中华人民共和国国家标准
ISO/IEC 27001:2022

信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求

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

目 录

前 言

ISO（国际标准化组织）是由各国标准化团体（ISO成员团体）组成的世界性联合会。制定国际标准的工作通常由ISO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保持联系的各国际官方或非官方组织也可以参加。ISO与国际电工委员会（IEC）密切地合作研究所有电工技术标准化事务。

本文件的编制及其后期维护程序见ISO/IEC导则第1 部分。尤其应注意，不同类型的ISO文件需要不同的审批标准。本文件按照ISO/IEC 导则第2 部分（见www.iso.org/directives 或 www.iec.ch/members_ experts/refdocs ）的编辑规则起草而成。

注意本文件的某些内容可能有专利限制。ISO不负责识别任何此类专利信息。关于本文件编制阶段已识别的专利信息，详情见本文引言与/或ISO已收到的专利声明清单（见www.iso.org/patents ）。

凡本文件中所使用的商标名称，仅为便于使用者使用，不构成对相关产品的认可。

关于与合格评价相关的ISO特殊术语和表述之解释，以及关于ISO遵守WTO 技术性贸易壁垒（TBT）的信息，见www.iso.org/iso/foreword.html 。 在IEC中，见www.iec.ch/understanding-standards.

本文件由联合技术委员会ISO/IEC JTC 1 信息技术, 分委员会SC27信息安全，网络安全和隐私保护编制。第三版取消并代替了第二版(ISO/IEC 27001:2013)，第二版已经过修订以与ISO/IEC 27002:2022保持一致。它还包含了ISO/IEC 27001:2013/COR 1:2014、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协调结构保持一致。

如对本文件有任何反馈和问题，请联系使用组织所在国家的标准化部门。您可以在 www.iso.org/mbmbers.html 和 www.iec.ch/nationalcommittees找到这些组织的完整清单。

0 引 言

0.1 总则

本文件提供建立、实现、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组织 的一项战略性决策。组织信息安全管理体系的建立和实现受组织的需要和目标、安全要求、组织所采用 的过程、规模和结构的影响。所有这些影响因素可能随时间发生变化。

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，并为相关方树立 风险得到充分管理的信心。

重要的是，信息安全管理体系是组织的过程和整体管理结构的一部分并集成在其中，并且在过程、 信息系统和控制的设计中要考虑到信息安全。期望的是，信息安全管理体系的实现程度要与组织的需 要相符合。

本文件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。

本文件中所表述要求的顺序不反映各要求的重要性或暗示这些要求要予实现的顺序。条款编号仅为方便引用。

ISO/IEC 27000 描述了信息安全管理体系的概要和词汇，引用了信息安全管理体系标准族（包括 ISO/IEC 27003[2]、ISO/IEC 27004\ISO/IEC 27005,以及相关术语和定义。

0.2 与其他管理体系标准的兼容性

本文件应用 ISO/IEC 合并导则附录 SL 中定义的高层结构、相同条款标题、相同文本、通用术语和 核心定义，因此维护了与其他采用附录 SL 的管理体系的标准具有兼容性。

附录 SL 中定义的通用途径对于选择运行单一管理体系来满足两个或更多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

本文件规定了在组织环境下建立、实现、维护和持续改进信息安全管理体系的要求。本文件还包括 了根据组织需求所剪裁的信息安全风险评估和处置的要求。

本文件规定的要求是通用的，适用于各种类型、规模或性质的组织。当组织声称符合本文件时，不 能排除第 4 章到第 10 章中所规定的任何要求。

2 规范性引用文件

下列文件的全部或部分内容以构成本文件要求的方式在本文件中进行了规范引用。凡是注日期的引用文件,仅注日期的版本适用于本文 件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ISO/IEC 27000 信息技术 安全技术 信息安全管理体系 概述和词汇（Information technology 一 Security techniques 一 Information security management systems 一 Overview and vocabulary）

3 术语和定义

ISO/IEC 27000 界定的术语和定义适用于本文件。

ISO 和 IEC 在下列地址保存了用于标准化的术语数据库:

——ISO 在线浏览平台:https://www.iso.org/obp

——IEC 百科:可在 https://www.electropedia.org/

4 组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的，且影响其实现信息安全管理体系预期结果能力的外部和内部事

注：对这些事项的确定，参见 ISO 31000:2009 [5]， 5.3 中建立外部和内部环境的内容。

4.2 理解相关方的需求和期望

组织应确定：

a） 信息安全管理体系相关方；

b） 这些相关方的有关要求。

c）信息安全管理体系中的哪些要求将得到处理。

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范围

组织应确定信息安全管理体系的边界及其适用性，以建立其范围。

在确定范围时，组织应考虑：

a） 4.1 中提到的外部和内部事项；

b） 4.2 中提到的要求；

c） 组织实施的活动之间的及其与其他组织实施的活动之间的接口和依赖关系。

该范围应形成文件化信息并可用。

4.4 信息安全管理体系

组织应按照本文件的要求，建立、实现、维护和持续改进信息安全管理体系，包括所需过程及其交互。

5 领导

5.1 领导和承诺

最高管理层应通过以下活动，证实对信息安全管理体系的领导和承诺：

a） 确保建立了信息安全策略和信息安全目标，并与组织战略方向一致；

b） 确保将信息安全管理体系要求整合到组织过程中；

c） 确保信息安全管理体系所需资源可用；

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达到预期结果；

f） 指导并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） 支持其他相关管理角色，以证实他们的领导按角色应用于其责任范围。

注：在本文件中提到的“业务”可广义的解释为对组织存在的目的发挥核心作用的活动。

5.2 方针

最高管理层应建立信息安全方针，该方针应：

a） 与组织意图相适宜；

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） 包括对满足适用的信息安全相关要求的承诺；

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） 形成文件化信息并可用；

f） 在组织内得到沟通；

g） 适当时，对相关方可用。

5.3 组织的角色，责任和权限

最高管理层应确保与信息安全相关角色的责任和权限得到分配和沟通。

最高管理层应分配责任和权限，以：

a） 确保信息安全管理体系符合本文件的要求；

b） 向最高管理者报告信息安全管理体系绩效。

注：最高管理层也可为组织内报告信息安全管理体系绩效，分配责任和权限。

6 规划

6.1 应对风险和机会的措施

6.1.1 总则

当规划信息安全管理体系时，组织应考虑 4.1 中提到的事项和 4.2 中提到的要求，并确定需要应对 的风险和机会，以：

a）确保信息安全管理体系可达到预期结果；

b） 预防或减少不良影响；

c） 达到持续改进。

组织应规划：

d） 应对这些风险和机会的措施；

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

组织应定义并应用信息安全风险评估过程，以：

a） 建立并维护信息安全风险准则，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） 识别风险责任人。

d） 分析信息安全风险：

1） 评估 6.1.2c） 1）中所识别的风险发生后，可能导致的潜在后果；

2） 评估 6.1.2c） 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 6.1.2a）中建立的风险准则进行比较；

2） 为风险处置排序已分析风险的优先级。

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 信息安全风险处置

组织应定义并应用信息安全风险处置过程，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处置选项；

b） 确定实现已选的信息安全风险处置选项所必需的所有控制；

注 1：当需要时，组织可设计控制，或识别来自任何来源的控制。

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

注 2：附录 A 包含了可能的信息安全控制的综合列表。本文件用户可在附录 A 的指导下，确保没有遗漏必要的信息安全控制。

注 3：附录 A 所列的控制并不是完备的，可能需要额外的信息安全控制。

d） 制定一个适用性声明，包含：

——必要的控制［见 6.1.3 b）和 c）］；

——选择的合理性说明；

——无论必要的控制是否已实施；

——对附录 A 中控制的删减的合理性说明；

e） 制定正式的信息安全风险处置计划；

f） 获得风险责任人对信息安全风险处置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处置过程的文件化信息。

注 4：本文件中的信息安全风险评估和处置过程与 ISO 31000 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规划

组织应在相关职能和层级上建立信息安全目标。

信息安全目标应：

a） 与信息安全方针一致；

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处置的结果；

d） 得到监视

e） 得到沟通；

f） 适当时更新。

g） 作为文件化的信息可获取。

组织应保留有关信息安全目标的文件化信息

在规划如何达到信息安全目标时，组织应确定：

h） 要做什么；

i） 需要什么资源；

j） 由谁负责；

k） 什么时候完成；

l） 如何评价结果。

6.3 变更的规划

当组织确定需要变更信息安全管理体系时，变更应有计划的进行。

7 支持

7.1 资源

组织应确定并提供建立、实现、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） 确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c） 适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；

d） 保留适当的文件化信息作为能力的证据。

注：适用的措施可包括，例如针对现有雇员提供培训、指导或重新分配；雇佣或签约有能力的人员。

7.3 意识

在组织控制下工作的人员应了解：

a） 信息安全方针；

b） 其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的沟通需求，包括：

a） 沟通什么；

b） 何时沟通；

c） 与谁沟通；

d） 谁来沟通；

e） 影响沟通的过程。

7.5 文件化信息

7.5.1 总则

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；

b） 为信息安全管理体系的有效性，组织所确定的必要的文件化信息。

注：不同组织有关信息安全管理体系文件化信息的详略程度可以是不同的，这是由于：

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；

3） 人员的能力。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的：

a） 标识和描述（例如标题、日期、作者或引用编号）；

b） 格式（例如语言、软件版本、图表）和介质（例如纸质的、电子的）；

c） 对适宜性和充分性的评审和批准。

7.5.3 文件化信息的控制

信息安全管理体系及本文件所要求的文件化信息应得到控制，以确保：

a） 在需要的地点和时间，是可用的和适宜使用的；

b） 得到充分的保护（如避免保密性损失、不恰当使用、完整性损失等）。

为控制文件化信息，适用时，组织应强调以下活动：

c） 分发、访问、检索和使用；

d） 存储和保护，包括保持可读性；

e） 控制变更（例如版本控制）；

f） 保留和处理。

组织确定的为规划和运行信息安全管理体系所必需的外来的文件化信息，应得到适当的识别，并予 以控制。

注：访问可能隐含着仅允许浏览文件化信息，或允许和授权浏览及更改文件化信息等决定。

8 运行

8.1 运行规划和控制

组织以应规划、实施和控制为了满足要求所需的过程，并通过：

——为过程建立准则；

——根据准则对过程实施控制

实施 6 中的措施。

组织应保持文件化信息达到必要的程度，以确信这些过程按计划得到执行。

组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

组织应确保外部提供的与 信息安全管理体系相关的过程、产品或服务是受控的。

8.2 信息安全风险评估

组织应考虑 6.1.2a）所建立的准则，按计划的时间间隔，或当重大变更提出或发生时，执行信息安全 风险评估。组织应保留信息安全风险评估结果的文件化信息。

8.3 信息安全风险处置

组织应实现信息安全风险处置计划。

组织应保留信息安全风险处置结果的文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a） 需要被监视和测量的内容，包括信息安全过程和控制；

b） 适用的监视、测量、分析和评价的方法，以确保得到有效的结果；所选的方法宜产生可比较和可再现的有效结果。

c） 何时应执行监视和测量；

d） 谁应监视和测量；

e） 何时应分析和评价监视和测量的结果；

f） 谁应分析和评价这些结果。

组织应保留适当的文件化信息作为监视和测量结果的证据。

组织应评价信息安全绩效以及信息安全管理体系的有效性。

9.2 内部审核

9.2.1 总则

组织应按计划的时间间隔进行内部审核，以提供信息，确定信息安全管理体系：

a） 是否符合：

1） 组织自身对信息安全管理体系的要求；

2） 本文件的要求。

b） 是否得到有效实现和维护。

9.2.2 内部审核方案

组织应：规划、建立、实现和维护审核方案（一个或多个），包括审核频次、方法、责任、规划要求和报告。

在建立内部审核方案时，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） 定义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层。

保留文件化信息作为审核方案实施和审核结果的证据。

9.3 管理评审

9.3.1 总则

最高管理层应按计划的时间间隔评审组织的信息安全管理体系，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） 以往管理评审提出的措施的状态；

b） 与信息安全管理体系相关的外部和内部事项的变化；

c） 与信息安全管理体系有关的相关方的需求和期望的变化；

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） 信息安全目标完成情况；

e） 相关方反馈；

f） 风险评估结果及风险处置计划的状态；

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定以及变更信息安全管理体系的任何需求。 组

织应保留文件化信息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，以控制并予以纠正；
   2） 处理后果；

b） 通过以下活动，评价采取消除不符合原因的措施的需求，以防止不符合再发生，或在其他地方 发生：
   1） 评审不符合；
   2） 确定不符合的原因；
   3） 确定类似的不符合是否存在，或可能发生；

c） 实现任何需要的措施；

d） 评审任何所采取的纠正措施的有效性；

e） 必要时，对信息安全管理体系进行变更。

纠正措施应与所遇到的不符合的影响相适合。

组织应保留文件化信息作为以下方面的证据：

f） 不符合的性质及所采取的任何后续措施；

g） 任何纠正措施的结果。

附录 A
(规范性附录)

Information security controls reference

参考信息安全控制

表 A.1 所列的信息安全控制是直接源自并与 ISO/IEC 27002:2022 第 5 章~第 18 章相对应，并在 6.1.3 环境中被使用。

表 A.1 — 信息安全控制

A.5	**组织控制**	
A.5.1	Policies for information security 信息安全策略	**Control** Information security policy and topic-specific policies shall be de- fined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. 控制 信息安全策略和有特定主题的策略应被定义，由管理者批准并发布、传达给所有相关人员和利益相关方。
A.5.2	Information security roles and Responsibilities 信息安全的角色和责任	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs. 控制 所有的信息安全角色和责任应按照组织需要予以定义和分配。
A.5.3	Segregation of duties 职责分离	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated. 控制 应分离冲突的职责及其责任范围
A.5.4	Management responsibilities 管理责任	**Control** Management shall require all personnel to apply information security in accordance with the established information security policy, top- ic-specific policies and procedures of the organization. 控制 管理层应要求所有人员按照组织已建立的信息安全策略、有特定主体的策略和规程应用信息安全。
A.5.5	Contact with authorities 与职能机构的联系	**Control** The organization shall establish and maintain contact with relevant authorities. *控制* 应建立并维护与相关职能机构的~~适当~~联系。
A.5.6	Contact with special interest groups 与特定相关方的联系	**Control** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations. 控制 组织应建立并维护与特定相关方、其他专业安全论坛和专业协会的~~适当~~联系。
A.5.7	Threat intelligence 威胁情报	**Control** Information relating to information security threats shall be collected and analysed to produce threat intelligence.

		控制 应收集与信息安全相关的信息并加以分析，形成威胁情报。
A.5.8	Information security in project management 项目管理中的信息安全	**Control** Information security shall be integrated into project management. 控制 应将信息安全融入项目管理中。
A.5.9	Inventory of information and other associated assets 信息和其他相关资产清单	**Control** An inventory of information and other associated assets, including owners, shall be developed and maintained. 控制 应建立并保持信息和其他相关资产的清单，包括所有者。
A.5.10	Acceptable use of information and other associated assets 信息和其他相关资产的可接受使用	**Control** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented 控制 应识别可接受的信息和其他相关资产的使用规则和处理程序，形成文件并加以实现。
A.5.11	Return of assets 资产归还	**Control** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement. *控制* 适宜时，人员和其他相关方在任用、合同或协议变更或终止时，应归还其占用的所有组织资产。
A.5.12	信息的分类	**Control** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements. 控制 信息应按照组织的信息安全需要，基于保密性、完整性、可获取性及相关方的要求进行分类。
A.5.13	Labelling of information 信息的标记	**Control** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. 控制 应按照组织采用的信息分类方案，制定并实现一组适当的信息标记 规程。
A.5.14	Information transfer信息传输	**Control** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties. 控制 应为组织及组织与外部各方之间所有类型的传输设施建立信息传输规则、规程或传输协议。
A.5.15	Access control 访问控制	**Control** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on busi- ness and information security requirements. 控制 应根据业务和信息安全要求，建立和实施对信息和其他相关资产的物理

		和逻辑访问控制规则。
A.5.16	Identity management 身份管理	**Control** The full life cycle of identities shall be managed. 控制 应对身份的全生命周期进行管理。
A.5.17	Authentication information 鉴别信息	**Control** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. 控制 应建立管理过程，对鉴别信息的分配和管理进行控制，包括就鉴别信息的适当处理向人员提供建议。
A.5.18	Access rights 访问权限	**Control** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control. 控制 应按照组织的特性主题策略和访问控制规则，对信息和其他相关资产的访问权限加以规定、审查、修改及撤销。
A.5.19	Information security in supplier Relationships 供应商关系中的信息安全	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. 控制 应识别并实施过程和程序，管理使用供应商产品和服务相关信息安全风险。
A.5.20	Addressing information security within supplier agreements 解决供应商协议中的信息安全问题	**Control** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. 控制 应基于供应商关系类型，建立相关信息安全要求，并与每个供应商达成一致。
A.5.21	Managing information security in the information and communication technology (ICT) supply chain 在信息与通信技术链ICT供应中管理信息安全	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. 控制 应定义和实施过程和程序，以管理与ICT产品和服务供应链相关的信息安全风险。
A.5.22	Monitoring, review and change management of supplier services 供应商服务的监视、评审和变更	**Control** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. 控制 组织应定期监视、审查、评价和管理供应商信息安全实践和服务交付中的变化。
A.5.23	Information security for use of cloud services 云服务使用信息安全	**Control** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.

		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过程。
A.5.24	Information security incident management planning and preparation 信息安全事件管理的规划和准备	**Control** The organization shall plan and prepare for managing information secu- rity incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. 控制 组织应通过定义、建立和沟通信息安全事件管理过程、角色和职责，为管理信息安全事件进行规划和准备。
A.5.25	Assessment and decision on information security events 信息安全事态评估和决策	**Control** The organization shall assess information security events and decide if they are to be categorized as information security incidents. 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。
A.5.26	Response to information security Incidents 信息安全事件的响应	**Control** Information security incidents shall be responded to in accordance with the documented procedures. 控制 应按照文件化的规程响应信息安全事件。
A.5.27	Learning from information security incidents 从信息安全事件中学习	**Control** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. 控制 应利用在信息安全事件中得到的知识来加强和改进信息安全控制。
A.5.28	Collection of evidence 证据的收集	Control The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events. 控制 组织应建立和实施规程来识别、收集、获取和保存与信息安全事态相关的证据。
A.5.29	Information security during disruption 中断中的信息安全	**Control** The organization shall plan how to maintain information security at an appropriate level during disruption. 控制 组织应策划在中断期间如何保持信息安全维持再一个适当的水平。
A.5.30	ICT readiness for business continuity 业务连续性的ITC准备	**Control** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. 应基于控制业务连续性目标和ITC连续性要求，规划、实施、维护和测试ITC准备。
A.5.31	Legal, statutory, regulatory and contractual requirements 法律、法规、规章和合同要求	**Control** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date. 控制 与信息安全相关的法律、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，应加以识别、 形成文件并保持更新。
A.5.32	Intellectual property rights 知识产权	**Control** The organization shall implement appropriate procedures to protect intellectual property rights. 控制 组织应实施适宜的程序来保护知识产权。
A.5.33	Protection of records 记录的保护	**Control** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release. 控制 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。
A.5.34	Privacyandprotectionofpersonal identifiable information (PII) 隐私和个人可识别信息保护	**Control** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. 控制 组织应依照适用的法律、法规和合同要求，识别并满足针对隐私保护和PII保护的要求
A.5.35	Independent review of information security 信息安全独立评审	**Control** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur. 控制 应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，包括人员、过程和技术，进 行评审。
A.5.36	Compliance with policies, rules and standards for information security 符合信息安全策略、准则和标准	**Control** Compliance with the organization's information security policy, top- ic-specific policies, rules and standards shall be regularly reviewed. 控制 应定期对符合组织的信息安全策略、有主题的特定策略、准侧和标准的情况进行评审。
A.5.37	Documented operating procedures 文件化的操作规程	**Control** Operating procedures for information processing facilities shall be documented and made available to personnel who need them. 控制 信息处理设施的操作规程应形成文件，并能够被有需要的人员获取。

6	**People controls 人员控制**	
A.6.1	Screening审查 （A.7.1.1）	**Control** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. 控制 应在加入组织之前，并在持续的基础上，考虑到适用的法律、法规和道德，对所有成为人员的候选人进行背景核查，并与业务要求、访问信息的分类和可感知的风险成比例。
A.6.2	Terms and conditions of em-Ployment 任用条款及条件 （A.7.1.2）	**Control** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security. 控制 聘用合同协议应规定人员和组织在信息安全方面的责任。
A.6.3	Information security awareness, education and training 信息安全意识、教育和培训 （A.7.2.2）	**Control** Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function. 控制 组织的人员和有关相关方应受到与其工作职能相关的适当的信息安全意识教育、培训和组织信息安全方针策略及规程的定期更新培训。
A.6.4	Disciplinary process 违规处理过程 （A.7.2.3）	**Control** A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation. 控制 应有正式的、且已被传达的违规处理过程以对信息安全违规的人员和其他有关的相关方采取措施。
A.6.5	Responsibilities after termination or change of employment 任用终止或变更的责任 （A.7.3.1）	**Control** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties. 控制 应确定任用终止或变更后仍有效的信息安全责任及其职责，传达至人员和其他有关的相关方并执行。
A.6.6	Confidentiality or non-disclosure Agreements 保密或不泄露协议 （A.13.2.4）	**Control** Confidentiality or non-disclosure agreements reflecting the organ- ization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. 控制 反映组织保密信息的保密协协议或不泄露协议应当被定义、文档化并定期评审，并且与个人或利益相关方进行签署
A.6.7	Remote working 远程工作 （A.6.2.2）	**Control** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.

		控制 当人员远程工作时，应采取安全措施，保护在组织场所外访问的、处理的或储存的信息。
A.6.8	Information security event reporting 信息安全事态报告 （A.16.1.2）	**Control** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. 控制 组织应为人员提供一种机制，来通过恰当的渠道及时报告观察到的或怀疑的信息安全事态。
7	**Physical controls 物理控制**	
A.7.1	Physical security perimeters 物理安全边界 （A.11.1.1）	**Control** Security perimeters shall be defined and used to protect areas that contain information and other associated assets. 控制 应定义和使用安全边界来保护包含信息和其他相关资产的区域。
A.7.2	Physical entry 物理入口 （A.11.1.2）	**Control** Secure areas shall be protected by appropriate entry controls and access points. 控制 安全区域应由适合的入口控制和接入点所保护。
A.7.3	Securing offices, rooms and facilities 办公室、房间和设施的安全保护 (A.11.1.3)	**Control** Physical security for offices, rooms and facilities shall be designed and implemented. 控制 应为办公室、房间和设施设计并采取物理安全措施。
A.7.4	Physical security monitoring 物理安全监视 (?)	**Control** Premises shall be continuously monitored for unauthorized physical access. 控制 应持续监视场所，防止未授权的物理访问。
A.7.5	Protecting against physical and environmental threats 物理和环境威胁的安全防护 (A.11.1.4)	**Control** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented. 控制 应设计和实施对物理和环境威胁保护，如自然灾害和其他对设施的有意或无意的物理威胁。
A.7.6	Working in secure areas 在安全区域工作 (A.11.1.5)	**Control** Security measures for working in secure areas shall be designed and implemented. 应设计和实施在安全区域工作的安全措施。
A.7.7	Clear desk and clear screen 清空桌面和屏幕策略 (A.11.2.9)	**Control** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced. 控制 应针对纸质和可移动存储介质，采取清理桌面策略；针对信息处处理设施清理屏幕策

		略 进行识别并恰当实施。
A.7.8	Equipment siting and protection 设备安置和保护 (A.11.2.1)	**Control** Equipment shall be sited securely and protected. 控制 设备应安全放置和保护
A.7.9	Security of assets off-premises 组织场所外的设备与资产安全 (A.11.2.6)	**Control** Off-site assets shall be protected. 应对组织场所外的资产进行保护。
A.7.10	Storage media 存储介质 (？A.8.3.1、A.8.3.2)、A.8.3.3	**Control** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements. 控制 存储介质应按照组织的分类方案和处理要求，对其采办、使用、运输和处置的生命周期进行管理。
A.7.11	Supporting utilities 支持性设施 (A.11.2.2)	**Control** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. *控制* 应保护信息处理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。
A.7.12	Cabling security 布缆安全 (A.11.2.3)	Control Cables carrying power, data or supporting information services shall be protected from interception, interference or damage. 控制 应保护承载电力、数据或支持信息服务的电缆免受窃听、干扰或损坏
A.7.13	Equipment maintenance 设备维护 (A.11.2.4)	**Control** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. 控制 设备应予以正确地维护，以确保其可用性、完整性和信息的保密性
A.7.14	Secure disposal or re-use of Equipment 设备的 处置或再利用 (A.11.2.7)	**Control** Items of equipment containing storage media shall be verified to en- sure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. 控制 包含储存介质的设备的所有部分应进行核查，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。

8	**Technological controls 技术控制**	
A.8.1	User end point devices 用户终端设备 (?)	**Control** Information stored on, processed by or accessible via user end point devices shall be protected. 控制 应保护储存在用户终端设备、通过用户终端设备处理或访问的信息的安全。
A.8.2	Privileged access rights 特许访问权 (A.9.2.3)	**Control** The allocation and use of privileged access rights shall be restricted and managed. 控制 应限制并管理特许访问权的分配和使用。
A.8.3	Information access restriction 信息访问限制 (A.9.4.1)	**Control** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. 控制 应按照已建立的有主题的特定访问控制策略，限制对信息和其他相关资产的访问。
A.8.4	Access to source code 源代码的访问控制 (A.9.4.5)	**Control** Read and write access to source code, development tools and software libraries shall be appropriately managed. 控制 应恰当管理源代码的读写访问、开发工具和软件库。
A.8.5	Secure authentication 安全鉴别 (A.9.4.2)	**Control** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. 控制 应基于信息访问限制和有主题的特定访问控制策略实施安全鉴别技术和程序。
A.8.6	Capacity management 容量管理 (A.12.1.3)	**Control** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements. 控制 应对资源的使用进行监视个按当前和预期的容量要求进行调整。
A.8.7	Protection against malware 防范恶意软件 (A.12.2.1)	**Control** Protection against malware shall be implemented and supported by appropriate user awareness. 控制 应防范恶意软件并由适宜的用户意识加以支持
A.8.8	Management of technical vulnerabilities 技术方面的脆弱性管理 （A.12.6.1）	**Control** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken. 控制 应获取在用的信息系统的技术方面的脆弱性信息，评价组织对这些脆弱性的暴露状况并采取适当的措施。

A.8.9	Configuration management 配置管理(?)	**Control** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed. 控制 应建立、实施、监视和评审硬件、软件、服务和网络的配置，并建立文档。
A.8.10	Information deletion 信息删除 （A.8.3.2）	**Control** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required. 控制 储存在信息系统、设备或其储存介质中的信息，当不再需要时应删除。
A.8.11	Data masking 数据屏蔽(?)	**Control** Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. 控制 应按照组织的有主题的特定访问控制策略和其他相关的有主题的特定策略和业务要求，并考虑适用的法规，使用数据屏蔽
A.8.12	Data leakage prevention 防止数据泄露 (?)	**Control** Data leakage prevention measures shall be applied to systems, net- works and any other devices that process, store or transmit sensitive information. 控制 数据泄露预防措施应应用于系统、网络和其他处理、储存或传输敏感信息的设备。
A.8.13	Information backup 信息备份 （A.12.3.1）	**Control** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. 控制 应按照达成一致的具有主题的特定备份策略，对信息、软件和系统镜像进行备份、加以维护，并定期 测试。
A.8.14	Redundancy of information pro- cessing facilities 信息处理设施冗余 （A.17.2.1）	**Control** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. 控制 信息处理设备应当实现冗余，以满足可用性要求
A.8.15	Logging日志 （A.12.4.1）	**Control** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed. 控制 应产生、储存、保护并分析记录活动、异常情况、故障和其他相关事态的日志。
A.8.16	Monitoring activities 监视活动 (?)	**Control** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential infor- mation security incidents.
A.8.17	Clock synchronization 时钟同步 （A.12.4.4）	**Control** The clocks of information processing systems used by the organization shall be synchronized to approved time sources.

		控制 组织使用的信息处理系统的时钟，应与批准的事件源同步。
A.8.18	Use of privileged utility programs 特权实用程序的使用 （A.9.4.4）	**Control** The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled. 控制 对于可能超越系统和应用控制的实用程序的使用应予以限制并严 格控制。
A.8.19	Installation of software on operational systems 运行系统的软件安装 （A.12.5.1）	**Control** Procedures and measures shall be implemented to securely manage software installation on operational systems. 控制 应实施运行系统软件安装安全管理程序和措施。
A.8.20	Networks security 网络安全 （A.13.1.1）	**Control** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. 控制 应对网络和网络设施进行安全管理和控制，以保护系统和应用中的信息。
A.8.21	Security of network services 网络服务的安全 （A.13.1.2）	**Control** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored. 控制 所有网络服务的安全机制、服务级别和管理要求应予以识别、实施并监视
A.8.22	Segregation of networks 网络中的隔离 （A.13.1.3）	**Control** Groups of information services, users and information systems shall be segregated in the organization’s networks. 控制 应在组织的网络中隔离信息服务、用户及信息系统。
A.8.23	Web filtering 网络筛选 (新增)	**Control** Access to external websites shall be managed to reduce exposure to malicious content. 控制 应对外网访问进行管理，以减少解除恶意内容
A.8.24	Use of cryptography 加密的使用 （A.10.1.1、A.10.1.2）	**Control** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. 控制 应定义并实施有效使用加密的规则，包括秘钥管理
A.8.25	Secure development life cycle 安全开发生命周期 (？)	**Control** Rules for the secure development of software and systems shall be established and applied. 控制 应建立并应用软件和系统的安全开发规则。

A.8.26	Application security require-ments 应用安全要求 （A.14.2.1）	**Control** Information security requirements shall be identified, specified and approved when developing or acquiring applications. 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。
A.8.27	Secure system architecture and engineering principles 安全系统架构与工程原则	**Control** Principles for engineering secure systems shall be established, docu- mented, maintained and applied to any information system development activities. 控制 应建立并保持安全系统工程原则，形成文件，并应用于任何信息系统开发活动
A.8.28	Secure coding 安全编码	**Control** Secure coding principles shall be applied to software development. 控制 安全编码原则应用于软件开发
A.8.29	Security testing in development and acceptance 开发和验收中的安全测试 （A.14.2.9）	**Control** Security testing processes shall be defined and implemented in the development life cycle. 控制 应定义安全测试过程并在开发生命周期中予以实施
A.8.30	Outsourced development 外包开发 （A.14.2.7）	**Control** The organization shall direct, monitor and review the activities related to outsourced system development. 控制 组织应指导、监视和评审与外包系统开发相关的活动
A.8.31	Separation of development, test and production environments 开发、测试和**生产环境**的分离 （A.12.1.4）	**Control** Development, testing and production environments shall be separated and secured. 控制 开发、测试和生产环境应分离并确保安全
A.8.32	Change management 变更管理 （A.12.1.2）	**Control** Changes to information processing facilities and information systems shall be subject to change management procedures. 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。
A.8.33	Test information 测试信息 （A.14.3.1）	**Control** Testinformation shall be appropriately selected, protected and managed. 控制 应恰当选择、保护和管理测试信息
A.8.34	Protection of information sys-tems during audit testing 审核测试过程中信息系统的保护 (A.12.7.1)	**Control** Audit tests and other assurance activities involving assessment of op- erational systems shall be planned and agreed between the tester and appropriate management. 控制 涉及运行系统评估的审核测试和其他保证活动应得到计划，并在测试人员和适当的管理层之间达成一致。

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—信息安全管理体系—指南

[3] iso /IEC 27004，信息技术—安全技术—信息安全管理—监测、测量、分析和评价

[4] iso /IEC/DIS 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

[6] ISO/IEC指令第1部分，ISO统一补充—ISO专用程序，2012