国际标准 ISO/IEC 27001-2022

2022

信息安全、网络安全和隐私保护-信息安全管理体系-要求

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

编译 樊山

国际标准 ISO/IEC 27001

信息安全、网络安全和隐私保护-信息安全管理体系-要求

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

翻译：樊山 （鹰眼翻译社区）

第三版

2022-10

目录

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了全球标准化的专门体系。作为 ISO 或 IEC 成员的国家机构通过各自组织为处理特定技术活动领域而设立的技术委员会参与国际标准的制定。ISO 和 IEC 技术委员会在共同感兴趣的领域进行合作。与 ISO 和 IEC 保持联系的其他国际组织，包括政府组织和非政府组织也参与了这项工作。

ISO/IEC 指令第 1 部分描述了用于编制本文件的程序及其进一步维护的程序。特别是，应注意不同类型文件所需的不同批准标准。本文件根据 ISO/IEC 指令第 2 部分的编辑规则起草（见 www.ISO.org/Directives 或 https://www.iec.ch/members_experts/refdocs）。

请注意，本文件的某些要素可能是专利权的主题。ISO 和 IEC 不对识别任何或所有此类专利权负责。文件开发过程中确定的任何专利权的详细信息将在引言和/或收到的 ISO 专利声明列表（见 www.ISO.org/patents）或 IEC 专利声明列表中（见 https://patents.iec.ch/）。

本文件中使用的任何商品名称都是为方便用户而提供的信息，不构成背书。

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

本文件由 ISO/IEC JTC 1 信息技术联合技术委员会 SC 27 信息安全、网络安全和隐私保护小组委员会编写。

第三版取消并取代了第二版（ISO/IEC 27001:2013），该版本已进行了技术修订。它还包含了技术勘误表 ISO/IEC 27001:2013/Cor 1:2014 和 ISO/IEC 2.7001:2013/Cor 2:2015。

主要变化如下：

-文本已与管理体系标准和 ISO/IEC 27002:2022 的协调结构保持一致。

关于本文件的任何反馈或问题都应提交给用户的国家标准机构。这些机构的完整清单可在 www.iso.org/members 上找到。html 和 https://www.iec.ch/national-committees。

介绍

0.1 概述

本文件旨在提供建立、实施、维护和持续改进信息安全管理体系的要求。采用信息安全管理体系是一个组织的战略决策。组织信息安全管理体系的建立和实施受组织的需求和目标、安全要求、使用的组织流程以及组织的规模和结构的影响。所有这些影响因素都将随着时间的推移而改变。

信息安全管理体系通过应用风险管理流程来保护信息的机密性、完整性和可用性，并向相关方提供充分管理风险的信心。

重要的是，信息安全管理体系是组织过程和总体管理结构的一部分并与之集成，并且在过程、信息系统和控制的设计中考虑信息安全。预计将根据本组织的需要扩大信息安全管理体系的实施规模。

内部和外部各方可使用本文件来评估组织满足自身信息安全要求的能力。

本文件中提出要求的顺序并不反映其重要性或暗示其实施顺序。列举列表项仅供参考。

ISO/IEC 27000 描述了信息安全管理系统的概述和词汇，参考了信息安全安全管理体系系列标准（包括 ISO/IEC 27003[2]、ISO/IEC 27004[3]和 ISO/IEC27005[4]）以及相关术语和定义。

0.2 与其他管理体系标准的兼容性

本文件采用 ISO/IEC 指令第 1 部分《综合 ISO 增补件》附录 SL 中定义的高层结构、相同的子条款标题、相同的文本、通用术语和核心定义，因此与采用附录 SL 的其他管理体系标准保持兼容性。

附录 SL 中定义的这种通用方法对于那些选择运行满足两个或多个管理系统标准要求的单一管理系统的组织来说是有用的。

信息安全、网络安全和隐私保护.信息安全管理系统.要求

1 范围

本文件规定了在组织范围内建立、实施、维护和持续改进信息安全管理体系的要求。本文件还包括针对组织需求量身定制的信息安全风险评估和处理要求。本文件中规定的要求是通用的，旨在适用于所有组织，无论其类型、规模或性质如何。当组织声称符合本文件要求时，不接受排除第 4 条至第 10 条规定的任何要求。

2 规范性引用文件

以下文件在正文中的引用方式使其部分或全部内容构成本文件的要求。对于注明日期的引用文件，仅引用的版本适用。对于未注明日期的引用文件，引用文件的最新版本（包括任何修订）适用。

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

3 术语和定义

在本文件中，ISO/IEC 27000 中给出的术语和定义适用。ISO 和 IEC 在以下地址维护用于标准化的术语数据库：

-ISO 在线浏览平台：可在 https://www.iso.org/obp/ui

-IEC 电子介质：网址：https://www.electropedia.org/

4 组织背景

4.1 了解组织及其背景

组织应确定与其目的相关且影响其实现信息安全管理体系预期结果的能力的外部和内部问题。

注：确定这些问题是指建立在 ISO 31000:2018[5]第 5.4.1 条所述组织的外部和内部环境。

4.2 了解相关方的需求和期望

组织应确定：

a） 与信息安全管理体系相关的相关方；

b） 相关方的相关要求；

c） 其中哪些要求将通过信息安全管理体系解决。

注：相关方的要求可以包括法律法规要求和合同义务。

4.3 确定信息安全管理系统的范围

组织应确定信息安全管理体系的边界和适用性，以确定其范围。

在确定该范围时，组织应考虑：

a） 4.1 中提到的外部和内部问题；

b） 4.2 中提到的要求；

c） 组织所执行的活动与其他组织所执行活动之间的接口和依赖关系。

范围应作为文件信息提供。

4.4 信息安全管理系统

组织应根据本文件的要求，建立、实施、维护和持续改进信息安全管理体系，包括所需的过程及其相互作用。

5 领导力

5.1 领导力和承诺

最高管理层应通过以下方式展示对信息安全管理体系的领导和承诺：

a） 确保制定信息安全政策和信息安全目标，并与组织的战略方向相一致；

b） 确保信息安全管理体系要求与组织流程的整合；

c） 确保信息安全管理体系所需的资源可用；

d） 传达有效信息安全管理和符合信息安全管理体系要求的重要性；

e） 确保信息安全管理体系达到预期结果；

f） 指导和支持人员对信息安全管理体系的有效性作出贡献；

g） 促进持续改进；和

h） 支持其他相关管理角色在其职责范围内发挥领导作用。

注：本文件中提及的“业务”可以广义地解释为是指那些对组织存在目的至关重要的活动。

5.2 政策

最高管理层应制定信息安全政策，以：

a） 适合组织的目的；

b） 包括信息安全目标（见 6.2）或提供信息安全目标设置框架；

c） 包括满足信息安全相关适用要求的承诺；

d） 包括持续改进信息安全管理系统的承诺。

信息安全政策应：

e） 作为文件化信息提供；

f） 在组织内部进行沟通；

g） 酌情提供给相关方。

5.3 组织角色、职责和权限

最高管理层应确保在组织内分配和传达与信息安全相关的职责和权限。

最高管理者应分配以下职责和权限：

a） 确保信息安全管理体系符合本文件的要求；

b） 向最高管理层报告信息安全管理体系的性能。

注：最高管理层还可以为报告组织内信息安全管理系统的绩效分配职责和权限。

6 规划

6.1 应对风险和机遇的行动

6.1.1 一般原则

在规划信息安全管理体系时，组织应考虑 4.1 中提到的问题和 4.2 中提到的要求，并确定需要解决的风险和机遇：

a） 确保信息安全管理体系能够实现预期结果；

b） 防止或减少不良影响；

c） 实现持续改进。

组织应计划：

d） 应对这些风险和机遇的行动；和

e） 如何

1） 将行动整合并实施到其信息安全管理体系流程中；和

2） 评估这些行动的有效性。

6.1.2 信息安全风险评估

组织应定义并应用信息安全风险评估流程，该流程应：

a） 建立并维护信息安全风险标准，包括：

1） 风险接受标准；和

2） 进行信息安全风险评估的标准；

b） 确保重复的信息安全风险评估产生一致、有效和可比的结果；

c） 识别信息安全风险：

1） 应用信息安全风险评估流程，识别与信息安全管理体系范围内造成信息的保密性、完整性和可用性损害的相关风险；和

2） 确定风险所有者；

d） 分析信息安全风险：

1） 评估如果 6.1.2 c）1）中确定的风险成为现实将产生的潜在后果；

2） 评估 6.1.2 c）1）中确定的风险发生的现实可能性；和

3） 确定风险等级；

e） 评估信息安全风险：

1） 将风险分析结果与6.1.2a）中规定的风险标准进行比较；和

2） 优先考虑风险处理的分析风险。

组织应保留有关信息安全风险评估过程的文件化信息。

6.1.3 信息安全风险处理

组织应定义并应用信息安全风险处理流程，以：

a） 考虑到风险评估结果，选择适当的信息安全风险处理方案；

b） 确定实施所选信息安全风险处理选项所需的所有控制措施；

注1：组织可根据需要设计控制措施，或从任何来源识别控制措施。

c） 将上述6.1.3 b）中确定的控制与附录A中的控制进行比较，并验证没有遗漏任何必要的控制；

注2 附件A包含可能的信息安全控制列表。本文件的用户应参阅附件A，以确保不忽略任何必要的信息安全控制。

注3 附件A中列出的信息安全控制并非详尽无遗，如有必要，可包括其他信息安全控制。

d） 编制适用性声明，其中包含：

- 必要的控制（见6.1.3 b）和c））；
- 纳入的理由；
- 是否实施了必要的控制；和
- 排除任何附件A控制的理由。

e） 制定信息安全风险处理计划；和

f） 获得风险所有者对信息安全风险处理计划的批准以及对剩余信息安全风险的接受。

组织应保留有关信息安全风险处理过程的文件化信息。

注 4：本文件中的信息安全风险评估和处理过程符合 ISO 31000[5]中提供的原则和通用指南。

6.2 信息安全目标及其实现计划

组织应在相关职能和级别制定信息安全目标。

信息安全目标应：

a) 符合信息安全政策；

b) 可测量（如果可行）；

c) 考虑适用的信息安全要求，以及风险评估和风险处理的结果；

d) 监测；

e) 沟通；

f) 视实际情况实施更新；

g) 作为文件信息提供。

组织应保留有关信息安全目标的文件化信息。

在规划如何实现其信息安全目标时，组织应确定：

h) 将要做什么；

i) 需要什么资源；

j) 谁将负责；

k) 何时完成；和

l) 如何评估结果。

6.3 变更计划

当组织确定需要对信息安全管理体系进行变更时，应按计划进行变更。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进信息安全管理体系所需的资源。

7.2 能力

组织应：

a） 确定在其控制下从事影响其信息安全绩效工作的人员的必要能力；

b） 确保这些人员具备适当的教育、培训或经验；

c） 在适用的情况下，采取措施获得必要的能力，并评估所采取措施的有效性；和

d） 保留适当的记录信息作为能力的证据。

注：适用的行动可以包括，例如：为现有员工提供培训、指导或重新分配；或雇用或签约合格人员。

7.3 意识

在组织控制下开展工作的人员应意识到：

a） 信息安全政策；

b） 它们对信息安全管理体系有效的贡献，包括提高信息安全性能的好处；和

c） 不符合信息安全管理体系要求的影响。

7.4 沟通

组织应确定与信息安全管理体系相关的内部和外部沟通的需求，包括：

a） 沟通内容；

b） 何时沟通；

c） 与谁沟通；

d） 如何沟通。

7.5 文件化的信息

7.5.1 一般原则

组织的信息安全管理体系应包括：

a） 本文件要求的文件化信息；和

b） 组织确定为信息安全管理体系有效性所必需的文件化信息。

注：由于以下原因，信息安全管理系统的文件化信息的范围因组织而异：

1） 组织的规模及其活动、过程、产品和服务的类型；

2） 过程及其相互作用的复杂性；和

3） 人的能力。

7.5.2 创建和更新

在创建和更新文件化信息时，组织应确保适当：

a） 标识和描述（如标题、日期、作者或参考号）；

b） 格式（如语言、软件版本、图形）和介质（如纸质、电子）；和

c） 审查和批准适用性和充分性。

7.5.3 文件化信息的控制

应控制信息安全管理体系和本文件要求的文件化信息，以确保：

a） 它是可用的，适合在需要的地方和时间使用；和

b） 它得到了充分的保护（例如，免受保密性损失、不当使用或完整性破坏）。

对于文件化信息的控制，组织应解决以下活动（如适用）：

c） 分发、访问、检索和使用；

d） 存储和保存，包括保存易读性；

e） 变更控制（如版本控制）；和

f） 保留和处置。

组织确定为信息安全管理体系的规划和运行所必需的外部来源的文件化信息，应视情况予以识别和控制。

注：访问可能意味着决定只允许查看记录的信息，或允许和授权查看和变更记录的信息等。

8 操作

8.1 运营规划和控制

组织应通过以下方式计划、实施和控制满足要求所需的过程，并实施第 6 条中确定的措施：

– 制定流程标准；

– 根据标准实施过程控制。

应在必要的范围内提供文件化信息，以确保过程已按计划进行。

组织应控制计划的变更，并审查意外变更的后果，必要时采取措施减轻任何不利影响。

组织应确保外部提供的与信息安全管理体系相关的过程、产品或服务得到控制。

8.2 信息安全风险评估

组织应根据 6.1.2 a）中规定的标准，在计划的时间间隔内或在提议或发生重大变更时进行信息安全风险评估。

组织应保留信息安全风险评估结果的书面信息。

8.3 信息安全风险处理

组织应实施信息安全风险处理计划。

组织应保留信息安全风险处理结果的书面信息。

9 绩效评估

9.1 监测、测量、分析和评价

组织应确定：

a） 需要监控和测量的内容，包括信息安全流程和控制；

b） 监控、测量、分析和评估的方法（如适用），以确保有效的结果。所选择的方法应产生可比且可重复的结果，以视为有效；

c） 何时进行监视和测量；

d） 由谁进行监测和测量；

e） 何时分析和评估监测和测量结果；

f） 谁将分析和评估这些结果。

应提供记录信息作为结果的证据。

组织应评估信息安全绩效和信息安全管理体系的有效性。

9.2 内部审计

9.2.1 一般原则

组织应按计划的时间间隔进行内部审计，以提供信息，说明信息安全管理体系是否：

a） 符合

1） 组织自身对其信息安全管理体系的要求；

2） 本文件的要求；

b） 有效实施和维护。

9.2.2 内部审计计划

组织应规划、建立、实施和维护审计计划，包括频率、方法、责任、规划要求和报告。

在制定内部审核计划时，组织应考虑相关过程的重要性和以往审核的结果。

组织应：

a） 确定每次审计的审计标准和范围；

b） 选择审计师并进行审计，以确保审计过程的客观性和公正性；

c） 确保向相关管理层报告审计结果；

文件化信息应作为审计计划和审计结果实施的证据。

9.3 管理评审

9.3.1 一般原则

最高管理者应按计划的时间间隔审查组织的信息安全管理体系，以确保其持续适用性、充分性和有效性。

9.3.2 管理评审输入

管理评审应考虑：

a） 先前管理评审的行动状态；

b） 与信息安全管理体系相关的外部和内部问题的变化；

c） 与信息安全管理体系相关的相关方需求和期望的变化；

d） 信息安全绩效反馈，包括以下方面的趋势：

1） 不符合项和纠正措施；

2） 监视和测量结果；

3） 审计结果；

4） 实现信息安全目标；

e） 相关方的反馈；

f） 风险评估结果和风险处理计划状态；

g） 持续改进的机会。

9.3.3 管理评审结果

管理评审的结果应包括与持续改进机会相关的决策以及信息安全管理体系变更的任何需求。

文件化信息应作为管理评审结果的证据。

10 改进

10.1 持续改进

组织应持续改进信息安全管理体系的适宜性、充分性和有效性。

10.2 不符合和纠正措施

当发生不符合时，组织应：

a） 对不符合项作出响应，如适用：

1） 采取措施控制和纠正；

2） 处理后果；

b） 评估采取行动消除不符合原因的必要性，以便不符合不再发生或不在其他地方发生，方法是：

1） 评审不符合项；

2） 确定不符合的原因；和

3） 确定是否存在或可能发生类似的不符合；

c） 实施所需的任何行动；

d） 审查采取的任何纠正措施的有效性；和

e） 如有必要，对信息安全管理体系进行变更。

f） 纠正措施应与所遇到的不符合的影响相适应。

g） 文件化信息应作为以下证据：

h） 不符合项的性质以及随后采取的任何措施，

i） 任何纠正措施的结果。

附录 A（规范性附录）信息安全控制参考

表 A.1 中列出的信息安全控制直接源自 ISO/IEC 27002:2022[1]第 5 条至第 8 条中列出的控制，并与之一致，应与 6.1.3 结合使用。

表 A.1-信息安全控制

5	组织控制	
5.1	信息安全政策	**控制** 信息安全政策和特定主题的政策应由管理层定义、批准、发布、传达给相关人员和相关方并由其确认，在计划的时间间隔内以及发生重大变化时进行审查。
5.2	信息安全角色和职责	**控制** 应根据组织需求定义和分配信息安全角色和职责。
5.3	职责分离	**控制** 相互冲突的职责和相互冲突的责任领域应分开。
5.4	管理职责	**控制** 管理层应要求所有人员按照既定的信息安全政策、组织的特定政策和程序应用信息安全。
5.5	与当局的联系	**控制** 组织应与相关部门建立并保持联系。
5.6	与特殊利益群体的联系	**控制** 组织应与特殊利益集团或其他专业安全论坛和专业协会建立并保持联系。
5.7	威胁情报	**控制** 应收集和分析与信息安全威胁有关的信息，以产生威胁情报。
5.8	项目管理中的信息安全	**控制** 信息安全应纳入项目管理。

5.9	信息和其他相关资产清单	**控制** 应编制和维护包括所有者在内的信息和其他相关资产清单。
5.10	信息和其他相关资产的可接受使用	**控制** 应确定、记录并实施可接受的使用规则和处理信息及其他相关资产的程序。
5.11	资产归还	**控制** 员工和其他相关方（视情况而定）应在其雇佣关系、合同或协议变更或终止时归还其拥有的所有组织资产。
5.12	信息分类	**控制** 应根据组织基于保密性、完整性、可用性和相关利益方要求的信息安全需求对信息进行分类。
5.13	信息标签	**控制** 应根据组织采用的信息分类方案制定并实施一套适当的信息标签程序。
5.14	信息传输	**控制** 组织内以及组织与其他方之间的所有类型的传输设施应制定信息传输规则、程序或协议。
5.15	访问控制	**控制** 应根据业务和信息安全要求制定和实施控制信息和其他相关资产的物理和逻辑访问的规则。
5.16	身份管理	**控制** 应在整个生命周期管理身份。
5.17	认证信息	**控制** 认证信息的分配和管理应通过管理流程进行控制，包括建议人员适当处理认证信息。
5.18	访问权限	**控制** 对信息和其他相关资产的访问权应根据组织的特定主题

		制定、审查、修改和删除访问控制政策和规则。
5.19	供应商关系中的信息安全	**控制** 应定义和实施流程和程序，以管理与使用供应商产品或服务相关的信息安全风险。
5.20	解决供应商协议中的信息安全问题	**控制** 应根据供应商关系类型确定相关信息安全要求，并与各供应商达成一致。
5.21	管理信息和通信技术（ICT）供应链中的信息安全	**控制** 应定义和实施流程和程序，以管理与 ICT 产品和服务供应链相关的信息安全风险。
5.22	供应商服务的监控、审查和变更管理	**控制** 组织应定期监测、审查、评估和管理供应商信息安全实践和服务交付的变化。
5.23	云服务使用的信息安全	**控制** 应根据组织的信息安全要求建立获取、使用、管理和退出云服务的流程。
5.24	信息安全事件管理规划和准备	**控制** 组织应通过定义、建立和沟通信息安全事件管理流程、角色和职责，为管理信息安全事件进行规划和准备。
5.25	信息安全事件的评估和决策	**控制** 组织应评估信息安全事件，并决定是否将其归类为信息安全事件。
5.26	应对信息安全事件	**控制** 信息安全事件应按照文件化程序进行响应。
5.27	从信息安全事件中吸取教训	**控制** 从信息安全事件中获得的知识应用于加强和改进信息安全控制。
5.28	收集证据	**控制**

		组织应建立并实施与信息安全事件有关的证据的识别、收集、获取和保存程序。
5.29	中断期间的信息安全	**控制** 组织应计划如何在中断期间将信息安全维持在适当水平。
5.30	ICT 为业务连续性做好准备	**控制** 应根据业务连续性目标和信通技术连续性要求，规划、实施、维护和测试 ICT 准备情况。
5.31	法律、法规、监管和合同要求	**控制** 与信息安全相关的法律、法规、监管和合同要求以及组织满足这些要求的方法应予以识别、记录并保持最新。
5.32	知识产权	**控制** 组织应实施适当的程序来保护知识产权。
5.33	记录保护	**控制** 应防止记录丢失、毁坏、篡改、未经授权的访问和未经授权发布。
5.34	个人身份信息（PII）的隐私和保护	**控制** 组织应根据适用法律法规和合同要求，确定并满足有关隐私保护和个人信息保护的要求。
5.35	信息安全独立审查	**控制** 组织管理信息安全的方法及其实施（包括人员、流程和技术）应按计划间隔或发生重大变化时进行独立审查。
5.36	遵守信息安全政策、规则和标准	**控制** 应定期审查组织信息安全政策、特定于主题的政策、规则和标准的合规性。
5.37	记录操作程序	**控制** 应记录信息处理设施的操作程序，并将其提供给需要的人员。

6	人员控制	
6.1	筛选	**控制** 在加入组织之前，应对所有拟成为人员的候选人进行背景调查，并考虑到适用的法律、法规和道德规范，并与业务要求、待访问信息的分类和感知风险成比例。
6.2	雇佣条款和条件	**控制** 雇佣合同协议应说明人员和组织对信息安全的责任。
6.3	信息安全意识、教育和培训	**控制** 组织和相关利益方的人员应接受适当的信息安全意识、教育和培训，并定期更新组织的信息安全政策、主题策略和程序与他们的工作职能相关。
6.4	纪律程序	**控制** 应对违反信息安全政策的人员和其他相关利益方采取行动，应正式制定并传达纪律程序。
6.5	雇佣终止或变更后的责任	**控制** 终止或变更雇佣关系后仍然有效的信息安全责任和义务应明确、执行并传达给相关人员和其他相关方。
6.6	保密或保密协议	**控制** 人员和其他相关方应确定、记录、定期审查和签署反映组织信息保护需求的保密或保密协议。
6.7	远程工作	**控制** 当人员远程工作时，应采取安全措施，以保护在组织场所外访问、处理或存储的信息。
6.8	信息安全事件报告	**控制** 组织应为人员提供一种机制，以便及时通过适当渠道报告观察到的或怀疑的信息安全事件。
7	物理控制	
7.1	物理安全周界	**控制**

		应定义并使用安全边界来保护包含信息和其他相关资产的区域。
7.2	物理入口	**控制** 安全区域应通过适当的入口控制和接入点进行保护。
7.3	保护办公室、房间和设施	**控制** 应设计并实施办公室、房间和设施的物理安全。
7.4	物理安全监控	**控制** 应持续监控场所是否存在未经授权的物理访问。
7.5	防止物理和环境威胁	**控制** 应设计和实施针对物理和环境威胁的保护措施，如自然灾害和其他有意或无意的基础设施物理威胁。
7.6	在安全区域工作	**控制** 应设计并实施在安全区域工作的安全措施。
7.7	清理桌面和屏幕	**控制** 应明确并适当执行纸张和可移动存储介质的桌面清理规则和信息处理设施的屏幕清理规则。
7.8	设备选址和保护	**控制** 设备应安全放置并加以保护。
7.9	场外资产的安全	**控制** 应保护场外资产。
7.10	存储介质	**控制** 应根据组织的分类方案和处理要求，在其获取、使用、运输和处置的整个生命周期内对存储介质进行管理。
7.11	配套设施	**控制** 应保护信息处理设施免受电力故障和其他因辅助设施故障造成的干扰。
7.12	布线安全	**控制** 应保护承载电力、数据或辅助信息服务的电缆免受拦截、

		干扰或损坏。
7.13	设备维护	**控制** 应正确维护设备，以确保信息的可用性、完整性和保密性。
7.14	设备的安全处置或再利用	**控制** 应验证包含存储介质的设备项目，以确保在处置或重新使用之前，任何敏感数据和许可软件已被删除或安全覆盖。
8	技术控制	
8.1	用户终端设备	**控制** 应保护存储在终端设备上、由终端设备处理或可通过终端设备访问的信息。
8.2	特权访问权限	**控制** 应限制和管理特权访问权限的分配和使用。
8.3	信息访问限制	**控制** 应根据既定的特定主题访问控制政策限制对信息和其他相关资产的访问。
8.4	访问源代码	**控制** 应适当管理对源代码、开发工具和软件库的读写访问。
8.5	安全身份验证	**控制** 应根据信息访问限制和特定主题的访问控制策略实施安全认证技术和程序。
8.6	容量管理	**控制** 应根据当前和预期的能力要求对资源的使用进行监测和调整。
8.7	防范恶意软件	**控制** 应对恶意软件进行保护，并通过适当的用户意识予以支持。

8.8	技术漏洞管理	**控制** 应获得使用中的信息系统的技术漏洞信息，评估组织暴露于此类漏洞的情况，并采取适当措施。
8.9	配置管理	**控制** 应建立、记录、实施、监控和审查硬件、软件、服务和网络的配置，包括安全配置。
8.10	信息删除	**控制** 当不再需要时，应删除存储在信息系统、设备或任何其他存储介质中的信息。
8.11	数据屏蔽	**控制** 应根据组织的访问控制专题政策和其他相关专题政策以及业务要求使用数据屏蔽，并考虑适用立法。
8.12	数据泄露预防	**控制** 数据泄漏预防措施应适用于处理、存储或传输敏感信息的系统、网络和任何其他设备。
8.13	信息备份	**控制** 信息、软件和系统的备份副本应按照商定的特定主题备份政策进行维护和定期测试。
8.14	信息处理设施的冗余	**控制** 信息处理设施的冗余度应足以满足可用性要求。
8.15	日志	**控制** 应制作、存储、保护和分析记录活动、异常、故障和其他相关事件的日志。
8.16	监测活动	**控制** 应监控网络、系统和应用程序的异常行为，并采取适当措施评估潜在的信息安全事件。
8.17	时钟同步	**控制** 组织使用的信息处理系统的时钟应与批准的时间源同

		步。
8.18	特权公用程序的使用	**控制** 应限制并严格控制能够超越系统和应用程序控制的公用程序的使用。
8.19	在操作系统上安装软件	**控制** 应实施程序和措施，以安全管理操作系统上的软件安装。
8.20	网络安全	**控制** 应保护、管理和控制网络和网络设备，以保护系统和应用程序中的信息。
8.21	网络服务的安全	**控制** 应识别、实施和监控网络服务的安全机制、服务级别和服务要求。
8.22	网络隔离	**控制** 信息服务组、用户组和信息系统组应在组织网络中隔离。
8.23	Web 过滤	**控制** 应管理对外部网站的访问，以减少对恶意内容的暴露。
8.24	密码学的使用	**控制** 应定义和实施有效使用密码的规则，包括密码密钥管理。
8.25	安全的开发生命周期	**控制** 应制定并应用软件和系统的安全开发规则。
8.26	应用程序安全要求	**控制** 在开发或获取应用程序时，应确定、规定和批准信息安全要求。
8.27	安全系统架构和工程原理	**控制** 应建立、记录、维护工程安全系统的原则，并将其应用于任何信息系统开发活动。
8.28	安全编码	**控制** 软件开发应采用安全编码原则。

8.29	开发和验收中的安全测试	**控制** 应在开发生命周期中定义和实施安全测试流程。
8.30	外包开发	**控制** 组织应指导、监督和审查与外包系统开发相关的活动。
8.31	开发、测试和生产环境的分离	**控制** 开发、测试和生产环境应分开并加以保护。
8.32	变更管理	**控制** 信息处理设施和信息系统的变更应遵守变更管理程序。
8.33	测试信息	**控制** 应适当选择、保护和管理测试信息。
8.34	在审计测试期间保护信息系统	**控制** 审计测试和其他涉及操作系统评估的保证活动应在测试人员和适当管理层之间进行规划和商定。

参考文献

[1] ISO/IEC 27002:2022，信息安全、网络安全和隐私保护-信息安全控制

[2] ISO/IEC 27003，信息技术-安全技术-信息安全管理系统-指南

[3] ISO/IEC 27004，信息技术-安全技术-信息安全管理-监控、测量、分析和评估

[4] ISO/IEC 27005，信息安全、网络安全和隐私保护——信息安全风险管理指南

[5] ISO 31000:2018，风险管理-指南