶意软件时系统已运行且已采取了必要的行动。 通过上传测试病毒检查恶意软件检测和修复系统对网页已全面有效安装部署。 **注**：对于桌面式个人计算机，检测和修复系统的典型输出日志存储在个人计算机中。对于服务器和外部设备，这些日志有时会通过诸如 syslog 之类的传输协议进行传输并存储在其他系统中。 对于用于查看或浏览网页的桌面式个人计算机，Web 浏览器中的检测功能可能不会生成表明该功能已在运行的日志记录。相反，大多数浏览器都会显示检测到未授权脚本的消息。
		设想的证据	——运行中的检测系统； ——检测系统输出的日志文件； ——检测系统警报记录； ——在 Web 浏览器中检测系统的消息； ——在 Web 浏览器中具有上传功能的 Web 服务器；
		方法	——检查/观察； ——测试与确认。
2	安全实施标准	作为预防控制措施，宜定期或例行更新恶意软件检测和修复软件以扫描计算机和介质文件。	
	安全实施标准技术注解	在大多数情况下，有自动更新样本文件或特征码的功能。	
	2.1	实践指南	检查恶意软件检测和修复软件自动或例行更新样本文件或特征码的设计。
		设想的证据	检测系统的设计或规范。
		方法	检查/评审
	2.2	实践指南	检查恶意软件检测和修复软件自动或定期更新样本文件或特征码的设置。
		设想的证据	检测系统的设置。
		方法	检查/观察
	2.3	实践指南	通过观察其样本文件或特征码的产品名称，版本和更新日志，检查样本文件或特征码已更新。 **注**：可能会在产品的帮助文件中看到检测和修复系统的产品名称及其版本的信息。
		设想的证据	检测/预防系统的信息，即： ——产品名称； ——产品版本； ——样本文件或特征码的版本。

表 B.18（续 3）

GB/T 22081-2016，12.2 恶意软件防范			
		方法	检查/观察

表 B.19

GB/T 22081-2016，12.3 备份			
	控制	**GB/T 22081-2016,12.3.1 信息备份** 宜按照既定的备份策略，对信息、软件和系统镜像进行备份，并定期测试。	
	控制的附加技术信息	为了适当地进行备份，宜根据备份策略定义组织标准，并将其反映到备份设计文档中。 在发生数据丢失事件（例如灾难或介质故障）的情况下，备份用于恢复基本信息或软件。 当组织设计备份时，宜根据组织的备份策略选择适当的备份站点，备份路径和备份方法。 在备份站点方面，组织宜选择现场或异地作为备份站点。在进行备份和还原时，现场备份比异地备份快得多。 通常选择异地备份，以防止火灾，洪水或地震等当地灾难的影响。 在备份路径方面，宜选择在线备份或离线备份。在线备份是指通过网络或通信线路备份数据。离线备份是指已备份的数据通过 DLT 或 CD / DVD 等可移动介质进行物理传输备份数据。 备份方法分为全量备份，增量备份和差异备份等几种选项。 全量备份是对所有选择备份的数据进行备份。 与其他方法相比，它将需要更多的时间和数据容量，但这是最简单、最容易恢复的方法。 增量备份是指对上次备份以来发生变化的数据进行备份。 与其他方法相比，它需要的时间和数据容量更少，但这是最复杂的恢复方法。 差异备份是指对自上次完全备份以来发生变化的数据进行备份。 与全量备份相比，它需要更少的时间和数据容量，并且是比增量备份更简单、更容易的恢复方法。	
1	安全实施标准	备份的程度（例如，全量或差异备份）和备份频率宜反映组织的业务需求，所涉及信息的安全要求以及信息对组织持续运行的重要性。	
	安全实施标准技术注解	根据业务需求，组织宜选择足够的备份/恢复时间和数据容量进行备份。 审核员宜评估是否选择了适当的备份方法来满足业务需求。 有关频率的示例如下： ——镜像或实时复制（当信息的重要性为最高级别时）； ——每天（当需要至少在一天之内恢复已备份的数据时）； ——每周； ——每月。	
	1.1	实践指南	检查备份设计是否基于安全实施标准。
		设想的证据	——备份规范文档； ——业务和安全要求定义文档； ——备份设计文档。
		方法	检查/评审
	1.2	实践指南	检查备份系统配置文件的设置是否如备份设计文档中所述。
		设想的证据	——备份设计文档； ——备份系统配置文件。

表 B.19（续）

GB/T 22081-2016，12.3 备份			
		方法	检查/评审
	1.3	实践指南	检查是否已按照备份设计文档中的说明进行了备份。
		设想的证据	——备份设计文档； ——日志文件； ——备份介质。
		方法	检查/观察
	1.4	实践指南	检查备份是否存储在大小正确且隔离的安全位置
		设想的证据	备份位置规范文件
		方法	检查/评审
2	安全实施标准	宜定期检查和测试恢复程序，以确保它们有效，并且可以在恢复操作程序中指定的时间内完成。	
	安全实施标准技术注解	恢复的复杂性和所需时间因所采用的方法而异；例如全量或差异备份。 恢复程序的测试和检查计划宜准备好并形成文件。	
	2.1	实践指南	检查测试和检查计划是否定期检查。
		设想的证据	测试和检查计划的检查记录。
		方法	检查/评审
	2.2	实践指南	检查测试计划是否已经过常规测试，以确保它们有效，并且可以在恢复操作程序中指定的时间内完成。
		设想的证据	——恢复测试记录； ——测试计划。
		方法	检查/评审

表 B.20

GB/T 22081-2016，12.4 日志和监视		
	控制	**GB/T 22081-2016,12.4.1 事态日志** 宜产生、维护并定期评审记录用户活动、异常、错误和信息安全事态的事态日志。
	控制的附加技术信息	为了检测未经授权的信息处理活动，记录用于跟踪用户、系统操作员、安全事件和系统活动的审计日志非常重要。 为分析是否发生未经授权的活动、安全事件，审计日志宜包含以下信息： ——用户 ID； ——日期和时间； ——登录和注销等关键事件； ——终端标识； ——网络地址和协议。

表 B.20（续 1）

GB/T 22081-2016，12.4 日志和监视			
1	安全实施标准	为了产生包括上述信息的必要记录，宜对产生日志的设备进行调整，或者对其应用一些规则。 记录方法取决于系统结构，系统架构和已实现的应用程序。 信息安全审核员宜考虑服务器和 PC 等不同系统架构的日志记录方法的差异。 有关系统结构的示例如： ——客户端服务器系统； ——基于网络的系统； ——瘦客户端系统； ——虚拟化; ——使用 ASP、SaaS 或云计算。 有关系统架构的示例如： ——UNIX, Linux; ——Windows; ——Mainframe； 有关的日志类型的示例如： ——系统日志； ——应用程序日志。 宜生成记录用户的活动、异常和信息安全事态的审计日志。审计日志宜包括如下相关内容： ——用户 ID； ——重要事态的日期、时间和细节，例如登录和退出； ——终端身份或位置（如果可能） ——成功的和被拒绝的对系统尝试访问的记录； ——成功的和被拒绝的对数据以及其他资源尝试访问的记录； ——系统配置的变更； ——系统工具程序和应用程序的使用； ——访问的文件和访问类型； ——网络地址和协议； ——访问控制系统发出的警报； ——防护系统的激活和停用，例如防病毒系统和入侵检测系统。	
	安全实施标准技术注解	根据业务需求，组织宜选择足够的备份/还原时间和数据容量进行备份。审核员宜评估是否选择了适当的备份方法来满足业务需求。事件日志可以包含敏感数据和个人身份信息。 宜采取适当的隐私保护措施。在可能的情况下，系统管理员不应有权删除或停用其自己的活动日志。 有关频率的示例如: ——镜像或实时复制（当信息的重要性为最高级别时）； ——每天（当需要至少在一天之内恢复已备份的数据时）； ——每周； ——每月。	
	1.1	实践指南	检查日志记录的系统设计是否基于安全性实施标准。

表 B.20（续 2）

GB/T 22081-2016，12.4 日志和监视			
		设想的证据	——规范文档； ——需求定义文档； ——软件设计文档。
		方法	检查/评审
	1.2	实践指南	检查日志记录的系统配置文件的设置是否如系统设计文档中所述。
		设想的证据	——软件设计文档； ——系统配置文件。
		方法	检查/评审
	1.3	实践指南	检查实际审计日志文件的记录是否如系统设计文档中所述。 注：在审计日志中，有一些记录会不断出现，而某些记录（例如错误记录）则不会出现。 为了检查系统是否记录仅在某些特定情况下出现的记录，信息安全审核员可能需要使用各种措施，包括生成测试用例，检查系统设计文档。
		设想的证据	日志文件。
		方法	检查/观察
	1.4	实践指南	在某些情况下，审计日志的存储期限由业务目的相关的合同和法律/法规定义。 例如，包含访问控制系统发出警报的审计日志，宜保存至事件因果关系调查完毕为止。 注：刚开始运行的相对较新的系统，其审计日志尚未在协议期内存储。 在这种情况下，为实现实践指南 2.3，需检查实践指南 2.1 和 2.2。
		设想的证据	日志文件。
		方法	检查/观察
2	安全实施标准	审计日志宜在约定的期限内留存，以协助将来的调查和访问控制监测。	
	安全实施标准技术注解	在某些情况下，审计日志的存储期限由业务目的相关的合同和法律/法规定义。 例如，包含访问控制系统发出警报的审计日志宜保存至事件因果关系调查完毕为止。 注意：刚开始运行的相对较新的系统，其审计日志尚未在协议期内存储。 在这种情况下，为实现实践指南 2.3，需检查实践指南 2.1 和 2.2。	
	2.1	实践指南	检查审计日志的存储期限是否如系统设计文档中所述。
		设想的证据	——日志文件； ——系统设计文档。
		方法	检查/评审
	2.2	实践指南	检查系统中审计日志存储期限的设置是否与系统设计文档中所述相符，或者设置审计日志在存储期限之前不可覆盖或删除。
		设想的证据	——日志文件； ——系统设计文档。
		方法	检查/评审

表 B.20（续 3）

GB/T 22081-2016，12.4 日志和监视			
	2.3	实践指南	通过查看日志文件的时间戳或日志中的时间记录，检查审计日志的存储期限超过约定期限。
		设想的证据	——日志文件； ——系统设计文档。
		方法	检查/评审
	控制	**GB/T 22081-2016，12.4.2 日志信息的保护** 记录日志的设施和日志信息宜加以保护，以防止篡改和未授权的访问。	
	控制的附加技术信息	系统日志通常包含大量信息，其中许多与信息安全监测无关。为帮助识别用于信息安全监测目的的重要事态，宜考虑将相应的消息类型自动地拷贝到第二份日志，或使用适合的系统实用工具或审计工具执行文件查询和合理化配置。	
1	安全实施标准	控制宜旨在防范未经授权的日志信息更改和日志设施运行问题。	
	安全实施标准技术注解	需要保护系统日志，因为如果其中的数据被修改或删除，可能导致一个错误的安全判断。实时复制日志到系统管理员和操作员控制范围外的系统，可用于日志防护。	
	1.1	实践指南	检查仅授权和特权用户可以访问日志文件。读写访问都宜仅限于特权用户。
		设想的证据	——访问日志服务器； ——访问日志； ——特权和非特权用户帐户。
		方法	测试与确认
	1.2	实践指南	检查所有日志文件是否通过安全连接传输到管理系统（即日志服务器或SIEM）。
		设想的证据	——访问日志服务器； ——访问用于传输日志信息的网络服务。
		方法	测试与确认
	1.3	实践指南	检查管理系统是否可以跟踪日志文件中的所有更改。
		设想的证据	——访问日志管理系统； ——访问日志文件。
		方法	测试与确认
	1.4	实践指南	检查是否可以识别日志文件中所有非特权或意外的更改。
		设想的证据	——哈希/签名的使用； ——访问日志管理。
		方法	测试与确认
	1.5	实践指南	检查特权和经过身份验证的用户是否无法操纵自己的日志文件。
		设想的证据	——特权用户帐户； ——访问日志管理。
		方法	测试与确认

表 B.20（续 4）

GB/T 22081-2016，12.4 日志和监视			
	1.6	实践指南	检查用户是否只能访问与其权限匹配的日志文件。
		设想的证据	——访问日志管理系统； ——访问日志； ——访问具有不同特权的两个用户帐户。
		方法	测试与确认
	1.7	实践指南	检查管理系统是否可以跟踪日志文件中的所有更改。
		设想的证据	检查日志文件是否已充分加密。
		方法	测试与确认
	1.8	实践指南	检查是否严格禁止未经授权访问日志管理系统。
		设想的证据	网络访问日志管理系统。
		方法	测试与确认
	1.9	实践指南	验证非授权访问告警，日志和通知的存储位置和属性。
		设想的证据	——访问日志管理系统； ——访问日志文件。
		方法	测试与确认
2	安全实施标准	审计日志宜在约定期限内留存，以协助将来的调查和访问控制监测。	
	安全实施标准技术注解	在某些情况下，审计日志的存储期限由业务目的相关的合同和法律/法规来定义。例如，包含访问控制系统发出警报的审计日志宜保存至事件因果关系调查完毕为止。 注意：刚开始运行的相对较新的系统，其审计日志尚未在协议期内存储。在这种情况下，为实现实践指南 2.3，需检查实践指南 2.1 和 2.2。	
	控制	**GB/T 22081-2016，12.4.4 时钟同步** 组织或安全域内的所有相关信息处理系统的时钟宜与单个基准时间源同步。	

表 B.21

GB/T 22081-2016，12.5 运行软件控制		
	控制	**GB/T 22081-2016，12.5.1 运行系统软件的安装** 宜实现运行系统软件安装控制规程。

表 B.22

GB/T 22081-2016，12.6 技术方面的脆弱性管理		
	控制	**GB/T 22081-2016，12.6.1 技术方面脆弱性的管理** 宜及时获取在用的信息系统的技术脆弱性信息，评价组织对这些脆弱性的暴露状况并采取适当的措施来应对相关风险。
	控制	**GB/T 22081-2016，12.6.2 软件安装限制** 宜建立并实现控制用户安装软件的规则。

表 B.23

GB/T 22081-2016，12.7 信息系统审计的考虑		
	控制	**GB/T 22081-2016，12.7.1 信息系统审计的控制** 涉及运行系统验证的审计要求和活动，宜谨慎地加以规划并取得批准，以便最小化业务过程的中断。

B.2.9 通信安全

表 B.24

GB/T 22081-2016，13.1 网络安全管理			
	控制	**GB/T 22081-2016，13.1.1 网络控制** 宜管理和控制网络以保护系统和应用中的信息。	
	控制的附加技术信息	网络服务是在网络计算环境上提供的服务，无论它是内部的还是外包的。当组织使用网络服务时，组织的保密信息可能以外包网络服务的方式传输。 因此，审核员宜考虑到外包网络服务提供者提供了必要的安全功能（例如加密和/或身份鉴别） 用于网络服务的系统示例为： ——DNS； ——DHCP； ——防火墙/VPN； ——防病毒检测器； ——IDS/IPS。	
1	安全实施标准	宜识别特殊服务的安全安排，例如安全特性、服务级别和管理要求。组织宜确保网络服务提供商实施了这些措施。	
	安全实施标准技术注解	为了使用网络服务，安全性布局安排对于保护通过它的信息很重要。 有关安全功能的要求通常包含在业务要求中。 与网络服务有关的安全功能示例为： ——防止窃听的加密； ——防止未经授权的访问的网络访问控制； ——针对恶意活动的 IDS / IPS； ——过滤未经授权访问网络的 URL； ——对意外安全事态的事件响应。	
	1.1	实践指南	检查由服务提供者提供的包括 SLA 的合同文档是否满足组织的业务，法律和安全要求。
		设想的证据	——合同文件； ——需求定义文档。
		方法	检查/评审
	1.2	实践指南	如果是内部，检查用于网络服务的系统设置是否如合网络服务设计文档中所述。

表 B.24（续 1）

GB/T 22081-2016，13.1 网络安全管理			
		设想的证据	——系统配置； ——网络服务设计文档。
		方法	检查/评审
	1.3	实践指南	如果是内部，检查网络服务系统中实际日志文件的记录是否如网络服务设计文档中所述。 网络服务记录示例： ——鉴别； ——加密； ——网络连接控制； ——网络速度； ——响应（如果是在线系统）； ——停机时间。
		设想的证据	——日志文件； ——警报消息； ——网络服务设计文档。
		方法	检查/观察
	控制	**GB/T 22081-2016，13.1.2，网络服务的安全** 所有网络服务的安全机制、服务级别和管理要求宜予以确定并包括在网络服务协议中，无论这些服务是由内部提供的还是外包的。	
	关于控制的附加技术信息	网络服务是在网络计算环境上提供的服务，无论它是内部的还是外包的。 当组织使用网络服务时，组织的保密信息可能以外包网络服务的方式传输。 因此，审核员宜考虑到外包网络服务提供者提供了必要的安全功能，例如加密和/或身份验证。 用于网络服务的系统示例为： ——DNS； ——DHCP； ——防火墙/VPN； ——防病毒 IDS / IPS。	
1	安全实施标准	网络服务提供者以安全方式管理约定服务的能力，宜确定并定期监视，且宜商定审计权利。 宜识别特殊服务的安全安排，例如安全特性、服务级别和管理要求。组织宜确保网络服务提供商实施了这些措施。	
	安全实施标准技术注解	网络服务包括接入服务、私有网络服务、增值网络和受控的网络安全解决方案，例如防火墙和入侵检测系统。 这些服务既包括简单的未受控的带宽也包括复杂的增值的提供。	
	1.1	实践指南	验证是否定期测试和确认了网络服务协议中包含的安全机制。
		设想的证据	——对网络服务协议的访问； ——对安全测试报告的访问。

表 B.24（续 2）

GB/T 22081-2016，13.1 网络安全管理			
		方法	检查
	1.2	实践指南	验证 IDS / IPS 是否可以识别各种自动攻击以及人为恶意活动。
		设想的证据	——已实施 IDS / IPS； ——访问 IDS / IPS 日志。
		方法	测试与确认
	1.3	实践指南	如果是内部，检查网络服务系统中实际日志文件的记录是否如网络服务设计文档中所述。 网络服务记录示例： ——鉴别； ——加密 ——网络连接控制； ——网络速度； ——响应（如果是在线系统）； ——停机时间。
		设想的证据	——访问独立的测试环境； ——已记录的防病毒/恶意软件保护策略。
		方法	测试与确认
	1.4	实践指南	通过身份鉴别测试和环境突破测试技术，验证对 VPN 和其他远程访问机制的访问是否受到适当限制 。
		设想的证据	——实施了 VPN 和/或其他允许访问网络的远程访问服务； ——远程访问点列表。
		方法	测试与确认
	控制	**GB/T 22081-2016,13.1.3 网络中的隔离** 宜在网络中隔离信息服务、用户及信息系统。	
	控制的附加技术信息	管理大型网络安全的一种方法是将该网络分成独立的网络域，选择网络域可基于可信级别（例如，公共访问域、桌面终端域、服务器域），也可基于独立的组织单元（例如，人力资源、财务、市场）或一些组合（例如，连接多个组织单元的服务器域）。不同的网络之间或者通过物理方式或者通过逻辑方式隔离（例如，虚拟专用网络）。	
1	安全实施标准	宜明确每个域的边界。网络域之间的访问是允许的，但宜通过在边界安装网关（例如，防火墙、过滤路由器）进行控制。宜基于对每个域安全要求的评估结果，确定网络域隔离准则和通过网关所允许的访问。评估宜遵循访问控制策略（见 9.1.1）、访问要求、所处理信息的价值和类别，还宜考虑到相关成本和加入适合的网关技术的性能影响。 由于无线网络的边界不好定义，因此其要求宜特别处理。对于敏感环境，宜考虑将所有无线访问作为外部连接处理（见 9.4.2），并且在允许访问内部网络之前，从内网中隔离无线访问，直到已经按照网络控制策略（见 13.1.1）通过网关访问。	

表 B.24（续 3）

GB/T 22081-2016，13.1 网络安全管理			
	安全实施标准技术注解	正在日益扩展的网络超出了组织边界，因为形成的业务伙伴可能需要信息处理和网络设施的互连或共享。这样的扩展可能增加对使用此网络的组织的信息系统进行未授权访问的风险，其中的某些系统由于其敏感性或关键性可能需要防范其他的网络用户。	
	1.1	实践指南	确认是否无法通过 ping 扫描，VLAN 跳频和/或引入新的虚拟接口来访问虚拟隔离的网络。
		设想的证据	通过 VLAN 进行网络隔离。
		方法	测试与确认
	1.2	实践指南	测试防火墙，以确认攻击者无法访问未经授权的网络，并且控制点不易受常见漏洞的影响。
		设想的证据	网络被防火墙隔离。
		方法	测试与确认
	1.3	实践指南	确认在单独网络中具有网络接口的系统是否定期接收安全更新，并且不容易受到常见漏洞的影响。具有在多个网络中的接口的易受攻击的系统可以用来转向其他受限制的网络。
		设想的证据	列出所有无线网络的文档。
		方法	测试与确认
	1.4	实践指南	确认场所中不存在未记录且可能被授权访问正常隔离网络的恶意访问点。
		设想的证据	列出所有无线网络的文档。
		方法	测试与确认

表 B.25

GB/T 22081-2016，13.2 信息传输		
	控制	**GB/T 22081-2016，13.2.1 信息传输策略和规程** 宜有正式的传输策略、规程和控制，以保护通过使用各种类型通信设施进行的信息传输。
	控制	**GB/T 22081-2016，13.2.2 信息传输协议** 协议宜解决组织与外部方之间业务信息的安全传输。
	控制	**GB/T 22081-2016，13.2.3 电子消息发送** 宜适当保护包含在电子消息发送中的信息。
	控制	**GB/T 22081-2016，13.2.4 保密或不泄露协议** 宜识别、定期评审和文件化反映组织信息保护需要的保密性或不泄露协议的要求。

B.2.10 系统获取、开发和维护

表 B.26

GB/T 22081-2016，14.1 信息系统的安全要求		
	控制	**GB/T 22081-2016，14.1.1 信息安全要求分析和说明** 新建信息系统或增强现有信息系统的要求中宜包括信息安全相关要求。

表 B.26（续 1）

<table>
<tr><td colspan="4">GB/T 22081-2016，14.1 信息系统的安全要求</td></tr>
<tr><td></td><td>控制</td><td colspan="2">GB/T 22081-2016，14.1.2 公共网络上应用服务的安全保护
宜保护在公共网络上的应用服务中的信息以防止欺诈行为、合同纠纷以及未经授权的泄露和修改。</td></tr>
<tr><td></td><td>有关控制的其他技术信息</td><td colspan="2">客户端和应用服务之间的通信宜被安全地处理。能通过以下方式实现：
——使用身份鉴别；
——使用文件化的过程批准内容；
——确保通信双方完全被告知其使用服务的授权；
——确定所有通信方满足所有安全要求；
——使用机制确保通信及其信息的完整性、保密性和真实性：
这些要求大部分能通过使用密码控制来实现（A.10）。法律方面要求宜在服务协议中处理。</td></tr>
<tr><td rowspan="12">1</td><td>安全实施标准</td><td colspan="2">公共网络应用服务的安全性与密码控制密切相关。这些控制能用于实现上面描述的许多目标。
鉴别和授权能通过使用众所周知的可信的认证协议来实现。为了确保客户端和公共网络上的应用程序服务之间的通信是保密的，可以通过使用已知的公钥密码进行密钥交换，使用对称密码(如块或流密码)进行加密来保护该服务。
通过使用强密码签名算法可以达到在公共网络上通信的完整性。</td></tr>
<tr><td>安全实施标准技术注解</td><td colspan="2">为了确保公共网络上的应用服务能够安全地抵御各种形式的威胁和攻击，宜确定所有的加密协议和算法都满足 A.10 密码控制中定义的控制。
通过公共网络访问的应用程序会受到一系列与网络相关的威胁，例如欺诈活动、合同纠纷或向公众泄露信息。因此，详细的风险评估和适当的控制选择是必不可少的。所需的控制通常包括用于身份鉴别和保护数据传输的密码方法。</td></tr>
<tr><td>1.1</td><td>实践指南</td><td>检查身份鉴别和授权信息和过程是否使用强的、众所周知的、经过测试的协议和算法来实现。</td></tr>
<tr><td></td><td>设想的证据</td><td>——访问实现的鉴别和授权过程；
——访问算法和协议；
——有效的身份鉴别信息。</td></tr>
<tr><td></td><td>方法</td><td>测试与确认</td></tr>
<tr><td>1.2</td><td>实践指南</td><td>验证应用程序能够抵抗各种协议级别的威胁和攻击。</td></tr>
<tr><td></td><td>设想的证据</td><td>——通信协议的访问；
——接入通信通道。</td></tr>
<tr><td></td><td>方法</td><td>测试与确认</td></tr>
<tr><td>1.3</td><td>实践指南</td><td>验证通信是否抵抗各种应用程序级别的威胁和攻击，如代码注入、特权升级、会话劫持和不安全的直接对象引用。</td></tr>
<tr><td></td><td>设想的证据</td><td>——对应用程序的非特权访问；
——特权访问应用程序。</td></tr>
<tr><td></td><td>方法</td><td>测试与确认</td></tr>
<tr><td>1.4</td><td>实践指南</td><td>列举和测试监视器和传感器的使用或不足，以正确识别和记录对资产的访问与互动，以获得质疑不可否认性的特定证据。记录下相互作用的程度。</td></tr>
</table>

表 B.26（续 2）

GB/T 22081-2016，14.1 信息系统的安全要求			
		设想的证据	访问日志和监控系统。
		方法	检查
	1.5	实践指南	验证所有交互方法都有适当的记录，并进行适当的身份识别。
		设想的证据	访问日志和监控系统。
		方法	检查
	1.6	实践指南	验证应用程序日志不能被应用程序用户删除。
		设想的证据	——访问应用程序
		方法	测试与确认
	控制	**GB/T 22081-2016， 14.1.3 应用服务事务的保护** 宜保护应用服务事务中的信息，以防止不完整的传输、错误路由、未授权的消息变更、未授权的泄露、未授权的消息复制或重放。	
	控制的附加技术信息	保护应用程序服务事务是实现和维护安全相关服务的重要因素。 这些服务使用信息进行身份验证、系统控制或一般通信。 这些信息可以包括登录凭据、系统命令、私有信息或更多需要保护的信息。 应用程序服务中所需的信息宜受到保护，免受各种攻击和威胁。	
1	安全实施标准	为了保护传递给应用程序服务的信息，建议确保： 1）为每一参与方使用数字签名； 2）在所有相关各方之间的通信路径上使用加密； 3）使用经过测试并已知是安全的协议； 4）使用协议，确保事务保持有效、机密和私有； 5）使用无法公开访问的系统来存储事务详细信息。	
	安全实施标准技术注解	所采取的控制的范围必须与每种形式的应用服务交易相关的风险水平相适应。	
	1.1	实践指南	确认所有的 SSL 证书都是有效的，并由一个对特定组织可信的证书颁发机构颁发。
		设想的证据	——使用中的 SSL 证书； ——访问应用服务。
		方法	测试与确认
	1.2	实践指南	检查各方之间的通信是否使用具有足够密钥长度的强加密算法加密。
		设想的证据	——合法加密方法和密钥长度； ——访问加密通信。
		方法	测试与确认
	1.3	实践指南	验证通信是否抵抗各种应用程序级别的威胁和攻击，如跨站点脚本、跨站点请求伪造和无效重定向和转发。
		设想的证据	——对应用程序的非特权访问； ——特权访问应用程序。
		方法	测试与确认

表 B.26（续 3）

GB/T 22081-2016，14.1 信息系统的安全要求			
	1.4	实践指南	测试应用程序或协议实现是否容易受到已知的攻击，如中间人攻击或重播攻击。
		设想的证据	——访问通信； ——标准通信协议。
		方法	测试与确认
	1.5	实践指南	确认应用程序保存的所有机密数据是安全储存的。
		设想的证据	访问应用程序数据库。
		方法	测试与确认
	1.6	实践指南	确认是否禁止外部访问数据库且所有访问都通过安全认证机制受到限制。
		设想的证据	访问应用程序数据库。
		方法	测试与确认
	1.7	实践指南	确认事务仍然有效，即使通过误路由或不完整的传输连接丢失。
		设想的证据	——访问通信； ——访问应用程序日志。
		方法	测试与确认
	1.8	实践指南	确认应用程序只使用最小权限。 确保没有比需要更多的权利。
		设想的证据	访问应用程序的数据库用户信息。
		方法	测试与确认

表 B.27

GB/T 22081-2016，14.2 开发和支持过程中的安全		
	控制	**GB/T 22081-2016，14.2.1 安全的开发策略** 针对组织内的开发，宜建立软件和系统开发规则并应用。
	控制	**GB/T 22081-2016，14.2.2 系统变更控制规程** 宜使用正式的变更控制规程来控制开发生命周期内的系统变更。
	控制	**GB/T 22081-2016，14.2.3 运行平台变更后对应用的技术评审** 当运行平台发生变更时，宜对业务的关键应用进行评审和测试，以确保对组织的运行和安全没有负面影响。
	控制	**GB/T 22081-2016，14.2.4 软件包变更的限制** 宜不鼓励对软件包进行修改，仅限于必要的变更，且对所有变更加以严格控制。
	控制	**GB/T 22081-2016， 14.2.5 系统安全工程原则** 宜建立、文件化和维护安全的系统工程原则，并应用到任何信息系统实现工作中。
	控制	**GB/T 22081-2016，14.2.6 安全的开发环境** 组织宜针对覆盖系统开发生命周期的系统开发和集成活动，建立安全开发环境，并予以适当保护。
	控制	**GB/T 22081-2016，14.2.7 外包开发** 组织宜督导和监视外包系统开发活动。
	控制	**GB/T 22081-2016，14.2.8 系统安全测试** 宜在开发过程中进行安全功能测试。

表 B.27（续）

GB/T 22081-2016，14.2　开发和支持过程中的安全		
	控制	**GB/T 22081-2016，14.2.9 系统验收测试** 宜建立对新的信息系统、升级及新版本的验收测试方案和相关准则。

表 B.28

GB/T 22081-2016，14.3　测试数据		
	控制	**GB/T 22081-2016，14.3.1 测试数据的保护** 测试数据宜认真地加以选择、保护和控制。

B.2.11　供应商关系

表 B.29

GB/T 22081-2016，15.1　供应商关系中的信息安全		
	控制	**GB/T 22081-2016，15.1.1 供应商关系的信息安全策略** 为降低供应商访问组织资产的相关风险，宜与供应商就信息安全要求达成一致，并形成文件。
	控制	**GB/T 22081-2016，15.1.2 在供应商协议中强调安全** 宜与每个可能访问、处理、存储、传递组织信息或为组织信息提供 IT 基础设施组件的供应商建立所有相关的信息安全要求，并达成一致。
	控制	**GB/T 22081-2016，15.1.3 信息与通信技术供应链** 供应商协议宜包括信息与通信技术服务以及产品供应链相关的信息安全风险处理要求。

表 B.30

GB/T 22081-2016，15.2　供应商服务交付管理		
	控制	**GB/T 22081-2016，15.2.1 供应商服务的监视和评审** 组织宜定期监视、评审和审核供应商服务交付。
	控制	**GB/T 22081-2016，　15.2.2 供应商服务的变更管理** 宜管理供应商所提供服务的变更，包括维护和改进现有的信息安全策略、规程和控制，管理宜考虑变更涉及到的业务信息、系统和过程的关键程度及风险的再评估。

B.2.12　信息安全事件管理

表 B.31

GB/T 22081-2016，16.1　信息安全事件的管理和改进		
	控制	**GB/T 22081-2016，16.1.1 责任和规程** 宜建立管理责任和规程，以确保快速、有效和有序地响应信息安全事件。
	控制	**GB/T 22081-2016，16.1.2 报告信息安全事态** 宜通过适当的管理渠道尽快地报告信息安全事态。

表 B.31（续）

GB/T 22081-2016，16.1　信息安全事件的管理和改进		
	控制	**GB/T 22081-2016，16.1.3 报告信息安全弱点** 宜要求使用组织信息系统和服务的员工和合同方注意并报告任何观察到的或可疑的系统或服务中的信息安全弱点。
	控制	**GB/T 22081-2016，16.1.4 信息安全事态的评估和决策** 宜评估信息安全事态并决定其是否属于信息安全事件。
	控制	**GB/T 22081-2016，16.1.5 信息安全事件的响应** 宜按照文件化的规程响应信息安全事件。
	控制	**GB/T 22081-2016，16.1.6 从信息安全事件中学习** 宜利用在分析和解决信息安全事件中得到的知识来减少未来事件发生的可能性和影响。
	控制	**GB/T 22081-2016，16.1.7 证据的收集** 组织宜确定和应用规程来识别、收集、获取和保存可用作证据的信息。

B.2.13　业务连续性管理的信息安全方面

表 B.32

GB/T 22081-2016，17.1　信息安全的连续性		
	控制	**GB/T 22081-2016，17.1.1 规划信息安全连续性** 组织宜确定在不利情况（如危机或灾难）下，对信息安全及信息安全管理连续性的要求。
	控制	**GB/T 22081-2016，17.1.2 实现信息安全连续性** 组织宜建立、文件化、实现并维护过程、规程和控制，以确保在不利情况下信息安全连续性达到要求的级别。
	控制	**GB/T 22081-2016，17.1.3 验证、评审和评价信息安全连续性** 组织宜定期验证已建立和实现的信息安全连续性控制，以确保这些措施在不利情况下是正当和有效的。

表 B.33

GB/T 22081-2016，17.2 冗余		
	控制	**GB/T 22081-2016， 17.2.1 信息处理设施的可用性** 信息处理设施宜具有足够的冗余以满足可用性要求。

B.2.14　符合性

表 B.34

GB/T 22081-2016，18.1 符合法律和合同要求		
	控制	**GB/T 22081-2016，18.1.1 适用的法律和合同要求的识别** 对每一个信息系统和组织而言，所有相关的法律、法规、规章和合同要求，以及为满足这些要求组织所采用的方法，宜加以明确地定义、形成文件并保持更新。

表 B.34（续）

GB/T 22081-2016，18.1 符合法律和合同要求		
	控制	**GB/T 22081-2016，18.1.2 知识产权** 宜实现适当的规程，以确保在使用具有知识产权的材料和具有所有权的软件产品时，符合法律、法规和合同的要求。
	控制	**GB/T 22081-2016，18.1.3 记录的保护** 宜根据法律、法规、规章、合同和业务要求，对记录进行保护以防其丢失、毁坏、伪造、未授权访问和未授权发布。
	控制	**GB/T 22081-2016，18.1.4 隐私和个人可识别信息保护** 宜依照相关的法律、法规和合同条款的要求，以确保隐私和个人可识别信息得到保护。
	控制	**GB/T 22081-2016，18.1.5 密码控制规则** 密码控制的使用宜遵从所有相关的协议、法律和法规。

表 B.35

GB/T 22081-2016，18.2 信息安全评审		
	控制	**GB/T 22081-2016，18.2.1 信息安全的独立评审** 宜按计划的时间间隔或在重大变化发生时，对组织的信息安全管理方法及其实现（如信息安全的控制目标、控制、方针策略、过程和规程）进行独立评审。
	控制	**GB/T 22081-2016，18.2.2 符合安全策略和标准** 管理者宜定期评审其责任范围内的信息处理和规程与适当的安全策略、标准和任何安全要求的符合性。
	控制	**GB/T 22081-2016，18.2.3 技术符合性评审** 宜定期评审信息系统与组织的信息安全策略和标准的符合性。

附 录 C
（资料性）
云服务技术性评估指南（基础设施即服务）

C.1 定位与目标

本附录为审核ISO/IEC 27017中的控制和实施指南的实施和运行提供指引。本附录可作为附录B的附加指南使用，附录B涉及GB/T 22081-2016给出的控制和实现指南。

本附录的目的是以基础设施即服务(见图C.1)为例，让审核员了解云服务的审核要点。由于重大的技术创新，提供云服务的系统是多样化的，且在不断变化。本附录没有设定具体的系统，但设定一些指标，作为评审方法、注解和评审目标的实践。

本附录为云服务提供者的工程师提供了一些见解，其中将整合采用的安全控制，以评审该服务宜如何验证，以及宜如何展示技术性评估线索。遵循此指南不仅允许审核员进行适当的审核，也允许云服务提供者设计特定的控制，以使其服务符合ISO/IEC 27017。

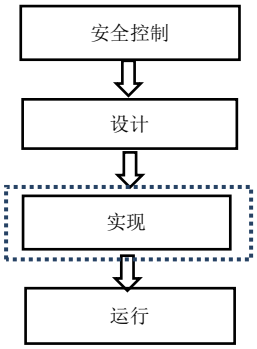

图 C.1 本附录的范围

C.2 和其他国际标准的关系

除ISO/IEC 27017外，以下标准与本附录有关：

a) ISO/IEC 27018，它定义了云服务中的 PII。
   1) 本附录涵盖了基础设施即服务。在基础设施即服务中，云服务客户自己负责存储在其使用的虚拟机上的信息的安全。这意味着云服务提供者不能管理虚拟机中的PII，因此这不在本文件的讨论范围内。
   2) 由云服务提供者负责维护的PII，包括云服务客户的信息。这由后文介绍的实现模型里的服务管理来管理和存储。此外，PII宜遵循ISO/ IEC 27018在服务管理中进行处理。
b) ISO/IEC 17788，本附录采用了该标准关于云计算的概述和词汇。
c) ISO/IEC 17789，适用于配置云服务的组件的基本思想。

虽然ISO/IEC 17789根据云计算的角色和活动定义了云计算架构，但在评审中要有云系统实现意识的观点，包括确认虚拟化机制配置。

因此，本附录提供了为云系统建模的实现模型，并将ISO/IEC 17789定义的功能组件映射到评审项目。

C.3 本附录的结构

本附录首先提出了一个以基础设施即服务为例建模的云服务环境。该模型描述了资源类型与虚拟化的关系，以及云服务客户和租户的概念。服务器、网络和存储被识别为一种资源类型。

技术性评估要求按照与附录B相同的格式，按模型、不同的资源类型和服务管理的共同主题顺序进行描述。见附录表C.1至表C.22。。

a) 典型技术说明：
   1） 与虚拟化实现相关的技术元素和指南的说明；
   2） 当存在多个实现方法时，将说明典型的方法。
b) ISO/IEC 27017 中定义的控制：
   1） 参考ISO/IEC 27017中与虚拟化相关的控制。
c) ISO/IEC 27017 中控制的技术性评审方法：
   1） ISO/IEC 27017中控制的评审方法指南；
   2） 当有多个实现方法时，说明其中的一个。

C.4 云服务（基础设施即服务）环境模型

C.4.1 引入模型的意义

由于云服务技术的多样性，对它们逐一进行详细的处理过于个性化和具体化。此外，云服务中使用的计算技术是新颖的且仍然处于技术发展过程中。考虑到这一点，将基于这些个性化/具体化技术的技术性评估方法进行标准化是不合适的。信息安全审核员(或评审员)可以记住这个方法论模型，并回想实际的技术实施是否基于控制的理念进行设计，以及在实际评估之前如何收集评估证据。

C.4.2 模型和组件

在本附录所假定的基础设施即服务中，环境是提供云服务的先决条件，云服务包括:

——云服务客户直接使用的虚拟资源；

——安装这些资源的虚拟化机制；

——用于控制和提供虚拟化机制的服务管理。

提供云服务的系统实现模型如图C.2所示。

该模型的一个重要观念是资源的虚拟化和分离。

在虚拟化机制中，物理资源作为虚拟资源提供，其访问权限通过租户与资源抽象和控制组件分离。

租户是一个聚集分配给每个受控制访问的虚拟资源的区域。可以按请求向云服务客户提供多个租户。通常，多个用户访问一个租户并执行信息处理。

这个模型有四个组件。其中物理资源、虚拟化机制和虚拟资源分为服务器、网络和存储三种资源类型。

物理资源是提供云服务所需的物理设备。它们由服务器设备、网络设备和存储设备组成。物理网络设备包括将服务器连接到网络的物理NIC。物理存储设备包括HBA和将服务器连接到存储设备的FC交换机。

a) 虚拟化机制用于生产云服务提供的虚拟资源。虚拟机管理程序适用于服务器虚拟化。VLAN、SDN适用于网络虚拟化。大多数存储设备包含这种存储机制。

b) 虚拟资源由虚拟化功能创建，并通过云服务提供给云服务客户，如虚拟机、虚拟网络、虚拟存储等。“虚拟资源”是指虚拟产生的资源集合的概念。

服务管理是使云服务提供者提供云服务，并为云系统提供与云服务客户的接口的系统。通过上述虚拟化功能，提供云服务所需的虚拟资源。它还监视和管理物理资源，并确保控制整个云环境能够正常运行。服务管理还包括门户功能、实用程序和API，允许云服务客户进行允许的操作，包括虚拟机的配置和激活/停用。

注：网络和存储可以通过服务器虚拟化。例如，虚拟机管理程序可以创建配置虚拟网络的虚拟化交换机，虚拟化服务器。

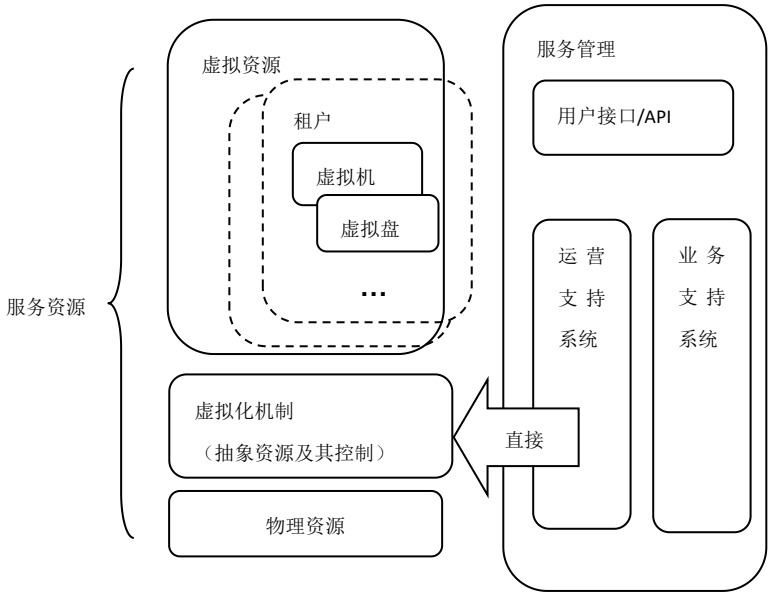

图 C.2 实现模型

C.4.3 与ISO/IEC 17789对应关系

ISO/IEC 17789中定义的功能组件实际上在该框架中通过用于实现每个组件的实现元素来实现，具体取决于目标资源类型或层。

以访问控制为例：

——物理磁盘的访问控制 （磁盘机）

——每个租户的访问控制（虚拟化机制）

——虚拟磁盘的访问控制 （虚拟化机制）

——每个VM的访问控制 （虚拟机各操作系统）

ISO/IEC 17789中定义的服务于云服务的多层功能和组件包含在本附录实施模型中的服务管理中。ISO/IEC 17789中定义的BSS或OSS包含在本附录的实施模型中。

与集成和安全相关的多层功能与上述访问权限一样，在其目标机制中实现。

C.5 实现模型中的公共实践

C.5.1 总则

本章描述了服务器虚拟化、网络虚拟化和存储虚拟化常见的检查实践，后续将进行解释。

C.5.2 云服务中虚拟化技术应用

如上文所述，虚拟化由用于虚拟化和虚拟资源的功能组成。在基础设施即服务中，云服务用户可以访问这些虚拟资源。

在云系统技术评审中，对虚拟化机制需要进行以下评估：

——运行安全：

- 由于虚拟化机制的运行直接影响到虚拟资源，查明虚拟化机制是否运行正常。

——环境的定义：

- 检查需要向云服务客户提供的日志和事件(错误通知、报警、超过阈值等)是否被定义为虚拟化机制的参数，以便收集和记录信息；
- 检查虚拟化机制和虚拟资源的冗余是否也被定义为虚拟化机制的参数，并检查其可用性。

——容量管理：

- 在每个虚拟化场景中，检查提供给云服务客户的虚拟资源与物理资源的关系是否被管理；
- 通常，云计算提供了与统计方法同时可用的逻辑资源。因此，提供的虚拟资源总量大于物理资源总量(超额预订、超额使用)。

C.5.3 虚拟化机制的公共方面技术性评估

C.5.3.1 运行安全

表 C.1

控制	ISO/IEC 27017:2015，12.1.2 变更管理
云服务提供者实现指南	云服务提供者宜向云服务客户提供有关云服务及其运行系统的变更的信息，这些变更可能会对云服务客户的信息安全造成不利影响。以下内容将帮助云服务客户确定变更对信息安全的影响： ——变更的类别； ——变更的计划日期和时间； ——对云服务和底层系统变更的技术说明； ——变更开始和完成的通知。 当云服务提供者提供依赖于云服务提供者同行的云服务时，云服务提供者需要将云服务提供者同行引起的变更通知云服务客户。
附加技术信息	云服务客户的潜在重大变更如下所示: a) 服务器： 1） 虚拟机管理程序更新或升级； 2） 虚拟机管理程序参数和环境定义的变更。 b) 网络： 1） VLAN 定义的改变； 2） 交换机、路由器、防火墙、负载均衡器等网络设备的配置、环境定义和参数的变更。 c) 存储： 1） 设备定义的变更； 2） SAN 分区等的变更。 d) 硬件： 1） 固件升级。 e) 软件： 1） 软件升级； 2） 应用程序的修复； 3） 应用安全的修复。 这些变更可能对云服务客户产生不同的影响。云服务客户和云服务提供者宜基于被告知的变更对其影响程度达成一致并决议是否通过变更

表 C.1（续）

控制		ISO/IEC 27017:2015，12.1.2 变更管理	
1	安全实施标准	在变更管理中，宜识别并适当通知直接或间接受影响的云服务客户。	
	安全实施标准技术注解	由于 IT 资源相互依赖，云服务客户使用其他依赖于相关资源的资源时也会受到影响。 通常，云服务的软硬件配置都在 CMDB 中维护。 每个云服务客户的软硬件资源也由 CMDB、OSS 或 BSS 进行管理。 硬件和软件与受硬件和软件变更影响的云服务客户之间的关系由这些系统管理。	
	1.1	实践指南	检查是否识别了使用要变更的 IT 资源的云服务客户。
		设想的证据	CMDB 的搜索结果等（云服务客户使用特定的 IT 资源的搜索结果）。
		方法	检查/观察
	1.2	实践指南	当 IT 资源之间存在依赖关系或影响时，检查是否理解相关关系。
		设想的证据	检查 CMDB 的结果等。 当 IT 资源之间存在依赖关系时，指定的特定 IT 资源所影响的其他 IT 资源的搜索结果。
		方法	检查/观察
	1.3	实践指南	检查宜提供给云服务客户的变更管理信息是否正确提供。 在提供的资料中检查下列事项： ——变更与云服务客户有关，并且（还宜提供间接影响）； ——提供与客户的协议或合理适当程度的影响。
		设想的证据	——向云服务客户发送邮件 ——面向云服务客户的门户。
		方法	检查/观察

表 C.2

控制		ISO/IEC 27017:2015，12.1.3 容量管理
云服务提供者实现指南		云服务提供者宜监控计算资源的总容量，以防止因资源短缺导致的信息安全事件。
附加技术信息		云服务提供者提供的计算资源宜包括： ——CPU 处理能力，核心存储； ——网络带宽； ——存储容量。 在云系统中，必须进行容量管理，以防止计算资源在高峰时间因临时使用计算资源而变得短缺。 容量管理不仅应在整个云系统中实现，而且应该在每个块中实现，因为计算资源可能不会在云系统块之外提供。
1	安全实施标准	定义宜添加计算资源的级别，并在达到该级别时采取必要的行动。

表 C.2（续）

控制		ISO/IEC 27017:2015，12.1.2 变更管理	
	安全实施标准技术注解	对计算资源设置一定的阈值，当计算资源利用率超过阈值时进行监视并发出告警。 通过使用云系统、IT 设备和软件等监控计算资源的使用情况。	
	1.1	实践指南	检查需要进行容量管理的计算资源是否按要求进行监视。
		设想的证据	——云系统监控定义； ——报告容量使用情况的输出。
		方法	检查/观察
	1.2	实践指南	检查所用容量超过阈值时，是否产生告警。
		设想的证据	——云监控系统告警设置（查看告警是否定义为阈值触发）； ——云监控系统的事件日志（检查过去是否发出过告警）。
		方法	检查/观察

表 C.3

控制		ISO/IEC 27017:2015，CLD.12.1.5 管理员的操作安全	
云服务提供者实现指南		云服务提供者宜向云服务客户提供他们所需要的有关关键操作和流程的文档。	
附加技术信息		通常，如果云计算环境变更失败，云服务客户将受到影响，无法使用云服务。 特别是删除和销毁存储上的数据，是对客户资产最严重的损害。 假定临时服务故障或禁用的云计算环境可能不会破坏资产，即使正在处理的事务被丢弃。	
1	安全实施标准	只有预先授权的操作员才能删除数据。	
	安全实施标准技术注解	用管理特权删除云服务客户使用的存储上的数据的操作需要不同于正常操作的身份验证。	
	1.1	实践指南	检查允许以管理特权进行操作的 ID 是否受到限制，并且使用的过程是否与正常过程不同。
		设想的证据	——用户 ID 列表，包括存储操作实用程序等。 ——使用管理特权的操作。
		方法	检查/观察

表 C.4

控制	ISO/IEC 27017:2015 ， 12.4.1 事态日志
云服务提供者实现指南	云服务提供者宜向云服务客户提供日志记录功能。

表 C.4（续）

控制		**ISO/IEC 27017:2015 ，12.4.1 事态日志**	
附加技术信息		如 ISO/IEC 27017“云服务的其他信息”所述，云服务提供者负责记录和监控本文档所述的基础设施即服务中的云计算基础设施组件。 包括： ——虚拟管理程序的日志和事件； ——防火墙和负载均衡器的日志和事件； ——存储设备和 SAN 设备的日志和事件 由于这些基础设施组件在云服务客户之间共享，所有云服务客户的日志和事件作为一个整体被记录下来。 因此，宜提取并提供只与相关云服务客户相关的日志。	
1	安全实施标准	收集将提供给服务客户的日志并监视事件。	
	安全实施标准技术注解	云计算基础设施组件提供日志输出和事件收集的功能。 日志输出由云计算基础设施组件的参数定义进行确定。	
	1.1	实践指南	检查是否为云计算基础架构组件定义了日志或事件收集设置。
		设想的证据	云技术基础设施组件参数的定义。
		方法	检查/观察

表 C.5

控制		**ISO/IEC 27017:2015 ，12.4.4 时钟同步**	
云服务提供者实现指南		云服务提供者宜向云服务客户提供关于云服务提供者所使用的时钟的信息，将基础设施组件投入服务客户可以将本地时钟与云时钟同步。	
附加技术信息		IaaS 云服务客户需要同步虚拟机与云计算环境的时间。 通常，虚拟机的时间同步方式如下: ——NTP 方法 ——Hypervisor 方法。	
1	安全实施标准	云服务提供者使用 NTP 或 Hypervisor 方法来提供同步虚拟机时间的方法。	
	安全实施标准技术注解	云服务客户需要按照提供的方法设置自己虚拟机的时间同步。	
	1.1	实践指南	检查云服务提供者是否提供时间同步方法。
		设想的证据	检查是否提供 NTP 服务器以及云服务客户是否可以通过 NTP 协议访问服务器的结果。 检查虚拟机管理程序是否提供时钟同步以及云服务客户是否可以使用该功能同步时钟的结果。
		方法	测试

表 C.6

控制		**ISO/IEC 27017:2015 ，CLD.12.4.5 云服务监控**	
云服务提供者实现指南		云服务提供者宜提供提供使云服务客户能够监视云服务运营中与云服务客户相关的特定方面的能力。例如，监视和检测云服务是否被用作攻击他人的平台，或者是否有敏感数据从云服务泄露。适当的访问控制宜确保监视功能的使用。这些功能宜只提供对有关云服务客户自己的云服务实例的信息的访问。 云服务提供者宜向云服务客户提供服务监视能力的文档。 监控宜提供与 12.4.1 中描述的事件日志一致的数据，并协助 SLA 条款。	
附加技术信息		一般来说，定义恶意使用云服务是困难的，超过一定数量的网络流量和存储访问将被检测。	
1	安全实施标准	使用日志或监视功能来检测云服务使用中出现的异常状态。	
	安全实施标准技术注解	见 12.4.1。	
	1.1	实践指南	检查是否定义了监控系统，以便检测到定义为恶意使用云服务的事件。
		设想的证据	监视系统测试参数的定义。
		方法	检查/观察

表 C.7

控制		**ISO/IEC 27017:2015 ，12.6.1 技术脆弱性管理**	
云服务提供者实现指南		云服务提供者宜向云服务客户提供有关技术脆弱性管理的信息，因为这些信息适用于云服务及其使用的信息系统。	
附加技术信息		技术脆弱性取决于软件版本。一般来说，由于云计算基础架构组件使用同一软件的多个版本，因此需要确定在使用的计算资源中是否存在脆弱性。	
1	安全实施标准	当在云计算基础设施组件中发现技术脆弱性时，识别使用带有脆弱性的计算资源的云服务客户，并向他们提供有关这些脆弱性的信息。 见 12.1.2 变更管理中的描述查找计算资源与云服务客户的关系。	
	安全实施标准技术注解	见 12.1.2 变更管理中的描述查找计算资源与云服务客户的关系。	
	1.1	实践指南	检查使用有脆弱性的计算资源的服务客户是否被识别并提供了技术脆弱性的信息。
		设想的证据	关于技术脆弱性和门户屏幕等的通知邮件。
		方法	检查/观察

C.6 服务器虚拟化

C.6.1 服务器虚拟化概述

C.6.1.1 服务器虚拟化是将一个物理服务器（由CPU、内存和输入/输出设备等组成)抽象为一组逻辑资源。一般情况下，服务器虚拟化的结构如图C.3所示。

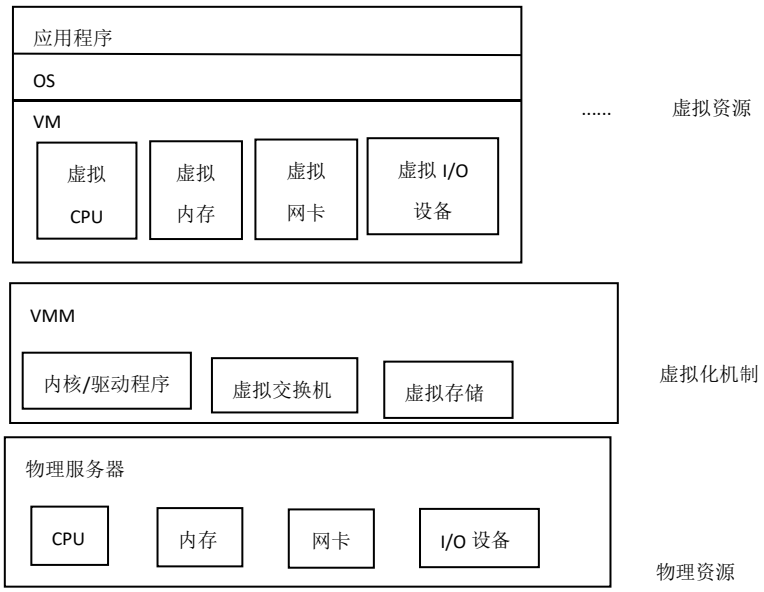

图 C.3 服务器虚拟化概述

C.6.1.2 CPU 虚拟化将客户虚拟机分配到物理服务器上的 VMM 的物理 CPU 上，成为运行在虚拟“核”上的虚拟化资源。

CPU虚拟化允许分配超过整个服务器物理CPU核数的虚拟CPU核数。

在超额分配时，VMM执行CPU调度和处理，例如切换分配到物理CPU核的虚拟CPU核。因此需要注意的是，多台虚拟机同时进行大量的处理会增加物理CPU的争用，占用CPU资源进行调度，造成分配前的延迟，影响处理性能。

C.6.1.3 内存虚拟化是在物理服务器内存上分配虚拟机内存。与CPU虚拟化类似，内存虚拟化允许超额分配，这意味着从虚拟机看到的总内存大小可以大于物理服务器上的实际内存大小。实现内存超额分配包括两种方式，一种是内存被动态分配给虚拟机，另一种是多个虚拟机可以共享相同的内存。两种方式下，分配给每个虚拟机的内存的最小值之和都应小于物理服务器的内存大小。

C.6.1.4 存储虚拟化是虚拟机的存储作为物理服务器存储上的文件集处理。然而，当虚拟服务器在物理服务器之间迁移而需要传输大量数据时，会存在占用频带和存储速度等方面的问题。因此，提供云服务的系统通常会安装一个公共存储服务器来提供SAN访问。

C.6.1.5 输入/输出（I/O）虚拟化是对一系列外设进行虚拟化，包括网卡、HBA卡和串口适配器。虚拟适配器端口用于连接到虚拟机（通过VMM设置将虚拟机设置为在VMM上工作），或者连接到物理服务器上的物理适配器端口。请注意，与内存CPU相比，HBA和网卡的I/O功能是高度共享，经常成为虚拟化功能的瓶颈。

C.6.2 云服务中服务器虚拟化应用

a) **服务器虚拟化中的租户分离**

在一般的虚拟环境设计中，虚拟服务器被设计成完全独立的资源，通过虚拟网络互联。

因此，隔离的虚拟机资源需要采取最低的网络安全措施。此外，虚拟化环境特别需要注意的是纠正由合法来源提供的虚拟化环境本身的漏洞。

另外，特殊的虚拟化环境可以为虚拟机之间的互联提供快速通信路由，或通过物理服务器的物理端口进行数据交换。因此，需要注意网卡以外的其他I/O。

为了保护虚拟资源，存在一种通过VMM或特权虚拟机访问内存和I/O的技术。使用这种技术，可以监视VM上的行为，可以检测无效的程序操作，以保护资源。但是，需要注意，即使来自VMM或特权虚拟机的访问对虚拟资源的安全性很有用，也不要随意使用这种技术，因为这可能会为恶意用户提供攻击通道。

b) **确保服务器虚拟化的可用性**

热迁移功能支持将虚拟机运行环境迁移到不同物理服务器上，而不需要关闭虚拟机。热迁移是通过在目标物理服务器的VMM上启动共享存储上的虚拟机映像，通过LAN传输缓存中的数据，以及后续进行虚拟化I/O来实现的。这种机制允许内存数据在热迁移时在LAN上流动，因此内存数据安全性和LAN安全性是关键。热迁移场景中，管理员在物理服务器之间迁移虚拟机，或者提供高可用性技术，当环境发生故障时，虚拟机可以自动在物理服务器之间迁移。

使用这种高可用性技术时，如果通过监控检测到故障，虚拟机所提供的服务将暂停一段时间，因为工作在故障物理服务器上的虚拟机映像需要在另一台正常工作的物理服务器上激活。还提供一种抗故障虚拟化环境的技术，以减少高可用性技术中出现的服务暂停时间。抗故障虚拟化环境包括在多个物理服务器上运行主虚拟机和辅助虚拟机，并在任何时候相互同步两个虚拟机。正常运行时，主虚拟机提供服务，备用虚拟机可以在故障发生时接管服务，以提供抗故障能力。注意，这两种技术都需要另一台物理服务器上的可用资源，而不是在同一台物理服务器上。

c) **服务器虚拟化中的容量管理**

使用合适的操作系统，可以在操作过程中动态分配虚拟化的内存或CPU资源。受限于物理服务器上可分配的资源，同时考虑其他虚拟机的资源使用情况，可能需要使用上述热迁移技术将虚拟机迁移到其他物理服务器上，以保证足够的空闲空间。物理服务器资源指标包括CPU核数、内存大小、磁盘I/O性能、磁盘大小、网络I/O性能。

通过将单个简单虚拟化环境提供的服务资源总数乘以虚拟化负载的开销，可以计算出总的资源需求。当考虑服务可用性时，应该确保每个物理服务器的资源留有余量。

资源指标关注点和服务提供的方式取决于云服务提供者的业务模型或SLA。无论如何，宜监测目前提供的资源和可用资源，以继续提供硬件资源是极其重要的。这种监视主要在服务管理中执行，以实现整个云服务环境的完整性。但需注意的是，可以在服务器虚拟化的VMM或特权虚拟机上安装资源使用监控工具

C.6.3 服务器虚拟化技术性评估

C.6.3.1 访问控制

有关服务器虚拟化中的隔离，见 C.6.2.1。

表 C.8

控制	**ISO/IEC 27017:2015 ， CLD. 9.5.1 虚拟计算环境中的隔离**
云服务提供者实现指南	云服务提供者宜对云租户的数据、虚拟化应用程序、操作系统、存储和网络实施适当的逻辑隔离，以：

表 C.8（续）

控制		ISO/IEC 27017:2015 ，CLD.9.5.1 虚拟计算环境中的隔离	
		——在多租户环境中隔离云租户使用的资源； ——隔离云服务提供者的内部管理资源与云租户使用的资源。 在多租户环境中，云服务提供者宜实施信息安全控制措施，实现云租户间的资源隔离。 云服务提供者宜考虑在云服务中运行云服务客户提供的软件的相关风险。	
附加技术信息		逻辑隔离的实现取决于应用于虚拟化的技术。	
1	安全实施标准	多租户环境中云服务客户的分离。	
	安全实施标准技术注解	虚拟机使用的内存和虚拟端口之间存在一条通信路径，这条路径可成为“虚拟资源”之间的通信路径。	
	1.1	实践指南	VM 之间可以直接访问非活动的功能。
		设想的证据	确认 VMM 里的 VM 之间直接访问的功能设置为非活动状态。
		方法	检查/观察，检查/评审
2	安全实施标准	云服务提供者内部管理与云服务客户的虚拟环境的隔离。	
	安全实施标准技术注解	在 VM-VMM 隔离中，VM-VM 管理的活动方式与上一节中提到的相同。此外，使用 VM-VMM 中实现安全性或可用性方面的工具创建通信路径时，这些工具的脆弱性可能成为 VM-VMM 配置中的漏洞。	
	2.1	实践指南	——应用虚拟化软件的隔离功能 ——在虚拟化环境中开启分区功能
		设想的证据	——确认 VMM 中的访问控制策略 ——确认透明页面共享在 VMM 中是非活动状态
		方法	检查/观察，检查/评审
	2.2	实践指南	虚拟系统集群的物理隔离
		设想的证据	确认物理服务器的虚拟化支持功能处于活动状态。
		方法	检查/观察，检查/评审
3	安全实施标准	执行脆弱性管理。	
	安全实施标准技术注解	宜在虚拟化平台（主机操作系统、Hypervisor 等)中使用基于安全措施（符合通用标准等)构建的产品。	
	3.1	实践指南	确认虚拟化平台中使用的产品在构建时考虑到了安全措施。
		设想的证据	虚拟化平台的基本设计文档。
		方法	检查/评审
	3.2	实践指南	在操作中共享脆弱性信息
		设想的证据	确认脆弱性信息共享状态 （查看门户网页等发布的信息)
		方法	检查/观察

表 C.9

控制		ISO/IEC 27017:2015，CLD.9.5.2 虚拟机加固	
云服务提供者实现指南		在配置虚拟机时,云服务客户和云服务提供者宜确保对每一个虚拟机实施适当的加固 （如仅启用云服务运行所需的端口、协议和服务)及部署适当的技术措施（如反恶意软件、日志记录)。	
附加技术信息		VM/VMM 和物理服务器不仅通过虚拟机操作系统实现,也通过虚拟机加固实现。由于它们紧密相关,所以虚拟机加固需要云服务客户和云服务提供者合作。	
1	安全实施标准	当配置虚拟机时，仅使必要的设备和/或服务生效。	
	安全实施标准技术注解	关于虚拟机加固,本控制没有重新解释如何增强虚拟服务器,因为可以应用通用服务器增强技术。但是，VMM 有一种技术可以为服务器提供安全性。如果使用此技术，其评审方法也宜符合 GB/T 22081 中定义的方法。	
	1.1	实践指南	确认在 VMM 中提供的 VM 功能配置最小化。
		设想的证据	确认的结果。
		方法	检查/观察，检查/评审
	1.2	实践指南	描述 VMM 或云服务管理默认提供的 VM 操作系统镜像中会添加哪些服务，并确认在云服务管理创建的新 VM 的配置界面中发布附加服务信息。
		设想的证据	确认的结果。
		方法	检查/观察，检查/评审
2	安全实施标准	创建虚拟环境时，降低提供虚拟环境的服务器受到恶意软件和脆弱性攻击的风险。	
	安全实施标准技术注解	基于虚拟化技术，可以使用通用操作系统添加各种应用程序，但宜避免不必要的角色、功能和应用程序。 VMM 宜专门用于专注于运行基本的基础架构元素，如防病毒软件、备份代理等。理想的做法是，使用可以消除所有脆弱性的功能齐全的 VMM。	
	2.1	实践指南	确认操作系统上的服务被限制为最小值。推荐操作系统配置最小化。
		设想的证据	检查 VMM 上的服务，并通过设计文档确认其是最小化配置。
		方法	检查/观察，检查/评审
	2.2	实践指南	确认在 VMM 和应用程序上正确地安装了安全更新。
		设想的证据	确认使用了更新工具，不需要执行安全更新。
		方法	检查/观察，测试
	2.3	实践指南	确认引导加载程序或 VMM 没有以任何方式被篡改。
		设想的证据	通过检查 UEFI 界面确认安全启动是激活的。
		方法	检查/观察
3	安全实施标准	在配置虚拟机时，确保每个虚拟机都部署适当的技术措施（如反恶意软件、日志记录)。	

表 C.9（续）

控制		ISO/IEC 27017:2015，CLD.9.5.2 虚拟机加固	
	安全实施标准技术注解	类似于管理服务器漏洞的常用做法，基于环境正在虚拟化这个事实，有一些软件（如驱动程序）可以更有效地使用准虚拟环境，还有一些软件可以从服务器管理客户机器等等，宜如此实现。	
	3.1	实践指南	收集虚拟环境中使用的工具和驱动程序的脆弱性信息，并准备一个模板向云服务客户公布更新。
		设想的证据	检查通知日志，云服务客户是否可以确认相关数据。
		方法	检查/观察

C.7 网络虚拟化

C.7.1 网络虚拟化概述

C.7.1.1 传统的网络虚拟化是一种在单个物理网络上实现多个独立通信的方法。但是，服务器虚拟化上的网络虚拟化，则是连接单个物理服务器中的多个虚拟机的一种方法。当虚拟机的物理服务器出现故障或物理资源的高使用率作为触发条件时，虚拟机可以移动到另一台物理服务器。其特点是，虚拟机可以继续保留相同的VLAN ID和IP地址。图C.4显示了虚拟机以及连接虚拟机的网络的配置概况。

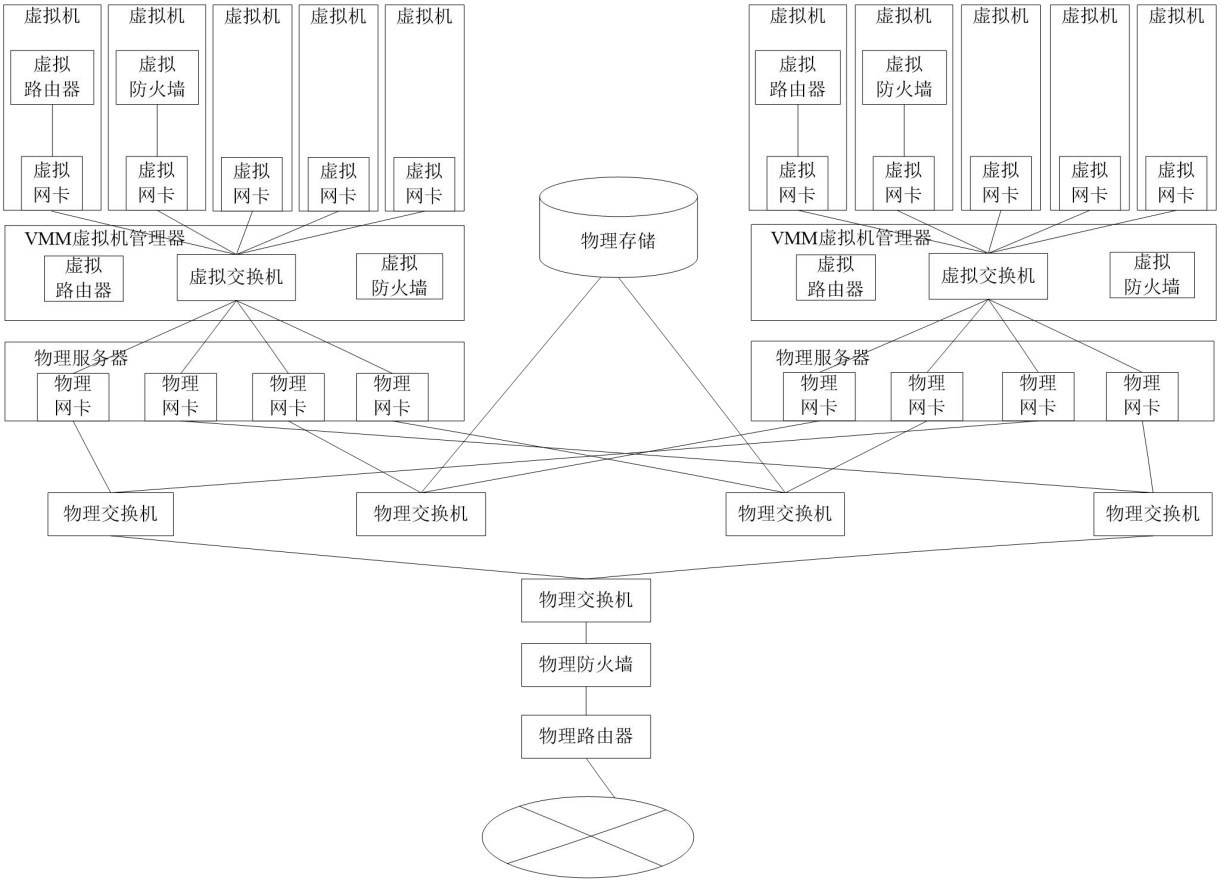

图 C.4 网络虚拟化概览

C.7.1.2 虚拟交换机是由虚拟机监视器提供的逻辑L2层交换机的功能，其位于物理NIC和虚拟机之间，并接收/发送帧。当物理网卡透明地中继帧时，虚拟交换机通过物理网卡连接到物理交换机。

C.7.1.3 虚拟网卡是由虚拟机监视器提供的逻辑网卡的功能，是把虚拟机连接到虚拟交换机上。

C.7.1.4 虚拟路由器是指由安装在虚拟机上的软件提供的逻辑路由器的功能，或指作为路由器的实际虚拟机。虚拟交换机也可以具有路由器的功能。

C.7.1.5 虚拟防火墙是指由安装在虚拟机上的软件提供的逻辑防火墙的功能，或指作为防火墙的实际虚拟机。

C.7.2 云服务中网络虚拟化应用

C.7.2.1 网络虚拟化中的租户分离

租户使用的虚拟机具有唯一的虚拟MAC地址和IP地址。由于以逻辑网络连接的一个或多个虚拟机是为每个租户分别设置的，因此租户在物理网络和物理服务器上都是分离的。

C.7.2.2 确保网络虚拟化中的可用性

如果一台物理服务器发生故障，可以通过将虚拟机和虚拟网络移动到另一台物理机，来保持其上虚拟机和虚拟网络的可用性。当在物理服务器上工作的物理网卡出现故障时，如果物理网卡有冗余配置，虚拟网络将跳到另一个物理网卡，而不更改实际的虚拟机，从而可以保持其可用性。

C.7.2.3 管理网络虚拟化中的带宽和地址空间

由于云服务通常在有限的物理网络上密集地建立许多虚拟网络，因此虚拟网络的逻辑带宽之和可能远远大于物理网络的物理带宽。此外，由于虚拟机可以在保持其VLAN ID 和/或IP地址的同时从一个物理服务器移动到另一个物理服务器，因此在物理交换机中设置的VLAN ID 的数目和/或学习到的MAC地址的数目要增加。

C.7.3 网络虚拟化技术性评估

C.7.3.1 访问控制

无。

C.7.3.2 密码

表 C.10

控制		ISO/IEC 27017:2015 ， 10.1.1 密码控制的使用策略
云服务提供者实现指南		云服务提供者宜向云服务客户提供有关其使用密码对其处理的信息进行保护的相关信息。云服务提供者还宜向云服务客户提供有关其可提供的任何能力的信息，以帮助云服务客户应用其自己的加密保护。
附加技术信息		云服务客户访问云服务时的通信是加密的。
1	安全实施标准	使用网络设备或服务器加密功能对用户数据进行加密。
	安全实施标准技术注解	加密使用诸如 SSL/TLS、SSH、IPSec 等加密协议。

表 C.10（续）

控制		ISO/IEC 27017:2015 ，10.1.1 密码控制的使用策略	
	1.1	实践指南	确认已为网络设备或服务器配置了加密通信。
		设想的证据	通信设备或服务器上的加密配置值。
		方法	检查/观察，检查/评审
	1.2	实践指南	使用数据包分析器监视通信路径上的流量，并确认有效负载已加密。
		设想的证据	数据包分析器的流量监视数据。
		方法	检查/观察，检查/评审

C.7.3.3 通信安全

表 C.11

控制		ISO/IEC 27017:2015，13.1.3 网络中的隔离	
云服务提供者实现指南		云服务提供者宜针对以下情况，强制隔离网络访问： ——多租户环境中租户之间的隔离； ——云服务提供者内部管理环境与云服务客户云计算环境的隔离。 在适当的情况下，云服务提供者宜帮助云服务客户验证云服务提供者实施的隔离。	
附加技术信息		对于云服务中的网络隔离，有在独立的物理资源上使用物理网络的物理隔离，以及在共享物理资源上使用逻辑网络的逻辑隔离。逻辑网络不仅可以在物理网络上扩展，也可以在物理服务器上扩展。	
1	安全实施标准	——当云服务客户分别使用单独的物理资源（如物理服务器、物理存储）时，他们对每个云服务客户，使用一个由独立通信设备和通信电缆组成的物理网络，作为每个云服务客户的特定网络。 ——当多个云服务客户作为租户共享相同的物理资源（如物理服务器、物理存储）时，它们为每个租户或虚拟机使用一个逻辑上独立的 VLAN。 —— 管理云服务客户使用的物理资源 （如物理服务器、物理存储）的云服务管理员/器，被连接到一个与云服务客户所不同的物理端口，并使用由物理上独立的通信设备和通信电缆组成的物理网络作为管理网络。 —— 管理云服务客户使用的物理资源 （如物理服务器、物理存储）的云服务管理员/器，被连接到一个与云服务客户所不同的逻辑端口，并使用一个逻辑独立的 VLAN 做为管理网络。	
	安全实施标准技术注解	当网络被物理隔离时，不同的 ID 将被应用于完全相同的物理资产上的多个物理端口。当网络被逻辑划分时，不同的 VLAN ID、VSAN ID 或子网掩码将被应用于完全相同的物理网络上的多个逻辑网络。	
	1.1	实践指南	确认为每个租户设置了独立的网络，且没有后门。
		设想的证据	网络的路由信息和分配给租户的网络 ID（交换表，路由表等）。
		方法	检查/观察，检查/评审

表 C.11（续）

控制		ISO/IEC 27017:2015，13.1.3 网络中的隔离	
	1.2	实践指南	确认只有授权人员才能访问租户的网络配置。
		设想的证据	分配给租户的网络访问权限（访问控制服务器，网络设备访问权限管理表等）
		方法	检查/观察，检查/评审
	1.3	实践指南	确认云服务提供者所使用的管理网络与其他网络独立配置，并且确保除云服务提供者之外，只有授权人员才能访问配置的管理网络。
		设想的证据	访问权限设置和被云服务提供者用来管理网络的路由信息。
		方法	检查/观察，检查/评审

表 C.12

控制		ISO/IEC 27017:2015 ，CLD.13.1.4 虚拟和物理网络之间的一致性	
云服务提供者实现指南		云服务提供者应根据物理网络的信息安全策略，定义和文档化虚拟网络配置的信息安全策略。云服务提供者宜确保无论用何种方式创建虚拟网络配置，虚拟网络配置与信息安全策略匹配。	
附加技术信息		如果配置物理资源（如物理交换机、物理路由器、物理线缆、物理服务器、物理存储）的方法独立于配置虚拟网络的方法（该虚拟网络将物理资源作为其路由的一部分），则手动调整这些设置的配置人员需要有实践经验和专注。有各种技术手段的例子，这些技术手段不仅依赖于执行配置的人员的技能，而且会自动地调整虚拟网络和物理网络的设置。	
1	安全实施标准	——各个控制部分与虚拟网络和物理网络相隔离，且采用了集成所有控制部分的网络架构。 —— 实现虚拟交换机功能的物理交换机，而不是虚拟交换机，用于控制物理交换机上的虚拟网络和物理网络。虚拟网络和物理交换机上的物理网络。 ——将虚拟交换机和物理交换机设置的变化同步到热迁移虚拟机的机制。此外，即使在虚拟机实时迁移之后，VLAN ID 也被完全扩展以使用相同的网络设置。 ——虚拟网络和物理网络的管理系统是统一的，这个统一的系统用于配置设置。	
	安全实施标准技术注解	由于故障或虚拟机热迁移导致的重新路由，虚拟网络在物理网络上的路由将发生变化。同时，当一台物理服务器上存在多个租户或多个 VM 时，将为物理服务器上的虚拟网络设备（虚拟交换机、虚拟路由器等）配置多个虚拟网络。	
	1.1	实践指南	确认虚拟网络存在一个物理路由。
		设想的证据	物理网络设备上配置的虚拟网络 ID ，在物理服务器的虚拟网络设备上配置的虚拟网络 ID。
		方法	检查/观察，检查/评审
	1.2	实践指南	确认虚拟网络与作为路由的物理网络的配置（例如路由、交换、过滤、带宽控制、优先级控制、访问控制）相一致。
		设想的证据	物理和虚拟网络设备上的路由器选择配置（交换表、路由表等）、过滤、带宽控制、优先级划分和访问控制配置。
		方法	检查/观察，检查/评审

C.8 存储虚拟化

C.8.1 存储虚拟化概述

C.8.1.1 存储虚拟化是指将物理存储（驱动器）虚拟化为逻辑存储。

通常，存储虚拟化的结构如图C.5所示。

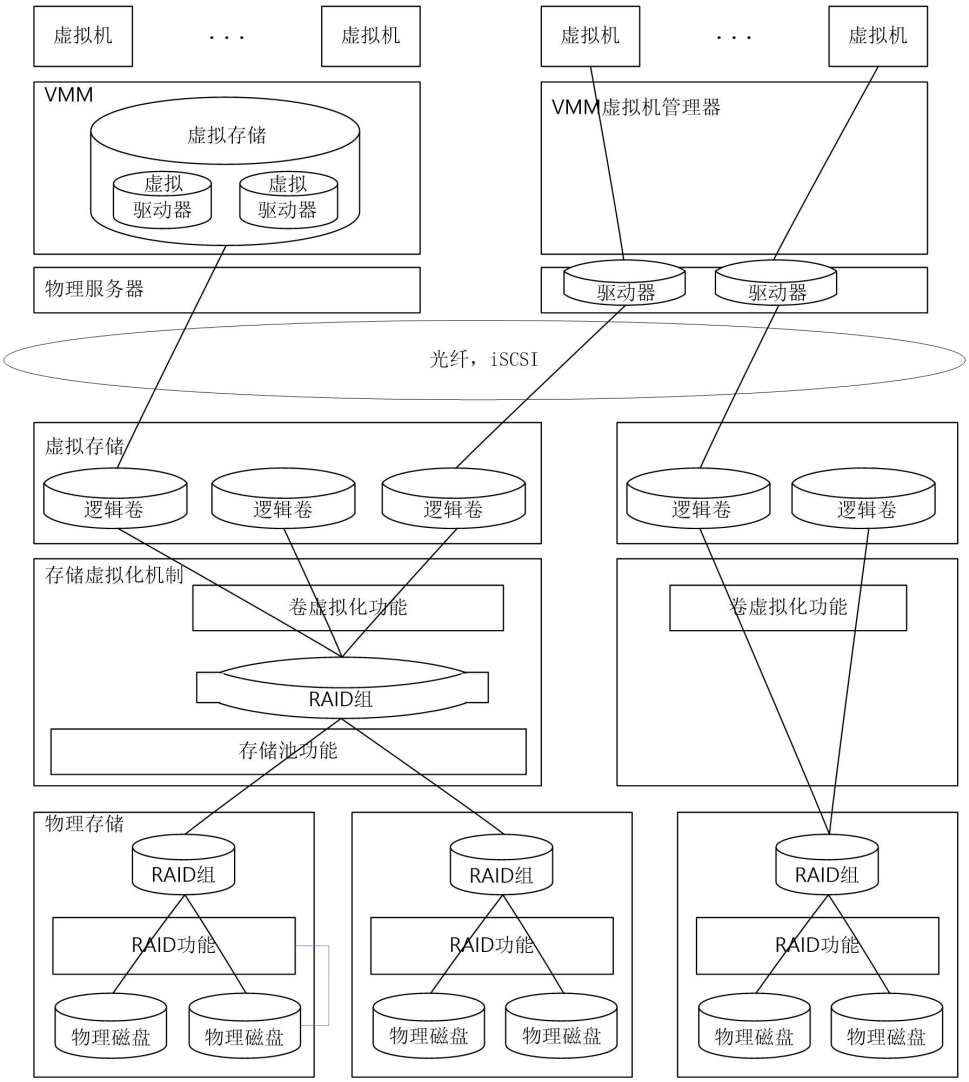

图 C.5 存储虚拟化概览

C.8.1.2 逻辑卷。存储虚拟化中最重要的元素是逻辑卷。逻辑卷是存储单元，Hypervisor 或虚拟机上的操作系统可以将其识别为存储中的虚拟资源。物理磁盘通过存储虚拟化功能进行虚拟化。

C.8.1.3 独立磁盘冗余阵列。近来，大量的存储设备被处理为诸如 RAID 组这样的逻辑卷，从抗故障的角度来看，多个物理磁盘被捆绑在一起，且具备一种有助于提高分布式数据的冗余性的机制。在多个物理磁盘上分布数据，提供了一种在物理磁盘被损坏时进行数据维护的机制。RAID 可以虚拟化区域，在这个区域上，多个物理磁盘可被捆绑为逻辑卷。

C.8.1.4 存储池。将物理磁盘或逻辑卷处理作为一个大逻辑卷（存储池）的功能。这种技术可以提高存储操作的灵活性，包括磁盘空间及其组合、在现有存储池中新增额外的物理磁盘来增加容量，这被称为

逻辑单元或逻辑设备（LDev）。

C.8.1.5 存储容量虚拟化。是一种在分配逻辑卷时，能够独立于存储器的物理容量，虚拟分配容量的功能。如果需要，在逻辑卷上存储数据时，此功能可以通过从存储池中动态分配存储区域来实现。此功能可有效利用存储资源。

C.8.1.6 SAN 分区。使用 FC 的 SAN 可以使用 FC 交换机将连接分隔成每个端口的分区。在虚拟化存储功能/技术中使用此分区功能进行分区时，会阻止对不同分区中存储的访问。

C.8.2 云服务中存储虚拟化应用

a) 存储虚拟化中的租户分离
   1） 存储虚拟化中的租户分离，是通过对每个租户的逻辑卷或SAN进行分区来实现的。注意，在 Hypervisor中创建的逻辑卷不一定分配给单个租户。
   2） 宜谨慎评估通过服务器的虚拟化功能实现的存储虚拟化，因为在服务器虚拟化中，进行存储虚拟化或租户分离时，无法通过逻辑卷实现租户分离。
b) 提高存储虚拟化的可用性功能
   1） 利用 RAID 技术、FC 交换机冗余技术、HBA和SAN 路由器配置SAN、物理存储设备的备份功能，可以提高云服务的可用性。
c) 存储虚拟化中的容量管理
   1） 存储虚拟化中应用了存储池和容量虚拟化，以便于对整个云服务中存储容量的管理，并简化对每个租户的逻辑卷容量管理。在这种情况下，需要同时管理提供给云服务的物理存储容量和提供给租户的逻辑存储容量。

C.8.3 存储虚拟化技术性评估

C.8.3.1 访问控制

表 C.13

控制		ISO/IEC 27017:2015 ，CLD.9.5.1 虚拟计算环境中的隔离
云服务提供者实现指南		云服务提供者宜对云服务客户数据、虚拟化应用程序、操作系统、存储和网络实施适当逻辑隔离，以便： ——在多租户环境中，云服务客户使用的资源的分离； ——将云服务提供者的内部管理与云服务客户使用的资源分离； 当云服务涉及多租户时，云服务提供者宜实施信息安全控制措施，以确保对不同租户使用的资源进行适当隔离。 云服务提供者宜考虑其提供的云服务中运行云服务客户提供的软件所产生相关的风险。
附加技术信息		典型的存储分隔方法如下： ——为每个租户创建逻辑卷，并在逻辑卷的基础上实现访问控制； ——使用 SAN 分区分离租户。
1	安全实施标准	基于存储虚拟化结构提供的划分功能，在云服务客户的基础上进行划分。
	安全实施标准技术注解	存储划分可以由 Hypervisor 实现。在这种情况下，由于存储虚拟化结构的原因，不需要在云服务客户基础上进行划分。

表 C.13（续）

控制		ISO/IEC 27017:2015 ， CLD.9.5.1 虚拟计算环境中的隔离	
	1.1	实践指南	在向租户提供逻辑卷的情况下，检查存储虚拟化功能的参数设置，是否访问权限仅限于租户。
		设想的证据	——存储设备参数 ——存储管理程序参数
		方法	检查/观察
	1.2	实践指南	在通过 SAN 分区分离租户的方法中，使用组成 SAN 的设备的参数设置，来检查分区是否分配给每个租户，以及不同租户之间的存储是否无法访问。
		设想的证据	构成 SAN 的光纤通道设备的分区定义
		方法	检查/观察

C.8.3.2 密码

表 C.14

控制		ISO/IEC 27017:2015 ， 10.1.1 密码控制的使用策略	
云服务提供者实现指南		云服务提供者宜向云服务客户提供有关其使用密码对其处理的信息进行保护的相关信息。云服务提供者还宜向云服务客户提供有关其可提供的所有能力的信息，以帮助云服务客户应用其自身的加密保护。	
附加技术信息		加密逻辑卷是实现存储加密的一种方法。	
1	安全实施标准	租户的数据使用逻辑卷加密功能进行加密。	
	安全实施标准技术注解	密钥的存储方式、加密范围等，因所使用的存储设备不同而异。	
	1.1	实践指南	在存储虚拟化中应用了逻辑卷加密功能的情况下，使用存储虚拟化功能提供的状态显示或实用程序功能检查相关逻辑卷是否被加密。
		设想的证据	——存储设备参数； ——存储管理程序参数。
		方法	检查/观察

C.8.3.3 运行安全

表 C.15

控制	ISO/IEC 27017:2015 ， 12.3.1 信息备份
云服务提供者实现指南	服务提供者宜向云服务客户提供其备份功能/能力的规范。适用时规范宜包括以下信息： ——备份的范围和计划； ——备份方法和数据格式，包括加密（必要时）；

表 C.15（续）

<table>
<tr><td colspan="2">控制</td><td colspan="2">ISO/IEC 27017:2015 ，12.3.1 信息备份</td></tr>
<tr><td colspan="2"></td><td colspan="2">——备份数据的保存期限；
——备份数据的完整性验证规程；
——从备份中恢复数据的规程和时间范围；
——测试备份功能的规程；
——备份的存储位置。
如果向云服务客户提供此类服务，云服务提供者宜提供对备份（如虚拟快照）的安全和隔离访问。</td></tr>
<tr><td colspan="2">附加技术信息</td><td colspan="2">如果由于某种原因，在存储虚拟化上实现虚拟化功能的存储设备或软件失效，则将保存所需的信息，可以将服务提供恢复到以前状态。
信息包括存储虚拟化功能的参数和逻辑卷的设置信息。</td></tr>
<tr><td rowspan="4">1</td><td>安全实施标准</td><td colspan="2">使用存储虚拟化功能或其他的系统实用程序，备份要保存的参数和定义信息。</td></tr>
<tr><td>安全实施标准技术注解</td><td colspan="2">如果变更虚拟存储资源会影响定义信息，则在变更触发时间或在合理的时间内更新备份数据。</td></tr>
<tr><td rowspan="3">1.1</td><td>实践指南</td><td>检查参数和定义信息是否已备份。
检查虚拟资源的变更以及备份的触发时间和周期是否有效。
检查是否可以从备份的信息中恢复以前的虚拟资源。</td></tr>
<tr><td>设想的证据</td><td>——存储设备参数；
——存储管理程序参数。</td></tr>
<tr><td>方法</td><td>检查/观察</td></tr>
</table>

C.9 服务管理

C.9.1 服务管理概述

服务管理是基础设施作为服务提供的一组功能，使云服务客户能够配置虚拟网络、服务器和存储。服务管理通过门户网站或其他方式，向云服务客户提供进行虚拟化配置的界面，并维护CMDB 中生成的设置。

云服务提供者提供的虚拟资源的安全配置由云服务客户负责进行配置。虚拟机操作系统的安全配置就是一个典型的例子。

另一方面，云服务客户不能直接访问虚拟化机制功能的配置和日志检索信息。为物理资源与虚拟结构或虚拟资源之间的关系，以及虚拟资源与云服务客户之间的关系提供关联也是服务管理的作用。一般情况下，这些关系的连接是通过CMDB实现的。

用户门户允许根据上述相关信息访问云服务客户的虚拟资源和虚拟化功能。此外，还向云服务客户提供显示通知和当前云系统上发生的事件的状态的功能。

图C.6显示了云计算模型中的服务管理系统。

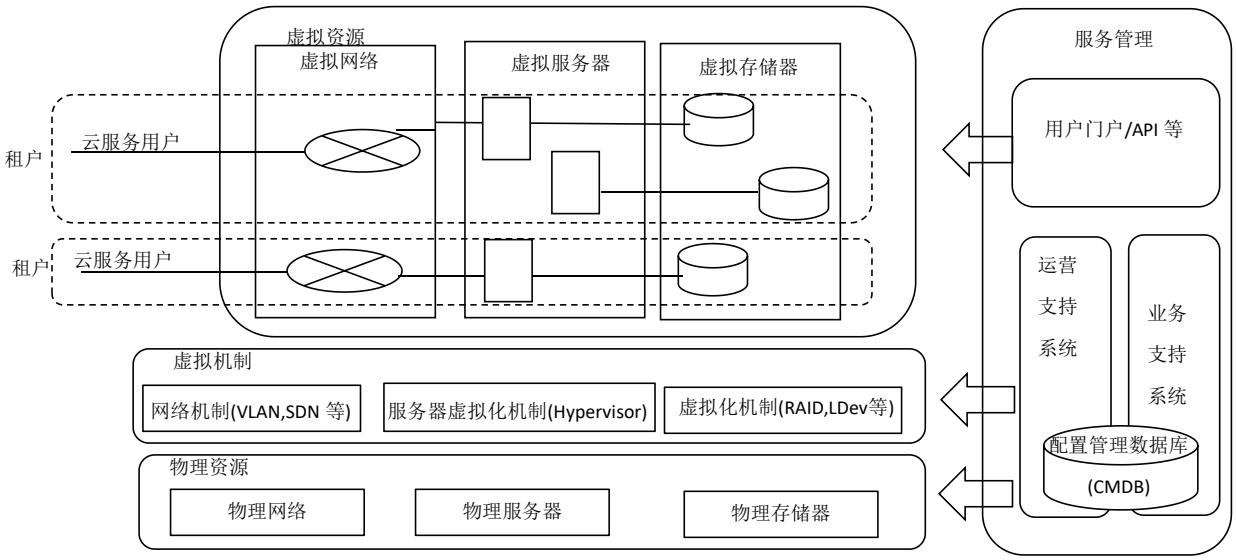

图 C.6 服务管理大纲

C.9.2 云服务中服务器虚拟化应用

a） 访问控制

1）每个虚拟化功能都具有对虚拟化功能本身的访问控制机制和对虚拟资源的访问控制机制。鉴别方法（口令）、应用访问权限的对象（用户ID等）和控制范围，因网络、服务器和存储部分的不同而异。服务管理通过在不同分类中应用适当的访问控制，实现对作为租户的云服务客户的统一访问控制。

b） 用户身份验证

1） 作为访问控制的前提，必须确保对云服务客户执行正确的身份鉴别。在服务管理中，用户门户和API是云服务客户的主要接口，但应在第一个访问点执行用户身份鉴别。

2） 用户授权的某些项目是由用户可用的最大资源、费用余额、合同和计费成本决定的。这些由BSS管理。

3） 另一方面，云服务客户对虚拟化功能的参数配置等，以及上述虚拟化功能的访问管理，由OSS管理。

c） 配置管理

1） 物理服务器和物理服务器上运行的虚拟服务器之间的关系，虚拟服务器和云服务的客户之间的关系，以及云服务客户之间的关系和合同条件，费用等,对于管理和运营云服务是必要的信息，在应用访问控制时也会使用这些关系信息。

2） 在服务管理中，涉及到配置相关的信息在CMDB中存储和管理。BSS和OSS参考此配置管理数据库，并在更新时进行操作。

d）事件管理

1） 物理服务器和物理服务器上运行的虚拟服务器之间的关系，虚拟服务器和云服务的客户之间的关系，以及云服务客户之间的关系和合同条件，费用等,对于管理和运营云服务是必要的信息，在应用访问控制时也会使用这些关系信息。

C.9.3 服务管理技术性评估

C.9.3.1 用户访问管理

表 C.16

控制		ISO/IEC 27017:2015，9.2.1 用户注册和注销	
云服务提供者实现指南		为了管理云服务客户的云服务用户对云服务的访问，云服务提供者宜向云服务客户提供用户注册和注销功能，以及使用这些功能的规范。	
附加技术信息		C9.2.1 的目的是在服务管理中添加和删除云服务用户。通常，云服务客户会运行活动资源的功能，在虚拟资源（如 VM OS）上进行用户的注册和删除。 云服务提供者也可以为云服务客户提供恢复其自身数据的能力。云服务客户恢复自己数据的方式必须独立于云服务提供者及其系统状态。 此外，云服务提供者宜向云服务客户提供无缝变更云服务提供者的服务，以减轻锁定风险。	
1	安全实施标准	云服务用户管理在服务管理中实现。 虚拟化功能的访问控制由服务管理控制，不向云服务客户公开提供。	
	安全实施标准技术注解	如果可以通过服务管理门户对云服务用户进行管理，则在服务管理门户中提供注册和删除的方法。 由于云服务客户的管理是一个重要的安全项，云服务提供商可在与用户取得联系后注册和删除上述云服务用户。	
	1.1	实践指南	确认云服务客户是否存在通过云服务客户门户、API 等注册或删除云服务用户的方法。
		设想的证据	——门户运行界面及运行结果； ——API 等接口及 API 操作结果。
		方法	检查/观察，测试

表 C.17

控制		ISO/IEC 27017:2015，9.2.2 用户访问供给	
云服务提供者实现指南		云服务提供者宜提供管理云服务客户的云服务用户的访问权限的功能，以及使用这些功能的规范。	
附加技术信息		C9.2.2 的目的是为服务管理中的云服务用户提供访问供给。 虚拟资源（例如 VM 操作系统）的访问设置不受 C9.2.2 的约束。	
1	安全实施标准	云服务用户管理在服务管理中实现。	
	安全实施标准技术注解	服务管理提供的云服务用户的访问权限管理，不一定需要与虚拟化功能中的访问权限管理相同。然而，有必要实施访问权限管理规范，将其作为服务管理呈现给云服务客户。 服务管理的访问供给作为门户中云服务用户的管理提供。 此控制中“云服务的其他信息”中提到的单点登录，是在服务管理门户等中实现的，SAML 可以作为一个典型的实现类型。	
	1.1	实践指南	确认门户中的用户控制中，提供了云服务用户访问权限管理功能。
		设想的证据	门户运行界面及运行结果。
		方法	检查/观察，测试

表 C.17（续）

控制		ISO/IEC 27017:2015，9.2.2 用户访问供给	
	1.2	实践指南	如果提供了单点登录功能，确认它可以与提供的协议等一起使用。
		设想的证据	——实现了单点登录的外部应用程序； ——通过外部应用程序访问服务管理的结果。
		方法	检查/观察，测试

表 C.18

控制		ISO/IEC 27017:2015，9.2.3 特许访问权管理	
云服务提供者实现指南		云服务提供者宜根据所识别的风险，提供足够的鉴别技术，以验证云服务客户的云服务管理员对云服务的管理能力。例如，云服务提供者可以提供多因素鉴别能力或启用第三方多因素鉴别机制。	
附加技术信息		C9.2.3 的目的是为服务管理中的云服务用户提供访问设置。 虚拟资源（例如 VM OS）的访问设置不受 C9.2.3 的约束。	
1	安全实施标准	此控制中定义的“强身份鉴别”在服务管理的门户身份鉴别等中实现。	
	安全实施标准技术注解	作为此控制中“强身份鉴别”的示例，多因素身份鉴别包括以下组件。 ——生物特征鉴别 ——除密码外，使用令牌进行身份鉴别 ——客户证书鉴别	
	1.1	实践指南	确认在服务管理中提供足够强的身份鉴别作为门户身份鉴别。
		设想的证据	云服务提供者提供的足够强的身份鉴别方法和测试结果
		方法	检查/观察，测试

表 C.19

控制		ISO/IEC 27017:2015 ，9.4.1 信息访问限制
云服务提供者实现指南		云服务提供者宜提供访问控制，允许云服务客户限制对其云服务，云服务功能和服务中维护的云服务客户数据的访问。
附加技术信息		C9.4.1 的目的是为服务管理中的云服务用户提供访问设置。 虚拟资源（例如 VM OS）的访问设置不受 C9.4.1 的约束。
1	安全实施标准	通过服务管理向云服务客户提供的信息和访问权限，仅限于云服务客户内部的租户，不得为其他租户提供任何信息或访问权限。 在可以定义基于客户处理的信息和访问权限的情况下，这些操作将通过门户中的客户管理功能等实现。
	安全实施标准技术说明	多个云服务客户共享云服务中虚拟化的功能。通过虚拟化访问控制功能实现租户分离，使每个云服务客户无法访问其他云服务客户的租户相关信息。 基于客户的访问控制可以在服务管理中实现，而不是使用虚拟化功能的访问控制。

表 C.19（续）

控制		ISO/IEC 27017:2015 ，9.4.1 信息访问限制	
	1.1	实践指南	通过使用信息提供和访问权限的管理功能，确认无法在门户中访问其他租户的信息。
		设想的证据	门户运行界面及运行结果
		方法	检查/观察，测试
	1.2	实践指南	在提供了基于客户的访问控制功能的情况下，确认在为客户配置的访问权限范围内可以访问云服务。
		设想的证据	——客户控制界面和门户中的操作等； ——对客户应用访问权限限制时的访问结果。
		方法	检查/观察，测试

表 C.20

控制		ISO/IEC 27017:2015 ，9.4.4 特权实用程序的使用	
云服务提供者实现指南		云服务提供者宜识别云服务中使用的任何实用程序的需求。 云服务提供者宜确保任何能够绕过正常操作或安全规程的实用程序的使用严格限于授权人员，并定期对这些程序的使用进行评审和审核。	
附加技术信息		虚拟化功能附带的实用程序可能会对云服务客户租户之外的资源产生影响。 如果云服务客户需要显示虚拟化功能状态等应用程序的结果，则宜以不影响其他客户的方式将结果提供给云服务客户。	
1	安全实施标准	禁止云服务客户直接使用提供云服务客户所需信息的虚拟化实用程序，以防对其他租户的不良影响。宜通过服务管理功能收集那些信息。	
	安全实施标准技术说明	C9.4.4 中的实用程序包括以下内容： ——检索与服务器虚拟化相关的虚拟服务器规格、日志、性能信息； ——检索网络虚拟化相关的流量信息等； ——检索与服务器虚拟化相关的卷副本、访问信息等。	
	1.1	实践指南	确认云服务客户提供的实用功能所提供的信息不包括与其他租户相关的信息。
		设想的证据	实用功能使用结果
		方法	检查/观察，测试
2	安全实施标准	当云服务客户在租户环境中使用实用程序进行虚拟化时，宜配置虚拟化参数，以确保不影响该租户之外的其他方。	
	安全实施标准技术注解	通常，很难在虚拟资源中使用与虚拟化功能绑定在一起的实用程序。 为了对 C9.4.4 进行技术性评估，有必要发现是否存在任何可能超出虚拟资源中必要资源并影响其他资源的实用程序，并对这些资源是否受到影响进行以下检查。	
	2.1	实践指南	对于可能影响其他资源的实用程序，确认在虚拟化功能中定义了阻止此操作的参数。 注：如果实际执行了此类测试，则宜考虑到这可能导致云计算环境中的故障。

表 C.20（续）

控制		ISO/IEC 27017:2015 ，9.4.4 特权实用程序的使用	
		设想的证据	虚拟化功能的参数定义等。
		方法	检查/观察

C.9.3.2 密码

表 C.21

控制		ISO/IEC 27017:2015，10.1.1 密码控制的使用策略	
云服务提供者实现指南		云服务提供者宜向云服务客户提供有关其使用密码技术保护其处理信息的情况。云服务提供者还宜向云服务客户提供有关其提供的可帮助云服务客户应用其自身密码保护的任何功能的信息。	
附加技术信息		在服务管理中，对门户加密访问等需使用此控制。	
1	安全实施标准	实施门户加密访问的一个典型例子是基于 SSL/TLS 的超文本传输协议。	
	安全实施标准技术注解	与服务管理门户的通信将使用超文本传输安全协议。	
	1.1	实践指南	确认超文本传输安全协议作为服务管理门户的协议。
		设想的证据	——用于访问门户的协议； ——用于访问门户的证书等。
		方法	检查/观察
2	安全实施标准	为了在服务管理中管理云服务客户和云服务用户的信息，控制“注解”中特定类型的信息将被存储。 根据云服务提供者的策略，必要时，宜将此控制中表示的加密应用于此信息。	
	安全实施标准技术注解	云管理所管理的数据加密是云服务提供者自身的安全控制，与此控制中定义的向云服务客户提供的功能不同。	
	2.1	实践指南	不适用
		设想的证据	不适用
		方法	-

C.9.3.3 信息安全事件管理

表 C.22

控制	ISO/IEC 27017:2015，16.1.2 报告信息安全事态
云服务提供者实现指南	云服务提供者宜提供以下机制: 云服务客户向提供者报告信息安全事态；

表 C.22（续）

控制		ISO/IEC 27017:2015，16.1.2 报告信息安全事态	
		云服务提供者向云服务客户报告信息安全事态； 云服务客户跟踪报告的信息安全事态的状态。	
附加技术信息		如“云服务的其他信息”所述，该机制通过电话、电子邮件等方式提供。	
1	安全实施标准	门户功能可作为云服务客户的接口提供，用于在服务管理中管理此控制中定义的信息安全事件。	
	安全实施标准技术注解	在服务管理中实现此功能时，将管理云服务客户提出的报告和云服务提供者提供的信息，云服务客户将具有了解相关事件当前情况的功能。	
	1.1	实践指南	确认门户提供有关信息安全事件的报告和评估态势的功能。
		设想的证据	信息安全事件相关界面及门户上的操作等。
		方法	检查/观察

C.10 ISO/IEC 27017 和本附录中的名称关系表

表C.23显示了ISO/IEC27017和本附录中的名称。

表 C.23

章条	标题	通用的	服务器虚拟化	网络虚拟化	存储虚拟化	服务管理
5	信息安全策略	非“技术性的”，不适用				
5.1	信息安全管理指导					
6	信息安全组织	非“技术性的”，不适用				
6.1	内部组织					
6.2	移动设备和远程工作					
CLD.6.3	云服务客户与云服务提供者的关系					
7	人力资源安全	非“技术性的”，不适用				
7.1	任用前					
7.2	任用中					
7.3	任用的终止和变更					
8	资产管理	“物理资源”超出范围，不适用				
8.1	有关资产的责任					

表 C.23（续 1）

章条	标题	通用的	服务器虚拟化	网络虚拟化	存储虚拟化	服务管理
CLD.8.1	有关资产的责任					
8.2	信息分级					
8.3	介质处理					
9	访问控制	——对云服务客户访问控制的描述基本在服务管理中完成。 ——本章不包括对云服务提供者的操作者的访问控制，但第 12 章包括。 ——本章包括虚拟化/虚拟资源功能中每个客户访问控制的可能设置。				
9.1	访问控制的业务要求	—	—	—	—	—
9.2	用户访问管理	R	R	R	R	9.2.1 9.2.2 9.2.3
9.3	用户责任	—	—	—	—	—
9.4	系统和应用访问控制	R	R	R	R	9.4.1 9.4.4
CLD.9.5	共享虚拟环境中云服务客户数据的访问控制	R	CLD.9.5.1 CLD.9.5.2	见 13.1.3	CLD.9.5.1	L
10	密码	——涵盖了虚拟化功能所需的加密情况。				
10.1	密码控制		10.1.1	10.1.1	10.1.1	10.1.1
11	物理和环境安全	“物理资源”超出范围，不适用				
11.1	安全区域	—	—	—	—	—
11.2	设备	—	—	—	—	—
12	运行安全	——关注服务提供者的操作者处理虚拟化功能/虚拟资源。				
12.1	运行规程和责任	12.1.2 12.1.3	L	L	L	L
CLD.12.1	运行规程和责任	CLD.12.1.5	L	L	L	L
12.2	恶意软件防范	—	—	—	—	—
12.3	备份	R	R	R	12.3.1	L
12.4	日志和监视	12.4.1 12.4.4	L	L	L	L
CLD.12.4	日志和监视	CLD.12.4.5	L	L	L	L

表 C.23（续 2）

章条	标题	通用的	服务器虚拟化	网络虚拟化	存储虚拟化	服务管理
12.5	运行软件控制	—	—	—	—	—
12.6	技术方面的脆弱性管理	12.6.1	L	L	L	L
12.7	信息系统审计的考虑	—	—	—	—	—
13	通信安全	——关注网络安全				
13.1	网络安全管理	R	R	13.1.3	L	-
CLD.13.1	日志和监视	R	R	CLD.13.1.4	L	L
13.2	信息传输	—	—	—	—	—
14	系统获取、开发和维护	不直接和技术模型相关，不适用				
14.1	信息系统的安全要求					
14.2	开发和支持过程中的安全					
14.3	测试数据	—	—	—	—	—
15	供应商关系	非“技术性的”，不适用				
15.1	供应商关系中的信息安全					
15.2	供应商服务交付管理	—	—	—	—	—
16	信息安全事件管理					
16.1	信息安全事件的管理和改进	R	R	R	R	16.1.2
17	业务连续性管理的信息安全方面					
17.1	信息安全的连续性					
17.2	冗余					
18	符合性					
18.1	符合法律和合同要求					
18.2	信息安全评审					

云服务提供者管理控制在 ISO/IEC27017 中没有定义。 表中字母说明如下：

L——主要用左边部分表示的内容来实现。

R——主要用右边部分表示的内容来实现。

注：空白单元格表示不需要技术注解。

附 录 D
（资料性）

GB/T 22081—2016/ISO/IEC 27002:2013 与 ISO/IEC 27002:2022 控制的对应关系

GB/T 22081—2016/ISO/IEC 27002:2013与ISO/IEC 27002:2022控制的对应关系见表D.1。

表 D.1 GB/T 22081—2016/ISO/IEC 27002:2013 与 ISO/IEC 27002:2022 控制的对应关系表

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
5 信息安全策略	
5.1 信息安全管理指导	
5.1.1 信息安全策略	5.1 信息安全策略
5.1.2 信息安全策略的评审	5.1 信息安全策略
6 信息安全组织	
6.1 内部组织	
6.1.1 信息安全的角色和责任	5.2 信息安全的角色和责任
6.1.2 职责分离	5.3 职责分离
6.1.3 与职能机构的联系	5.5 与职能机构的联系
6.1.4 与特定相关方的联系	5.6 与特定相关方的联系
6.1.5 项目管理中的信息安全	5.8 项目管理中的信息安全
6.2 移动设备和远程工作	
6.2.1 移动设备策略	8.1 用户终端设备
6.2.2 远程工作	6.7 远程工作
7 人力资源安全	
7.1 任用前	
7.1.1 审查	6.1 审查
7.1.2 任用条款及条件	6.2 任用条款及条件
7.2 任用中	
7.2.1 管理责任	5.4 管理责任
7.2.2 信息安全意识、教育和培训	6.3 信息安全意识、教育和培训
7.2.3 违规处理过程	6.4 违规处理过程
7.3 任用的终止和变更	
7.3.1 任用终止或变更的责任	6.5 任用终止或变更的责任

表D.1 （续1）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
8 资产管理	
8.1 有关资产的责任	
8.1.1 资产清单	5.9 信息和其他相关资产的清单
8.1.2 资产的所属关系	5.9 信息和其他相关资产的清单
8.1.3 资产的可接受使用	5.10 信息和其他相关资产的可接受使用
8.1.4 资产归还	5.11 资产归还
8.2 信息分级	
8.2.1 信息的分级	5.12 信息的分级
8.2.2 信息的标记	5.13 信息的标记
8.2.3 资产的处理	5.10 信息和其他资产的可接受使用
8.3 介质处理	
8.3.1 移动介质的管理	7.10 存储媒体
8.3.2 介质的处置	7.10 存储媒体
8.3.3 物理介质的转移	7.10 存储媒体
9 访问控制	
9.1 访问控制的业务要求	
9.1.1 访问控制策略	5.15 访问控制
9.1.2 网络和网络服务的访问	5.15 访问控制
9.2 用户访问管理	
9.2.1 用户注册和注销	5.16 身份管理
9.2.2 用户访问供给	5.18 访问权
9.2.3 特定访问权管理	8.2 特定访问权
9.2.4 用户的秘密鉴别信息管理	5.17 鉴别信息
9.2.5 用户访问权的评审	5.18 访问权
9.2.6 访问权的移除或调整	5.18 访问权
9.3 用户责任	
9.3.1 秘密鉴别信息的使用	5.17 鉴别信息

表D.1 （续2）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
9.4 系统和应用访问控制	
9.4.1 信息访问限制	8.3 信息访问限制
9.4.2 安全登录规程	8.5 安全鉴别
9.4.3 口令管理系统	5.17 鉴别信息
9.4.4 特权实用程序的使用	8.18 特权实用程序的使用
9.4.5 程序源代码的访问控制	8.4 访问源代码
10 密码	
10.1 密码控制	
10.1.1 密码控制的使用策略	8.24 密码的使用
10.1.2 密钥管理	8.24 密码的使用
11 物理和环境安全	
11.1 安全区域	
11.1.1 物理安全边界	7.1 物理安全边界
11.1.2 物理入口控制	7.2 物理入口
11.1.3 办公室、房间和设施的安全保护	7.3 办公室、房间和设施的安全保护
11.1.4 外部和环境威胁的安全防护	7.5 物理和环境威胁的安全防护
11.1.5 在安全区域工作	7.6 在安全区域工作
11.1.6 交接区	7.2 物理入口
11.2 设备	
11.2.1 设备安置和保护	7.8 设备安置和保护
11.2.2 支持性设施	7.11 支持性设施
11.2.3 布缆安全	7.12 布缆安全
11.2.4 设备维护	7.13 设备维护
11.2.5 资产的移动	7.10 存储媒体
11.2.6 组织场所外的设备与资产安全	7.9 组织场所外资产安全
11.2.7 设备的安全处置或再利用	7.14 设备的安全处置或再利用
11.2.8 无人值守的用户设备	8.1 用户终端设备

表D.1 （续3）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
11.2.9 清理桌面和屏幕策略	7.7 清理桌面和屏幕
12 运行安全	
12.1 运行规程和职责	
12.1.1 文件化的操作规程	5.37 文件化的操作规程
12.1.2 变更管理	8.32 变更管理
12.1.3 容量管理	8.6 容量管理
12.1.4 开发、测试和运行环境的分离	8.31 开发、测试和运行环境的分离
12.2 恶意软件防范	
12.2.1 恶意软件的控制	8.7 恶意软件防范
12.3 备份	
12.3.1 信息备份	8.13 信息备份
12.4 日志和监视	
12.4.1 事态日志	8.15 日志
12.4.2 日志信息的保护	8.15 日志
12.4.3 管理员和操作员日志	8.15 日志
12.4.4 时钟同步	8.17 时钟同步
12.5 运行软件控制	
12.5.1 运行系统的软件安装	8.19 运行系统的软件安装
12.6 技术方面的脆弱性管理	
12.6.1 技术方面脆弱性的管理	8.8 技术方面脆弱性的管理
12.6.2 软件安装限制	8.19 运行系统的软件安装
12.7 信息系统审计的考虑	
12.7.1 信息系统审计的控制	8.34 审计测试期间信息系统防护
13 通信安全	
13.1 网络安全管理	
13.1.1 网络控制	8.20 网络安全
13.1.2 网络服务的安全	8.21 网络服务的安全

表D.1 （续4）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
13.1.3 网络中的隔离	8.22 网络隔离
13.2 信息传输	
13.2.1 信息传输策略和规程	5.14 信息传输
13.2.2 信息传输协议	5.14 信息传输
13.2.3 电子消息发送	5.14 信息传输
13.2.4 保密或不泄露协议	6.6 保密或不泄露协议
14 系统获取、开发和维护	
14.1 信息系统的安全要求	
14.1.1 信息安全要求分析和说明	5.8 项目管理中的信息安全
14.1.2 公共网络上应用服务的安全保护	8.26 应用安全要求
14.1.3 应用服务事务的保护	8.26 应用安全要求
14.2 开发和支持过程中的安全	
14.2.1 安全的开发策略	8.25 安全开发生命周期
14.2.2 系统变更控制规程	8.32 变更管理
14.2.3 运行平台变更后对应用的技术评审	8.32 变更管理
14.2.4 软件包变更的限制	8.32 变更管理
14.2.5 系统安全工程原则	8.27 安全系统架构和工程原则
14.2.6 安全的开发环境	8.31 开发、测试和运行环境的分离
14.2.7 外包开发	8.30 外包开发
14.2.8 系统安全测试	8.29 开发和验收中安全测试
14.2.9 系统验收测试	8.29 开发和验收中安全测试
14.3 测试数据	
14.3.1 测试数据的保护	8.33 测试信息
15 供应商关系	
15.1 供应商关系中的信息安全	
15.1.1 供应商关系的信息安全策略	5.19 供应商关系中的信息安全
15.1.2 在供应商协议中强调安全	5.20 在供应商协议中强调安全

表 D.1 （续 5）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
15.1.3 信息与通信技术供应链	5.21 管理 ICT 供应链中信息安全
15.2 供应商服务交付管理	
15.2.1 供应商服务的监视和评审	5.22 供应商服务的监视、评审和变更管理
15.2.2 供应商服务的变更管理	5.22 供应商服务的监视、评审和变更管理
16 信息安全事件管理	
16.1 信息安全事件的管理和改进	
16.1.1 责任和规程	5.24 信息安全事件管理的规划和准备
16.1.2 报告信息安全事态	6.8 信息安全事态报告
16.1.3 报告信息安全弱点	6.8 信息安全事态报告
16.1.4 信息安全事态的评估和决策	5.25 信息安全事态的评估和决策
16.1.5 信息安全事件的响应	5.26 信息安全事件的响应
16.1.6 从信息安全事件中学习	5.27 从信息安全事件中学习
16.1.7 证据的收集	5.28 证据的收集
17 业务连续性管理的信息安全方面	
17.1 信息安全的连续性	
17.1.1 规划信息安全连续性	5.29 中断期间的信息安全
17.1.2 实现信息安全连续性	5.29 中断期间的信息安全
17.1.3 验证、评审和评价信息安全连续性	5.29 中断期间的信息安全
17.2 冗余	
17.2.1 信息处理设施的可用性	8.14 信息处理设施的冗余
18 符合性	
18.1 符合法律和合同要求	
18.1.1 适用的法律和合同要求的识别	5.31 法律、法规、监管和合同要求
18.1.2 知识产权	5.32 知识产权
18.1.3 记录的保护	5.33 记录的保护
18.1.4 隐私和个人可识别信息保护	5.34 隐私和个人可识别信息保护
18.1.5 密码控制规则	5.31 法律、法规、监管和合同要求

表 D.1 （续 6）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
18.2 信息安全评审	
18.2.1 信息安全的独立评审	5.35 信息安全的独立评审
18.2.2 符合安全策略和标准	5.36 符合信息安全策略、规则和标准
18.2.3 技术符合性评审	5.36 符合信息安全策略、规则和标准 8.8 技术方面脆弱性的管理

参 考 文 献

[1] GB/T 19011-2021 管理体系审核指南（ISO 19011:2018,IDT）
[2] GB/T 22080-2016 信息技术 安全技术 信息安全管理体系 要求
[3] GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南
[4] GB/T 25067-2020 信息技术 安全技术 信息安全管理体系审核和认证机构要求
[5] GB/T 28450-2020 信息技术 安全技术 信息安全管理体系审核指南
[6] GB/T 31722-2015 信息技术 安全技术 信息安全风险管理
[7] ISO Guide 73, Risk management -Vocabulary
[8] ISO/IEC 27002:2022 Information technology—Cybersecurity and privacy protection—Information security controls
[9] ISO/IEC 27017, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
[10] NIST Special publication （SP） 800-53A, Guide for reviewing the controls in federal information systems, July 2008. Available from: https://csrc.nist.gov/publications/PubsSPs.html
[11] Federal Office for Information Security（BSI）. Germany, Standard 100-1, Information Security Management Systems （ISMS）; 100-2, IT-Grundschutz Methodology; 100-3, Risk Analysis based on IT-Grundschutz and IT-Grundschutz Catalogues, 100-4, Business Continuity Management （available in German and English）. Available from:https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html
[12]Information Security Forum, The Standard of Good Practice for Information Security, 2007. Available from:https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/
[13] Institute For Security And Open Methodologies. Open-Source Security Testing Methodology Manual. Available from: http://www.isecom.org/research/osstmm.html