ISO/IEC 27001 2022

信息安全，网络安全与隐私保护
——信息安全管理体系
——要求

中文试译稿 v1.3

翻译 汤季洪

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建立的技术委员会参与国际标准的制定，以处理特定领域的技术活动。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保持联系的其他政府和非政府国际组织也参与此项工作。

ISO/IEC导则第1部分描述了用于编制本标准以及旨在进一步维护本标准的规程。特别是，应注意不同类型的文件需要不同的审批标准。本标准根据ISO/IEC导则第2部分的编辑规则起草（参见www.iso.org/directives 或者www.iec.ch/members_experts/refdocs ）。

请注意，本标准中的某些内容可能是专利权的主题。ISO和IEC不负责识别任何或所有此类专利权。在文档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专利声明列表中列出（参见www.iso.org/patents）或收到的IEC专利声明列表（参见patents.iec.ch）。

本标准中使用的任何商品名称都是为了方便用户而提供的信息，并不构成认可。

有关标准的自愿性质的解释、与合格评定相关的ISO特定术语和表述的含义，以及有关ISO遵守《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。IEC的有关信息请参见www.iec.ch/understanding-standards。

本标准由ISO/IEC JTC 1联合技术委员会信息技术分委员会SC 27信息安全、网络安全和隐私保护编写。

第三版取消并取代了已经过技术修订的第二版(ISO/IEC 27001:2013)，并

包含其技术勘误ISO/IEC 27001:2013/Cor 1:2014和ISO/IEC 27001:2013/Cor 2:2015。

主要变化如下：

— 行文与管理体系标准的协调结构和ISO/IEC 27002:2022保持一致。

关于本标准的任何反馈或问题应提交给用户的国家标准机构。这些机构的完整清单可在以下网址找到：

www.iso.org/members.html

www.iec.ch/national-committees

引言

0.1 总则

本标准提供建立、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，并使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予以实现的顺序。所列项目仅供参考。

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系列标准(包括ISO/IEC 27003[2]，ISO/IEC 27004[3]和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

本标准应用ISO/IEC导则第1部分附录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

本标准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处置的要求。本标准规定的要求是通用的，适用于各种类型、规模或性质的组织。当一个组织声称符合本标准时，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

以下文件在文本中被引用，其部分或全部内容构成本标准的要求。对于注明日期的参考文献，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—信息安全管理体系—概述和词汇

3术语和定义

就本标准而言，以下术语和定义适用。

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：https://www.iso.org/obp

—IEC电子词典：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项。

注：对这些事项的确定，参见ISO 31000:2018中5.4.1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) 这些相关方与信息安全相关的要求。

c) 这些要求中，哪些将通过信息安全管理体系来达成。

[译者注：标黄部分为相对上一版的差异，下同]

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

组织应按照本标准的要求，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，显性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，使他们能显性证实他们的领导作用按角色应用于其责任范围。

注：本标准中提到的“业务”可以广义地解释为对组织存在的目的至关重要的那些活动。

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：

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6.1.2 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6.1.3 b)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清单。本标准用户可在附录A的指导下，确保没有遗漏必要的控制。

注3：附录A所列的信息安全控制并不是完备的，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（见6.1.3 b）和c））；

— 选择该控制的合理性说明；

— 无论该必要控制是否已实现；以及

— 对附录A控制删减的合理性说明；

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：本标准中的信息安全风险评估和处置过程与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) 被监视；

e) 得到沟通；

f) 适当时更新；

g) 作为文件化信息提供。

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 变更规划

当组织确定需要对信息安全管理体系进行变更时，变更应当有计划地进行。

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：适用的措施能包括，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；

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) 本标准要求的文件化信息；

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标准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：

— 为过程建立标准；

— 根据标准实施过程控制。

文件化信息应在必要的范围内可用，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。

应保留适当的文件化信息作为结果的证据。

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) 本标准的要求。

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。

当建立内部审核方案时，应考虑相关过程的重要性和以往审核的结果。

组织应：

a) 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；

文件化信息应保持可用，以作为审核方案和审核结果的证据。

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 管理评审的输入

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。

文件化信息应保持可用，以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。

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）
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

[译者注：下表中内容与本人翻译的ISO/IEC 27002:2022试译稿v1.5同步]

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的策略，由管理层批准，发布，与相关工作人员和相关方沟通并得到他们的认可，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** 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该被分离。
5.4	管理层责任	**控制** 管理层应要求所有工作人员根据组织的既定信息安全方针、特定主题的策略和规程来应用信息安全。
5.5	与职能机构的联系	**控制** 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** 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**

		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受的使用	**控制** 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规程。
5.11	资产归还	**控制** 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，应归还其持有的所有组织资产。
5.12	信息分级	**控制** 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，对信息进行分级。
5.13	信息标签	**控制** 应根据组织采用的信息分级方案，制定并实施一套适当的信息标签规程。
5.14	信息传递	**控制** 信息传递的规则、规程或协议应在所有类型的信息传递机能中落实到位，包括在组织内部以及组织与其他方之间。
5.15	访问控制	**控制** 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** 应该管理身份的整个生命周期。
5.17	鉴别信息	**控制** 身份鉴别信息的分配和管理应藉由一个管理过程来控制，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** 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	供应商关系中的信息安全	**控制**

		应定义和实施过程和规程，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	在供应商协议中强调信息安全	**控制** 应建立相关的信息安全要求，并根据供应商关系的类型与每个供应商达成一致。
5.21	管理 ICT 供应链中的信息安全	**控制** 应定义和实施过程和规程，以管理与ICT产品和服务供应链相关的信息安全风险。
5.22	供应商服务的监视、评审和变更管理	**控制** 组织应定期对供应商信息安全实践和服务提供进行监视、评审、评估并管理变更。
5.23	使用云服务的信息安全	**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过程。
5.24	信息安全事件管理的规划与准备	**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，以规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** 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** 应根据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** 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	证据收集	**控制** 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规程。
5.29	中断期间的信息安全	**控制** 组织应规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** 应根据业务连续性目标和ICT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** 应识别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，将其文件化并跟进最新进展。
5.32	知识产权	**控制** 组织应当实施适当的规程来保护知识产权。
5.33	记录保护	**控制** 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	隐私和 PII 保护	**控制** 组织应根据适用的法律法规和合同要求，确定并满足有关隐私和PII保护的要求。
5.35	信息安全独立评审	**控制** 组织管理信息安全的方法及其实施（包括人员、过程和技术）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	符合信息安全策略、规则和标准	**控制** 应定期评审组织的信息安全方针、特定主题的策略、规则和标准的符合性。
5.37	文件化的操作规程	**控制** 信息处理设施或机能的操作规程应文件化并可供需要的人使用。
6 人员控制		
6.1	甄选	**控制** 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级和感知的风险相称。
6.2	雇佣条款和条件	**控制** 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** 组织的人员和相关利益方，应按其工作职能，接受关于组织的信息安全策略、特定主题策略和规程的适当的、定期更新的信息安全意识、教育和培训。
6.4	纪律处分过程	**控制**

		应正式发布和沟通纪律处分过程，以便对违反信息安全策略的工作人员和其他相关方实施反制。
6.5	雇佣关系终止或变更后的责任	**控制** 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，并向相关人员和其他相关方沟通。
6.6	保密或不披露协议	**控制** 反映组织信息保护需求的保密或不披露协议应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** 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** 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	物理安全边界	**控制** 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** 安全区域应通过适当的入口控制和访问点进行保护。
7.3	办公室、房间和设施的安全保护	**控制** 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** 应对经营场所进行持续监视，防止未经授权的物理访问。
7.5	抵御物理和环境威胁	**控制** 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** 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** 应定义并适当强制针对纸张和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** 设备应安全放置并受到保护。
7.9	组织场所外的资产的安全	**控制** 应保护组织场所外的资产。
7.10	存储介质	**控制** 应根据组织的分级方案和处理要求，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** 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** 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** 应验证包含存储介质的设备，以确保在作废或再利用之前任何敏感数据和授权软件已被移除或安全覆盖。
8 技术控制		
8.1	用户终端设备	**控制** 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	特许访问权	**控制** 应限制和管理特许访问权的分配和使用。
8.3	信息访问约束	**控制** 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的策略进行约束。
8.4	访问源代码	**控制** 应对源代码、开发工具和软件库的读写访问进行适当管理。

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规程。
8.6	容量管理	**控制** 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** 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	技术方面的脆弱性的管理	**控制** 应获取有关正在使用的信息系统的技术方面的脆弱性的信息，宜评估组织暴露于此类脆弱性的风险，并采取适当的措施。
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介质中的信息。
8.11	数据遮盖	**控制** 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** 处理、存储或传输敏感信息的系统、网络和任何其他设备应实施防止数据泄露的措施。
8.13	信息备份	**控制** 应根据已获批准的备份相关特定主题的策略，维护和定期测试信息、软件和系统的备份副本。
8.14	信息处理设施或机能的冗余	**控制** 信息处理设施或机能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** 应生成记录活动、异常、故障和其他相关事态的日志，并存储、保护和分析。
8.16	活动监视	**控制**

		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** 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** 应约束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** 对于在操作系统上安装软件，应实施规程和措施来安全地管理。
8.20	网络安全	**控制** 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** 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** 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** 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** 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** 应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** 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** 应建立、记录、维护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** 软件开发中应当应用安全编码原则。
8.29	开发和验收中的安全性测试	**控制** 应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**

		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** 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** 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** 应适当选择、保护和管理测试信息。
8.34	在审计测试期间对信息系统的保护	**控制** 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规划和协商。

参考文献

[1] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls

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

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

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

[5] ISO 31000:2018, Risk management — Guidelines