INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition

2022-10

Information security, cybersecurity and privacy protection — 信息安全，网络安全和隐私保护

Information security management systems — Requirements 信息安全管理体系—要求

说明:

ISO/IEC 27001：2022 刚发布不久，暂无权威机构发布的中文版本，为力求精准和精炼，本文中中文译文翻译过程中比对了权威机构发布的 ISO/IEC 27001：2013 和 ISO 9001：2015 中文版本。本文仅限于交流和学习使用，请勿用于商业用途。

ISO IEC 27001 学习笔记

微信扫描二维码，关注我的公众号

1 Scope 范围

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.

本文件规定了在组织的环境下建立、运行、维护、持续改进信息安全管理体系的要求。本文件还包括根据组织需求裁切的信息安全风险评估和处理的要求。本文件中所列的要求是通用的，适用于各种类型、规模和性质的组织。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 Normative references 规范性引用文件

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.

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。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, Information technology — Security techniques — Information security management systems — Overview and vocabulary

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 Terms and definitions 术语和定义

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

ISO/IEC27000 界定的术语和定义适用于本文件。

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

ISO 和 IEC 维护的用于标准化的术语数据库地址如下：

— ISO Online browsing platform: available at

https://www.iso.org/obp

— ISO 在线浏览平台：https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

— IEC 电子开放平台：https://www.electropedia.org/

4 Context of the organization 组织环境

4.1 Understanding the organization and its context 理解组织及其环境

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.

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。

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].

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

4.2 Understanding the needs and expectations of interested parties 理解相关方的需求和期望

The organization shall determine:

组织应确定：

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

a) 信息安全管理体系相关方；

b) the relevant requirements of these interested parties;

b) 这些相关方的相关要求；

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

c) 哪些要求可以通过信息安全管理体系得到解决。

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

注：相关方的要求可包括法律、法规要求和合同义务

4.3 Determining the scope of the information security management system 确定信息安全管理体系范围

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

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。

When determining this scope, the organization shall consider:

在确定范围时，组织应考虑：

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

a) 4.1 中提到的外部和内部事项；

b) the requirements referred to in 4.2;

b) 4.2 中提到的要求；

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

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。

The scope shall be available as documented information.

该范围应形成文件化信息并可用。

4.4 Information security management system 信息安全管理体系

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.

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，包括信息安全管理体系所需的过程及其相互作用。

5 Leadership 领导作用

5.1 Leadership and commitment 领导和承诺

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

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

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

b) 确保将信息安全管理体系要求整合到组织过程中；

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

c) 确保信息安全管理体系所需资源可用；

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

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

e) 确保信息安全管理体系达到预期结果；

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

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) promoting continual improvement; and

g) 促进持续改进；以及

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

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。

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.

注：本文件使用的“业务”一词可广义地理解为涉及组织存在目的的核心活动。

5.2 Policy 方针

Top management shall establish an information security policy that:

最高管理层应建立信息安全方针，该方针应：

a) is appropriate to the purpose of the organization;

a) 与组织意图相适宜；

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

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

c) 包括对满足适用的信息安全相关要求的承诺；

d) includes a commitment to continual improvement of

the information security management system.

d) 包括对持续改进信息安全管理体系的承诺。

The information security policy shall:

信息安全方针应：

e) be available as documented information;

e) 形成文件化信息并可用；

f) be communicated within the organization;

f) 在组织内得到沟通；

g) be available to interested parties, as appropriate.

g) 适当时，对相关方可用。

5.3 Organizational roles, responsibilities and authorities 组织的角色、职责和权限

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

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。

Top management shall assign the responsibility and authority for:

最高管理层应分配责任和权限，以：

a) ensuring that the information security management

system conforms to the requirements of this document;

a) 确保信息安全管理体系符合本文件的要求；

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

b) 向最高管理者报告信息安全管理体系绩效。

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

注：最高管理层也可为组织内报告信息安全管理体系绩效，分配职责和权限。

6 Planning 策划

6.1 Actions to address risks and opportunities 应对风险和机会的措施

6.1.1 General 总则

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:

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

a) 确保信息安全管理体系可达到预期结果；

b) prevent, or reduce, undesired effects;

b) 预防或减少不良影响；

c) achieve continual improvement.

c) 达到持续改进。

The organization shall plan:

组织应策划：

d) actions to address these risks and opportunities; and

d) 应对这些风险和机会的措施；以及

e) how to

e) 如何：

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

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；以及

2) evaluate the effectiveness of these actions.

2) 评价这些措施的有效性。

6.1.2 Information security risk assessment 信息安全风险评估

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

组织应定义并应用信息安全风险评估过程，以：

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

a) 建立并维护信息安全风险准则，包括：

1) the risk acceptance criteria; and

1) 风险接受准则；以及

2) criteria for performing information security risk assessments;

2) 信息安全风险评估实施准则。

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

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) identifies the information security risks:

c) 识别信息安全风险：

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

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;以及

2) identify the risk owners;

2) 识别风险责任人。

d) analyses the information security risks:

d) 分析信息安全风险:

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

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

2) 评估 6.1.2 c) 1)中所识别的风险实际发生的可能性;

3) determine the levels of risk;

3) 确定风险级别。

e) evaluates the information security risks:

e) 评价信息安全风险:

1) compare the results of risk analysis with the risk

criteria established in 6.1.2 a); and

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；以及

2) prioritize the analysed risks for risk treatment.

2）为风险处置排序已分析风险的优先级。

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

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 Information security risk treatment 信息安全风险处置

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

组织应定义并应用信息安全风险处置过程，以：

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

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

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；

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

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

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；

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.

注 2：附录 A 包含了可能需要的信息安全控制列表。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。

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

注 3：附录 A 所列的信息安全控制并不是完备的，如果有需要，可以包含额外的信息安全控制。

d) produce a Statement of Applicability that contains:

d) 制定一个适用性声明（SOA），其包含：

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

— 必要的控制（见 6.1.3 b）和 c））；

— justification for their inclusion;

— 其选择的合理说明；

— whether the necessary controls are implemented or not; and

— 无论该必要的控制是否已实现；以及

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

— 及对附录 A 控制删减的合理性说明。

e) formulate an information security risk treatment plan; and

e) 制定正式的信息安全风险处置计划；

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

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。

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

组织应保留有关信息安全风险处置过程的文件化信息。

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].

注 4：本文件中的信息安全风险评估和处置过程与ISO31000[5]中给出的原则和通用指南相匹配。

6.2 Information security objectives and planning to achieve them 信息安全目标及其实现策划

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

组织应在相关职能和层级上建立信息安全目标。

The information security objectives shall:

信息安全目标应：

a) be consistent with the information security policy;

a) 与信息安全方针一致；

b) be measurable (if practicable);

b) 可测量(如可行)；

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

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) be monitored;

d) 予以监视；

e) be communicated;

e) 予以沟通；

f) be updated as appropriate;

f) 适时更新；

g) be available as documented information.

g) 形成文件化信息并可用。

The organization shall retain documented information on the information security objectives.

组织应保留有关信息安全目标的文件化信息。

When planning how to achieve its information security objectives, the organization shall determine:

在策划如何达到信息安全目标时，组织应确定：

h) what will be done;

h) 要做什么；

i) what resources will be required;

i) 需要什么资源；

j) who will be responsible;

j) 由谁负责；

k) when it will be completed; and

k) 什么时候完成；

l) how the results will be evaluated.

l) 如何评价结果。

6.3 Planning of changes 变更的策划

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

当组织确定需要对信息安全管理体系进行变更时，变更应按所策划的方式实施。

7 Support 支持

7.1 Resources 资源

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

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 Competence 能力

The organization shall:

组织应：

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

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

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

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) retain appropriate documented information as evidence of competence.

d) 保留适当的文件化信息作为能力的证据。

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

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；或者雇佣或签约有能力的人员。

7.3 Awareness 意识

Persons doing work under the organization's control shall be aware of:

在组织控制下工作的人员应知晓：

a) the information security policy;

a) 信息安全方针；

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

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；以及

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

c) 不符合信息安全管理体系要求带来的影响。

7.4 Communication 沟通

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

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) on what to communicate;

a) 沟通什么；

b) when to communicate;

b) 何时沟通；

c) with whom to communicate;

c) 与谁沟通；

d) how to communicate.

d) 如何沟通。

7.5 Documented information 文件化信息

7.5.1 General 总则

The organization's information security management system shall include:

组织的信息安全管理体系应包括：

a) documented information required by this document; and

a) 本文件要求的文件化信息；以及

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

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。

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

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

1) 组织的规模及其活动、过程、产品和服务的类型；

2) the complexity of processes and their interactions; and

2) 过程及其相互作用的复杂性；以及

3) the competence of persons.

3) 人员的能力。

7.5.2 Creating and updating 创建和更新

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

创建和更新文件化信息时，组织应确保适当的：

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

a) 标识和描述(例如标题、日期、作者或引用编号)；

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

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) review and approval for suitability and adequacy.

c) 对适宜性和充分性的评审和批准。

7.5.3 Control of documented information 文件化信息的控制

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

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

a) 在需要的场合和时机，均可获得并适用;

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

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)。

For the control of documented information, the

organization shall address the following activities, as applicable:

为控制文件化信息，适用时，组织应进行以下活动：

c) distribution, access, retrieval and use;

c) 分发，访问，检索和使用；

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

d) 存储和保护，包括保持可读性；

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

e) 控制变更(例如，版本控制)；以及

f) retention and disposition.

f) 保留和处置。

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.

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

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.

注：对文件化信息的“访问”可能意味着仅允许查阅，或者意味着允许查阅并授权修改等其他权限。

8 Operation 运行

8.1 Operational planning and control 运行策划和控制

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

为了满足要求以及实施条款 6 中确定的措施，组织应通过以下措施对所需的过程进行策划、实施和控制：

— establishing criteria for the processes;

— 建立过程准则；

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

— 按照准则实施过程控制；

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

文件化信息应在必要的程度上予以保持，以确信这些过程按策划得到执行。

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

组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻不利影响。

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

组织应确保外部提供的，且与信息安全管理体系有关的过程、产品或服务受到控制。

8.2 Information security risk assessment 信息安全风险评估

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).

组织应考虑 6.1.2 a)所建立的准则，按策划的时间间隔，或当重大变更提出或发生时，执行信息安全风险评估。

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

组织应保留信息安全风险评估结果的文件化信息。

8.3 Information security risk treatment 信息安全风险处置

The organization shall implement the information security risk treatment plan.

组织应实施信息安全风险处置计划。

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

组织应保留信息安全风险处置结果的文件化信息。

9 Performance evaluation 绩效评价

9.1 Monitoring, measurement, analysis and evaluation 监视、测量、分析和评价

The organization shall determine:

组织应确定：

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

a) 需要被监视和测量的内容，包括信息安全过程和控制；

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;

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) when the monitoring and measuring shall be performed;

c) 何时应执行监视和测量；

d) who shall monitor and measure;

d) 应由谁来监视和测量；

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

e) 何时应分析和评价监视和测量的结果；

f) who shall analyse and evaluate these results.

f) 应由谁来分析和评价这些结果。

Documented information shall be available as evidence of the results.

适当的文件化信息应予以保留，以作为结果的证据。

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

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 Internal audit 内部审核

9.2.1 General 总则

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

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

a) conforms to

a) 是否符合：

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

1) 组织自身对信息安全管理体系的要求；

2) the requirements of this document;

2) 本文件的要求；

b) is effectively implemented and maintained.

b) 是否得到有效的实施和保持。

9.2.2 Internal audit programme 内部审核方案

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

reporting.

组织应策划、建立、实施和保持一项或多项审核方案，其中包括频率、方法、责任、策划要求和报告。

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

建立内部审核方案时，组织应考虑到有关过程的重要性和以前审核的结果。

The organization shall:

组织应：

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

a) 定义每次审核的审核准则和审核范围；

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

b) 选择审核员并实施审核，以确保审核过程的客观性和公正性；

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

c) 确保将审核结果报告至相关管理层。

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

文件化信息应予以保留，以作为审核方案实施和审核结果的证据。

9.3 Management review 管理评审

9.3.1 General 总则

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

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

9.3.2 Management review inputs 管理评审输入

The management review shall include consideration of:

管理评审应考虑：

a) the status of actions from previous management reviews;

a) 以往管理评审所采取措施的情况；

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

b) 与信息安全管理体系相关的内外部事项的变化；

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

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

d) 有关信息安全绩效的反馈，包括以下方面的趋势:

1) nonconformities and corrective actions;

1) 不符合和纠正措施；

2) monitoring and measurement results;

2) 监视和测量结果；

3) audit results;

3) 审核结果；

4) fulfilment of information security objectives;

4) 信息安全目标完成情况；

e) feedback from interested parties;

e) 相关方反馈；

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

f) 风险评估结果及风险处置计划的状态；

g) opportunities for continual improvement.

g) 持续改进的机会。

9.3.3 Management review results 管理评审输出

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.

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。

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

文件化信息应予以保留，以作为管理评审结果的证据。

10 Improvement 改进

10.1 Continual improvement 持续改进

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

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 Nonconformity and corrective action 不符合及纠正措施

When a nonconformity occurs, the organization shall:

当发生不符合时，组织应：

a) react to the nonconformity, and as applicable:

a) 对不符合做出反应,适用时：

1) take action to control and correct it;

1) 采取措施，以控制并予以纠正；

2) deal with the consequences;

2) 处置后果；

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

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) reviewing the nonconformity;

1) 评审不符合；

2) determining the causes of the nonconformity; and

2) 确定不符合的原因；以及

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

3) 确定类似的不符合是否存在，或可能发生；

c) implement any action needed;

c) 实施任何需要的措施；

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

d) 评审任何所采取的纠正措施的有效性；以及

e) make changes to the information security management system, if necessary.

e) 必要时，对信息安全管理体系进行变更。

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

纠正措施应与所遇到的不符合的影响相适合。

Documented information shall be available as evidence of:

文件化信息应予以保留，以作为以下方面的证据：

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

f) 不符合的性质及所采取的任何后续措施；

g) the results of any corrective action.

g) 任何纠正措施的结果。

Annex A 附录 A

Information security controls reference 参考信息安全控制

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.

表 A.1 所列的信息安全控制是直接源自并与 ISO/IEC 27002:2022[1]第 5 章~第 8 章相对应，并在 6.1.3 环境中被使用。

Table A.1 — Information security controls

表 A.1 — 信息安全控制

5	**Organizational controls 组织控制**	
5.1	policies for information security 信息安全策略	**Control 控制** 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. 信息安全策略和特定主题的策略应被定义，由管理者批准，发布、传达给所有员工和外部相关方，并按策划的时间间隔或当重大变化发生时进行信息安全策略评审。
5.2	Information security roles and responsibilities 信息安全角色和职责	**Control 控制** Information security roles and responsibilities shall be defined and allocated according to the organization needs. 应依据组织需求定义信息安全职责和角色。
5.3	Segregation of duties 职责分离	**Control 控制** Conflicting duties and conflicting areas of responsibility shall be segregated. 应分离冲突的职责及其责任范围。
5.4	Management responsibilities 管理职责	**Control 控制** 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. 管理者应要求所有员工按照组织已建立的策略、特定主题的策略和规程应用信息安全。
5.5	Contact with authorities 与职能机构的联系	**Control 控制** The organization shall establish and maintain contact with relevant authorities. 组织应建立和维护与相关职能机构的联系。
5.6	Contact with special interest Groups 与特殊利益团的联系	**Control 控制** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations. 组织应建立和维护与特殊利益团，或其他专业安全论坛和专业协会的联系。
5.7	Threat intelligence 威胁情报	**Control 控制** Information relating to information security threats shall be collected and analysed to produce threat intelligence. 与信息安全威胁相关的信息应被收集和

		被分析，以获得威胁情报。
5.8	Information security in project management 项目管理中的信息安全	**Control 控制** Information security shall be integrated into project management. 信息安全应被整合到项目管理中。
5.9	Inventory of information and other associated assets 信息和其他关联资产清单	**Control 控制** An inventory of information and other associated assets, including owners, shall be developed and maintained. 应编制和维护信息和其他关联资产清单，包含其所有者。
5.10	Acceptable use of information and other associated assets 信息和其他关联资产的可接受使用	**Control 控制** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented. 应识别信息和其他关联资产的可接受使用规则，以及其处理规程，形成文件并加以实施。

5.11	Return of assets 资产归还	**Control 控制** 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. 员工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。
5.12	Classification of information 信息的分级	**Control 控制** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements. 信息应按照基于保密性、完整性、可用性以及相关方要求的组织的信息安全需求进行分级。
5.13	Labelling of information 信息的标记	**Control 控制** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the

		information classification scheme adopted by the organization. 应按照组织采用的信息分级方案，制定并实施一组适当的信息标记规程。
5.14	Information transfer 信息传输	**Control 控制** 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. 应为组织内部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、规程或协议。
5.15	Access control 访问控制	**Control 控制** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. 应根据业务和信息安全需求，建立对信息和其他关联资产的物理和逻辑访问的控制规则，并予以实施。

5.16	Identity management 身份管理	**Control 控制** The full life cycle of identities shall be managed. 应管理身份的整个生命周期。
5.17	Authentication information 鉴别信息	**Control 控制** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. 应通过正式的管理过程控制鉴别信息的分配和管理，包括建议人员适当处理鉴别信息。
5.18	Access rights 访问权	**Control 控制** 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. 应根据组织特定主题的访问控制策略和

		规则对信息和其他关联资产的访问权进行分配、评审、修改和删除。
5.19	Information security in supplier relationships 供应商关系中的信息安全	**Control 控制** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. 为管理使用供应商提供的产品或服务所带来的信息安全风险，相关过程和规程应被定义，并予以实施。
5.20	Addressing information security within supplier agreements 在供应商协议中强调信息安全	**Control 控制** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. 应基于供应商关系类型，建立相关信息安全要求，并与各供应商就信息安全要求达成一致。
5.21	Managing information security in the information	**Control 控制** Processes and procedures shall be defined and implemented to manage the information security risks associated with

	and communication technology (ICT) supply chain 信息与通信技术(ICT)供应链的信息安全管理	the ICT products and services supply chain. 为管理信息与通信技术(ICT)产品和服务供应链相关的信息安全风险，相关过程和规程应被定义，并予以实施。
5.22	Monitoring, review and change management of supplier services 供应商服务的监视、评审和变更管理	**Control 控制** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. 组织应定期监视、评审、评价供应商信息安全实践和服务交付，并应管理过程中的变更。
5.23	Information security for use of cloud services	**Control 控制** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the

	使用云服务的信息安全	organization's information security requirements. 应根据组织信息安全要求，为获取、使用、管理和退出云服务建立流程。
5.24	Information security incident management planning and preparation 信息安全事件管理的策划和准备	**Control 控制** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. 组织应定义、建立和沟通信息安全事件管理过程、角色和职责，以策划和准备信息安全事件的管理。
5.25	Assessment and decision on information security events 信息安全事态的评估和决策	**Control 控制** The organization shall assess information security events and decide if they are to be categorized as information security incidents. 组织应评估信息安全事态并决定其是否属于信息安全事件。
5.26	Response to	**Control 控制**

	information security incidents 信息安全事件的响应	Information security incidents shall be responded to in accordance with the documented procedures. 组织应按照文件化的规程响应信息安全事件。
5.27	Learning from information security incidents 从信息安全事件中学习	**Control 控制** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. 应利用在信息安全事件中得到的知识来增强和提升信息安全控制。
5.28	Collection of evidence 证据的收集	**Control 控制** The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events. 组织应建立识别、收集、获取和保存信息安全事件的相关证据的规程，并予以实施。
5.29	Information	**Control 控制**

	security during disruption 中断时的信息安全	The organization shall plan how to maintain information security at an appropriate level during disruption. 组织应策划如何在中断期间将信息安全维持在适当的水平。
5.30	ICT readiness for business continuity 业务连续性的信息与通信技术 (ICT) 的准备	**Control 控制** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. 应基于业务连续性目标和信息与通信技术（ICT）连续性要求，策划信息与通信技术（ICT）的准备，并予以实施，保持和测试。
5.31	Legal, statutory, regulatory and contractual requirements 法律、法规、规章和合同要求	**Control 控制** 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. 应识别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，并形成文件和保持更新。
5.32	Intellectual property rights 知识产权	**Control 控制** The organization shall implement appropriate procedures to protect intellectual property rights. 组织应实施适当的规程，以保护知识产权。
5.33	Protection of records 记录的保护	**Control 控制** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release. 记录应进行保护以防其丢失、毁坏、伪造、未授权访问和未授权发布。
5.34	Privacy and protection of personal identifiable information (PII) 隐私和个人身份信息的保护	**Control 控制** 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. 组织应根据适用的法律法规和合同要求，识别并满足关于隐私保护和个人身份信

		息(PII)保护的要求。
5.35	Independent review of information security 信息安全的独立评审	**Control 控制** 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. 应按策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施包括人员、过程和技术应进行独立评审。
5.36	Compliance with policies, rules and standards for information security 策略、规则和信息安全标准的符合性	**Control 控制** Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed. 应定期评审组织信息安全策略、特定主题的策略、规则和标准的符合性。
5.37	Documented	**Control 控制**

	operating procedures 文件化的操作规程	Operating procedures for information processing facilities shall be documented and made available to personnel who need them. 信息处理设施的操作规程应形成文件，并提供给有需要的人员使用。
6	**People controls 人员控制**	
6.1	Screening 审查	**Control 控制** 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. 在其加入组织之前，应对所有任用候选者的背景进行验证核查，并在其基础之上，考虑适用的法律、法规和道德规范，以及与业务要求、访问信息的等级和察觉的风

		险相适宜。
6.2	Terms and conditions of employment 任用条款及条件	**Control 控制** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security. 雇佣合同协议应声明员工和组织对信息安全的职责。
6.3	Information security awareness, education and training 信息安全意识、教育和培训	**Control 控制** 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. 组织和相关方的员工，应按其工作职能，接受适当的意识、教育和培训，以及定期更新的组织信息安全策略、特定主题策略及规程。
6.4	Disciplinary	**Control 控制**

	process 违规处理过程	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. 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员工和其他相关方采取措施。
6.5	Responsibilities after termination or change of employment 任用终止或变更的职责	**Control 控制** 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. 应确定任用终止或变更后仍有效的信息安全职责和义务，传达至相关员工和其他相关方并执行。
6.6	Confidentiality or non-disclosure agreements	**Control 控制** Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information

	保密或不泄露协议	shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. 应识别、文件化和定期评审反映组织信息保护需要的保密性或不泄露协议，并由员工和其他相关方签署。
6.7	Remote working 远程工作	**Control 控制** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises. 当员工远程工作时，应实施安全措施，以保护在组织场所以外所访问的、处理的或存储的信息。
6.8	Information security event reporting 信息安全事态报告	**Control 控制** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. 组织应提供一种机制，使人员能够通过适

		当的渠道及时报告观察到的或可疑的信息安全事态。
7	**Physical controls 物理控制**	
7.1	Physical security perimeters 物理安全边界	**Control 控制** Security perimeters shall be defined and used to protect areas that contain information and other associated assets. 应定义和使用安全边界来保护包信息和其他相关资产的区域。
7.2	Physical entry 物理入口	**Control 控制** Secure areas shall be protected by appropriate entry controls and access points. 安全区域应由适合的入口控制和访问点所保护。
7.3	Securing offices, rooms and facilities 办公室、房间和设施的安全	**Control 控制** Physical security for offices, rooms and facilities shall be designed and implemented. 应为办公室、房间和设施设计并采取物理安全措施。
7.4	Physical	**Control 控制**

	security monitoring 物理安全监视	Premises shall be continuously monitored for unauthorized physical access. 边界应被持续监视，以防止未授权的物理访问。
7.5	Protecting against physical and environmental threats 物理和环境威胁的防护	**Control 控制** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented. 应设计和实施针对物理和环境威胁（例如，自然灾害和对基础设施的其他有意或无意的物理威胁）的保护措施。
7.6	Working in secure areas 在安全区域工作	**Control 控制** Security measures for working in secure areas shall be designed and implemented. 在安全区域工作的安全措施应被设计和被实施。
7.7	Clear desk and clear screen 清空桌面和屏	**Control 控制** Clear desk rules for papers and removable storage media and clear screen rules for

	幕	information processing facilities shall be defined and appropriately enforced. 针对纸质和可移动存储介质的清理桌面策略，以及针对信息处理设施的清理屏幕策略，应被定义和适当执行。
7.8	Equipment siting and protection 设备安置和保护	**Control 控制** Equipment shall be sited securely and protected. 设备应安全的安置和保护。
7.9	Security of assets off-premises 组织场所外的资产安全	**Control 控制** Off-site assets shall be protected. 组织场所外的资产应被保护。
7.10	Storage media 存储介质	**Control 控制** 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. 存储介质应按照组织的分类方案和处理

		要求，对其获取、使用、运输和处置的生命周期进行管理。
7.11	Supporting utilities 支持性设施	Control 控制 Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. 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。
7.12	Cabling security 布缆安全	**Control 控制** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage. 应保护传输电力、数据或支持信息服务的电缆不受拦截、干扰或损坏。
7.13	Equipment maintenance 设备维护	**Control 控制** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. 设备应予以正确地维护,以确保其持续的

		可用性、完整性和信息的保密性。
7.14	Secure disposal or re-use of equipment 设备的安全处置或再利用	**Control 控制** 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. 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**	
8.1	User end point devices 用户终端设备	**Control 控制** Information stored on, processed by or accessible via user end point devices shall be protected. 存储在、由用户终端设备处理或通过用户终端设备访问的信息应受到保护。
8.2	Privileged access rights 特许访问权	**Control 控制** The allocation and use of privileged access rights shall be restricted and managed. 应限制和管理特许访问权的分配和使用。

8.3	Information access restriction 信息访问限制	**Control 控制** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. 应按照建立的访问控制的特定主题策略限制信息和其他关联的资产的访问。
8.4	Access to source code 源代码的访问	**Control 控制** Read and write access to source code, development tools and software libraries shall be appropriately managed. 对源代码、开发工具和软件库的读写访问应得到适当的管理。
8.5	Secure authentication 安全鉴别	**Control 控制** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. 应基于信息安全访问限制和访问控制的特定主题策略，实施安全鉴别技术和规程。
8.6	Capacity	**Control 控制**

	management 容量管理	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements. 应根据当前和预期的容量需求，对资源的使用进行监视和调整。
8.7	Protection against malware 恶意软件防范	**Control 控制** Protection against malware shall be implemented and supported by appropriate user awareness. 恶意软件的防范应被实施，并通过适当的用户意识来支持该过程。
8.8	Management of technical vulnerabilities 技术方面脆弱性的管理	**Control 控制** 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. 应及时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。
8.9	Configuration management	**Control 控制** Configurations, including security

	配置管理	configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed. 硬件、软件、服务和网络的配置(包括安全配置)应被建立文件化的清单，并予以实施、监视和评审。
8.10	Information deletion 信息删除	**Control 控制** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required. 存储在信息系统、设备或任何其他存储介质中的信息，当不再需要时应予以删除。
8.11	Data masking 数据脱敏	**Control 控制** 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. 应根据组织访问控制的特定主题策略和其他相关特定主题的策略，以及业务需

		求，并考虑适用的法律，使用数据脱敏。
8.12	Data leakage prevention 数据泄露防护	Control 控制 Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information. 数据泄露防护措施应应用于处理、存储或传输敏感信息的系统、网络和任何其他设备。
8.13	Information backup 信息备份	**Control 控制** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. 应按照备份的特定主题策略，对信息、软件和系统镜像进行维护，并定期测试。
8.14	Redundancy of information processing facilities 信息处理设施的冗余	**Control 控制** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. 信息处理设施应被实施，并有足够的冗余，以满足可用性要求。

8.15	Logging 日志	**Control 控制** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed. 记录活动、异常、故障和其他相关事件的日志应产生、存储、保护和分析。
8.16	Monitoring activities 监视活动	**Control 控制** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. 应监控网络、系统和应用程序的异常行为，并采取适当行动评估潜在的信息安全事件。
8.17	Clock synchronization 时钟同步	**Control 控制** The clocks of information processing systems used by the organization shall be synchronized to approved time sources. 本机构所使用之资讯处理系统之时钟应与经批准的时间源同步。
8.18	Use of privileged	**Control 控制** The use of utility programs that can be

	utility programs 特权实用程序的使用	capable of overriding system and application controls shall be restricted and tightly controlled. 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。
8.19	Installation of software on operational systems 运行系统的软件安装	**Control 控制** Procedures and measures shall be implemented to securely manage software installation on operational systems. 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	Networks security 网络安全	**Control 控制** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. 应防护、管理和控制网络和网络设备以保护系统和应用中的信息。
8.21	Security of network services	**Control 控制** Security mechanisms, service levels and service requirements of network services

	网络服务的安全	shall be identified, implemented and monitored. 网络服务的安全机制、服务级别和管理要求应予以识别、实施和监视。
8.22	Segregation of networks 网络隔离	**Control 控制** Groups of information services, users and information systems shall be segregated in the organization's networks. 应在组织网络中隔离信息服务、用户及信息系统所使用的网络。
8.23	Web filtering 网页过滤	**Control 控制** Access to external websites shall be managed to reduce exposure to malicious content. 应对外部网站的访问进行管理，以减少暴露于恶意内容。
8.24	Use of cryptography 密码学的使用	**Control 控制** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. 有效使用密码学的规则，包括密钥的管

		理，应被定义，并予以实施。
8.25	Secure development life cycle 安全的开发生命周期	**Control 控制** Rules for the secure development of software and systems shall be established and applied. 软件和系统的安全开发规则应被建立，并予以应用。
8.26	Application security requirements 应用安全要求	**Control 控制** Information security requirements shall be identified, specified and approved when developing or acquiring applications. 当开发或获取应用时，信息安全要求应被识别、规定和批准。
8.27	Secure system architecture and engineering principles 安全系统架构和工程原则	**Control 控制** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities. 应建立和维护文件化的工程安全系统原则，并应用于任何的信息系统开发活动。
8.28	Secure coding	**Control 控制**

	安全编码	Secure coding principles shall be applied to software development. 安全编码原则应被应用于软件开发。
8.29	Security testing in development and acceptance 开发和验收中的安全测试	**Control 控制** Security testing processes shall be defined and implemented in the development life cycle. 在开发生命周期中，安全测试过程应被定义，并予以实施。
8.30	Outsourced development 外包的开发	**Control 控制** The organization shall direct, monitor and review the activities related to outsourced system development. 组织应指导、监视和评审外包的系统开发的相关活动。
8.31	Separation of development, test and production environments 开发、测试和生产环境的分离	**Control 控制** Development, testing and production environments shall be separated and secured. 开发、测试和生产环境应被分离，并予以保护。

8.32	Change management 变更管理	**Control 控制** Changes to information processing facilities and information systems shall be subject to change management procedures. 信息处理设施和信息系统的变更应遵循于变更管理规程。
8.33	Test information 测试信息	**Control 控制** Test information shall be appropriately selected, protected and managed. 测试信息应被适当帅选、保护和管理。
8.34	Protection of information systems during audit testing 审计测试时的信息系统的保护	**Control 控制** Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. 涉及运行系统验证的审计测试和其他保证活动应由测试人员和适当的管理人员策划和商定。