国际标准

ISO/IEC
27001

第3版
2022-10

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

ISO/IEC 27001

目 次

前　言

国际标准化组织(ISO)是由各国标准化团体(ISO 成员团体)组成的世界性的联合会。制定国际标准工作通常由 ISO 的技术委员会完成。各成员团体若对某技术委员会确定的项目感兴趣，均有权参加该委员会的工作。与 ISO 保持联系的各国际组织(官方的或非官方的)也可参加有关工作。ISO 与国际电工委员会(IEC)在电工技术标准化方面保持密切合作的关系。

制定本标准及其后续标准维护的程序在 ISO/IEC 指引 第 1 部分均有描述。应特别注意用于各不同类别 ISO 文件批准准则。本标准根据 ISO/IEC 导则第 2 部分的规则起草(见 www.iso.org/directives)。(见 www.iso. org/directives 或 www. iec. ch/members_experts/refdocs) 。

本标准中的某些内容有可能涉及一些专利权问题，对此应引起注意。ISO 不负责识别任何这样的专利权问题。在标准制定期间识别的专利权细节将出现在引言/或收到的 ISO 专利权声明清单中（www.iso.org/patents）。

本标准中使用的任何商品名称仅为方便用户而提供的信息， 不构成代言。

ISO 与合格评定相关的特定术语和表述含义的解释以及 ISO 遵循的世界贸易组织（WTO）贸易技术壁垒（TBT）原则关信息访问以下 URLL：www.iso.org/iso/foreword.html.。在 IEC 中， 请参见 www. iec. ch/understanding-standards

本标准由 ISO/IEC JTC 1 联合技术委员会， 信息技术 SC 27 小组委员会“信息安全、 网络安全和隐私保护”编写。

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

主要变化如下:

——文本已与管理体系标准的统一结构和 ISO/IEC 27002: 2022 保持一致。

关于本标准的任何反馈或问题都应直接向用户的国家标准机构提出。 这些机构的完整名单可以在 www.iso. org/members. html 和 www. iec. ch/national-committees 上找到。

引　言

0.1　总则

本标准用于为建立、 实施、 保持和持续改进信息安全管理体系提供要求。 采用信息安全管理体系是组织的一项战略决策。 组织信息安全管理体系的建立和实施受其需求、目标、 安全要求、所采用的过程以及组织的规模和结构的影响。 所有这些影响因素会不断发生变化。

信息安全管理体系通过应用风险管理过程来保持信息的保密性、 完整性和可用性， 以充分管理风险并给予相关方信心。

信息安全管理体系是组织过程和整体管理结构的一部分并与其整合在一起是非常重要的。 信息安全在设计过程、 信息系统、 控制措施时就要考虑信息安全。 按照组织的需要实施信息安全管理体系，是本标准所期望的。

本标准可被内部和外部各方用于评估组织的能力是否满足自身的信息安全要求。

本标准中要求的顺序并不能反映他们的重要性或意味着他们的实施顺序。 列举的条目仅用于参考目的。

ISO/IEC 27000 描述了信息安全管理体系的概述和词汇， 引用了信息安全管理体系标准族 ISO/IEC 27003 [2] ， ISO/IEC 27004 [3] and ISO/IEC 27005 [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

本标准采用 ISO/IEC 指令第 1 部分 ISO 综合补充附件 SL 中定义的高级结构、相同的子条款标题、相同的文本、 通用术语和核心定义， 因此保持与采用附件 SL 的其他管理体系标准的兼容性。

附件 SL 中定义的这种通用方法对于那些选择使用单一管理体系来满足两种或两种以上管理体系标准要求的组织是有用的。

信息安全、网络安全和隐私保护

——信息安全管理体系——要求

1 范围

本标准规定了在组织环境下建立、实现、保持和持续改进信息安全管理体系的要求。本标准还包括了根据组织需求所剪裁的信息安全风险评估和应对的要求。本标准规定的所有要求是通用的，适用于各种类型、不同规模或性质的组织。

当一个组织声称符合本标准时，不能删减 4 至 10 章所规定的任何要求。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。 凡是注日期的引用文件， 仅注日期的版本适用于本标准。凡是不注日期的引用文件， 其最新版本（包括所有的修改单） 适用于本标准。

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

3 术语和定义

本标准采用 ISO/IEC 27000-2018 中所确立的术语和定义。

ISO和IEC设有用于标准化的术语数据库，地址如下：

——ISO 在线浏览平台：http://www.iso.org/obp

——IEC 电力维基百科：https://www.electropedia.org/

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨相关并影响其实现信息安全管理体系预期结果的能力的各种外部和内部因素。

注：对这些因素的确定，参见 ISO 31000:2018 中 5.4.1 理解组织及其环境的内容。

4.2 理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有关的相关方；

b)与信息安全管理体系有关的相关方的要求。

c)这些要求中，哪些将通过信息安全管理体系来解决。

注：相关方的要求可包括法律、法规要求和合同义务。

4.3 确定信息安全管理体系的范围

组织应确定信息安全管理体系的边界及其适用性，以确定其范围。

在确定范围时，组织应考虑：

a)4.1 中提及的各种外部和内部因素；

b)4.2 中提及的相关方的要求；

c)组织实施的活动之间及其与其他组织实施的活动之间的接口和依赖关系。

范围应作为成文信息可被获取。

4.4 信息安全管理体系

组织应按照本标准的要求，建立、实现、保持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 领导作用

5.1 领导作用和承诺

最高管理者应通过以下活动，证实对信息安全管理体系的领导作用和承诺：

a)确保制定信息安全方针和信息安全目标，并与组织战略方向相一致；

b)确保将信息安全管理体系要求融入组织的过程中；

c)确保信息安全管理体系所需的资源是可获得的；

d)沟通有效的信息安全管理及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实现其预期结果；

f)指导和支持相关人员为信息安全管理体系的有效性做出贡献；

g)促进持续改进；

h)支持其他相关管理者在其职责范围内发挥领导作用。

注：本标准中提及的“业务”一词可广义地理解为涉及组织存在的目的核心活动。

5.2 方针

最高管理者应制定信息安全方针，信息安全方应：

a)与组织宗旨相适应；

b)包括信息安全目标（见6.2）或为设定信息安全目标提供框架；

c)包括对满足适用信息安全要求的承诺；

d)包括对持续改进信息安全管理体系的承诺。

信息安全方针应：

e)形成成文信息并可获取；

f)在组织内得到沟通；

g)适宜时，对相关方所获取。

5.3 组织的岗位、职责和权限

最高管理者应确保与信息安全相关岗位、职责和权限在组织内得到分配和沟通。最高管理者应分配职责和权限，以：

a)确保信息安全管理体系符合本标准的要求；

b)向最高管理者报告信息安全管理体系绩效。

注：最高管理者也可为组织内报告信息安全管理体系绩效，分配职责和权限。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

当策划信息安全管理体系时，组织应考虑4.1中提及的因素和4.2中提及的要求，并确定需要应对的风险和机遇，以：

a)确保信息安全管理体系能够实现其预期结果；

b)预防或减少不良影响；

c)实现持续改进。

组织应策划：

d)应对这些风险和机遇的措施；

e)如何：

1）将这些措施整合到信息安全管理体系过程中，并予以实现；

2）评价这些措施的有效性。

6.1.2 信息安全风险评估

组织应规定并应用信息安全风险评估过程，以：

a)建立并保持信息安全风险准则，包括:

1)风险接受准则；

2)信息安全风险评估实施准则。

b)确保反复的信息安全风险评估产生一致的、有效的和可比较的结果；

c)识别信息安全风险：

1)应用信息安全风险评估过程，以识别信息安全管理体系范围内与信息保密性、完整性和可用性损失有关的风险；

2)确定风险责任人；

d)分析信息安全风险：

1)评估 6.1.2 c) 1)中所识别的风险发生后，可能导致的潜在后果；

2)评估 6.1.2 c) 1)中所识别的风险实际发生的可能性；3)确定风险级别；

e)评价信息安全风险：

1)将风险分析结果与 6.1.2 a)中建立的风险准则进行比较；

2)为风险应对对已分析风险进行优先排序。组织应保留有关信息安全风险评估过程的成文信息。

6.1.3 信息安全风险应对

组织应规定并应用信息安全风险应对过程，以：

a)在考虑风险评估结果的基础上，选择适合的信息安全风险应对方案；

b)确定实现所选择的信息安全风险应对方案所必需的所有控制措施；

注 1：当需要时，组织可设计控制措施，或识别来自任何来源的控制措施。

c)将 6.1.3 b)确定的控制措施与附录 A 中的控制措施进行比较，并验证没有忽略必要的控制措施；

注 2：附录 A 包含了可能的信息安全控制措施的清单。本标准使用者可在附录 A 的指导下，确保没有遗漏必要的控制措施。

注 3：附录 A 所列的信息安全控制措施并不是完备的，可能需要额外的控制。

d)制定一个适用性声明，包含：

— 必要的控制措施（见 6.1.3 b）和 c））；

— 选择该控制措施的合理性说明；

— 无论该必要控制措施是否已实现；以及

— 对附录 A 控制措施删减的合理性说明；

e)制定正式的信息安全风险应对计划；

f)获得风险责任人对信息安全风险应对计划以及对信息安全残余风险的接受的批准。

组织应保留有关信息安全风险应对过程的成文信息。

注 4：本标准中的信息安全风险评估和应对过程与 ISO 31000[5]中给出的原则和通用指南相匹配。

6.2 信息安全目标及其实现的策划

组织应在相关职能和层次上建立信息安全目标。信息安全目标应：

a)与信息安全方针保持一致；

b)可测量（如可行）；

c)考虑适用的信息安全要求，以及风险评估和风险应对的结果；

d)予以监视；

e)予以沟通；

f)适时更新；

g)作为成文信息可获取。

组织应保留有关信息安全目标的成文信息。在策划如何实现信息安全目标时，组织应确定：

h)要做什么；

i)需要什么资源；

j)由谁负责；

k)何时完成；

l)如何评价结果。

6.3 变更的策划

当组织确定需要对信息安全管理体系进行变更时，变更应按所策划的方式实施。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持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)确定在组织控制下从事会影响组织信息安全绩效的工作人员的必要能力；

b)基于适当的教育、培训或经验，确保这些人员是胜任的；

c)适用时，采取措施以获得所需的能力，并评价所采取措施的有效性；

d)保留适当的成文信息，作为人员能力的证据。

注：适当措施可包括对在职人员进行培训、 辅导或重新分配工作， 或者聘用、 外包胜任的人员。

7.3 意识

在组织控制下工作的人员应知晓：

a)信息安全方针；

b)他们对信息安全管理体系有效性的贡献，包括改进信息安全绩效带来的益处；

c)不符合信息安全管理体系要求带来的后果。

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的沟通需求，包括：

a)沟通什么；

b)何时沟通；

c)与谁沟通；

d)如何沟通。

7.5 成文信息

7.5.1 总则

组织的信息安全管理体系应包括：

a)本标准要求的成文信息；

b)组织所确定的、 为确保信息安全管理体系有效性所需的成文信息。

注：对于不同组织， 质量管理体系成文信息的多少与详略程度可以不同， 取决于：

1）组织的规模， 以及活动、 过程、 产品和服务的类型；

2）过程及其相互作用的复杂程度；

3）人员的能力。

7.5.2 创建和更新

在创建和更新成文信息时，组织应确保适当的：

a)标识和说明 例如标题、日期、作者或索引编号）；

b)格式（例如语言、软件版本、图表）和载体（例如纸质的、电子的）；

c)评审和批准， 以保持适宜性和充分性。

7.5.3 成文信息的控制

应控制信息安全管理体系和本标准所要求的成文信息，以确保：

a)在需要的场合和时机， 均可获得并适用；

b)予以妥善保护（如防止泄密、 不当使用或缺失）。

为控制成文信息，适用时，组织应进行以下活动：

c)分发，访问，检索和使用；

d)存储和保护，包括保持可读性；

e)更改控制（例如版本控制）；

f)保留和处理。

对于组织确定的策划和运行信息安全管理体系所必需的来自外部的成文信息，组织应进行适当识别，并予以控制。

注： 对成文信息的“访问”可能意味着仅允许查阅， 或者意味着允许查阅并授权修改。

8 运行

8.1 运行的策划和控制

组织应策划、实施和控制满足要求所需的过程，并通过以下方式实施第 6 章中确定的措施：

——为过程建立准则；

——根据准则实施过程控制。

成文信息应在必要的范围内可用，以确信这些过程已按策划执行。组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻不利影响。

组织应确保与信息安全管理体系相关的、由外部提供的过程、产品或服务受控。

8.2 信息安全风险评估

组织应考虑 6.1.2 a)所建立的准则，按策划时间间隔，或当重大变更提出或发生时，实施信息安全风

险评估。组织应保留信息安全风险评估结果的成文信息。

8.3 信息安全风险应对

组织应实施信息安全风险应对计划。组织应保留信息安全风险应对结果的成文信息。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a)需要监视和测量什么，包括信息安全过程和控制；

b)需要用什么方法进行监视、 测量、 分析和评价， 以确保结果有效。所选的方法应产生可比较和可再现的有效结果；

c)何时实施监视和测量 ；

d)谁应监视和测量；

e)何时对监视和测量的结果进行分析和评价 ；

f)谁应分析和评价这些结果。

应保留适当的成文信息，以作为结果的证据。

组织应评价信息安全的绩效和有效性。

9.2 内部审核

9.2.1 总则

组织应按照策划的时间间隔进行内部审核， 以提供有关信息安全管理体系的下列信息

a)是否符合；

1）组织自身的信息安全管理体系要求 ；

2）本标准的要求。

b)是否得到有效的实施和保持。

9.2.2 内部审核方案

组织应策划、制定、实施和保持（一个或多个）审核方案，审核方案包括审核频次、方法、职责、策划要求和报告。

当制定内部审核方案时，应考虑相关过程的重要性和以往审核的结果。组织应：

a)规定每次审核的审核准则和范围；

b)选择审核员并实施审核，确保审核过程的客观性和公正性；

c)确保将审核结果报告至相关管理者；

保留成文信息，作为实施审核方案以及审核结果的证据。

9.3 管理评审

9.3.1 总则

最高管理者应按照策划的时间间隔对组织的信息安全管理体系进行评审，以确保其持续的适宜性、充分性
和有效性 。

9.3.2 管理评审输入

管理评审应考虑：

a)以往管理评审所采取措施的情况 ；

b)与信息安全管理体系相关的外部和内部因素的变化；

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)有关信息安全绩效的反馈，包括以下方面的趋势：

1）不符合和纠正措施；

2）监视和测量结果；

3）审核结果；

4）信息安全目标的实现程度；

e)相关方反馈；

f)风险评估结果及风险应对计划的状态；

g)持续改进的机会。

9.3.3 管理评审输出

管理评审输出应包括与持续改进机会相关的决定以及变更信息安全管理体系的任何需求。

成文信息应保留并可获取，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 不符合及纠正措施

当发生不符合时，组织应：

a)对不符合做出反应，适用时：

1）采取措施以控制和纠正不符合 ；

2）处置后果；

b)通过下列活动， 评价是否需要采取措施， 以消除产生不合格的原因， 避免其再次发生或者在其他场合发生：

1）评审不符合；

2）确定不符合的原因；

3）确定是否存在或可能发生类似的不符合；

c)实施所需的措施；

d)评审所采取的纠正措施的有效性；

e)需要时 变更质量管理体系；

纠正措施应与不符合所产生的影响相适应。

应保留成文信息，作为下列事项的证据：

f)不符合的性质以及随后所采取的措施；

g)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 中所列的信息安全控制措施直接源自 ISO/IEC 27002:2022 第 5 至 8 章，并与之保持一致，并应在 6.1.3 语境中被使用。表 A.1 信息安全控制

5 组织控制		
5.1	信息安全策略	控制措施 应定义信息安全方针（即最高级策略）和特定主题策略，由管理层批准，发布，传达给相关人员和相关方并得到他们的认可，并在计划的时间间隔和发生重大变化时进行评审。
5.2	信息安全角色和职责	控制措施 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	控制措施 相互冲突的职责和相互冲突的责任领域应该被分离。
5.4	管理层责任	控制措施 管理层应要求所有人员根据组织的既定信息安全策略、特定主题策略和程序来应用信息安全。
5.5	与职能机构的联系	控制措施 组织应当与相关职能机构建立并保持联系。
5.6	与特定相关方的联系	控制 组织应与特定相关方或其他专业安全论坛、专业协会建立并保持联系。
5.7	威胁情报	控制措施 应收集并分析与信息安全威胁相关的信息，以产生威胁情报。
5.8	项目管理中的信息安全	控制措施 项目管理中应纳入信息安全。
5.9	信息和其他相关资产的清单	控制 应开发和维护信息和其他相关资产（包括所有者）的清单。
5.10	信息和其他相关资产的可接	控制措施

	受的使用	应确定、记录和实施处理信息和其他相关资产的可接受的使用规则和程序。
5.11	资产归还	控制措施 员工和其他相关方在变更或终止其雇佣关系、合同或协议时，应归还其拥有的所有组织资产。
5.12	信息分类	控制措施 应根据组织的信息安全需求，基于机密性、完整性、可用性和相关方的要求，对信息进行分类。
5.13	信息标签	控制措施 应当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	信息传递	控制措施 组织内部以及组织与其他方之间所有类型的信息传递设施都应当有信息传递的规则、程序或协议。
5.15	访问控制	控制措施 应根据业务和信息安全要求建立和实施控制规则，控制对信息和其他相关资产的物理和逻辑访问。
5.16	身份管理	控制措施 应该管理身份的整个生命周期。
5.17	鉴别信息	控制措施 身份鉴别信息的分配和管理应由管理流程控制，包括就身份鉴别信息的适当处理向员工提供建议。
5.18	访问权限	控制措施 应根据组织关于访问控制的特定主题策略和规则来提供、评审、修改和删除对信息和其他相关资产的访问权限。
5.19	供方关系中的信息安全	控制措施 应定义和实施流程和程序，以管理与使用供方产品或服务相关的信

		息安全风险。
5.20	在供应商协议中强调信息安全	控制措施 应建立相关的信息安全要求，并根据供方关系的类型与每个供方达成一致。
5.21	管理 ICT 供应链中的信息安全	控制措施 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	供方服务的监视、评审和变更管理	控制措施 组织应当定期监视、评审、评估和管理供方信息安全实践和服务提供方面的变化。
5.23	使用云服务的信息安全	控制措施 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	信息安全事件管理的策划与准备	控制措施 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，以策划和准备好管理信息安全事件。
5.25	信息安全事态的评估和决策	控制措施 组织应评估信息安全事态，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 应根据记录的程序应对信息安全事件。
5.27	从信息安全事件中吸取教训	控制措施 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	控制措施 组织应建立并实施识别、收集、获取和保存信息安全事态相关证据的程序。
5.29	中断期间的信息安全	控制措施 组织应策划如何在中断期间将信息安全保持在适当的级别。

5.30	ICT 为业务连续性做好准备	控制措施 应根据业务连续性目标和 ICT 连续性要求，策划、实施、保持和测试 ICT 准备情况。
5.31	法律、法规、监管和合同要求	控制措施 应当识别、记录和更新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。
5.32	知识产权	控制措施 组织应当实施适当的程序来保护知识产权。
5.33	记录保护	控制措施 应防止记录丢失、毁坏、伪造、未经授权的访问和未经授权的发布。
5.34	PII 隐私和保护	控制措施 组织应根据适用的法律法规和合同要求，确定并满足有关 PII 隐私和保护的要求。
5.35	信息安全独立评审	控制措施 组织管理信息安全的方法及其实施（包括人员、流程和技术）应在计划的时间间隔或发生重大变化时进行独立评审。
5.36	信息安全策略、规则和标准的遵从性	控制措施 应定期评审是否符合组织的信息安全策略、特定主题策略、规则和标准。
5.37	文件化的操作程序	控制措施 信息处理设施的操作程序应记录在案并可供需要的人使用。
6 人员控制		
6.1	评审	控制措施 应在加入本组织之前对所有候选人进行背景核查，并持续考虑适用的法律、法规和道德规范，与业务要求、需要访问的信息的分类和感知的风险相称。
6.2	雇佣条款和条件	控制措施

		雇佣合同协议应规定员工和组织的信息安全责任。
6.3	信息安全意识、教育和培训	控制措施 组织的人员和相关方，应按其工作职能，接受关于组织的信息安全策略、特定主题策略和程序的适当的、定期更新的信息安全意识、教育和培训。
6.4	纪律程序	控制措施 纪律程序应正式发布和沟通，以便对违反信息安全策略的人员和其他相关方采取措施。
6.5	雇佣关系终止或变更后的责任	控制措施 应定义、执行在雇佣关系终止或变更后仍然有效的信息安全责任和义务，并传达给相关人员和其他相关方。
6.6	保密或不披露协议	控制措施 反映组织信息保护需求的保密或不披露协议应当由员工和其他相关方识别、形成文件、定期评审和签署。
6.7	远程工作	控制措施 当员工远程工作时，应实施安全措施来保护在组织场所之外访问、处理或存储的信息。
6.8	报告信息安全事态	控制措施 组织应提供一种机制，让员工通过适当的渠道及时报告观察到的或怀疑的信息安全事态。
7 物理控制		
7.1	物理安全周界	控制措施 应该定义安全边界，并用于保护包含信息和其他相关资产的区域。
7.2	物理入口	控制措施 安全区域应通过适当的入口控制和访问点进行保护。
7.3	保护办公室、房间和设施	控制措施 应设计和实施办公室、房间和设施的物理安全。

7.4	物理安全监视	控制措施 应对场所进行持续监视，防止未经授权的物理访问。
7.5	抵御物理和环境威胁	控制措施 应设计和实施针对物理和环境威胁的保护措施，如自然灾害和对基础设施的其他有意或无意的物理威胁。
7.6	在安全区域工作	控制措施 应设计并实施在安全区域工作的安全措施。
7.7	桌面清理和屏幕清理	控制措施 应定义并适当强制针对纸张和可移动存储介质的桌面清理规则，以及信息处理设施的屏幕清理规则。
7.8	设备安置和保护	控制措施 设备应安全放置并受到保护。
7.9	场外资产的安全	控制措施 应保护场外资产。
7.10	存储介质	控制措施 应根据组织的分类方案和处理要求，在采购、使用、运输和作废的整个生命周期中对存储介质进行管理。
7.11	支持性设施	控制 应对信息处理设施进行保护，使其免受电力故障和其他由支持设施故障造成的中断的影响。
7.12	布线安全	控制措施 承载电力、数据或支持信息服务的电缆应受到保护，以免被截取、干扰或损坏。
7.13	设备维护	控制措施 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	设备的安全作废或再利用	控制措施 应验证包含存储介质的设备，以确保任何敏感数据和许可软件在作

		废或再利用之前已被删除或安全覆盖。
8 技术控制		
8.1	用户终端设备	控制措施 存储在用户终端设备上、由用户终端设备处理或可通过用户终端设备访问的信息应受到保护。
8.2	特殊访问权	控制措施 应该限制和管理特殊访问权的分配和使用。
8.3	信息访问约束	控制措施 对信息和其他相关资产的访问应根据既定的关于访问控制的特定主题策略进行约束。
8.4	获取源代码	控制措施 应对源代码、开发工具和软件库的读写权限进行适当管理。
8.5	安全身份认证	控制 应根据信息访问约束和访问控制的特定主题策略来实施安全的身份认证技术和程序。
8.6	容量管理	控制措施 应根据当前和预期的容量要求监视和调整资源的使用。
8.7	防范恶意软件	控制措施 应实施针对恶意软件的防护，并籍由适当的用户意识来支持。
8.8	技术漏洞的管理	控制措施 应当获取有关正在使用的信息系统的技术漏洞的信息，应当评估组织暴露于此类漏洞的风险，并采取适当的措施。
8.9	配置管理	控制措施 应建立、记录、实施、监视和评审硬件、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	数据遮盖	控制措施 应根据组织访问控制和其他相关的特定主题策略、业务需求和适用的法律，实施数据遮盖。
8.12	防止数据泄漏	控制措施 防止数据泄露的措施应适用于处理、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	控制措施 应根据已获批准的备份相关特定主题策略，维护和定期测试信息、软件和系统的备份副本。
8.14	信息处理设备的冗余	控制措施 信息处理设施的实施应具有足够的冗余，以满足可用性要求。
8.15	日志	控制措施 应生成、存储、保护和分析记录活动、异常、故障和其他相关事态的日志。
8.16	活动监视	控制措施 应监视网络、系统和应用程序的异常行为，并采取适当的措施来评估潜在的信息安全事件。
8.17	时钟同步	控制措施 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	特权实用程序的使用	控制措施 应该限制和严格控制能够凌驾系统和应用程序控制的实用程序的使用。
8.19	在操作系统上安装软件	控制措施 对于在操作系统上安装软件，应实施程序和措施来安全地管理。
8.20	网络安全	控制措施 应对网络和网络设备进行保护、管理和控制，以保护系统和应用程

		序中的信息。
8.21	网络服务的安全性	控制措施 应指明、实施和监视网络服务的安全机制、服务级别和服务要求。
8.22	网络隔离	控制措施 信息服务、用户和信息系统应该在组织的网络中按分组进行隔离。
8.23	web 过滤	控制措施 应管理对外部网站的访问，以减少被恶意内容影响的机会。
8.24	密码学的使用	控制措施 应定义和实施有效使用加密技术的规则，包括加密密钥管理。
8.25	安全开发生命周期	控制措施 应该建立和施行软件和系统安全开发的规则。
8.26	应用程序安全要求	控制措施 在开发或采购应用程序时，应识别、详述和审批信息安全要求。
8.27	安全系统架构和工程原理	控制措施 应建立、记录、保持安全系统工程的原则，并将其应用于任何信息系统开发活动。
8.28	安全编码	控制措施 软件开发中应该应用安全编码原则。
8.29	开发和验收中的安全性测试	控制措施 应该在开发生命周期中定义和实现安全测试过程。
8.30	外包开发	控制措施 组织应指导、监视和评审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	控制措施 开发、测试和生产环境应该分离并分别保护。
8.32	变更管理	控制措施 信息处理设施和信息系统的变更应遵循变更管理程序。
8.33	测试信息	控制措施

		应适当选择、保护和管理测试信息。
8.34	审计测试期间信息系统的保护	控制措施 涉及操作系统评估的审计测试和其他保证活动应在测试人员和适当的管理人员之间进行策划和协商。

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——信息安全管理体——指南

[3] ISO/IEC 27004 信息技术.安全技术.信息安全管理——监视、测量、分析和评价

[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