ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 22080—2025/ISO/IEC 27001:2022
代替 GB/T 22080—2016

网络安全技术　信息安全管理体系　要求

Cybersecurity technology—Information security management systems—Requirements

（ISO/IEC 27001:2022，Information security，cybersecurity and privacy protection—Information security management systems—Requirements，IDT）

2025-06-30 发布　　2026-01-01 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/T 22080—2016《信息技术　安全技术　信息安全管理体系　要求》,与 GB/T 22080—2016 相比,除编辑性改动外,主要技术变化如下:

a) 增加了“组织应确定气候变化是否是一个相关事项”(见 4.1);

b) 增加了“组织应确定哪些要求将通过信息安全管理体系来解决”[见 4.2c)];

c) 更改了“信息安全风险处置”中适用性声明相关要求[见 6.1.3d),2016 年版的 6.1.3d)];

d) 增加了“针对变更的规划”要求(见 6.3);

e) 更改了信息安全控制参考,包括对部分原有的控制进行合并、增加新的控制和调整控制的展示方式(见附录 A,2016 年版的附录 A)。

本文件等同采用 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》。

本文件做了下列最小限度的编辑性改动:

——为与我国技术标准体系协调,标准名称改为《网络安全技术　信息安全管理体系　要求》;

——纳入 ISO/IEC 27001:2022/Amd 1:2024《信息安全、网络安全和隐私保护　信息安全管理体系　要求》修正案 1:与气候行动相关的变化,并用双垂线在对应有变化的条款外侧标示。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中国电子技术标准化研究院、中国合格评定国家认可中心、中国网络安全审查认证和市场监管大数据中心、北京安信天行科技有限公司、中国信息安全测评中心、黑龙江省网络空间研究中心、中电长城网际系统应用有限公司、山东省标准化研究院、亚信科技(成都)有限公司、深圳市腾讯计算机系统有限公司、南方电网数字电网集团信息通信科技有限公司、中国烟草总公司湖北省公司、北京天融信网络安全技术有限公司、唯品会(中国)有限公司、杭州安恒信息技术股份有限公司、广州赛宝认证中心服务有限公司、中国船级社质量认证有限公司、北京赛西认证有限责任公司、启明星辰信息技术集团股份有限公司、北京中金云网科技有限公司、浙江网商银行股份有限公司、北京时代新威信息技术有限公司、中国石油天然气股份有限公司西北销售分公司。

本文件主要起草人:许玉娜、付志高、王秉政、林阳荟晨、尤其、魏立茹、翟亚红、陈青民、陆丽、杨婧婧、王琰、曲家兴、方舟、白瑞、杨霄璇、闵京华、白旭东、王姣、朱雪峰、公伟、廖双晓、刘震宇、王琼、杨斯可、寇增杰、周禹、王拓、鲁立、孙毅、赵丽华、杨天识、程燕、史艳语、王连强、谢建林、刘杰、于慧超。

本文件及其所代替文件的历次版本发布情况为:

——2008 年首次发布为 GB/T 22080—2008,2016 年第一次修订;

——本次为第二次修订。

引　言

0.1　概述

本文件提供了建立、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求和目标、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。

对组织而言，重要的是要将信息安全管理体系整合到组织的过程和整体管理结构中，使之成为后者的一部分，并在组织的过程、信息系统和控制的设计中要考虑信息安全。信息安全管理体系的实现程度是要与组织的需求相符合。

本文件能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。

本文件表述要求的顺序并不反映各要求的重要性，也不意味着实现这些要求时的顺序。条款编号仅是为了方便引用。

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（包括 ISO/IEC 27003、ISO/IEC 27004 和 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 Directives，Part1 附录 SL 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 的管理体系标准的兼容性。

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多个管理体系标准要求的组织是有用的。

网络安全技术　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。本文件还规定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，不接受排除第4章到第10章中规定的任何要求。

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。

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—Security techniques—Information security management systems—Overview and vocabulary)

注：GB/T 29246—2023　信息安全技术信息安全管理体系概述和词汇(ISO/IEC 27000:2018，IDT)

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维护的用于标准化的术语数据库网址如下：

——ISO在线浏览平台：https://www.iso.org/obp；

——IEC电子百科：https://www.electropedia.org。

4　组织环境

4.1　理解组织及其环境

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

组织应确定气候变化[1)]是否是一个相关事项。

注：对这些事项的确定，见GB/T 24353—2022中5.4.1建立外部和内部环境。

4.2　理解相关方的需求和期望

组织应确定：

a)　信息安全管理体系的相关方；

b)　这些相关方的有关要求；

c)　哪些要求将通过信息安全管理体系予以解决。

注1：相关方的要求包括法律、法规和合同义务。

注2：相关方可能提出与气候变化相关的要求。

1)　有关气候变化的更多信息，见ISO和国际认可论坛(IAF)关于管理体系标准中增加气候变化因素的联合公报。

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。

组织应根据以下内容确定信息安全管理体系范围：

a) 4.1 中提到的外部和内部事项；

b) 4.2 中提到的要求；

c) 组织实施的活动与其他组织实施的活动之间的接口和依赖关系。

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，包括所需的过程及其相互作用。

5 领导

5.1 领导和承诺

最高管理层应通过以下活动，证实其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方针和信息安全目标，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的业务过程中；

c) 确保信息安全管理体系所需资源可用；

d) 沟通有效信息安全管理的重要性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) 指导并支持相关人员为信息安全管理体系的有效性作出贡献；

g) 促进持续改进；

h) 支持其他相关管理角色在职责范围内证实其领导作用。

注：本文件中提到的“业务”能广义地解释为对组织的意图具有核心意义的活动。

5.2 方针

最高管理层应建立信息安全方针，该方针应：

a) 与组织的意图相适宜；

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：

a) 形成文件化信息并可用；

b) 在组织内得到沟通；

c) 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在组织内得到分配和沟通。

最高管理层应分配责任和权限，以便：

a) 确保信息安全管理体系符合本文件的要求；

b) 向其报告信息安全管理体系绩效。

注：最高管理层也能在组织内分配报告信息安全管理体系绩效的责任和权限。

6 规划

6.1 应对风险和机会的措施

6.1.1 通则

当规划信息安全管理体系时，组织应明确 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，以便：

a） 确保信息安全管理体系能达到预期结果；

b） 预防或减少不良影响；

c） 达到持续改进。

组织应规划：

a） 应对这些风险和机会的措施；

b） 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） 确保重复实施的信息安全风险评估能产生一致的、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） 对已分析的风险进行风险处置优先级排序。

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：组织能按需设计控制，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，并验证没有遗漏必要的控制；

注 2：附录 A 包含了可能的信息安全控制清单。本文件的用户在附录 A 的指引下，确保没有忽略必要的信息安全

控制。

注 3：附录 A 所列的信息安全控制并不是完备的，且如有必要，组织能引入额外的信息安全控制。

d） 制定适用性声明，其包含：

——必要的控制[见 6.1.3b)和 c)]；

——选择这些控制的合理性说明；

——必要的控制是否已实现；

——删减附录 A 中控制的合理性说明；

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的批准和对信息安全残余风险的接受。

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 GB/T 24353—2022 中给出的原则和通用指南相一致。

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） 适当时予以更新；

g） 形成文件化信息且可用。

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：

a） 要做什么；

b） 需要什么资源；

c） 由谁负责；

d） 何时完成；

e） 如何评价结果。

6.3 针对变更的规划

当组织确定需要变更信息安全管理体系时，应对这些变更的实施进行规划。

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） 确定在其控制下工作且影响其信息安全绩效的人员的必要能力；

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：适用的措施可能包括：例如，针对现有雇员提供培训、指导或重新分配工作；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) 如何沟通。

7.5 文件化信息

7.5.1 通则

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) 组织所确定的、对于信息安全管理体系有效性所必需的文件化信息。

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能是不同的，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，以确保其：

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（例如，避免保密性损失、不恰当使用、完整性损失）。

为控制文件化信息，适用时，组织应开展以下活动：

c) 分发、访问、检索和使用；

注：访问可能隐含着仅允许浏览文件化信息，或允许并授权浏览和更改文件化信息等的决定。

d) 存储和保护，包括保持可读性；

e) 对变更的控制（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。

8 运行

8.1 运行规划和控制

为了满足要求并实现第6章中确定的措施，组织应通过以下方式来规划、实现和控制所需的过程：

——建立过程的准则；

——根据准则实现对过程的控制。

文件化信息应可用，其程度足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。

组织应确保由外部提供的与信息安全管理体系有关的过程、产品或服务是受控的。

8.2 信息安全风险评估

组织应依据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结果，才会被视为有效；

c) 何时执行监视和测量；

d) 谁监视和测量；

e) 何时分析和评价监视和测量的结果；

f) 谁分析和评价这些结果。

作为结果证据的文件化信息应可用。

组织应评价信息安全绩效和信息安全管理体系的有效性。

9.2 内部审核

9.2.1 通则

组织应按计划的时间间隔进行内部审核，以提供下列相关信息：

a) 信息安全管理体系是否符合：

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) 信息安全管理体系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、实施和维护审核方案(一个或多个),包括审核频次、方法、责任、规划要求和报告。

组织应根据相关过程的重要性和以往审核的结果,建立审核方案。

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。

作为审核方案实施和审核结果证据的文件化信息应可用。

9.3 管理评审

9.3.1 通则

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 管理评审的输入

管理评审应包括下列相关信息。

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) 信息安全管理体系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) 不符合与纠正措施;

   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 管理评审的结果

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。

作为管理评审结果证据的文件化信息应可用。

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 不符合与纠正措施

当发生不符合时,组织应:

a) 对不符合做出反应,且适用时:

1） 采取措施，对其予以控制和纠正；
2） 处理其后果；

b） 通过以下活动，评价采取消除不符合原因的措施的需求，以防止不符合再次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，或是否可能发生；

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。

纠正措施应与所发生的不符合的影响相适应。

作为以下证据的文件化信息应可用：

a） 不符合的性质及所采取的任何后续措施；

b） 任何纠正措施的结果。

附 录 A
（规范性）
信息安全控制参考

表 A.1 所列的信息安全控制是直接源自 GB/T 22081—2024 第 5 章至第 8 章中所列的信息安全控制并与之相一致，应与 6.1.3 一起使用。

表 A.1 信息安全控制

5	组织控制	
5.1	信息安全策略	**控制** 应定义信息安全方针和特定主题策略，由管理层批准后发布，传达并让相关工作人员和相关方知悉，按计划的时间间隔以及在发生重大变更时对其进行评审
5.2	信息安全角色和责任	**控制** 信息安全角色和责任应根据组织需求进行定义和分配
5.3	职责分离	**控制** 应分离相互冲突的职责和责任范围
5.4	管理责任	**控制** 管理层应要求所有工作人员根据组织已建立的信息安全方针、特定主题策略和规程，履行信息安全责任
5.5	与职能机构的联系	**控制** 组织应建立并维护与相关职能机构的联系
5.6	与特定相关方的联系	**控制** 组织应建立并维护与特定相关方或其他专业安全论坛和专业协会的联系
5.7	威胁情报	**控制** 应收集并分析信息安全威胁相关的信息，以生成威胁情报
5.8	项目管理中的信息安全	**控制** 应将信息安全整合到项目管理中
5.9	信息及其他相关资产的清单	**控制** 应编制和维护信息及其他相关资产（包括资产拥有者）的清单
5.10	信息及其他相关资产的可接受使用	**控制** 应识别、文件化并实施信息及其他相关资产的可接受使用规则和处理规程
5.11	资产归还	**控制** 适宜时，工作人员和其他相关方在任用、合同或协议变更及终止时，应归还其拥有的所有组织资产
5.12	信息分级	**控制** 应根据组织基于保密性、完整性、可用性的信息安全需求以及相关方的要求，对信息进行分级

表 A.1　信息安全控制（续）

5.13	信息标记	**控制** 应按组织采用的信息分级方案，制定并实施适当的信息标记规程
5.14	信息传输	**控制** 应为组织内部以及组织与其他各方之间所有类型的传输设施，制定信息传输规则、规程或协议
5.15	访问控制	**控制** 应基于业务和信息安全要求，建立和实施信息及其他相关资产的物理和逻辑访问控制规则
5.16	身份管理	**控制** 应管理身份的全生存周期
5.17	鉴别信息	**控制** 应通过管理过程控制鉴别信息的分配和管理，包括向工作人员提供鉴别信息的适当处理建议
5.18	访问权限	**控制** 应根据组织访问控制的特定主题策略和规则来提供、评审、修改和删除信息及其他相关资产的访问权限
5.19	供应商关系中的信息安全	**控制** 应定义并实施过程和规程，以管理供应商产品或服务使用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** 应根据供应商关系的类型建立相关的信息安全要求，并与每个供应商达成一致
5.21	管理信息通信技术供应链中的信息安全	**控制** 应定义并实施过程和规程，以管理与信息通信技术(ICT)产品和服务供应链相关的信息安全风险
5.22	供应商服务的监视、评审和变更管理	**控制** 组织应定期监视、评审、评价和管理供应商信息安全实践和服务交付的变更
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，建立云服务的获取、使用、管理和退出过程
5.24	信息安全事件管理规划和准备	**控制** 组织应通过定义、建立和传达信息安全事件管理过程、角色和责任，为管理信息安全事件做出规划和准备
5.25	信息安全事态的评估和决策	**控制** 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	信息安全事件的响应	**控制** 应按文件化的规程响应信息安全事件
5.27	从信息安全事件中学习	**控制** 应使用从信息安全事件中得到的知识来加强和改进信息安全控制

表 A.1 信息安全控制（续）

5.28	证据收集	**控制** 组织应建立并实施包括识别、收集、获取和保存信息安全事态相关证据的规程
5.29	中断期间的信息安全	**控制** 组织应制定在中断期间将信息安全维持在适当级别的计划
5.30	业务连续性的信息通信技术就绪	**控制** 应根据业务连续性目标和信息通信技术(ICT)连续性要求，策划、实施、维护和测试 ICT 的就绪
5.31	法律、法规、规章和合同要求	**控制** 应识别与信息安全相关的法律、法规、规章和合同要求，以及组织满足这些要求的方法，并将其文件化且保持更新
5.32	知识产权	**控制** 组织应实施适当的规程来保护知识产权
5.33	记录的保护	**控制** 应保护记录不被丢失、破坏、篡改、未经授权的访问和未经授权的发布
5.34	隐私和个人可识别信息保护	**控制** 组织应根据适用的法律、法规和合同要求，识别并满足有关隐私保护和个人可识别信息(PII)保护的要求
5.35	信息安全的独立评审	**控制** 组织管理信息安全的方法及其实现，包括人员、过程和技术，应在计划的时间间隔内或发生重大变化时进行独立评审
5.36	符合信息安全的策略、规则和标准	**控制** 应定期评审与组织信息安全方针、特定主题策略、规则和标准的符合性
5.37	文件化的操作规程	**控制** 信息处理设施的操作规程应形成文件，并对有需要的工作人员可用
6	**人员控制**	
6.1	审查	**控制** 加入组织前，应对所有拟录用工作人员的候选人进行背景审查，并在入职后持续进行，同时考虑适用的法律、法规和道德规范，与业务要求、访问信息的级别和感知到的风险相适宜
6.2	任用条款和条件	**控制** 应在任用合同协议中规定工作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** 组织工作人员和相关方应接受适宜的信息安全意识、教育和培训，并获得与其工作职能相关的组织信息安全方针、特定主题策略和规程的定期更新信息
6.4	违规处理过程	**控制** 应正式制定违规处理过程并将之传达给工作人员和相关方，以便对违反信息安全策略的工作人员和其他相关方采取措施

表 A.1　信息安全控制（续）

6.5	任用终止或变更后的责任	**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义务，传达至相关工作人员和其他相关方并执行
6.6	保密或不泄露协议	**控制** 应识别、文件化、定期评审反映组织信息保护需求的保密或不泄露协议，并与工作人员和其他相关方签署
6.7	远程工作	**控制** 应在工作人员远程工作时实施安全措施，以保护在组织场所外所访问的、处理的或存储的信息
6.8	信息安全事态的报告	**控制** 组织应提供机制，使工作人员通过适当渠道及时报告观察到的或可疑的信息安全事态
7	**物理控制**	
7.1	物理安全边界	**控制** 应定义并使用安全边界来保护包含信息及其他相关资产的区域
7.2	物理入口	**控制** 安全区域应由适当的入口控制和访问点保护
7.3	办公室、房间和设施的安全保护	**控制** 应对办公室、房间和设施的物理安全进行设计，并予以实施
7.4	物理安全监视	**控制** 应持续监视场所，以防止发生未经授权的物理访问
7.5	物理和环境威胁防范	**控制** 应对物理和环境威胁的防范进行设计并予以实施，例如，自然灾害和其他对基础设施有意或无意的物理威胁
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** 应定义并适当地执行纸质和可移动存储媒体的桌面清理规则和信息处理设施的屏幕清理规则
7.8	设备安置和保护	**控制** 应安全地安置并保护设备
7.9	组织场所外的资产安全	**控制** 应保护组织场所外的资产
7.10	存储媒体	**控制** 存储媒体应在其获取、使用、运输和处置的整个生存周期内，按组织的分级方案和处理要求进行管理

表 A.1 信息安全控制（续）

7.11	支持性设施	**控制** 应保护信息处理设施使其免于由支持性设施的故障而引起的电源故障和其他中断
7.12	布缆安全	**控制** 应保护传输电力、数据或支持信息服务的电缆免受窃听、干扰或损坏
7.13	设备维护	**控制** 设备应予以正确的维护，以确保信息的可用性、完整性和保密性
7.14	设备的安全处置或重复使用	**控制** 应对包含存储媒体的设备的所有部分进行核查，以确保在处置或重复使用之前，任何敏感数据和获得许可的软件已被删除或安全地覆写
8	**技术控制**	
8.1	用户终端设备	**控制** 应保护用户终端设备所存储或处理的，或通过其访问的信息
8.2	特许访问权限	**控制** 应限制和管理特许访问权限的分配和使用
8.3	信息访问限制	**控制** 应按已建立的访问控制特定主题策略，限制对信息及其他相关资产的访问
8.4	源代码的访问	**控制** 应对源代码、开发工具和软件库的读写访问进行适当的管理
8.5	安全鉴别	**控制** 应根据信息访问限制和访问控制的特定主题策略实施安全的鉴别技术和规程
8.6	容量管理	**控制** 应根据当前和预期的容量需求，监视和调整资源的使用
8.7	恶意软件防范	**控制** 应实施恶意软件防范，并通过适当的用户意识教育予以支持
8.8	技术脆弱性管理	**控制** 应获取有关使用中的信息系统的技术脆弱性的信息，评价组织暴露于此类脆弱性的风险，并采取适当措施
8.9	配置管理	**控制** 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媒体中的信息
8.11	数据脱敏	**控制** 应根据组织关于访问控制的特定主题策略和其他相关的特定主题策略以及业务要求使用数据脱敏，并考虑到适用的法律法规

表 A.1　信息安全控制（续）

8.12	数据防泄露	**控制** 数据防泄露措施应用于处理、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商定的备份特定主题策略进行维护和定期测试
8.14	信息处理设施的冗余	**控制** 信息处理设施应具有足够的冗余以满足可用性要求
8.15	日志	**控制** 应生成、存储、保护和分析用于记录活动、异常、故障及其他相关事态的日志
8.16	监视活动	**控制** 应监视网络、系统和应用程序，以发现异常行为，并采取适当措施评价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	特权实用程序的使用	**控制** 应限制并严格控制可能超越系统和应用程序控制的实用程序的使用
8.19	运行系统软件的安装	**控制** 应实施规程和措施以安全地管理运行系统上的软件安装
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** 应在组织的网络中隔离信息服务组、用户组和信息系统组
8.23	网页过滤	**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	密码技术的使用	**控制** 应定义并实施有效使用密码技术的规则，包括密钥管理
8.25	安全开发生存周期	**控制** 应建立并应用软件和系统安全开发规则
8.26	应用程序安全要求	**控制** 在开发或获取应用程序时，应识别、规定和批准信息安全要求
8.27	系统安全架构和工程原则	**控制** 应建立、文件化、维护系统安全工程的原则，并将其应用于所有的信息系统开发活动

表 A.1 信息安全控制（续）

8.28	安全编码	**控制** 软件开发中应应用安全编码原则
8.29	开发和验收中的安全测试	**控制** 应在开发生存周期中定义和实施安全测试过程
8.30	开发外包	**控制** 组织应指导、监视和评审系统开发外包相关的活动
8.31	开发、测试和生产环境的隔离	**控制** 应隔离并保护开发、测试和生产环境
8.32	变更管理	**控制** 信息处理设施和信息系统的变更应遵循变更管理规程
8.33	测试信息	**控制** 应适当地选择、保护和管理测试信息
8.34	在审计测试中保护信息系统	**控制** 应对涉及运行系统评估的审计测试和其他保障活动进行规划，并在测试人员和适合的管理人员之间达成一致

参 考 文 献

[1] GB/T 22081—2024 网络安全技术信息安全控制(ISO/IEC 27002:2022,IDT)

[2] GB/T 24353—2022 风险管理 指南(ISO 31000:2018,IDT)

[3] ISO/IEC 27003 Information technology—Security techniques—Information security management systems—Guidance

[4] ISO/IEC 27004 Information technology—Security techniques—Information security management—Monitoring, measurement, analysis and evaluation

[5] ISO/IEC 27005 Information security, cybersecurity and privacy protection—Guidance on managing information security risks

[6] ISO/IEC Directives, Part 1 Procedures for the technical work—Consolidated ISO supplement—Procedures specific to ISO

[7] IAF/ISO Joint Communiqué on the addition of Climate Change considerations to Management Systems Standards