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 27001:2022）

版本记录	修订记录	修订人	日期
V1.0	项目组初稿		**2023.3.7**

目　录

0 引言

0.1 总则

本标准提供建立、实施、保持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施受组织的需要和目标、安全要求、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，并给相关方建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、信息系统和控制措施的设计中要考虑到信息安全。信息安全管理体系的实施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。

本文件中表述要求的顺序不反映各要求的重要性或实施顺序。条款编号仅为方便引用。

0 Introduction

0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization, The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes,information systems,and controls. t is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 参考信息安全管理体系标准族（包括 ISO/IEC 27003[2]、ISO/IEC 27004[3]、ISO/IEC 27005[4]）及相关术语和定义，给出了信息安全管理体系的概述和词汇。

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2],1SO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 与其他管理体系标准的兼容性

本文件应用了 ISO/IEC 导则第一部分的 ISO 补充部分附录 SL 中定义的高层结构、同一子条款标题、同一文本、通用术语和核心定义，因此保持了与其它采用附录SL的管理体系标准的兼容性。

附录 SL 定义的通用方法有助于组织选择实施单一管理体系来满足两个或多个管理体系标准要求。

0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement.and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

1. 范围

本标准规定了在组织环境下建立、实施、运行、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而 进行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。组织声称符合本文件时，对于第 4 章到第 10 章的要求不能删减。

1 Scope

This document specifies the requirements for establishing,implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document

2 规范性引用文件

以下标准在本文中的引用方式使其部分或全部内容构成本文件的要求。凡是注日 期的引用文件，只有引用的版本适用于本文 件；凡是不注日期的引用文件，其最新版本（包括任何修改）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。

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000,Information technology -- Security techniques - Information security management systems-- Overview and vocabulary

3 术语和定义

ISO/IEC 27000 中的术语和定义适用于本文件。

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

IEC Electropedia：可在 https://www.electropedia.org

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/1EC 27000 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

ISO Online browsing platform: available at https://www.iso.org/obp

IEC Electropedia: available at 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情况。

注：对这些情况的确定，参见ISO31000：2018[5]，5.4.1 中建立外部和内部环境的内容。

4 Context o the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(S) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018[5].

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) 这些相关方的相关要求；

c) 其中哪些要求将通过信息安全管理系统解决。

注：相关方的要求可包括法律法规要求和合同义务。

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

NOTE The requirements of interested parties can include legal and regulatory requirements and contractual obligations.

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情况；

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。

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2;

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

4.4 信息安全管理体系

组织应按照本文件的要求，建立、实施、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。

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system,including the processes needed and their interactions, in accordance with the requirements of this document.

5 领导力

5.1 领导力和承诺

最高管理者应通过以下方式证明信息安全管理体系的领导力和承诺：

a) 确保信息安全方针和信息安全目标已建立，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) 传达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；

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

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有效性做出贡献；

g) 促进持续改进；

h) 支持其他相关管理者角色，在其职责范围内展现领导力。

备注：本文件中提到的“业务”可以广义地解释为指组织存在目的的核心活动。

e) ensuring that the information security management system achieves its intended outcome(S);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement;and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 方针

最高管理者应建立信息安全方针，方针应：

a) 与组织意图相适宜；

b) 包括信息安全目标（见 6.2）或为信息安全目标的设定提供框架；

c) 包括对满足适用的信息安全要求的承诺；

d) 包括持续改进信息安全管理体系的承诺。

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives(see 6.2)or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security;

d) includes a commitment to continual improvement of the information security management system.

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。

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization;

g) be available to interested parties,as appropriate.

5.3 组织的角色，职责和权限

最高管理者应确保与信息安全相关角色的职责和权限得到分配和沟通。

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。

5.3 Organizational roles,responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for;

a) ensuring that the information security management system conforms to the requirements of this document;

b) reporting on the performance of the information security management system to top management.

NOTE Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

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 中提到的问题和 4.2 中提到的要求，确定需要应对的风险和机会，以：

a) 确保信息安全管理体系能实现预期结果；

b) 预防或减少意外的影响；

c) 实现持续改进。

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，并予以实施；

2) 评价这些措施的有效性。

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent,or reduce,undesired effects;

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and portunities; and

e) how to

1) integrate and implement the actions into its information security management system processes; and

2)evaluate the effectiveness of these actions.

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) 建立和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。

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

1) the risk acceptance criteria;and

2) criteria for performing information security risk assessments;

b) 确保重复的信息安全风险评估可产生一致的、有效的和可比较的结果；

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

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；

c) identifies the information security risks:

1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality,integrity and availability for information within the scope of the information security management system;and

2) identify the risk owners;

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；

d) analyses the information security risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c)1) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3) determine the levels of risk;

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) 排列已分析风险的优先顺序，以便于风险处置。

e) evaluates the information security risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a);and

2) prioritize the analysed risks for risk treatment.

组织应保留信息安全风险评估过程的文件化信息。

The organization shall retain documented information about the information security risk assessment process.

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) 确定实施已选的信息安全风险处置选项所必需的全部控制措施；

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 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，以核实没有遗漏必要的控制措施；

注 2：附录 A 包含了控制目标和控制措施的综合列表。本文件用户可使用附录A，以确保没有忽略必要的控制措施。

注 3：附件 A 中所列的信息安全控制措施并非详尽无遗，如有必要，可包括其他信息安全控制。

6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE 1 Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

d) 编制一份适用性声明，其中包括：

--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措施；和

--排除任何附录 A 控制的理由。

e) 制定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，及对信息安全残余风险的接受。

组织应保留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[5]中给出的原则和通用指南是一致的。

d) produce a Statement of Applicability that contains:

---- the necessary controls(see 6.1.3 b) and c));

---- justification for their inclusion;

---- whether the necessary controls are implemented or not; and

---- the justification for excluding any of the Annex A controls.

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000[5].

6.2 信息安全目标和实现规划

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；

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable(if practicable);

c) take into account applicable information security requirements,and results from risk assessment and risk treatment;

d) 被监控

e) 得到沟通；

f) 在适当时更新；

g) 作为文件信息提供

组织应保留信息安全目标的文件化信息。

在规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) 什么时候完成；

l) 如何评价结果。

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine:

h) what will be done;

i) what resources will be required;

j) who will be responsible;

k) when it will be completed;and

l) how the results will be evaluated.

6.3 策划变更

当组织确定需要变更信息安全管理体系时，变更应当有计划的进行

6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

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 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

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。

7.2 Competence The organization shall:

a) determine the necessary competence.of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable,take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;and

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include,for example:the provision of training to, the mentoring of, or the re-assignment of current employees;or the hiring or contracting of competent persons.

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。

7.3 Awareness

Persons doing work under the organization's control shall be aware of:a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance;and

c) the implications of not conforming with the information security management system requirements.

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) 沟通内容；

b) 沟通时间；

c) 沟通对象；

d) 如何沟通

e)

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate.

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) 组织为有效实施信息安全管理体系所确定的必要的文件化信息。

注：不同组织的信息安全管理体系文件化信息的详略程度取决于：

1) 组织的规模及其活动、过程、产品和服务的类型；

2) 过程的复杂性及其相互作用；

3) 人员的能力。

7.5 Documented information

7.5.1 General

The organization's information security management system shall include:

a) documented information required by this document; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE The extent of documented information for an information security management system can differ from one organization to another due to:

1) the size of organization and its type of activities,processes,products and services;

2) the complexity of processes and their interactions; and

3) the competence of persons.

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、作者或编号）；

b) 格式（例如语言、软件版本、图表）和介质（例如纸质、电子介质）；

c) 对适宜性和充分性的评审和批准。

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description(e.g.a title, date, author, or reference number);

b) format(e.g.language,software version,graphics) and media(e.g.paper,electronic);and

c) review and approval for suitability and adequacy.

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予以控制，以确保：

a) 在需要的地点和时间，是可用和适宜的；

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，组织应开展以下活动：

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) 保留和处置。

7.5.3 Control of documented information

Documented information required by the information security management system and by this document shall be controlled to ensure:

a) it is available and suitable for use,where and when it is needed;and

b) it is adequately protected(e.g.from loss of confidentiality,improper use,or loss of integrity).

For the control of documented information,the organization shall address the following activities, as applicable:

c) distribution,access,retrieval and use;

d) storage and preservation,including the preservation of legibility;

e) control of changes(e.g.version control);and

f) retention and disposition.

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：访问隐含着允许仅浏览文件化信息，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

组织应计划、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 条中确定的行动：

--制定流程标准；

--根据标准实施过程控制

文件化信息达到必要的程度，以确信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、产品或服务受到控制。

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system,shall be identified as appropriate,and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information,etc.

8 Operation

8.1 Operational planning and control

The organization shall plan,implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

---- establishing criteria for the processes;

---- implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled

.8.2 信息安全风险评估

组织应考虑 6.1.2 a)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。

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur,taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 信息安全风险处置

组织应实施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。

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

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措施；

b) 监视、测量、分析和评价的方法，适当时，该方法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。

应提供记录信息作为结果的证据。

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。

9 Performance evaluation

9.1 Monitoring,measurement,analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured,including information security processes and controls;

b) the methods for monitoring,measurement,analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated;

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

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，提供信息以确定信息安全管理体系是否：

a) 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) 得到有效实施和保持。

9.2.2 内部审核计划

组织应计划、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。在制定内部审计计划时，组织应考虑相关过程和以前审计的结果。

组织应：

a） 确定每次审计的审计标准和范围；

b） 选择审核员，实施审核，确保审核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实施的证据以及审计结果。

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

1) the organization's own requirements for its information security management system;

2) the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan,establish,implement and maintain an audit programme(s),including the frequency, methods, responsibilities,planning requirements and reporting.

When establishing the internal audit programme(s),the organization shall consider the importance of the processes concerned and the results of previous audits. The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit programme(s)and the audit results.

9.3 管理评审

9.3.1 总则

最高管理者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) 以往管理评审要求采取措施的状态；

b) 与信息安全管理体系相关的外部和内部情况的变化；

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) 信息安全绩效有关的反馈，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 Management review

9.3.1 General

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability,adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance,including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) Fulfillment of information security objectives;

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

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。

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews.

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 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability,adequacy and effectiveness of the information security management system.

10.2 不符合和纠正措施

当发生不符合时，组织应：

a) 对不符合做出反应，适用时：

1) 采取措施控制并纠正不符合；

2) 处理后果；

b) 通过以下方法，评价采取消除不符合原因的措施的需求，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) 实施需要的措施；

d) 评审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程度相适应。

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后续措施；

g) 纠正措施的结果。

10.2 Nonconformity and corrective action

When a nonconformity occurs,the organization shall:

a) react to the nonconformity,and as applicable:

1) take action to control and correct it;

2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere,by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity;and

3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system,if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken,

g) the results of any corrective action.

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 章至第 8 章，以及应使用在 6.1.3 上下文中列出的控制，并与之保持一致。

Annex A (normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

Table A.1 — Information security controls

表 A.1 - 信息安全控制

5	**Organizational c ontrols 组织控制**	
5.1	Policies for information security	Control Information security policy and topic-specific policies shall be defined, 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.
5.1	信息安全的策略	控制：信息安全策略和特定策略宜被定义，由管理者批准、发布与，相关人员和利益相关方进行沟通和确认，并在计划的时间间隔 和发生重大变化时进行评审。
5.2	Information security roles and responsibilities	Control Information security roles and responsibilities shall be defined and allocated according to the organization needs.
5.2	信息安全角色和责任	控制：应根据组织的需要定义和分配信息安全的角色和职责。
5.3	Segregation of duties	Control Conflicting duties and conflicting areas of responsibility shall be segregated.
5.3	职责分离	控制：应分离冲突的职责及其责任范围
5.4	Management responsibilities	Control Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

5.4	管理责任	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和 规程应用信息安全。
5.5	Contact with authorities	Control The organization shall establish and maintain contact with relevant authorities.
5.5	与职能机构的联系	控制：组织应与相关职能机构建立并保持联系。
5.6	Contact with special interest groups	Control The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
5.6	与特定相关方的联系	控制：该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	Threat intelligence	Control Information relating to information security threats shall be collected and analysed to produce threat intelligence.
5.7	安全威胁情报	控制：应收集和分析与信息安全威胁有关的信息，以生成威胁情报。
5.8	Information security in project management	Control Information security shall be integrated into project management.
5.8	项目管理中的信息安全	控制：应将信息安全纳入项目管理中。
5.9	Inventory of information and other associated assets	Control An inventory of information and other associated assets, including owners, shall be developed and maintained.
5.9	信息及相关资产清单	控制：应编制和维护信息和相关资产清单，包括拥有者。
5.10	Acceptable use of information and other associated assets	Control Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.
5.10	信息及与其相关资产的使用准则	控制：应确定、记录和实施可接受的使用规则和处理信息和其他 相关资产的程序。

5.11	Return of assets	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.
5.11	资产归还	控制 所有员工和其他相关方应在其雇佣、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	Classification of information	Control Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.
5.12	信息的分级	控制 应根据组织的信息安全需求，基于保密性、完整性、可用性和相 关利益方的要求，对信息进行分级。
5.13	Labelling of information	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.
5.13	信息的标记	控制 应根据本组织通过的信息分级方案制定和实施一套适当的信息 标记程序。
5.14	Information transfer	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.
5.14	信息传输	控制 应为组织内以及组织与其他方之间的所有类型的传输设施制定 信息传输规则、程序或协议。
5.15	Access control	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.
5.15	访问控制	控制 应基于业务和信息安全要求，建立并实施对信息和其他相关资产 的物理和逻辑访问规则的控制
5.16	Identity management	Control The full life cycle of identities shall be managed.
5.16	身份管理	控制

		应对身份的全生命周期进行管理。
5.17	Authentication information	Control Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.
5.17	鉴别信息	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。
5.18	Access rights	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.
5.18	访问权限	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。
5.19	Information security in supplier relationships	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.
5.19	供应商关系中的信息安全	控制：应定义和实施过程和程序，以管理与使用供应商的产品或 服务相关的信息安全风险。
5.20	Addressing information security within supplier agreements	Control Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
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，制定相关的信息安全要求，并 与每个供应商达成一致。
5.21	Managing information security in the information and communication technology (ICT) supply chain	Control Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
5.21	管理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	Monitoring, review and change management of supplier services	Control The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service

		delivery.
5.22	供应商服务的监视、评审和变更管理	控制：组织应定期监测、审查、评估和管理供应商信息安全实践 和服务交付方面的变化。
5.23	Information security for use of cloud services	Control Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.
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，建立对云服务的获取、使用 管理 、和退出的流程。
5.24	Information security incident management planning and preparation	Control The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.
5.24	信息安全事件（incident）管理计划和准备	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 色和责任，规划和准备管理信息安全事件。
5.25	Assessment and decision on information security events	Control The organization shall assess information security events and decide if they are to be categorized as information security incidents.
5.25	信息安全事态(event)的评估和决定	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	Response to information security incidents	Control Information security incidents shall be responded to in accordance with the documented procedures.
5.26	信息安全事件（incidents）响应	控制：宜按照文件化的规程响应信息安全事件。
5.27	Learning from information security incidents	Control Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.
5.27	从信息安全事件（incidents）中学习	控制：从信息安全事件中获取知识应用于加强和改进信息安全控制。
5.28	Collection of evidence	Control The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence

		related to information security events.
5.28	证据的收集	控制：组织应建立并实施识别、收集、获取和保存信息安全事件 相关证据的程序。
5.29	Information security during disruption	Control The organization shall plan how to maintain information security at an appropriate level during disruption.
5.29	中断期间的信息安全	控制：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 readiness for business continuity	Control ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.
5.30	信息技术为业务连续性做好准备	控制：基于业务连续性的目标和 ICT 信息技术连续性的要求，规划、实施、维护和测试 ICT 准备情况。
5.31	Legal, statutory, regulatory and contractual requirements	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.
5.31	法律、法规、监管和合同要求	控制：应识别、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	Intellectual property rights	Control The organization shall implement appropriate procedures to protect intellectual property rights.
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	Protection of records	Control Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.
5.33	记录的保护	控制：记录应被保护以防止丢失、损坏、伪造，未经授权的访问 和未经授权的发布。
5.34	Privacy and protection of personal identifiable information (PII)	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.
5.34	隐私和 PII 保护	控制：组织应根据使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	Independent review of information security	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.
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审查。
5.36	Compliance with policies, rules and standards for information security	Control Compliance with the organization's information security policy, topic specific policies, rules and standards shall be regularly reviewed.
5.36	遵循信息安全政策、规则和标准	控制：应定期审查是否符合组织的信息安全策略、专题策略、规 则和标准。
5.37	Documented operating procedures	Control Operating procedures for information processing facilities shall be documented and made available to personnel who need them.
5.37	文件化的操作程序	控制：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	People controls 人员控制	
6.1	Screening	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.
6.1	审查	宜按照相关法律法规和道德规范，在所有任用候选者加入组织之前，对其背景进行验证核查，并与业务要求、访问信息的等级和 察觉的风险相适宜。

6.2	Terms and conditions of employment	Control The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.
6.2	任用条款及条件	宜在员工和合同方的合同协议中声明他们和组织对信息安全的 责任。
6.3	Information security awareness, education and training	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.
6.3	信息安全意识、教育和培训	组织所有员工和相关的合同方，宜按其工作职能，接受适当的意 识教育和培训，及组织策略和规程的定期更新的信息。
6.4	Disciplinary process	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.
6.4	违规处理过程	宜有正式的、且已被传达的违规处理过程以对信息安全违规的员 工和其他相关利益方采取措施。
6.5	Responsibilities after termination or change of employment	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.
6.5	任用终止或变更的责任	宜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 至员工或合同方并执行。
6.6	Confidentiality or non-disclosure agreements	Control Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.
6.6	保密或不泄露协议	应识别、文件化和定期评审反映组织对信息保护需要的保密或不 泄露协议的要求，并由员工和其他相关利益方签署。

6.7	Remote working	Control Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises.
6.7	远程工作	当员工远程工作时，应实施安全措施，以保护在组织场所之外访问、处理或存储的信息。
6.8	Information security event reporting	Control The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.
6.8	信息安全事态（event）报告	组织应提供一种机制，使员工能通过适当渠道及时报告观察的或 怀疑的信息安全事件。
7	Physical controls 物理控制	
7.1	Physical security perimeters	Control Security perimeters shall be defined and used to protect areas that contain information and other associated assets.
7.1	物理安全边界	控制：宜定义和使用安全边界来保护敏感或关键信息和信息处理 设施的区域。
7.2	Physical entry	Control Secure areas shall be protected by appropriate entry controls and access points.
7.2	物理入口	控制：安全区域宜由适合的人口控制所保护，以确保只有授权的 人员才允许访问。
7.3	Securing offices, rooms and facilities	Control Physical security for offices, rooms and facilities shall be designed and implemented.
7.3	办公室、房间和设施安全	控制：宜为办公室、房间和设施设计并采取物理安全措施。
7.4	Physical security monitoring	Control Premises shall be continuously monitored for unauthorized physical access.
7.4	物理安全监控	控制：应持续检测房舍是否有未经授权的物理访问。

7.5	Protecting against physical and environmental threats	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.
7.5	外部和环境威胁安全防护	控制：应设计和实施保护措施，防止物理和环境威胁，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	Working in secure areas	Control Security measures for working in secure areas shall be designed and implemented.
7.6	在安全区域工作	控制：宜设计和实施在安全区域工作的安全措施。
7.7	Clear desk and clear screen	Control Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
7.7	清理桌面和屏幕	控制：宜针对纸质和可移动存储介质，采取清理桌面策略；宜针 对信息处理设施，采用清理屏幕策略。
7.8	Equipment siting and protection	Control Equipment shall be sited securely and protected.
7.8	设备安置和保护	控制：设备宜放置在安全的地方并受到保护。
7.9	Security of assets off-premises	Control Off-site assets shall be protected.
7.9	场所外资产的安全	控制：外部资产宜得到保护。
7.10	Storage media	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.
7.10	存储介质	控制：应根据组织的分类计划和处理要求，在获取、使用、运输 和处置的整个证明周期内对存储介质进行管理。
7.11	Supporting utilities	Control Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.

7.11	支持性设施	控制：宜保护设备使其免于由支持性设施的实效而引起的电源故 障和其他中断。
7.12	Cabling security	Control Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.
7.12	布缆安全	控制：宜保证传输数据或支持信息服务的电源布缆和通讯布缆免 受窃听、干扰或损坏。
7.13	Equipment maintenance	Control Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.
7.13	设备维护	控制：设备宜予以正确地维护，以确保其持续的可用性、完整性 和保密性。
7.14	Secure disposal or re -use of equipment	Control Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
7.14	设备的安全处置或再利用	控制：包含储存介质的设备的所有部分宜进行核查，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	
8.1	User end point devices	Control Information stored on, processed by or accessible via user end point devices shall be protected.
8.1	用户终端设备	控制 保护用户终端设备上存储、处理或访问的信息。
8.2	Privileged access rights	Control The allocation and use of privileged access rights shall be restricted and managed.
8.2	特权访问权	宜限制和管理特殊访问权的分配和使用。
8.3	Information access restriction	Control Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.
8.3	信息访问限制	在访问控制方面，宜根据已建立的特定主题方针限制访问信息和 其他相关资产。

8.4	Access to source code	Control Read and write access to source code, development tools and software libraries shall be appropriately managed.
8.4	源代码的访问	宜适当管理对源代码、开发工具和软件库的读写访问。
8.5	Secure authentication	Control Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.
8.5	安全认证	宜基于信息访问限制和访问控制的特定主题方针实施安全身份 验证技术和程序。
8.6	Capacity management	Control The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.
8.6	容量管理	宜根据当前和预期的能力要求监控和调整资源的使用情况。
8.7	Protection against malware	Control Protection against malware shall be implemented and supported by appropriate user awareness.
8.7	防范恶意软件	宜通过适当的用户意识实施和支持恶意软件防护。
8.8	Management of technical vulnerabilities	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.
8.8.	技术脆弱性管理	宜获得有关所用信息系统技术漏洞的信息，评估组织暴露于此类 漏洞的情况，并采取适当措施。
8.9	Configuration management	Control Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.
8.9	配置管理	控制：配置包括安全配置，对硬件、软件、服务以及网络都宜建立、记录、实施、监测和审查。

8.10	Information deletion	Control Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.
8.10	信息删除	控制：存储在信息系统、设备或其它任何存储媒介的信息，在不 需要时应删除。
8.11	Data masking	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.
8.11	数据脱敏	控制：应根据组织访问控制和其它相关的特定主题策略、业务需 求和适用的法律，实施数据脱敏。
8.12	Data leakage prevention	Control Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.
8.12	数据防泄漏	控制：数据防泄漏措施应适用于处理、存储或传输敏感信息的系统、网络和任何其他设备。
8.13	Information backup	Control Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
8.13	信息备份	控制：应按照既定的备份策略，对信息、软件和系统镜像进行备份，并定期测试。
8.14	Redundancy of information processing facilities	Control Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
8.14	信息处理设施冗余	控制：信息处理设施应当实现冗余，以满足可用性要求。
8.15	Logging	Control Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.

8.15	日志	控制：宜产生、存储、保护和分析记录用户活动、异常、错误和 其他相关事态的日志。
8.16	Monitoring activities	Control Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
8.16	行为监控	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 措施评估潜在的信息安全事件
8.17	Clock synchronization	Control The clocks of information processing systems used by the organization shall be synchronized to approved time sources.
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	Use of privileged utility programs	Control The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.
8.18	特权实用程序的使用	控制：应限制和严格控制能够覆盖系统和应用程序控制的实用程 序的使用。
8.19	Installation of software on operational systems	Control Procedures and measures shall be implemented to securely manage software installation on operational systems.
8.19	运行系统的软件安装	控制：应实施程序和措施以安全地管理操作系统上的软件安装。
8.20	Networks security	Control Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.
8.20	网络安全	控制：网络和网络设备应受到保护、管理和控制，以保护系统和 应用程序中的信息。
8.21	Security of network services	Control Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.
8.21	网络服务的安全	控制：应确定、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	Segregation of networks	Control Groups of information services, users and information systems shall be segregated in the organization’s networks.
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的网络中隔离 。
8.23	Web filtering	Control Access to external websites shall be managed to reduce exposure to malicious content.
8.23	网页过滤	控制：应管理对外部网站的访问，以减少面临恶意内容的可能。
8.24	Use of cryptography	Control Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.
8.24	密码使用	控制：应定义和实施有效使用密码学的规则，包括密码密钥管理 。
8.25	Secure development life cycle	Control Rules for the secure development of software and systems shall be established and applied.
8.25	安全的开发声生命周期	控制：应该建立和应用软件和系统的安全开发规则。
8.26	Application security requirements	Control Information security requirements shall be identified, specified and approved when developing or acquiring applications.
8.26	应用程序的安全要求	控制：应根据组织的需要定义和分配信息安全的角色和职责。
8.27	Secure system architecture and engineering principles	Control Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.
8.27	安全系统架构和工程原理	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	Secure coding	Control Secure coding principles shall be applied to software development.
8.28	安全开发	应将安全编码原则应用于软件开发。

8.29	Security testing in development and acceptance	Control Security testing processes shall be defined and implemented in the development life cycle.
8.29	开发和验收中的安全测试	应在开发生命周期中定义和实施安全测试过程。
8.30	Outsourced development	Control The organization shall direct, monitor and review the activities related to outsourced system development.
8.30	外包开发	组织应指导、监控和评审与外包系统开发相关的活动。
8.31	Separation of development, test and production environments	Control Development, testing and production environments shall be separated and secured.
8.31	开发、测试和生产环境的分离	开发、测试和生产环境应该分离并受到保护。
8.32	Change management	Control Changes to information processing facilities and information systems shall be subject to change management procedures.
8.32	变更管理	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	Test information	Control Test information shall be appropriately selected, protected and managed.
8.33	测试信息	应适当选择、保护和管理测试信息。
8.34	Protection of information systems during audit testing	Control Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.
8.34	审计测试期间的信息系统保护	测试人员和适当的管理层应计划和商定涉及操作系统评估的审 计测试和其他保证活动。

Bibliography

[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