INTERNATIONAL STANDARD

国际标准

ISO 28000

Second edition
第二版
2022-03-15

Security and resilience — Security management systems — Requirements

安全和韧性–安全管理体系–要求

国际标准化组织

Reference number
ISO 28000:2022(E)
编号:ISO 28000

ISO copyright office 国家标准化组织版权处

Ch. de Blandonnet 8 • CP 401

CH-1214 Vernier, Geneva, Switzerland

Tel. +41 22 749 01 11

Fax +41 22 749 09 47

copyright@iso.org

www.iso.org

Contents 目录

Page 页码

Foreword 前言

ISO 28000:2022

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.
国际标准化组织（ISO）是国家标准机构（ISO 成员机构）的全球联盟。ISO 技术委员会通常承担制定国际标准的工作。对已成立技术委员会的课题感兴趣的每个成员机构都有权在该委员会中派出代表。与 ISO 联络的国际组织、政府和非政府组织也可参与这些工作。ISO 与国际电工委员会（IEC)在所有电工标准化领域密切合作。

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).
ISO/IEC 导则第 1 部分中描述了用于制定本标准的程序以及用于进一步保持的程序。特别是，宜注意不同类型的 ISO 文件所需的不同审批标准。本文件是根据 ISO/IEC 导则第 2 部分的编写规定起草的（参阅 www.iso.org/directives）。

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).
请注意，本文件的某些内容可能是专利权的对象。ISO 不负责对识别任何或所有此类专利权。本标准编制中确定的任何专利权的详细信息将显示在引言和（或）收到的 ISO 专利声明列表中（参阅 www.ISO.org/patents）。

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.
本标准中使用的任何商品名称都是为方便使用而提供的信息，不构成对其支持。

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

有关标准的自愿性的解释、与合格评定相关的 ISO 特定术语和措辞的含义，以及有关 ISO 在技术性贸易壁垒(TBT)中遵守世界贸易组织(WTO)原则的信息，参阅 www.iso.org/iso/foreword.html。

This document was prepared by Technical Committee ISO/TC 292, Security and resilience.
本标准由 ISO/TC 292 安全性和韧性技术委员会制定。

This second edition cancels and replaces the first edition (ISO 28000:2007), which has been technically revised, but maintains existing requirements to provide continuity for organizations using the previous edition. The main changes are as follows:
本标准第二版取消并取代了第一版（ISO 28000:2007），第一版已经过技术修订，但保留了为组织提供连续性使用第一版的要求。主要变化如下：

— recommendations on principles have been added in Clause 4 to give better coordination with ISO 31000;
在第 4 章中增加了关于原则的建议，以更好地融入 ISO 31000；

— recommendations have been added in Clause 8 for better consistency with ISO 22301, facilitating integration including:
为了更好地与 ISO 22301 保持相符，在第 8 章中添加了一些建议，以促进整合，包括：

— security strategies, procedures, processes and treatments;
安全策略、程序、流程和处置；

— security plans.
安全计划

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.
关于本标准中的任何反馈或问题都宜提交给用户所在的国家标准机构。这些国家机构的完整列表，请参阅 www.iso.org/members.html。

Introduction 引言

Most organizations are experiencing an increasing uncertainty and volatility in the security environment. As a consequence, they face security issues that impact on their objectives, which they want to address systematically within their management system. A formal approach to security management can contribute directly to the business capability and credibility of the organization.
大多数组织都在安全的环境中经历着越来越多的不确定性和波动性。因此，他们面临着影响其目标的安全问题，希望在管理体系内系统地解决这些问题。正式的安全管理方法可以直接提升组织的业务能力和可信度。

This document specifies requirements for a security management system, including those aspects critical to the security assurance of the supply chain. It requires the organization to:
本标准规定了安全管理系统的要求，包括对保障供应链安全至关重要的要求。要求组织：

— assess the security environment in which it operates including its supply chain (including dependencies and interdependencies);
评估运营的安全环境，包括供应链（包括依赖关系和相互依赖关系）；

— determine if adequate security measures are in place to effectively manage security-related risks;
确定是否有足够的安全措施来有效管理安全相关的风险；

— manage compliance with statutory, regulatory and voluntary obligations to which the organization subscribes;
管理组织对法律法规和自愿义务的遵守情况；

— align security processes and controls, including the relevant upstream and downstream processes and controls of the supply chain to meet the organization's objectives.
调整安全过程和控制措施，包括供应链相关的上游和下游过程和控制措施，以满足组织目标要求。

Security management is linked to many aspects of business management. They include all activities controlled or influenced by organizations, including but not limited to those that impact on the supply chain. All activities, functions and operations should be considered that have an impact on the security management of the organization including (but not limited to) its supply chain.
安全管理与业务管理的许多方面相关联。涵盖了受组织控制或影响的所有活动，包括但不限于影响供应链的活动。宜考虑对组织的安全管理有影响的所有活动、职能和运营活动，包括（但不限于）其供应链。

With regard to the supply chain, it has to be considered that supply chains are dynamic in nature. Therefore, some organizations managing multiple supply chains may look to their providers to

meet related security standards as a condition of being included in that supply chain in order to meet requirements for security management.
关于供应链，必须考虑到其本质上是动态的。因此，一些管理多个供应链的组织可能希望其供应商满足相关安全标准，作为纳入该供应链的条件，以满足安全管理的要求。

This document applies the Plan-Do-Check-Act (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's security management system, see Table 1 and Figure 1.
本标准将计划-实施-检查-处置（PDCA）模型应用于策划、建立、实施、运行、监视、评审、保持和持续改进组织安全管理体系的有效性，参阅表 1 和图 1。

Table 1 — Explanation of the PDCA model
表 1：PDCA 模型的说明

Plan (Establish) 策划 (建立)	Establish security policy, objectives, targets, controls, processes and procedures relevant to improving security in order to deliver results that align with the organization's overall policies and objectives. 建立与提升安全相关的安全方针、目标、指标、控制措施、过程和程序，以实现与组织方针和目标相符的结果。
Do (Implement and operate) 实施 (实施和运行)	Implement and operate the security policy, controls, processes and procedures. 实施和运行安全方针、控制措施、过程和程序。
Check (Monitor and review) 检查 (监视和评审)	Monitor and review performance against security policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement. 根据安全方针和目标，监视和检查绩效，将结果报告给管理层评审，并确定和授权采取补救和改进措施。
Act (Maintain and improve) 处置 (保持和改进)	Maintain and improve the security management system by taking corrective action, based on the results of management review and reappraising the scope of the security management system and security policy and objectives. 根据管理评审的结果，通过采取纠正措施，保持和改进安全管理体系，并重新评估安全管理体系的范围、安全方针和目标。

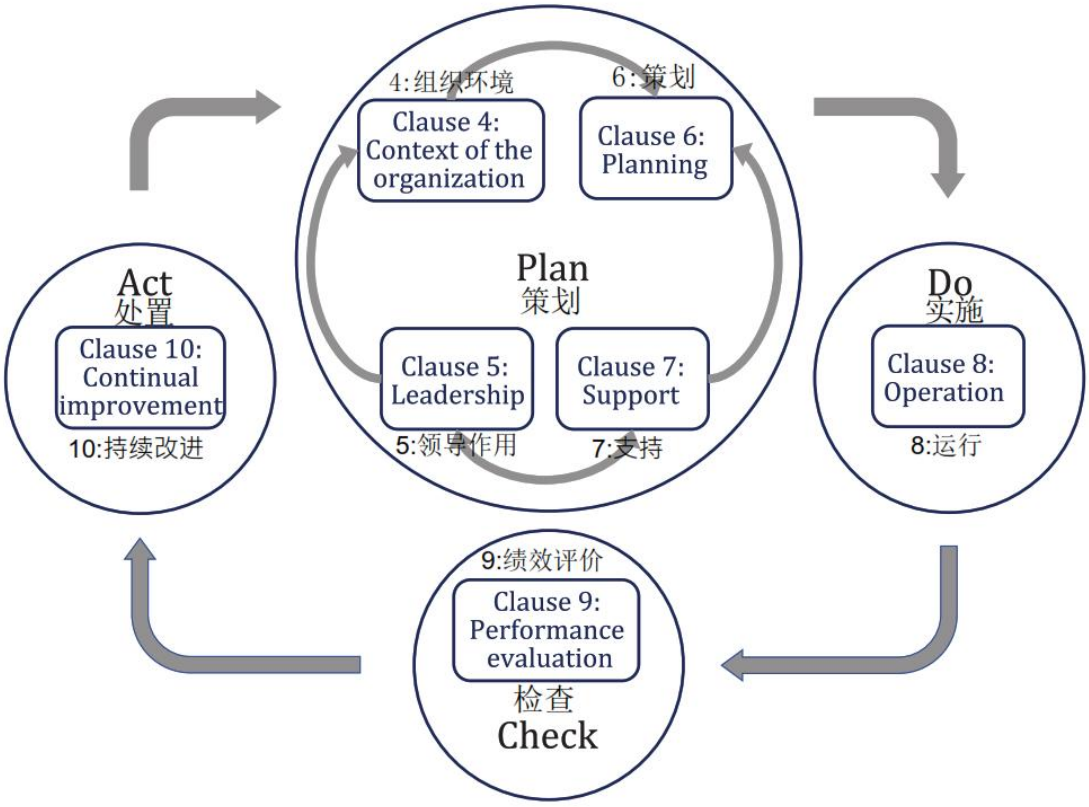

Figure 1 — PDCA model applied to the security management system
图 1：PDCA 模型在安全管理系统中的应用

This ensures a degree of consistency with other management system standards, such as ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001, etc., thereby supporting consistent and integrated implementation and operation with related management systems.
本标准确保与其他管理体系标准在一定程度上的相符性，如 ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001 等，从而支持相关管理体系的相符性和一体化实施和运行。

For organizations that so wish, conformity of the security management system to this document may be verified by an external or internal auditing process.
对于有意愿的组织，可通过外部或内部审核过程验证安全管理体系是否符合本标准。

This page deliberately left blank
此页特意留白

Security and resilience — Security management systems — Requirements
安全和韧性—安全管理体系—要求

1 Scope 范围

This document specifies requirements for a security management system, including aspects relevant to the supply chain.
本标准规定了安全管理体系的要求，包括与供应链相关的要求。

This document is applicable to all types and sizes of organizations (e.g. commercial enterprises, government or other public agencies and non-profit organizations) which intend to establish, implement, maintain and improve a security management system. It provides a holistic and common approach and is not industry or sector specific.
本标准适用于拟建立、实施、保持和改进安全管理体系的所有类型和规模的组织（如商业企业、政府或其他公共机构和非营利组织）。它提供了一种全面和通用的方法，而不是仅适用于特定的行业或部门。

This document can be used throughout the life of the organization and can be applied to any activity, internal or external, at all levels.
本标准可在组织的全生命周期中使用，并且可应用于各层级内部或外部的任何活动。

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.
下列文件中的内容通过文中的规范性引用而构成本标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

ISO 22300, Security and resilience — Vocabulary
ISO 22300，安全和韧性 术语

3 Terms and definitions 术语和定义

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply. ISO and IEC maintain terminological databases for use in standardization at the following addresses:
ISO 22300 定义的术语和定义以及下列术语和定义适用于本标准。ISO 和 IEC 用以下地址保持标准化的术语数据库：

— 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 电子百科：https://www.electropedia.org/

3.1 Organization 组织

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (3.7)
为实现目标(3.7)，由职责、权限和相互关系构成自身功能的一个人或一组人。
Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.
注 1：组织包括但不限于个体经营者、公司、集团、商行、企事业单位、行政管理机构、合伙制企业、慈善机构或社会机构，或者上述组织的某部分或其组合，无论是否为法人组织、公有或私有。
Note 2 to entry: If the organization is part of a larger entity, the term “organization” refers only to the part of the larger entity that is within the scope of the security management system (3.5).
注 2：如果组织是较大实体的一部分，则“组织”一词仅指较大实体中在全管理体系（3.5）范围内的部分。

3.2 Interested party (preferred term) 相关方（首选术语）
stakeholder (admitted term) 利益相关方（许用术语）

person or organization (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity
interested party
可影响决策或活动、受决策或活动所影响，或者自认为受决策或活动影响的个人或组织（3.1）。

3.3 Top management 最高管理者

person or group of people who directs and controls an organization (3.1) at the highest level
在最高层指挥和控制组织（3.1）的一个人或一组人。
Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.
注 1：最高管理者有权在组织内授权和提供资源。
Note 2 to entry: If the scope of the management system (3.4) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

注 2：若管理体系（3.4）的范围仅覆盖组织的一部分，则最高管理者是指那些指挥和控制该部分的人员。

3.4 Management system 管理体系

set of interrelated or interacting elements of an organization (3.1) to establish policies (3.6) and objectives (3.7), as well as processes (3.9) to achieve those objectives

组织（3.1）用于建立方针（3.6）和目标（3.7）以及实现这些目标的过程（3.9）的一组相互关联或相互作用的要素。

Note 1 to entry: A management system can address a single discipline or several disciplines.

注 1：一个管理体系可针对单个或多个领域。

Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning and operation.

注 2：体系要素包括组织的结构、角色和职责、策划和运行。

3.5 Security management system 安全管理体系

system of coordinated policies (3.6), processes (3.9) and practices through which an organization manages its security objectives (3.7)

组织通过协调方针（3.6）、过程(3.9)和实践系统管理其安全目标（3.7）的体系。

3.6 Policy 方针

intentions and direction of an organization (3.1) as formally expressed by its top management (3.3)

由组织最高管理者(3.3)正式表述的组织(3.1)宗旨和方向。

3.7 Objective 目标

result to be achieved

要实现的结果

Note 1 to entry: An objective can be strategic, tactical, or operational.

注 1：目标可以是战略性的、战术性的或运行层面的

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide or specific to a project, product and process (3.9).

注 2：目标可涉及不同领域（如财务的、健康安全的和环境）。例如它们可以是组织范围的或特定的项目、产品和过程（3.9）。

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, as a purpose, as an operational criterion, as a security objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

注 3：目标可按其他方式来表述，例如：按预期结果、宗旨、运行准则来表述目标；按某安全目标或使用其它近义词（如目的、重点和标的等）来表述目标。

Note 4 to entry: In the context of security management systems (3.5), security objectives are set by the organization (3.1), consistent with the security policy (3.6), to achieve specific results.

注 4：在安全管理体系（3.5）的背景下，为实现与安全方针（3.6）相符的特定结果由组织（3.1）制定的安全目标。

3.8 Risk 风险

effect of uncertainty on objectives (3.7)

不确定性对目标(3.7)的影响

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

注 1：影响是指对预期的偏离。它可以是积极的、消极的或两者兼有，可以处理、创造或产生机会和威胁。

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

注 2：目标可以有不同的方面和类别，可以应用在不同的层次上。

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

注 2：风险通常表现为风险来源、潜在事件、其后果和可能性。

3.9 Process 过程

set of interrelated or interacting activities that uses or transforms inputs to deliver a result

将输入变成或转化为输出的一系列相互关联或相互作用的实现目标的活动。

Note 1 to entry: Whether the result of a process is called an output, a product or a service depends on the context of the reference.

注 1：过程的结果称为输出、产品还是服务取决于环境。

3.10 Competence 能力

ability to apply knowledge and skills to achieve intended results

运用知识和技能实现预期结果的本领。

3.11 Documented information 成文信息

information required to be controlled and maintained by an organization (3.1) and the medium on which it is contained

组织(3.1)需要控制并保持的信息及其载体。

Note 1 to entry: Documented information can be in any format and media, and from any source.

注 1：成文信息可以任何形式和载体存在，并可来自任何来源。

Note 2 to entry: Documented information can refer to:

注 2：成文信息可涉及：

— the management system (3.4), including related processes (3.9);
管理体系(3.4)，包括相关过程(3.9)；

— information created in order for the organization to operate (documentation);
为组织运行而创建的信息（文件）；

— evidence of results achieved (records).
结果实现的证据（记录）。

3.12 Performance 绩效

measurable result 可测量的结果

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

注 1：绩效可能涉及定量或定性的结果。

Note 2 to entry: Performance can relate to managing activities, processes (3.9), products, services, systems or organizations (3.1).

注 2：绩效可能涉及活动、过程(3.9)、产品、服务、体系或组织(3.1)的管理。

3.13 Continual improvement 持续改进

recurring activity to enhance performance (3.12)

提高绩效(3.12)的循环活动。

3.14 Effectiveness 有效性

extent to which planned activities are realized and planned results are achieved

完成策划的活动并得到策划结果的程度。

3.15 Requirement 要求

need or expectation that is stated, generally implied or obligatory

明示的、通常隐含的或必须满足的需求或期望。

Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization (3.1) and interested parties (3.2) that the need or expectation under consideration is implied.

注 1："通常隐含的"是指，对组织(3.1)和相关方(3.2)而言，按惯例或常见做法，对这些需求或期望加以考虑是不言而喻的。

Note 2 to entry: A specified requirement is one that is stated, e.g. in documented information (3.11).

注 2：规定的要求是指经明示的要求，如成文信息(3.11)中所阐明的要求。

3.16 Conformity 符合

fulfilment of a requirement (3.15)

满足要求(3.15)

3.17 Nonconformity 不符合

non-fulfilment of a requirement (3.15)
未满足要求(3.15)

3.18 Corrective action 纠正措施

action to eliminate the cause(s) of a nonconformity (3.17) and to prevent recurrence
为消除不符合（3.17）的原因并防止再次发生而采取的措施。

3.19 Audit 审核

systematic and independent process (3.9) for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled
为获得审核证据并对其进行客观评价，以确定满足审核准则的程度所进行的系统的和独立的过程(3.9)

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).
注 1：审核可以是内部（第一方）审核或外部（第二方或第三方）审核，也可以是一种结合（结合两个或多个领域）的审核。

Note 2 to entry: An internal audit is conducted by the organization (3.1) itself, or by an external party on its behalf.
注 2：内部审核由组织（3.1）自行实施或由外部方代表其实施。

Note 3 to entry: “Audit evidence” and “audit criteria” are defined in ISO 19011.
注 3：“审核证据”和“审核准则”的定义见 ISO 19011。

3.20 Measurement 测量

process(3.9) to determine a value
确定值的过程(3.9)。

3.21 Monitoring 监视

determining the status of a system, a process (3.9) or an activity
确定体系、过程(3.9)或活动的状态。

Note 1 to entry: To determine the status, there can be a need to check, supervise or critically observe.
注 1：为了确定状态，可能需要检查、监督或批判地观察。

4 Context of the organization 组织环境

4.1 Understanding the organization and its context 理解组织和组织环境

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its security management system including the requirements of its supply chain.
组织应确定与其宗旨相关并影响其实现安全管理体系预期结果的能力的内部和外部议题，包括其供应链的要求。

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

4.2.1 General 总则

The organization shall determine:
组织应确定：

— the interested parties that are relevant to the security management system;
与安全管理体系有关的相关方

— the relevant requirements of these interested parties;
相关方的要求

— which of these requirements will be addressed through the security management system.
通过安全管理体系应对这些要求

4.2.2 Legal, regulatory and other requirements 法律法规和其他要求

The organization shall:
组织应：

a) implement and maintain a process to identify, have access to and assess the applicable legal, regulatory and other requirements related to its security;
实施和保持过程以识别、获取和评估与安全相关适用的法律、法规和其他要求；

b) ensure that these applicable legal, regulatory and other requirements are taken into account in implementing and maintaining its security management system;
确保在实施和保持安全管理体系时考虑到这些适用的法律、法规和其他要求；

c) document this information and keep it up to date;
将这些信息形成文件并保持更新；

d) communicate this information to relevant interested parties as appropriate.
适当时，将此信息传达给有关的相关方。

4.2.3 Principles 原则

4.2.3.1 General 总则

The purpose of security management within the organization is the creation and, in particular, the protection of value.
组织安全管理的目的是创造价值，特别是保护价值。

The organization should apply the principles given in Figure 2 and described in 4.2.3.2 to 4.2.3.9.
组织宜应用图 2 和 4.2.3.2 至 4.2.3.9 中描述的原则。

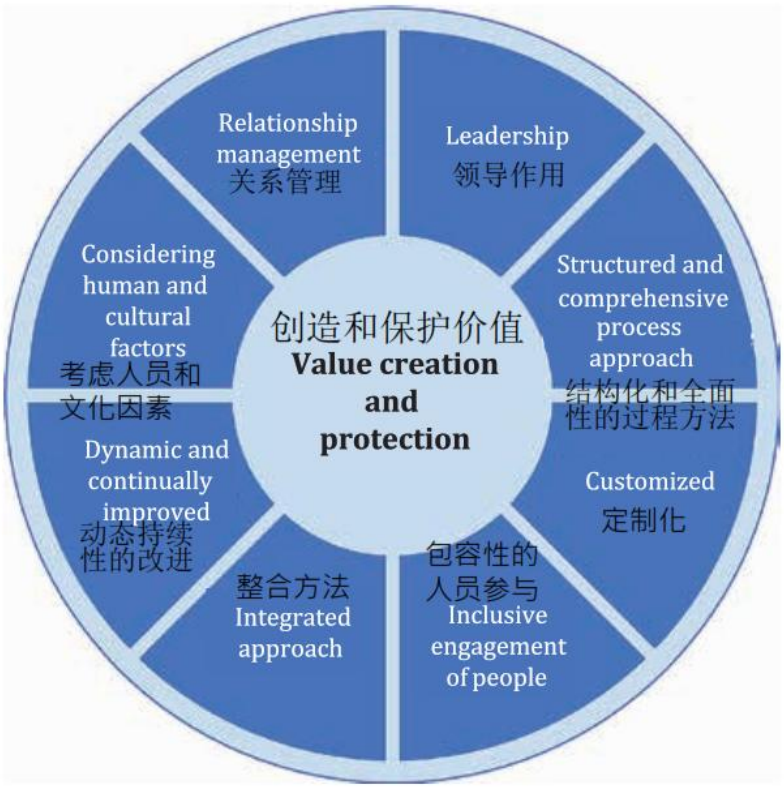

Figure 2 — Principles
图 2：原则

4.2.3.2 Leadership 领导作用

Leaders at all levels should establish unity of purpose and direction. They should create conditions to align the organization's strategies, policies processes and resources to achieve its objectives. Clause 5 explains the requirements with regard to this principle.
各级领导宜统一宗旨和方向。宜创造条件，调整组织的战略、方针、过程和资源以实现组织目标。第 5 章解释了与该原则有关的要求。

4.2.3.3 Structured and comprehensive process approach based on best available information 基于最佳有效信息的结构化和全面性的过程方法

A structured and comprehensive approach to security management including the supply chain should contribute to consistent and comparable results, which are achieved more effectively and efficiently when activities are understood and managed as interrelated processes functioning as a coherent system.
包括供应链在内的结构化和全面性的安全管理方法宜有助于产生一致的和可比较的结果，当活动被理解和管理为一个连贯系统运行的相互关联的过程时，可以更有效和更高效地实现这些结果。

4.2.3.4 Customized 定制化

The security management system should be customized and proportionate to the organization's external and internal context and needs. It should be related to its objectives.
安全管理系统宜是个性化的，并与组织的外部和内部环境和需求相符。宜与目标相关。

4.2.3.5 Inclusive engagement of people 包容性的人员参与

The organization should involve interested parties appropriately and in a timely manner. It should consider their knowledge, views and perceptions appropriately to improve awareness of and facilitate informed security management. The organization should ensure that everybody at all levels is respected and involved.
组织宜适当及时地引入相关方参与，宜适当考虑他们的知识、观点和看法，以提高对安全管理体系的认知，并促进其熟悉安全管理体系。组织宜确保各级人员都受到尊重和参与。

4.2.3.6 Integrated approach 整合方法

Security management is an integral part of all organizational activities. It should be integrated with all other management systems of the organization.
安全管理是所有组织活动的组成部分。宜与组织的所有其他管理系统相融合。

The organization's risk management – whether formal, informal or intuitive – should be integrated into the security management system.
组织的风险管理，无论是正式的、非正式的还是直觉的，都宜融入到安全管理系统中。

4.2.3.7 Dynamic and continually improved 动态持续性的改进

The organization should have an ongoing focus on improvement through learning and experience to maintain the level of performance, to react to changes and to create new opportunities as the external and internal context of the organization changes.
组织宜通过学习和经验不断关注改进安全管理体系，以保持绩效水平，对变化做出反应，并随着组织的外部和内部环境的变化创造新的机会。

4.2.3.8 Considering human and cultural factors 考虑人员和文化因素

Human behaviour and culture significantly influence all aspects of security management and should be considered at each level and stage. Decisions should be based on the analysis and evaluation of data and information to ensure they result in greater objectivity, confidence in decision-making and are more likely to produce desired results. Individual perceptions should be considered.
人员行为和文化对安全管理的各个方面都有重大影响，宜在每个层级和阶段加以考虑。决策宜基于对数据和信息的分析和评估，以确保其更具客观性，对决策更有信心，更有可能产生预期结果。宜考虑个人观点。

4.2.3.9 Relationship management 关系管理

For sustained success, the organization should manage its relationships with all relevant interested parties as they might influence the performance of the organization.
为了持续成功，组织宜管理与所有有关相关方的关系，因为它们可能会影响组织的绩效。

4.3 Determining the scope of the security management system 确定组织安全管理体系的范围

The organization shall determine the boundaries and applicability of the security management system to establish its scope.
组织应界定安全管理体系的边界和适用性以确定其范围。

When determining this scope, the organization shall consider:
在确定范围时，组织应考虑：

— the external and internal issues referred to in 4.1;
4.1 中所提及的内部和外部议题

— the requirements referred to in 4.2.
4.2 中所提及的要求

The scope shall be available as documented information.
该范围应为可获得的成文信息。

Where an organization chooses to have any process that affects conformity with its security management system externally provided, the organization shall ensure that such processes are controlled. The necessary controls for and responsibilities of such externally provided processes shall be identified within the security management system.
如果组织选择外部提供的任何影响安全管理体系符合性的过程，应确保这些过程得到控制。应在安全管理体系中确定此类外部提供过程的必要控制措施和责任。

4.4 Security management system 安全管理体系

The organization shall establish, implement, maintain and continually improve a security management system, including the processes needed and their interactions, in accordance with the requirements of this document.
组织应按照本标准的要求，建立、实施、保持和持续改进安全管理体系，包括所需的过程及过程间相互作用。

5 Leadership 领导作用

5.1 Leadership and commitment 领导作用和承诺

Top management shall demonstrate leadership and commitment with respect to the security management system by:
最高管理者应通过以下方式证实在安全管理体系方面的领导作用和承诺：

— ensuring that the security policy and security objectives are established and are compatible with the strategic direction of the organization;
确保安全方针和目标得以建立，并与组织战略方向相符；

— ensuring that the requirements and expectations of the organization's interested parties are identified and monitored, and appropriate timely action is taken to manage these expectations to ensure the integration of the security management system requirements into the organization's business processes;
确保识别和监视组织相关方的要求和期望，并及时采取适当的措施来管理这些期望，以确保将安全管理体系要求融入到组织的业务过程；

— ensuring the integration of the security management system requirements into the organization's business processes;
确保安全管理体系要求融入组织业务过程；

— ensuring that the resources needed for the security management system are available;
确保可获得安全管理体系所需的资源；

— communicating the importance of effective security management and of conforming to the security management system requirements;
就安全管理的有效性和符合安全管理体系要求的重要性进行沟通；
— ensuring that the security management system achieves its intended result(s);
确保安全管理体系实现预期结果；
— ensuring the viability of the security management objectives, targets and programmes;
确保安全管理目标、指标和方案的可行性；
— ensuring any security programmes generated from other parts of the organization complement the security management system;
确保从组织的其他部分获取的任何安全方案能改进安全管理体系；
— directing and supporting persons to contribute to the effectiveness of the security management system;
指导和支持人员为安全管理体系的有效性做出贡献；
— promoting continual improvement of the organization's security management system;
促进持续改进安全管理体系；
— supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.
支持其他相关角色展示在职责领域内的领导作用；

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：本标准所提及的"业务"可从广义上理解为涉及组织存在目的至关重要的活动。

5.2 Security policy 安全方针

5.2.1 Establishing the security policy 建立安全方针

Top management shall establish a security policy that:
最高管理者应建立安全方针，该方针应：
a) is appropriate to the purpose of the organization;
符合组织的宗旨；
b) provides a framework for setting security objectives;
为制定安全目标提供框架；
c) includes a commitment to meet applicable requirements;
包括满足适用要求的承诺；
d) includes a commitment to continual improvement of the security management system;
包括持续改进安全管理体系的承诺；

e) considers the adverse impact that the security policy, objectives, targets, programmes, etc. can have on other aspects of the organization.

考虑安全方针、目标、指标、方案等对组织其他活动产生的不利影响。

5.2.2 Security policy requirements 安全方针的要求

The security policy shall:

安全方针应：

— be consistent with other organizational policies;
与组织的其他方针相符；

— be consistent with the organization's overall security risk assessment;
符合组织的整体安全风险评估；

— provide for its review in case of the acquisition of, or a merger with, other organizations, or other changes to the business scope of the organization which could affect the continuity or relevance of the security management system;
在收购或合并其他组织或该组织的业务范围发生可能影响安全管理体系的连续性或相关性的其他变化时进行评审；

— describe and allocate primary accountability and responsibility for outcomes;
描述和分配主要职责和为结果担责；

— be available as documented information;
作为成文信息而可被获取；

— be communicated within the organization;
在组织内予以沟通；

— be available to interested parties, as appropriate.
适当时，可为相关方所获取。

NOTE Organizations can choose to have a detailed security management policy for internal use which would provide sufficient information and direction to drive the security management system (parts of which can be confidential) and have a summarized (non-confidential) version containing the broad objectives for dissemination to their interested parties.

注：组织可选择制定详细的内部安全管理方针，以便提供充足的信息和指示，从而推动安全管理体系（部门内容可能为机密信息），并制定包含如下信息的简述版本（非机密信息）：向其他相关方传播的广义目标。

5.3 Roles, responsibilities and authorities 岗位、职责和权限

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

最高管理者应确保组织相关角色的职责、权限得到分配和沟通。

Top management shall assign the responsibility and authority for:
最高管理者应分配职责和权限以：

a) ensuring that the security management system conforms to the requirements of this document;
确保安全管理体系符合本标准的要求；

b) reporting on the performance of the security management system to top management.
向最高管理者报告安全管理体系的绩效。

6 Planning 策划

6.1 Actions to address risks and opportunities 应对风险和机遇的措施

6.1.1 General 总则

When planning for the 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:
在策划安全管理体系时，组织应考虑 4.1 所提及的议题和 4.2 所提及的要求，并确定所需应对的风险和机遇，以

— give assurance that the security management system can achieve its intended result(s);
确保安全管理体系实现预期结果；

— prevent, or reduce, undesired effects;
防止或减少不期望的影响；

— achieve continual improvement.
实现持续改进。

The organization shall plan:
组织应策划：

a) actions to address these risks and opportunities;
应对这些风险和机遇的措施；

b) how to:
如何：

— integrate and implement the actions into its security management system processes;
在安全管理体系过程中整合并实施这些措施；

— evaluate the effectiveness of these actions.
评估措施的有效性。

The purpose of managing risks is the creation and protection of value. Managing risk shall be integrated into the security management system. Risks related to the security of the organization and its interested parties are addressed in 8.3.
管理风险的目的是创造并保护价值。风险管理应融入安全管理体系。与组织及其相关方应对的安全相关的风险见 8.3 。

6.1.2 Determining security-related risks and identifying opportunities 确定安全相关的风险和识别机会

Determining security-related risks and identifying and exploiting opportunities requires a proactive risk assessment which shall include consideration of, but not be limited to:
确定安全相关风险，识别和利用机会需要积极主动的进行风险评估，其中应包括但不限于：

a) physical or functional failures and malicious or criminal acts;
物理或功能故障以及恶意或犯罪行为；

b) environmental, human and cultural factors and other internal or external contexts, including factors outside the organization's control affecting the organization's security;
环境、人员和文化因素及其他内部或外部环境，包括组织无法控制的影响安全的因素；

c) the design, installation, maintenance and replacement of security equipment;
设计、安装、维护和更换安保设备；

d) the organization's information, data, knowledge and communication management;
组织的信息、数据、知识和沟通管理；

e) information related to security threats and vulnerabilities;
相关安全威胁和漏洞的信息；

f) the interdependencies between suppliers.
供应商间的相互依赖关系。

6.1.3 Addressing security-related risks and exploiting opportunities 应对安全相关的风险并利用机会

The evaluation of the identified security-related risk shall provide input to (but not be limited to):
对已识别的安全相关风险的评估应提供输入（但不限于）：

a) the organization's overall risk management;
组织整体的风险管理；

b) risk treatment;
风险处置；

c) security management objectives;

安全管理目标；

d) security management processes;
安全管理过程；

e) the design, specification and implementation of the security management system;
安全管理体系的设计、规范和实施；

f) the identification of adequate resources including staffing;
确定充足的资源，包括人员的配备；

g) the identification of training needs and the required level of competence.
确定培训需求和所需的能力水平。

6.2 Security objectives and planning to achieve them 安全目标及其实现的策划

6.2.1 Establishing security objectives 制定安全目标

The organization shall establish security objectives at relevant functions and levels. The security objectives shall:
组织应在相关职能和层级上制定安全目标。安全目标应：

a) be consistent with the security policy;
与安全方针相符；

b) be measurable (if practicable);
测量（可行时）；

c) take into account applicable requirements;
考虑适用的要求

d) be monitored;
得到监视

e) be communicated;
予以沟通；

f) be updated as appropriate;
适当时予以更新。

g) be available as documented information.
作为可获得的成文信息。

6.2.2 Determining security objectives 确定安全目标

When planning how to achieve its security objectives, the organization shall determine:
策划如何实现安全目标时，组织应确定：

— what will be done;
要做什么；

— what resources will be required;
所需资源；
— who will be responsible;
由谁负责；
— when it will be completed;
何时完成；
— how the results will be evaluated.
如何评价结果；

When establishing and reviewing its security objectives, an organization shall take into account:
在制定和评审安全目标时，组织应考虑：

a) technological, human, administrative and other options;
技术、人力、管理和其他选项；
b) views of and impacts on appropriate interested parties.
适用的相关方的观点和影响。

The security objectives shall be consistent with the organization's commitment to continual improvement.
安全目标应与组织对持续改进的承诺相符。

6.3 Planning of changes 变更的策划

When the organization determines the need for changes to the security management system, including those identified in Clause 10, the changes shall be carried out in a planned manner.
当组织确定对其安全管理体系变更时，包括第 10 章识别的变更，变更应按所策划的方式实施。

The organization shall consider:
组织应考虑：

a) the purpose of the changes and their potential consequences;
变更目的及其潜在后果；
b) the integrity of the security management system;
安全管理体系的完整性；
c) the availability of resources;
资源的可获得性；
d) the allocation or reallocation of responsibilities and authorities.
职责和权限的分配和再分配。

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 security management system.
组织应确定并提供建立、实施、保持和持续改进安全管理体系所需资源。

7.2 Competence 能力

The organization shall:
组织应：

— determine the necessary competence of person(s) doing work under its control that affects its security performance;
根据对安全绩效的影响，确定其管理下的工作人员应具备的必要能力；

— ensure that these persons are competent on the basis of appropriate education, training, or experience and are appropriately security cleared;
确保人员在适当的教育、培训或实践经验的基础上具备胜任工作的能力和通过了适当的安全审查；

— where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;
在适用时，采取措施以获得必备的能力，并评价措施的有效性；

Appropriate documented information shall be available as evidence of competence.
应提供适当的成文信息作为人员能力的证据。

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of currently employed persons; or the hiring or contracting of competent persons.
注：适用措施可包括：向现有所雇人员提供培训、辅导或重新分配工作；或聘用、外包能胜任工作的人员等。

7.3 Awareness 意识

Persons doing work under the organization's control shall be aware of:
组织应确保在其控制下的工作人员了解：

— the security policy;
安全方针；

— their contribution to the effectiveness of the security management system, including the benefits of improved security performance;

对安全管理体系有效性的贡献，包括提升安全绩效的益处；

— the implications of not conforming with the security management system requirements;
不符合安全管理体系要求的后果；

— their roles and responsibilities in achieving compliance with the security management policy and procedures and with the requirements of the security management system, including emergency preparedness and response requirements.
在遵守安全管理方针和程序以及安全管理体系要求方面的角色和职责，包括应急准备和响应要求。

7.4 Communication 沟通

The organization shall determine the internal and external communications relevant to the security management system, including:
组织应确定与安全管理体系有关的内外部沟通，包括：

— on what it will communicate;
沟通什么；

— when to communicate;
何时沟通；

— with whom to communicate;
与谁沟通；

— how to communicate;
如何沟通；

— the sensitivity of information prior to dissemination.
信息传播前的敏感性。

7.5 Documented information 成文信息

7.5.1 General 总则

The organization's security management system shall include:
组织的安全管理体系应包括：

a) documented information required by this document;
本标准要求的成文信息；

b) documented information determined by the organization as being necessary for the effectiveness of the security management system.
由组织确定的为实现安全管理体系绩效而必需的成文信息

The documented information shall describe the responsibilities and authorities for achieving security management objectives and targets, including the means and timelines to achieve those objectives and targets.
成文信息应描述实现安全管理目标和指标的责任和权限，包括实现这些目标和指标的手段和时间表。

NOTE The extent of documented information for a security management system can differ from one organization to another due to:
注：对于不同组织，安全管理体系成文信息的程度可以不同，取决于：

— the size of organization and its type of activities, processes, products and services;
组织的规模及其活动、过程、产品和服务的类型；
— the complexity of processes and their interactions;
过程及其相互作用的复杂程度；
— the competence of persons.
人员的能力。

The organization shall determine the value of information, and establish the level of integrity required and the security controls to prevent unauthorized access.
组织应确定信息的价值，并建立所需的完整性等级和安全控制，以防止非授权访问。

7.5.2 Creating and updating documented information 创建和更新信息

When creating and updating documented information, the organization shall ensure appropriate:
创建和更新成文信息时，组织应确保适当的：

— identification and description (e.g. a title, date, author, or reference number);
标识和说明（如标题、日期、作者或索引编号）；
— format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
形式（如语言文字、软件版本、图表）与载体（如纸质的、电子的）；
— review and approval for suitability and adequacy.
评审和批准，以确保适宜性和充分性。

7.5.3 Control of documented information 成文信息的控制

Documented information required by the security management system and by this document shall be controlled to ensure:
安全管理体系和本标准所要求的成文信息应予以控制，以确保：

a) it is available and suitable for use, where and when it is needed;
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);
予以妥善保护（如防止泄密、不当使用或缺失）。

c) it is periodically reviewed and revised as necessary, and approved for adequacy by authorized personnel;
必要时定期评审和修订，并由授权人员批准其充分性；

d) obsolete documents, data and information are promptly removed from all points of issue and points of use, or otherwise assured against unintended use;
及时从所有已发布和已使用的地方删除过时的文件、数据和信息，或以其他方式确保这些成文信息不会被使用；

e) archival documents, data and information retained for legal or knowledge preservation purposes or both are suitably identified.
适当识别为满足法律要求或知识存储而保留的档案文件、数据和信息。

For the control of documented information, the organization shall address the following activities, as applicable:
为控制成文信息，适用时，组织应关注下列活动

— distribution, access, retrieval and use;
分发、访问、检索和使用；

— storage and preservation, including preservation of legibility;
存储和防护，包括保持可读性；

— control of changes (e.g. version control);
变更控制（如版本控制）；

— retention and disposition.
保留和处置。

Documented information of external origin determined by the organization to be necessary for the planning and operation of the security management system shall be identified, as appropriate, and controlled.
对于组织确定的策划和运行安全管理体系所必需的来自外部的成文信息，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.
注：对成文信息的访问可能意味着仅允许查阅，或允许查阅并授权修改。

8 Operation 运行

8.1 Operational planning and control 运行的策划和控制

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:
为满足要求和实施第 6 章所确定的措施，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.
为了确信过程按策划进行，在必要的范围内应可获取成文信息。

8.2 Identification of processes and activities 确定过程和活动

The organization shall identify those processes and activities that are necessary for achieving:
组织应确定实现以下目标所需的过程和活动：

a) compliance with its security policy;
遵守安全方针；

b) compliance with legal, statutory and regulatory security requirements;
遵守法律、法规和安全监管的要求；

c) its security management objectives;
安全管理目标；

d) the delivery of its security management system;
交付安全管理系统；

e) the required level of security of the supply chain.
供应链所需的安全级别。

8.3 Risk assessment and treatment 风险评估和处置

The organization shall implement and maintain a risk assessment and treatment process.
组织应实施并保持风险评估和处置的流程。

NOTE The process for risk assessment and treatment is addressed in ISO 31000.
注：ISO 31000 中阐述了风险评估和处置流程。

The organization should:
组织宜

a) identify its security-related risks, prioritizing them to the resources required for its security management;
识别安全相关的风险，按安全管理所需的资源排序；

b) analyse and evaluate the identified risks;
分析和评估识别的风险；

c) determine which risks require treatment;
确定哪些风险需要处置；

d) select and implement options to address those risks;
选择并实施处理这些风险的方案；

e) prepare and implement risk treatment plans.
制定和实施处置风险的计划。

NOTE Risks in this subclause relate to the security of the organization and its interested parties. Risks and opportunities related to the effectiveness of the management system are addressed in 6.1.
注：本条款中的风险与组织及其相关方的安全有关。与管理体系有效性相关的风险和机遇见 6.1。

8.4 Controls 控制措施

The processes listed in 8.2 shall include controls for human resource management, as well as the design, installation, operation, refurbishment and modification of security-related items of equipment, instrumentation and information technology, as appropriate. Where existing arrangements are revised or new arrangements introduced that could have impact on security management, the organization shall consider the associated security-related risks before their implementation. The new or revised arrangements to be considered shall include:
8.2 中列出的过程应包括对人力资源管理的控制措施及适用的设备、器械和信息技术的安全相关项目的设计、安装、运行、改造和改良。如果在改进现有布局或引入新布局时可能对安全管理产生影响，组织应在实施前考虑相关的安全风险。有待考虑的新的或改进后的布局应包括：

a) revised organizational structure, roles or responsibilities;
改进后的组织结构、角色或职责；

b) training, awareness and human resource management;
培训、意识和人力资源管理；

c) revised security management policy, objectives, targets or programmes;
改进后安全管理的方针、目标、指标或方案；

d) revised processes and procedures;
改进后的过程和程序；

e) the introduction of new infrastructure, security equipment or technology, which may include hardware and/or software;
引入新的基础设施、安全设备或技术，可包括硬件和（或）软件；

f) the introduction of new contractors, suppliers or personnel, as appropriate;
根据具体情况引入新承包商、供应商或人员；

g) the requirements for security assurance of external suppliers.
外部供应商的安全保证要求。

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.
组织应控制计划的变更并评审非预期变更的后果，必要时采取措施减轻任何不利影响。

The organization shall ensure that externally provided processes, products or services that are relevant to the security management system are controlled.
组织应确保与安全管理体系相关的外部提供的过程、产品或服务受到控制。

8.5 Security strategies, procedures, processes and treatments 安全策略、程序、流程和处置

8.5.1 Identification and selection of strategies and treatments 策略和处置的识别和选择

The organization should implement and maintain systematic processes for analysing vulnerabilities and threats related to security. Based on this vulnerability and threat analysis and consequent risk assessment, the organization should identify and select a security strategy which comprises one or more procedures, processes and treatments.
组织宜实施和保持系统流程以分析安全相关的漏洞和威胁。基于此漏洞和威胁的分析和风险评估的结果，组织宜识别和选择包括一个或多个程序、流程和处置的安全策略。

Identification should be based on the extent to which strategies, procedures, processes and treatments:
识别策略和处置宜基于以下策略、程序、流程和处置的程度：

a) maintain the organization's security;
维护组织的安全；

b) reduce the likelihood of security vulnerability;
降低出现安全漏洞的可能性；

c) reduce the likelihood of a threat being actualised;
降低威胁发生的可能性；

d) shorten the period of any security treatment deficiencies and limit their impact;
缩短任何安全处理缺陷的期限并限制影响；

e) provide for the availability of adequate resources.
提供充足的资源。

Selection should be based on the extent to which strategies, processes and treatments:
选择策略和处置宜基于以下策略、流程和处置的程度：

— meet the requirements to protect the organization's security;
满足保护组织安全的要求；
— consider the amount and type of risk the organization may or may not take;
考虑组织可能承担或不承担的风险的数量和类型；
— consider the associated costs and benefits.
考虑相关成本和收益。

8.5.2 Resource requirements 所需要求

The organization shall determine the resource requirements to implement the selected security procedures, processes and treatments.
组织应确定资源要求以实施选定的安全程序、过程和处置。

8.5.3 Implementation of treatments 处置的实施

The organization shall implement and maintain selected security treatments.
组织应实施和保持选定的安全处置。

8.6 Security plans 安全计划

8.6.1 General 总则

The organization shall establish and document security plans and procedures based on the selected strategies and treatments. The organization shall implement and maintain a response structure that will enable timely and effective warning and communication of vulnerabilities related to security and imminent security threats or ongoing security violations to relevant interested parties. The response structure shall provide plans and procedures to manage the organization during an imminent security threat or an ongoing security violation.
组织应基于选定的策略和处置制定和记录安全计划和程序。组织应实施并保持响应机制以便及时有效地预警和沟通有关相关方安全和迫在眉睫的安全威胁或正在进行的安全违规事件的漏洞。响应机制应提供计划和程序以管理组织迫在眉睫的安全威胁或持续的安全违规事件。

8.6.2 Response structure 响应机制

The organization shall implement and maintain a structure, identifying a designated person or one or more teams responsible for responding to vulnerabilities and threats related to security. The roles and responsibilities for the designated person or each team and the relationship between the person or teams shall be clearly identified, communicated and documented.
组织应实施和维持一个机制，确定负责指定人员或一个或多个团队应对安全漏洞和威胁。应明确确定、沟通和记录指定人员或每个团队的角色和责任以及人员或团队之间的关系。

Collectively, the teams should be competent to:
总体而言，这些团队宜具备以下能力：

a) assess the nature and extent of a security threat and its potential impact;
评估安全威胁的性质和程度及其潜在影响；

b) assess the impact against pre-defined thresholds that justify initiation of a formal response;
根据预先定义的阈值评估影响，以证明启动正式响应是合理的；

c) activate an appropriate security response;
启动适当的安全响应；

d) plan actions that need to be undertaken;
策划需要采取的措施；

e) establish priorities using life safety as the first priority;
以生命安全至上，确定优先事项；

f) monitor the effects of any variation in vulnerabilities related to security, changes to the intent and capability of threat actors or security violations and the organization's response;
监视与安全相关漏洞的任何变化影响、产生威胁的人员意图和能力的变化或安全违规事件以及组织的响应；

g) activate the security treatments;
启动安全处置；

h) communicate with relevant interested parties, authorities and the media;
与有关相关方、行政机构和媒体进行沟通；

i) contribute to a communication plan with communication management.
为沟通管理中的沟通计划做出贡献。

For each designated person or team there should be:
每个指定人员或团队宜有：

— identified staff, including alternates with the necessary responsibility, authority and competence to perform their designated role;
确定包括具有履行指定角色所需的责任、权限和能力的候补人员在内的员工；

— documented procedures to guide their actions including those for the activation, operation, coordination and communication of the response.

指导行动的文件化程序，包括响应机制的启动、运行、协调和沟通。

8.6.3 Warning and communication 预警和沟通

The organization should document and maintain procedures for:

组织宜文件化并保持程序以：

a) communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate;

与有关相关方进行内部和外部沟通，包括沟通内容、时间、与谁沟通以及如何沟通；

NOTE The organization can document and maintain procedures for how, and under what circumstances, the organization communicates with employees and their emergency contacts.

注：组织可以文件化和保持组织如何以及在何种情况下与员工及其紧急联系人进行沟通的程序。

b) receiving, documenting and responding to communications from interested parties, including any national or regional risk advisory system or equivalent;

对来自相关方的沟通进行接收、记录和响应，包括任何国家或区域风险预警系统或类似系统；

c) ensuring the availability of the means of communication during a security violation, vulnerability or threat;

确保在安全违规事件、漏洞或威胁期间沟通手段可用；

d) facilitating structured communication with responders to security threats and/or violations;

促进与响应者对安全威胁和（或）违规行为的结构化沟通；

e) providing details of the organization's media response following a security violation, including a communications strategy;

对安全违规事件发生后组织的媒体响应提供详细信息，包括沟通策略；

f) recording the details of the security violation, the actions taken and the decisions made.

对安全违规事件、采取的措施以及做出的决策进行详细记录。

Where applicable, the following should also be considered and implemented:

适当时，下列事项宜被考虑和实施：

— alerting interested parties potentially impacted by an actual or impending security violation;

向受到正在发生或者即将发生的安全违规事件潜在影响的相关方进行预警；

— ensuring appropriate coordination and communication between multiple responding organizations.

确保多个响应组织之间的适当协调和沟通。

The warning and communication procedures shall be exercised as part of the organization's testing and training programme.
预警和沟通程序作为组织测试和培训方案的一部分，应进行演练。

8.6.4 Content of the security plans 安全计划的内容

The organization shall document and maintain security plans. Those plans should provide guidance and information to assist teams to respond to a security vulnerability, threat and/or violation and to assist the organization with the response and restoring its security.
组织应文件化并保持安全计划。这些计划宜提供指导和信息以协助团队应对安全漏洞、威胁和（或）违规事件，并协助组织进行响应和恢复安全。

Collectively, security plans should contain:
总体而言，安全计划宜包括

a) details of the actions that the teams will take to:
团队将采取的措施的细节：
   1) continue or restore the agreed security status;
   继续或恢复约定的安全状态；
   2) monitor the impact of the actual or impending security threats, vulnerabilities or violation and the organization's response to it;
   监视正在发生或即将发生的安全威胁、漏洞或违规的影响以及组织对其的响应；

b) reference to the pre-defined threshold(s) and process for activating the response;
参考预先定义的阈值和启动响应过程；

c) procedures to restore the security of the organization;
恢复组织安全的程序；

d) details to manage the immediate consequences of a security vulnerability and threat or actual or impending security violation giving due regard to:
管理安全漏洞和威胁或已经发生或即将发生的安全违规事件的直接后果的详细信息，要考虑：
   1) the welfare of individuals;
   个人福利；
   2) the value of the assets, information and personnel potentially compromised;
   可能受损的资产、信息和人员的价值；
   3) the prevention of (further) loss or unavailability of core activities.
   防止（进一步）损失或核心业务的无法履行。

Each plan should include:
每项计划宜包括：

— its purpose, scope and objectives;
目的、范围和目标;
— the roles and responsibilities of the team that will implement the plan;
执行计划的团队的角色和职责;
— the actions to implement the solutions;
执行解决方案的措施;
— the information needed to activate (including activation criteria), operate, coordinate and communicate the team's actions;
启动（包括启动准则）、运行、协调和沟通团队行动所需的信息;
— internal and external interdependencies;
内部和外部的相互依赖关系;
— its resource requirements;
资源要求;
— its reporting requirements;
报告要求;
— a process for standing down.
退出过程。

Each plan should be usable and available at the time and place at which it is required.
计划宜在需要的时间和地点可用。

8.6.5 Recovery 恢复

The organization shall have documented processes to restore the organization's security from any temporary measures adopted before, during and after a security violation.
组织应有用以在安全违规事件之前、期间和之后从所采用的任何临时措施中恢复组织安全的成文过程。

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:
— what needs to be monitored and measured;
需要监视和测量的内容;
— the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
监视、测量、分析和评价方法，适用时，确保得到有效的结果;
— when the monitoring and measuring shall be performed;

何时应进行监视和测量；

— when the results from monitoring and measurement shall be analysed and evaluated.
何时应对监视和测量结果进行分析和评价。

Documented information shall be available as evidence of the results.
应提供成文信息作为结果的证据。

The organization shall evaluate the performance and the effectiveness of the security management system.
组织应评价安全管理体系绩效和有效性。

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 security management system:
组织应按策划的时间间隔实施内部审核，提供信息以表明安全管理体系是否：

a) conforms to:
符合：
   1) the organization's own requirements for its security management system;
   组织自身的安全管理体系要求；
   2) the requirements of this document;
   本标准的要求；

b) is effectively implemented and maintained.
得到有效实施和保持。

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、实施和保持一个或多个审核方案，包括频次、方法、职责、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.
在建立内部审核方案时，组织应考虑相关过程的重要性和以往审核结果。

The organization shall:
组织应：

a) define the audit objectives, criteria and scope for each audit;
规定每次审核的目标、审核准则和范围；

b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
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 managers.
确保向相关管理者报告审核结果；

d) verify that the security equipment and personnel are appropriately deployed;
验证安全设备和人员的部署是否适合；

e) ensure that any necessary corrective actions are taken without undue delay to eliminate detected nonconformities and their causes;
确保及时采取必要的纠正措施，以消除发现的不符合及其原因；

f) ensure that follow-up audit actions include the verification of the actions taken and the reporting of verification results.
确保后续审核活动包括验证所采取的措施和报告验证结果。

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.
应提供成文信息作为审核方案实施和审核结果的证据。

The audit programme, including any schedule, shall be based on the results of risk assessments of the organization's activities and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results.
包括任何时间表的审核方案应基于对组织活动的风险评估结果和以往的审核结果。审核程序应包括范围、频率、方法和能力，以及进行审核和汇报结果的责任和要求。

9.3 Management review 管理评审

9.3.1 General 总则

Top management shall review the organization's security management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.
最高管理者应按策划的时间间隔对组织的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。

The organization shall consider the results of analysis and evaluation, and the outputs from management review, to determine if there are needs or opportunities relating to the business or to the security management system that shall be addressed as part of continual improvement.
组织应考虑分析和评估的结果以及管理评审的输出，以确定是否存在与业务或安全管理体系相关的需要或机会，这些需要或机会应作为持续改进的一部分。

NOTE The organization can use the processes of the security management system, such as leadership, planning and performance evaluation, to achieve improvement.
注：组织可以使用安全管理体系的过程，如领导作用、策划和绩效评价以实现改进。

9.3.2 Management review inputs 管理评审输入

The management review shall include:
管理评审应包括：

a) the status of actions from previous management reviews;
以往管理评审所采取措施的状态；

b) changes in external and internal issues that are relevant to the security management system;
与安全管理体系相关的内部和外部议题的变化；

c) changes in needs and expectations of interested parties that are relevant to the security management system;
与安全管理体系相关的相关方的需求和期望的变化

d) information on the security performance, including trends in:
安全绩效方面的信息，包括以下方面的趋势：

1) nonconformities and corrective actions;
不符合和纠正措施；

2) monitoring and measurement results;
监视和测量的结果；

3) audit results;
审核结果；

e) opportunities for continual improvement;
持续改进的机会；

f) results of audits and evaluations of compliance with legal requirements and other requirements to which the organization subscribes;
对法律法规要求和组织同意遵守的其他要求的合规性审核和评价的结果；

g) communication(s) from external interested parties, including complaints;
来自相关方有关信息的沟通，包括投诉；

h) the security performance of the organization;

组织的安全绩效；

i) the extent to which objectives and targets have been met;
目标和指标的实现程度；

j) status of corrective actions;
纠正措施的状态；

k) follow-up actions from previous management reviews;
以往管理评审的后续措施；

l) changing circumstances, including developments to legal, regulatory and other requirements (see 4.2.2) related to security aspects;
持续变化的环境，包括与安全方面相关的法律、法规和其他要求（见 4.2.2）的发展；

m) recommendations for improvement.
改进建议。

9.3.3 Management review results 管理评审结果

The results of the management review shall include decisions related to continual improvement opportunities and any need for changes to the security management system.
管理评审的结果应包括与持续改进机会有关的决定和对安全管理体系进行所需的变更。

Documented information shall be available as evidence of the results of management reviews.
应提供成文信息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 security management system. The organization should actively seek opportunities for improvement, even if not prompted by vulnerabilities related to security and imminent security threats or ongoing security violations to relevant interested parties.
组织应持续改进安全管理体系的适宜性、充分性和有效性。即使不存在与安全相关的漏洞和迫在眉睫的安全威胁或有关相关方的持续安全违规事件，组织也宜积极寻求改进机会。

10.2 Nonconformity and corrective action 不符合项和纠正措施

When a nonconformity occurs, the organization shall:
当不符合发生时，组织应：

a) react to the nonconformity, and as applicable:

及时对不符合做出反应，并在适用时：

1) take action to control and correct it;
采取措施以控制和纠正不符合；
2) deal with the consequences;
处置后果；

b) evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by:
通过下列活动，评价是否需要采取措施以消除产生不符合的原因，避免其再次发生或者在其他场合发生：

1) reviewing the nonconformity;
评审不符合；
2) determining the causes of the nonconformity;
确定不符合的原因；
3) determining if similar nonconformities exist, or can potentially occur;
确定是否存在或可能发生类似的不符合。

c) implement any action needed;
实施所需的任何措施；

d) review the effectiveness of any corrective action taken;
评审所采取的纠正措施的有效性；

e) make changes to the security management system, if necessary.
必要时，变更安全管理体系。

Corrective actions shall be appropriate to the effects of the nonconformities encountered.
纠正措施应与不符合所产生的影响程度相符。

Documented information shall be available as evidence of:
应提供成文信息作为以下方面的证据：

— the nature of the nonconformities and any subsequent actions taken;
不符合的性质以及所采取的任何后续措施；
— the results of any corrective action;
任何纠正措施的结果；
— the investigation of security-related:
相关的安全调查：
  — failures, including near misses and false alarms;
  故障，包括漏报和虚假警报；
  — incidents and emergency situations;
  事件和紧急情况；
  — nonconformities;
  不符合。

— taking action to mitigate any consequences arising from such failures, incidents or nonconformities.

采取措施减轻因此类故障、事件或不符合而引起的任何后果。

Procedures shall require that all proposed corrective actions are reviewed through the assessment process of security-related risk prior to implementation unless immediate implementation forestalls imminent exposures to life or public safety.

根据程序的规定，在实施之前应通过安全威胁和风险评估流程对提出的所有纠正措施进行评审，除非立即实施可马上防止对生命或公共安全造成迫在眉睫的影响。

Any corrective action taken to eliminate the causes of actual and potential nonconformities shall be appropriate to the magnitude of the problems and commensurate with the security-management- related risks likely to be encountered.

为了消除实际和潜在不符合项而采取的任何纠正措施应与问题的严重性相符，并与可能遭受的安全管理相关的威胁和风险相符。

Bibliography 参考文献

[1] ISO 9001, Quality management systems — Requirements

ISO 9001 质量管理体系 要求

[2] ISO 14001, Environmental management systems — Requirements with guidance for use

ISO 14001 环境管理体系 要求及使用指南

[3] ISO 19 011, Guidelines for auditing management systems

ISO 19 011 管理体系审核指南

[4] ISO 22301, Security and resilience — Business continuity management systems — Requirements

ISO 22301 安全和韧性 业务连续性管理体系 要求

[5] ISO/ IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27001 信息技术 安全技术 信息安全管理系统 要求

[6] ISO 28001, Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance

ISO 28001 供应链安全管理体系 实施供应链安全、评估和计划的最佳实践 要求和指南

[7] ISO 28002, Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use

ISO 28002 供应链安全管理体系 供应链韧性的开发 要求和使用指南

[8] ISO 28003, Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems

ISO 28003 供应链安全管理体系 供应链安全管理体系审核和认证机构的要求

[9] ISO 28004-1, Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles

ISO 28004-1 供应链安全管理体系 ISO 28000 实施指南 第 1 部分：一般原则

[10] ISO 28004-3, Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)

ISO 28004-3　供应链安全管理体系 ISO 28000 实施指南 第 3 部分：中小业务采用 ISO 28000 的附加特定指南(海港除外)

[11] ISO 28004-4, Security management systems for the supply chain —Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective

ISO 28004-4，供应链安全管理体系 ISO 28000 实施指南　第 4 部分：如符合 ISO 28001 管理目标，则关于实施 ISO 28000 的附加具体指南

[12] ISO 31000, Risk management — Guidelines

ISO 31000 风险管理　指南

[13] ISO 45001, Occupational health and safety management systems — Requirements with guidance for use

ISO 45001 职业健康安全管理体系 要求及使用指南

[14] ISO Guide 73, Risk management — Vocabulary

ISO 指南 73 风险管理 术语

This page deliberately left blank
此页特意留白