

Information technology- Security techniques

-Information security management systems-Requirements

信息技术-安全技术-信息安全管理体系统-要求

## Foreword

### 前 言

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

ISO（国际标准化组织）和IEC（国际电工委员会）是为国际标准化制定专门体制的国际组织。国家机构是ISO或IEC的成员，他们通过各自的组织建立技术委员会参与国际标准的制定，来处理特定领域的技术活动。ISO和IEC技术委员会在共同感兴趣的领域合作。其他国际组织、政府和非政府等机构，通过联络ISO和IEC参与这项工作。ISO和IEC已经在信息技术领域建立了一个联合技术委员会ISO/IECJTC1。

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

国际标准的制定遵循ISO/IEC 导则第2部分的规则。

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

联合技术委员会的主要任务是起草国际标准，并将国际标准草案提交给国家机构投票表决。国际标准的出版发行必须至少75%以上的成员投票通过。

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

本文件中的某些内容有可能涉及一些专利权问题，这一点应该引起注意。ISO和IEC不负责识别任何这样的专利权问题。

ISO/IEC 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

ISO/IEC 27001 由联合技术委员会ISO/IEC JTC1（信息技术）分委员会SC27（安全技术）起草。

This second edition cancels and replaces the first edition (ISO/IEC 27001:2005), which has been technically revised.

第二版进行了技术上的修订，并取消和替代第一版（ISO/IEC 27001:2005）。

GOOAnn

## 0 Introduction

### 引言

## 0.1 General

### 0.1 总则

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

本标准用于为建立、实施、保持和持续改进信息安全管理体系提供要求。采用信息安全管理体系是组织的一项战略性决策。一个组织信息安全管理体系的建立和实施受其需要和目标、安全要求、所采用的过程以及组织的规模和结构的影响。所有这些影响因素会不断发生变化。

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

信息安全管理体系通过应用风险管理过程来保持信息的保密性、完整性和可用性，以充分管理风险并给予相关方信心。

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

信息安全管理体系是组织过程和整体管理结构的一部分并与其整合在一起是非常重要的。信息安全在设计过程、信息系统、控制措施时就要考虑信息安全。按照组织的需要实施信息安全管理体系，是本标准所期望的。

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

本标准可被内部和外部相关方使用，评估组织的能力是否满足组织自身信息安全要求。

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

本标准中要求的顺序并不能反映他们的重要性或意味着他们的实施顺序。列举的条目仅用于参考目的。

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

ISO/IEC 27000 描述了信息安全管理系统的概述和词汇，参考了信息安全管理标准族（包括ISO/IEC 27003、ISO/IEC 27004 和ISO/IEC 27005）以及相关的术语和定义。

## **0.2 Compatibility with other management system standards**

### **0.2 与其他管理体系的兼容性**

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

本标准应用了 ISO/IEC 导则第一部分 ISO 补充部分附录 SL 中定义的高层结构、相同的子章节标题、相同文本、通用术语和核心定义。因此保持了与其它采用附录 SL 的管理体系标准的兼容性。

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

附录 SL 定义的通用方法对那些选择运作单一管理体系（可同时满足两个或多个管理体系标准要求）的组织来说是十分有益的。

# Information technology — Security techniques — Information security management systems — Requirements

信息技术-安全技术-信息安全管理体系-要求

## 1 Scope

### 1 范围

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

本标准从组织环境的角度，为建立、实施、运行、保持和持续改进信息安全管理体系规定了要求。

This International Standard 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 International Standard 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 International Standard.

本标准还规定了为适应组织需要而定制的信息安全风险评估和处置的要求。本标准规定的要求是通用的，适用于各种类型、规模和特性的组织。组织声称符合本标准时，对于第4章到第10章的要求不能删减。

## 2 Normative references

### 2 规范性引用文件

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

下列文件的全部或部分内容在本文件中进行了规范引用，对于其应用是必不可少的。凡是注日期的引用文件，只有引用的版本适用于本标准；凡是不注日期的引用文件，其最新版本（包括任何修改）适用于本标准。

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

### 3 术语和定义

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

ISO/IEC 27000中的术语和定义适用于本标准。

## 4 Context of the organization

## 4 组织环境

### 4.1 Understanding the organization and its context

#### 4.1 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.

组织应确定与其目标相关并影响其实现信息安全管理体系统期结果的能力的外部 and 内部问题。

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].

注：确定这些问题涉及到建立组织的外部 and 内部环境，在ISO 31000:2009[5]的5.3节考虑了这一事项。

### 4.2 Understanding the needs and expectations of interested parties

#### 4.2 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; and
- b) the requirements of these interested parties relevant to information security.

- a) 与信息安全管理体系统有关的相关方；
- b) 这些相关方与信息安有关的要求

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

注：相关方的要求可能包括法律法规要求和合同义务。

### 4.3 Determining the scope of the information security management system

#### 4.3 确定信息安全管理体系统的范围

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统的边界和适用性，以建立其范围。

When determining this scope, the organization shall consider:

当确定该范围时，组织应考虑：

- a) the external and internal issues referred to in 4.1;
- b) the requirements referred to in 4.2; and
- c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. The scope shall be available as documented information.

- a) 在 4.1 中提及的外部 and 内部问题；
- b) 在 4.2 中提及的要求；
- c) 组织所执行的活动之间以及与其它组织的活动之间的接口和依赖性范围应文件化并保持可用性。

#### **4.4 Information security management system**

##### **4.4 信息安全管理体糸**

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

组织应按照本标准的要求建立、实施、保持和持续改进信息安全管理体糸。



## **5 Leadership**

### **5 领导**

#### **5.1 Leadership and commitment**

##### **5.1 领导和承诺**

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

高层管理者应通过下列方式展示其关于信息安全管理体的领导力和承诺:

- a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
  - b) ensuring the integration of the information security management system requirements into the organization's processes;
  - c) ensuring that the resources needed for the information security management system are available;
  - d) communicating the importance of effective information security management and of conforming to the information security management system requirements;
  - e) ensuring that the information security management system achieves its intended outcome(s);
  - f) directing and supporting persons to contribute to the effectiveness of the information security management system;
  - g) promoting continual improvement; and
  - h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.
- a) 确保建立信息安全方针和信息安全目标, 并与组织的战略方向保持一致;
  - b) 确保将信息安全管理体要求整合到组织的业务过程中;
  - c) 确保信息安全管理体所需资源可用;
  - d) 传达信息安全管理有效实施、符合信息安全管理体要求的重要性;
  - e) 确保信息安全管理体实现其预期结果;
  - f) 指挥并支持人员为信息安全管理体的有效实施作出贡献;
  - g) 促进持续改进;
  - h) 支持其他相关管理角色在其职责范围内展示他们的领导力。

#### **5.2 Policy**

##### **5.2 方针**

Top management shall establish an information security policy that:

高层管理者应建立信息安全方针, 以:

- a) is appropriate to the purpose of the organization;
- b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;
- c) includes a commitment to satisfy applicable requirements related to information security;

d) includes a commitment to continual improvement of the information security management system. The information security policy shall:

- e) be available as documented information;
- f) be communicated within the organization; and
- g) be available to interested parties, as appropriate.

a) 适于组织的目标;

b) 包含信息安全目标（见6.2）或设置信息安全目标提供框架;

c) 包含满足适用的信息安全相关要求的承诺;

d) 包含信息安全管理体系统持续改进的承诺。

信息安全方针应:

e) 文件化并保持可用性;

f) 在组织内部进行传达;

g) 适当时，对相关方可用。

### **5.3 Organizational roles, responsibilities and authorities**

#### **5.3 组织角色、职责和权限**

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

高层管理者应确保分配并传达了信息安全相关角色的职责和权限。

Top management shall assign the responsibility and authority for:

高层管理者应分配下列职责和权限:

a) ensuring that the information security management system conforms to the requirements of this International Standard; and

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

a) 确保信息安全管理体系统符合本标准的要求;

b) 将信息安全管理体系统的绩效报告给高层管理者。

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

注：高层管理者可能还要分配在组织内部报告信息安全管理体系统绩效的职责和权限。

## **6 Planning**

### **6 规划**

#### **6.1 Actions to address risks and opportunities**

##### **6.1 应对风险和机会的措施**

###### **6.1.1 General**

###### **6.1.1 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:

当规划信息安全管理体系时，组织应考虑4.1中提及的问题和4.2中提及的要求，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);
- b) prevent, or reduce, undesired effects; and
- c) achieve continual improvement.

The organization shall plan:

- d) actions to address these risks and opportunities; and
- e) how to
  - 1) integrate and implement the actions into its information security management system processes;
  - 2) evaluate the effectiveness of these actions.

- a) 确保信息安全管理体系能实现其预期结果；
- b) 防止或减少意外的影响；
- c) 实现持续改进。

组织应规划：

- d) 应对这些风险和机会的措施；
- e) 如何
  - 1) 整合和实施这些措施并将其纳入信息安全管理体系过程；
  - 2) 评价这些措施的有效性。

###### **6.1.2 Information security risk assessment**

###### **6.1.2 信息安全风险评估**

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

组织应定义并应用风险评估过程，以：

- a) establishes and maintains information security risk criteria that include:
  - 1) the risk acceptance criteria; and
  - 2) criteria for performing information security risk assessments;
- b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

- c) identifies the information security risks:
  - 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
  - 2) identify the risk owners;
- d) analyses the information security risks:
  - 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;
  - 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and
  - 3) determine the levels of risk;
- e) evaluates the information security risks:
  - 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and
  - 2) prioritize the analysed risks for risk treatment.

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

- a) 建立并保持信息安全风险准则，包括：
  - 1) 风险接受准则；
  - 2) 执行信息安全风险评估的准则；
- b) 确保重复性的信息安全风险评估可产生一致的、有效的和可比较的结果；
- c) 识别信息安全风险：
  - 1) 应用信息安全风险评估过程来识别信息安全管理体制范围内的信息丧失保密性、完整性和可用性的相关风险；
  - 2) 识别风险负责人；
- d) 分析信息安全风险：
  - 1) 评估 6.1.2 c) 1) 中所识别风险发生后将导致的潜在影响；
  - 2) 评估 6.1.2 c) 1) 中所识别风险发生的现实可能性；
  - 3) 确定风险级别；
- e) 评价信息安全风险：
  - 1) 将风险分析结果同6.1.2 a) 建立的风险准则进行比较；
  - 2) 为实施风险处置确定已分析风险的优先级。

组织应定义并应用风险评估过程，以：

组织应保留信息安全风险评估过程的文件记录信息。

### 6.1.3 Information security risk treatment

#### 6.1.3 信息安全风险处置

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

- a) select appropriate information security risk treatment options, taking account of the risk assessment results;
- b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

组织应定义并应用信息安全风险处置过程，以：

- a) 在考虑风险评估结果的前提下，选择适当的信息安全风险处置选项：

b) 为实施所选择的信息安全风险处置选项，确定所有必需的控制措施；

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

注：组织可按要求设计控制措施，或从其他来源识别控制措施。

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) 所确定的控制措施与附录A 的控制措施进行比较，以核实没有遗漏必要的控制措施；

NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.

NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.

注1：附录A包含了一份全面的控制目标和控制措施的列表。本标准用户可利用附录A以确保不会遗漏必要的控制措施。

注2：控制目标包含于所选择的控制措施内。附录A所列的控制目标和控制措施并不是所有的控制目标和控制措施，组织也可能需要另外的控制目标和控制措施。

d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;

e) formulate an information security risk treatment plan; and

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

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

d) 产生适用性声明。适用性声明要包含必要的控制措施（见6.1.3 b) 和c)）、对包含的合理性说明（无论是否已实施）以及对附录A 控制措施删减的合理性说明；

e) 制定信息安全风险处置计划；

f) 获得风险负责人对信息安全风险处置计划以及接受信息安全残余风险的批准。

组织应保留信息安全风险处置过程的文件记录信息。

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

注：本标准中的信息安全风险评估和处置过程可与 ISO 31000[5]中规定的原则和通用指南相结合。

## 6.2 Information security objectives and planning to achieve them

### 6.2 信息安全目标和规划实现

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

组织应在相关职能和层次上建立信息安全目标。

信息安全目标应:

- a) be consistent with the information security policy;
- b) be measurable (if practicable);
- c) take into account applicable information security requirements, and results from risk assessment and risk treatment;
- d) be communicated; and
- e) be updated as appropriate.

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

- f) what will be done;
- g) what resources will be required;
- h) who will be responsible;
- i) when it will be completed; and
- j) how the results will be evaluated.

- a) 与信息安全方针一致;
- b) 可测量 (如可行);
- c) 考虑适用的信息安全要求以及风险评估和风险处置结果;
- d) 被传达;
- e) 适当时进行更新。

组织应保留关于信息安全目标的文件记录信息。

当规划如何实现其信息安全目标时, 组织应确定:

- f) 要做什么;
- g) 需要什么资源;
- h) 由谁负责;
- i) 什么时候完成;
- j) 如何评价结果。

## **7 Support**

### **7 支持**

#### **7.1 Resources**

##### **7.1 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、实施、保持和持续改进信息安全管理体系所需的资源。

#### **7.2 Competence**

##### **7.2 能力**

The organization shall:

- a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;
- b) ensure that these persons are competent on the basis of appropriate education, training, or experience;
- c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- d) retain appropriate documented information as evidence of competence.

组织应：

- a) 确定从事影响信息安全执行工作的人员在组织的控制下从事其工作的必要能力；
- b) 确保人员在适当教育，培训和经验的基础上能够胜任工作；
- c) 适用时，采取措施来获得必要的的能力，并评价所采取措施的有效性；
- d) 保留适当的文件记录信息作为能力方面的证据。

NOTE Applicable actions may 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：例如适当措施可能包括为现有员工提供培训、对其进行指导或重新分配工作；雇用或签约有能力的人员。

#### **7.3 Awareness**

##### **7.3 意识**

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

- a) the information security policy;
- b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
- c) the implications of not conforming with the information security management system requirements.

人员在组织的控制下从事其工作时应意识到：

- a) 信息安全方针；

- b) 他们对有效实施信息安全管理体的贡献，包括信息安全绩效改进后的益处；
- c) 不符合信息安全管理体系要求可能的影响。

## **7.4 Communication**

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

- a) on what to communicate;
- b) when to communicate;
- c) with whom to communicate;
- d) who shall communicate; and
- e) the processes by which communication shall be effected.

组织应确定有关信息安全管理体系在内部和外部进行沟通的需求，包括：

- a) 什么需要沟通；
- b) 什么时候沟通；
- c) 跟谁进行沟通；
- d) 由谁负责沟通；
- e) 影响沟通的过程。

## **7.5 Documented information**

### **7.5 文件记录信息**

#### **7.5.1 General**

##### **7.5.1 总则**

The organization's information security management system shall include:

- a) documented information required by this International Standard; and
- b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

组织的信息安全管理体系应包括：

- a) 本标准要求的文件记录信息；
- b) 组织为有效实施信息安全管理体系确定的必要的文件记录信息。

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

注：不同组织的信息安全管理体系文件记录信息的详略程度取决于：

- 1) the size of organization and its type of activities, processes, products and services;
  - 2) the complexity of processes and their interactions; and
  - 3) the competence of persons.
- 1) 组织的规模及其活动、过程、产品和服务的类型；
  - 2) 过程的复杂性及其相互作用；
  - 3) 人员的能力。

#### **7.5.2 Creating and updating**

##### **7.5.2 创建和更新**



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

- a) identification and description (e.g. a title, date, author, or reference number);
- b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
- c) review and approval for suitability and adequacy.

创建和更新文件记录信息时，组织应确保适当的：

- a) 标识和描述（例如：标题、日期、作者或参考编号）；
- b) 格式（例如：语言，软件版本，图表）和介质（例如：纸质介质，电子介质）；
- c) 评审和批准其适用性和充分性。

### **7.5.3 Control of documented information**

#### **7.5.3 文件记录信息的控制**

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

- a) it is available and suitable for use, where and when it is needed; and
- b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

信息安全管理体系和本标准所要求的文件记录信息应予以控制，以确保：

- a) 无论何时何地需要，它都是可用并适合使用的；
- b) 它被充分保护（例如避免丧失保密性、使用不当或丧失完整性）。

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

- c) distribution, access, retrieval and use;
- d) storage and preservation, including the preservation of legibility;
- e) control of changes (e.g. version control); and
- f) retention and disposition.

对于文件记录信息的控制，适用时，组织应处理下列问题：

- c) 分发、访问、检索和使用；
- d) 存储和保存，包括可读性的保持；
- e) 变更控制（例如版本控制）；
- 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.

组织为规划和实施信息安全管理体系确定的必要的外部原始文件记录信息，适当时应予以识别并进行控制。

NOTE Access implies 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：访问隐含一个权限决策：仅能查看文件记录信息，或有权去查看和变更文件记录信息等。

## **8 Operation**

### **8 运行**

#### **8.1 Operational planning and control**

##### **8.1 运行的规划和控制**

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

组织应规划、实施和控制满足信息安全要求所需的过程，并实施6.1中确定的措施。组织还应实施这些规划来实现6.2中所确定的信息安全目标。

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

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

The organization shall ensure that outsourced processes are determined and controlled.

组织应保持文件记录信息达到必要的程度：有信心证明过程是按计划执行的。

组织应控制计划的变更，评审非预期变更的后果，必要时采取措施减缓负面影响。

组织应确保外包的过程已确定，并处于可控状态。

#### **8.2 Information security risk assessment**

##### **8.2 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).

考虑到6.1.2 a) 中建立的风险评估执行准则，组织应按计划的时间间隔执行信息安全风险评估，当重大变更被提出或发生时也应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记录信息。

#### **8.3 Information security risk treatment**

##### **8.3 信息安全风险处置**

The organization shall implement the information security risk treatment plan.

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

组织应实施信息安全风险处置计划。

组织应保留信息安全风险处置结果的文件记录信息。

## **9 Performance evaluation**

## 9 绩效评价

### 9.1 Monitoring, measurement, analysis and evaluation

#### 9.1 监视、测量、分析和评价

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

The organization shall determine:

- a) what needs to be monitored and measured, including information security processes and controls;
- b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
- a) 什么需要监视和测量，包括信息安全过程和控制措施；
- b) 监视、测量、分析和评价的方法，适用时，确保结果有效；

**NOTE** The methods selected should produce comparable and reproducible results to be considered valid.

注：选择的方法最好产生可比较和可再现的结果，这样才能被认为是有效的。

- c) when the monitoring and measuring shall be performed;
- d) who shall monitor and measure;
- e) when the results from monitoring and measurement shall be analysed and evaluated;
- f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

- c) 什么时候应执行监视和测量；
- d) 谁应实施监视和测量；
- e) 什么时候应对监视和测量的结果进行分析和评价；
- f) 谁应分析和评价这些结果。

组织应保留适当的文件记录信息作为监视和测量结果的证据。

### 9.2 Internal audit

#### 9.2 内部审核

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

组织应按计划的时间间隔进行内部审核，以提供信息确定信息安全管理体系是否：

- a) conforms to
- a) 符合

- 1) the organization's own requirements for its information security management system;
- 2) the requirements of this International Standard;
- 1) 组织自身信息安全管理体系的要求；

2) 本标准的要求;

b) is effectively implemented and maintained. The organization shall:

c) plan, establish, implement and maintain an audit program me(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit program me(s) shall take into consideration the importance of the processes concerned and the results of previous audits;

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

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

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

g) retain documented information as evidence of the audit program me(s) and the audit results.

b) 得到有效的实施和保持。

组织应:

c) 规划、建立、实施和保持审核方案, 包括频次、方法、职责、计划要求和报告。审核方案应考

虑所关注过程的重要性以及以往审核的结果;

d) 为每次审核定义审核准则和审核范围;

e) 审核员的选择和审核的实施应确保审核过程的客观性和公正性;

f) 确保审核结果报告给相关的管理者;

g) 保留文件记录信息作为审核方案和审核结果的证据。

### 9.3 Management review

#### 9.3 管理评审

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

管理者应按计划的时间间隔评审组织的信息安全管理体系, 以确保其持续的适宜性、充分性和有效性。

管理评审应包括下列方面的考虑:

a) the status of actions from previous management reviews;

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

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

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) fulfilment of information security objectives;

d) feedback from interested parties;

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

f) opportunities for continual improvement.

- a) 以往管理评审的措施的状态;
- b) 与信息安全管理体系统相关的外部 and 内部问题的变更;
- c) 信息安全绩效的反馈, 包括下列方面的趋势:
  - 1) 不符合和纠正措施;
  - 2) 监视和测量结果;
  - 3) 审核结果;
  - 4) 信息安全目标的实现;
- d) 相关方的反馈;
- e) 风险评估的结果和风险处置计划的状态;
- f) 持续改进的机会。

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

The organization shall retain documented information as evidence of the results of management reviews.

管理评审的输出应包括与持续改进机会有关的决定, 以及变更信息安全管理体系统的所有需求。组织应保留文件记录信息作为管理评审结果的证据。

## **10 Improvement**

### **10 改进**

#### **10.1 Nonconformity and corrective action**

##### **10.1 不符合和纠正措施**

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

- 1) take action to control and correct it; and
- 2) deal with the consequences;

当发生不符合时，组织应：

a) 对不合作作出反应，适用时：

- 1) 采取措施控制并纠正不符合；
- 2) 处理后果；

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

- 1) reviewing the nonconformity;
- 2) determining the causes of the nonconformity; and
- 3) determining if similar nonconformities exist, or could potentially occur;

b) 为确保不符合不再发生或不在其他地方发生，通过下列方式评价消除不符合原因的措施需求：

- 1) 评审不符合；
- 2) 确定不符合的原因；
- 3) 确定是否存在或可能发生相似的不符合；

c) implement any action needed;

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

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

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

The organization shall retain documented information as evidence of:

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

g) the results of any corrective action.

c) 实施所需的措施；

d) 评审所采取纠正措施的有效性；

e) 必要时，对信息安全管理体系实施变更。

纠正措施应与所遇不符合的影响相适应。

组织应保留文件记录信息作为下列事项的证据：

f) 不符合的性质以及所采取的所有后续措施；

g) 所有纠正措施的结果。

#### **10.2 Continual improvement**

##### **10.2 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的适宜性、充分性和有效性。

GOOANN

**Table A.1 – Control objectives and controls**

<b>A.5 Security Policies</b> 安全方针		
<b>A.5.1 Management direction for information security</b> 信息安全管理指导  Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.  目标：依据业务要求和相关法律法规提供管理指导并支持信息安全。		
A.5.1.1	Policies for information security 信息安全方针	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.  一组信息安全方针应被建立、由管理层批准、发布并传达给所有员工和外部相关方。
A.5.1.2	Review of the policies for information security 信息安全方针的评审	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.  宜按计划的时间间隔或当重大变化时进行信息安全方针评审，以确保它持续的适宜性、充分性和有效性。
<b>A.6 Organisation of information security</b> 信息安全组织		
<b>A.6.1 Internal organisation</b> 内部组织  Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation.  目标：建立管理框架，启动和控制组织内信息安全的实施和运行。		
A.6.1.1	Information security roles and responsibilities 信息安全角色和职责	All information security responsibilities shall be defined and allocated.  所有的信息安全职责宜予以定义与分配。
A.6.1.2	Segregation of duties 职责分割	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.  冲突的责任及职责范围宜加以分割，以降低未授权或无意识的修改或者



		不当使用组织资产的机会。
A.6.1.3	Contact with authorities 与政府部门的联系	Appropriate contacts with relevant authorities shall be maintained. 宜保持与政府相关部门的适当联系。
A.6.1.4	Contact with special interest groups 与特定利益集团的联系	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained. 宜保持与特定利益集团、其他安全专家组和专业协会的适当联系。
A.6.1.5	Information security in project management 项目管理中的信息安全	Information security shall be addressed in project management, regardless of the type of the project. 无论何种类型的项目，宜将信息安全融入到项目管理中。
<b>A.6.2 Mobile devices and teleworking</b> 移动设备和远程工作 Objective: To ensure the security of teleworking and use of mobile devices. 目标：确保远程工作和移动设备使用的安全		
A.6.2.1	Mobile device policy 移动设备策略	A policy and supporting security measures shall be adopted to manage against the risks introduced by using mobile devices. 宜采用策略及和支持性安全措施来管理使用移动设备所带来的风险。
A.6.2.2	Teleworking 远程工作	A policy and supporting security measures shall be implemented to protect information accessed , processed or stored on teleworking sites. 宜实施策略和支持性安全措施来保护在远程站点访问、处理或存储的信息。
<b>A.7 Human resource security</b> 人力资源安全		
<b>A.7.1 Prior to employment</b> 任用之前 Objective: To ensure that employees and contractors understand their responsibilities and are suit-able for the roles for which they are considered. 目标：确保雇员、承包方人员理解其职责、考虑对其承担的角色是适合的。		
A.7.1.1	Screening 审查	Background verification checks on all candidates for employment

		<p>shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.</p> <p>关于所有任用的候选者的背景验证核查应按照相关法律法规、道德规范和对应的业务要求、被访问信息的类别和察觉的风险来执行。</p>
A.7.1.2	<p>Terms and conditions of employment</p> <p>任用条款和条件</p>	<p>The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.</p> <p>与员工和承包商的合同协议应规定他们和组织的信息安全责任。</p>
<p><b>A.7.2 During employment</b></p> <p>任用中</p> <p>Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.</p> <p>目标：确保所有的雇员和合同方意识到并履行其信息安全责任。</p>		
A.7.2.1	<p>Management responsibilities</p> <p>管理职责</p>	<p>Management shall require all employees and external party users to apply security in accordance with established policies and procedures of the organization.</p> <p>管理者宜要求所有雇员和外部用户按照组织已建立的方针策略和规程对安全尽心尽力。</p>
A.7.2.2	<p>Information security awareness, education and training</p> <p>信息安全意识、教育和培训</p>	<p>All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.</p> <p>组织的所有雇员，适当时，包括合同方，应受到与其工作职能相关的适当的意识教育、培训和组织方针策略及规程的定期更新培训。</p>
A.7.2.3	<p>Disciplinary process</p> <p>纪律处理过程</p>	<p>There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.</p> <p>宜有一个正式并已传达的纪律处理过程，以对于安全违规的雇员进行处理。</p>
<p><b>A.7.3 Termination and change of employment</b></p> <p>任用的终止或变化</p> <p>Objective: To protect the organization's interests as part of the process of changing or terminating employment.</p>		

目标：宜将保护组织的利益融入到任用变化或终止的处理流程中。		
A.7.3.1	Termination or change of employment responsibilities 任用终止或变化的职责	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or external party user and enforced. 任用终止或变化后仍然有效的信息安全责任和义务应被定义，并向雇员与第三方人员进行传达与执行。
<b>A.8 Asset management</b> 资产管理		
<b>A.8.1 Responsibility for assets</b> 对资产负责 Objective: To achieve and maintain appropriate protection of organizational assets. 目标：实现和保持对组织资产的适当保护。		
A.8.1.1	Inventory of assets 资产清单	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. 宜识别信息和信息处理设施相关的资产，编制并维护这些资产的清单。
A.8.1.2	Ownership of assets 资产责任人	Assets maintained in the inventory shall be owned. 资产清单中维护的信息资产宜指定责任人。
A.8.1.3	Acceptable use of assets 资产的可接受使用	Rules for the acceptable use of information and assets associated with information and information processing facilities shall be identified, documented and implemented. 信息与信息及信息处理设施有关的资产可接受使用规则应被确定、形成文件并加以实施。
A.8.1.4	Return of assets 资产的归还	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement. 所有的雇员、承包方人员和第三方人员在终止任用、合同或协议时，应归还他们使用的所有组织资产。
<b>A.8.2 Information classification</b> 信息分类 Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. 目标：确保信息受到与其对组织的重要性保持一致适当级别的保护。		

A.8.2.1	Classification of information 信息的分类	Information shall be classified in terms of legal requirements value, criticality and sensitivity to unauthorized disclosure or modification. 信息应按照它对组织的价值、法律要求、敏感性和关键性予以分类，以保护信息免受未经授权泄露或篡改。。
A.8.2.2	Labeling of information 信息标记	An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. 应按照组织所采纳的分类机制建立和实施一组适合的信息标记规程。
A.8.2.3	Handling of assets 资产处理	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization. 应按照组织所采纳的分类机制建立和实施一组适合的信息处理规程。
<b>A.8.3 Media handling</b> 介质处置 Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media. 目标：防止存储在介质上的信息遭受未经授权泄露、修改、移动或销毁。		
A.8.3.1	Management of removable media 可移动介质的管理	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. 应根据组织所采用的分类方案来实施可移动介质管理程序。
A.8.3.2	Disposal of media 介质的处置	Media shall be disposed of securely when no longer required, using formal procedures. 不再需要的介质，应使用正式的程序安全地处置。
A.8.3.3	Physical media transfer 物理介质传输	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. 包含信息的介质在运送时，应防止未授权的访问、不当使用或损坏。
<b>A.9 Access control</b> 访问控制		
<b>A.9.1 Business requirements of access control</b> 访问控制的业务要求 Objective: To restrict access to information and information processing facilities.		

目标：限制信息与信息处理设施的访问		
A.9.1.1	Access control policy 访问控制策略	An access control policy shall be established, documented and reviewed based on business and security requirements. 访问控制策略应建立、形成文件，并基于业务和安全要求进行评审。
A.9.1.2	Policy on the use of network services 使用网络服务的策略	Users shall only be provided with access to the network and network services that they have been specifically authorized to use. 用户应只能访问已获专门授权使用的网络和网络服务服务。
<b>A.9.2 User access management</b> 用户访问管理 Objective: To ensure authorized user access and to prevent unauthorized access to systems and services. 目标：确保授权用户访问系统和服务，并防止未授权的访问。		
A.9.2.1	User registration and de-registration 用户注册和注销	A formal user registration and de-registration process shall be implemented to enable assignment of access rights. 应实施正式的用户注册及注销流程来分配访问权限。
A.9.2.2	User access provisioning 用户访问提供	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. 无论什么类型的用户，在对其分配或撤销所有系统和服务的权限时，都应实施一个正式的用户访问提供流程。
A.9.2.3	Management of privileged access rights 特殊权限管理	The allocation and use of privileged access rights shall be restricted and controlled. 应限制和控制特殊访问权限的分配及使用。
A.9.2.4	Management of secret authentication information of users 用户安全鉴别信息的管理	The allocation of secret authentication information shall be controlled through a formal management process. 应通过一个正式的管理过程对安全鉴别信息的分配进行控制。
A.9.2.5	Review of user access rights 用户访问权的复查	Asset owners shall review users' access rights at regular intervals. 资产所有者应定期对用户的访问权进行复查。
A.9.2.6	Removal or adjustment of access rights 撤销或调整访问权限	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or

		<p>adjusted upon change.</p> <p>所有雇员和第三方人员对信息和信息处理设施的访问权应在任用、合同或协议终止时删除，或在变化时调整。</p>
<b>A.9.3 User responsibilities</b> <b>用户职责</b> <p>Objective: To make users accountable for safeguarding their authentication information.</p> <p>目标：确保用户对保护他们的鉴别信息负有责任。</p>		
A.9.3.1	<p>Use of secret authentication information</p> <p>安全鉴别信息的使用</p>	<p>Users shall be required to follow the organization's security practices in the use of secret authentication information.</p> <p>应要求用户遵循组织的安全防护措施来使用安全鉴别信息。</p>
<b>A.9.4 System and application access control</b> <b>系统和应用访问控制</b> <p>Objective: To prevent unauthorized access to systems and applications.</p> <p>目标：防止对系统和应用的非授权访问。</p>		
A.9.4.1	<p>Information access restriction</p> <p>信息访问限制</p>	<p>Access to information and application system functions shall be restricted in accordance with the access control policy.</p> <p>信息和应用系统功能的访问应依照访问控制策略加以限制。</p>
A.9.4.2	<p>Secure log-on procedures</p> <p>安全登陆规程</p>	<p>Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.</p> <p>访问控制策略要求时，访问系统和应用应通过安全登录规程加以控制。</p>
A.9.4.3	<p>Password management system</p> <p>口令管理系统</p>	<p>Passwords management systems shall be interactive and shall ensure quality passwords.</p> <p>口令管理系统应是交互式的，并确保优质的口令。</p>
A.9.4.4	<p>Use of privileged utility programs</p> <p>特权使用程序的使用</p>	<p>The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.</p> <p>对于能超越系统和应用程序控制措施的实用工具的使用应加以限制并严格控制。</p>
A.9.4.5	<p>Access control to program source code</p> <p>对程序源代码的访问控制</p>	<p>Access to program source code shall be restricted.</p> <p>应限制访问程序源代码。</p>

<b>A.10 Cryptography</b> 密码学		
<b>A.10.1 Cryptographic controls</b> 密码控制 Objective: To ensure proper and effective use of cryptography to protect the confidentiality authenticity or integrity of information. 目标：确保适当并有效的密码的使用来保护信息的保密性、真实性或完整性。		
A.10.1.1	Policy on the use of cryptographic controls 使用密码控制的策略	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. 应开发和实施使用密码控制措施来保护信息的策略。
A.10.1.2	Key management 密码管理	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle. 应开发和实施一个贯穿生命周期的密码密钥使用、保护和生命期管理策略。
<b>A.11 Physical and environmental security</b> 物理和环境安全		
<b>A.11.1 Secure areas</b> 安全区域 Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. 目标：防止对组织信息和信息处理设施的未授权物理访问、损坏和干扰。		
A.11.1.1	Physical security perimeter 物理安全周边	Security perimeters shall be defined and used to protect areas that contain either sensitive or or critical information and information processing facilities. 应定义并使用安全周边来保护包含任何敏感或关键的信息和信息处理设施的区域。
A.11.1.2	Physical entry controls 物理入口控制	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. 安全区域应由适合的入口控制所保护，以确保只有授权的人员才允许访问。
A.11.1.3	Securing office, room and facilities 办公室、房间和设施	Physical security for offices, rooms and facilities shall be designed and applied.

	的安全保护	应为办公室、房间和设施设计并采取物理安全措施。
A.11.1.4	Protecting against external end environmental threats 外部和环境威胁的安全防护	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. 为防止自然灾害，恶意攻击或以外事件引起的破坏，应设计和采取物理保护措施。
A.11.1.5	Working in secure areas 在安全区域工作	Procedures for working in secure areas shall be designed and applied 应设计和应用在安全区域工作的规程。
A.11.1.6	Delivery and loading areas 交接区	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. 访问点（例如交接区）和未授权人员可进入办公场所的其他地点应加以控制，如果可能，应与信息处理设施隔离，以避免未授权访问。
<b>A.11.2 Equipment</b> <b>设备安全</b> Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations. 目标：防止资产的丢失、损坏、失窃或危及资产安全以及组织的运营。		
A.11.2.1	Equipment siting and protection 设备安置和保护	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. 应安置或保护设备，以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会。
A.11.2.2	Supporting utilities 支持性设施	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. 应保护设备使其免于由支持性设施的失败而引起的电源故障和其他中断。
A.11.2.3	Cabling security 布缆安全	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage. 应保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听、干扰或损坏。
A.11.2.4	Equipment	Equipment shall be correctly maintained to ensure its continued



	maintenance 设备维护	availability and integrity. 设备应予以正确地维护，以确保其持续的可用性和完整性。
A.11.2.5	Removal of assets 资 产的移动	Equipment, information or software shall not be taken off-site without prior authorization. 设备、信息或软件在授权之前不应带出组织场所。
A.11.2.6	Security of equipment and assets off-premises 组织场所外的设备和 资产安全	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises. 应对组织场所的设备采取安全措施，要考虑工作在组织场所以外的不同风险。
A.11.2.7	Secure disposal or re-use of equipment 设备的安全处置或再 利用	All 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. 包含存储介质的设备的所有项目应进行验证，以确保在处置之前，任何敏感信息和注册软件已被删除或安全地写覆盖。
A.11.2.8	Unattended user equipment 无人值守的用户设备	Users shall ensure that unattended equipment has appropriate protection. 用户应确保无人值守的用户设备有适当的保护。
A.11.2.9	Clear desk and clear screen policy 清空桌面和屏幕策略	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. 应采取清空桌面上文件、可移动存储介质的策略和清空信息处理设施屏幕的策略。
<b>A.12 Operations security</b> 操作安全		
<b>A.12.1 Operational procedures and responsibilities</b> 操作程序和职责 Objective: To ensure correct and secure operations of information processing facilities. 目标：确保正确、安全的操作信息处理设施。		
A.12.1.1	Documented operating procedures 文件化的操作程序	Operating procedures shall be documented and made available to all users who need them. 操作程序应形成文件并对所有需要的用户可用。
A.12.1.2	Change management	Changes to the organization, business processes, information

	变更管理	<p>processing facilities and systems that affect information security shall be controlled.</p> <p>对组织、业务流程、信息处理设施和系统中影响信息安全方面的变更应加以控制。</p>
A.12.1.3	Capacity management 容量管理	<p>The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.</p> <p>资源的使用应加以监视、调整，并作出对于未来容量要求的预测，以确保拥有所需的系统性能。</p>
A.12.1.4	Separation of development, testing and operational environments 开发、测试和运行设施分离	<p>Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.</p> <p>开发、测试和运行环境应分离，以减少未授权访问或改变运行系统的风险。</p>
<b>A12.2 Protection from malware</b> 防范恶意软件 Objective: To ensure that information and information processing facilities are protected against malware. 目标：确保对信息和信息处理设施的保护，防止恶意软件。		
A.12.2.1	Controls against malware 控制恶意软件	<p>Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.</p> <p>应结合适当的用户意识实施恶意软件的检测、预防和恢复的控制措施。</p>
<b>A.12.3 Backup</b> 备份 Objective: To protect against loss of data. 目标：防止数据丢失		
A.12.3.1	Information backup 信息备份	<p>Backup copies of information, software and system images shall be taken and tested regularly in accordance with the agreed backup policy.</p> <p>应按照已设的备份策略，定期备份和测试信息、软件和系统镜像。</p>
<b>A.12.4 Logging and monitoring</b> 日志记录和监视		

<p>Objective: To record events and generate evidence.</p> <p>目标：记录事件并生成证据</p>		
A.12.4.1	<p>Event logging</p> <p>事件日志</p>	<p>Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.</p> <p>应产生并保持记录用户活动、异常情况、故障和信息安全事件的审计日志，并定期对事件日志进行评审。</p>
A.12.4.2	<p>Protection of log information</p> <p>日志信息的保护</p>	<p>Logging facilities and log information shall be protected against tampering and unauthorized access</p> <p>记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。</p>
A.12.4.3	<p>Administrator and operator logs</p> <p>管理员和操作员日志</p>	<p>System administrator and system operator activities shall be logged, protected and regularly reviewed.</p> <p>系统管理员和系统操作员活动应记入日志，并对其进行保护和定期评审。</p>
A.12.4.4	<p>Clock synchronisation</p> <p>时钟同步</p>	<p>The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to single reference time source.</p> <p>一个组织或安全域内的所有相关信息处理设施的时钟应使用单一基准时间源进行同步。</p>
<p><b>A.12.5 Control of operational software</b></p> <p>运行软件的控制</p> <p>Objective: To ensure the integrity of operational systems.</p> <p>目标：确保运行系统的完整性</p>		
A.12.5.1	<p>Installation of software on operational systems</p> <p>运行系统软件安装</p>	<p>Procedures shall be implemented to control the installation of software on operational systems.</p> <p>应有规程来控制运行系统上安装软件。</p>
<p><b>A.12.6 Technical vulnerability management</b></p> <p>技术脆弱性管理</p> <p>Objective: To prevent exploitation of technical vulnerabilities.</p> <p>目标：防止技术脆弱性被利用</p>		
A.12.6.1	<p>Management of technical vulnerabilities</p> <p>技术脆弱性管理</p>	<p>Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures</p>

		<p>taken to address the associated risk.</p> <p>应及时得到现用信息系统技术脆弱性的信息，评价组织对这些脆弱性的暴露程度，并采取适当的措施来处理相关的风险。</p>
A.12.6.2	<p>Restrictions on software installation</p> <p>软件安装限制</p>	<p>Rules governing the installation of software by users shall be established and implemented.</p> <p>应建立并实施用户安装软件控制规则。</p>
<p><b>A.12.7 Information systems audit considerations</b></p> <p>信息系统审计考虑</p> <p>Objective: To minimize the impact of audit activities on operational systems.</p> <p>目标：将审计活动对运行系统的影响最小化。</p>		
A.12.7.1	<p>Information systems audit controls</p> <p>信息系统审计控制措施</p>	<p>Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.</p> <p>涉及对运行系统核查的审计要求和活动，应谨慎地加以规划并取得批准，以便最小化造成业务过程中断的风险。</p>
<p><b>A.13 Communications security</b></p> <p>通信安全</p>		
<p><b>A.13.1 Network security management</b></p> <p>网络安全管理</p> <p>Objective: To ensure the protection of information in networks and its supporting information processing facilities.</p> <p>目标：确保网络及信息处理设施中信息收到保护。</p>		
A.13.1.1	<p>Network controls</p> <p>网络控制</p>	<p>Networks shall be managed and controlled to protect information in systems and applications.</p> <p>应对网络进行管理和控制，以保护系统及应用中的信息。</p>
A.13.1.2	<p>Security of network services</p> <p>网络服务的安全</p>	<p>Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.</p> <p>安全机制、服务级别以及所有网络服务的管理要求应予以确定并包括在所有网络服务协议中，无论这些服务是由内部提供的还是外包的。</p>
A.13.1.3	<p>Segregation in networks</p> <p>网络隔离</p>	<p>Groups of information services, users and information systems shall be segregated on networks.</p>

		应在网络中隔离信息服务、用户和信息系统。
<b>A.13.2 Information transfer</b> <b>信息传输</b> Objective: To maintain the security of information transferred within an organization and with any external entity. 目标：保持组织内以及与组织外信息传输的安全。		
A.13.2.1	Information transfer policies and procedures 信息交换策略和规程	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. 应有正式的交换策略、规程和控制措施，以保护通过使用各种类型通信设施的信息交换。
A.13.2.2	Agreements on information transfer 信息传输协议	Agreements shall address the secure transfer of business information between the organization and external parties. 应建立组织和外部各方之间的业务信息的安全传输协议。
A.13.2.3	Electronic messaging 电子消息发送	Information involved in electronic messaging shall be appropriately protected. 包含在电子消息发送中的信息应给予适当的保护。
A.13.2.4	Confidentiality or non-disclosure agreements 保密或不泄露协议	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented. 应识别、定期评审反映组织信息保护需要的保密性或不泄露协议的要求，并将其形成文档。
<b>A.14 System acquisition, development and maintenance</b> <b>系统获取、开发和维护</b>		
<b>A.14.1 Security requirements of information systems</b> <b>信息系统的安全要求</b> Objective: To ensure that security is an integral part of information systems across the entire lifecycle. This includes in particular specific security requirement for information systems which provide services over public networks. 目标：确保信息安全成为信息系统生命周期的组成部分，包括向公共网络提供服务的信息系统的特定安全要求。		
A.14.1.1	Security requirements analysis and	The information security related requirements shall be included in the requirements for new information systems or enhancements to

	specification 安全要求分析和说明	existing information systems.  新建信息系统或改进现有信息系统要求中应包括信息安全相关的要求。
A.14.1.2	Securing applications services on public networks 公共网络应用服务的安全	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.  应保护应用服务中通过公共网络传输的信息，以防止欺诈活动、合同纠纷、未授权的泄露和修改。
A.14.1.3	Protecting application services transactions 保护应用服务交易	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.  应用服务中的信息应受保护，以防止不完全传输、错误路由、未授权的信息篡改、未授权的泄露、未授权的信息复制或重放。
<b>A.14.2 Security in development and support processes</b> 开发和支持过程中的安全 Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems. 目标：确保在信息系统开发生命周期内设计与实施信息安全。		
A.14.2.1	Secure development policy 安全开发策略	Rules for the development of software and systems shall be established and applied to developments within the organization.  应在组织内部建立并应用软件和系统的开发规则。
A.14.2.2	System change control procedures 系统变更控制规程	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures  应对软件包的修改进行劝阻，只限于必要的变更，且对所有的变更加以严格控制。
A.14.2.3	Technical review of applications after operating platform changes 操作系统变更后应用技术评审	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.  当操作系统发生变更时，应对业务的关键应用进行评审和测试，以确保对组织的运行或安全没有负面影响。
A.14.2.4	Restrictions on changes to software packages 软件包变更的限制	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.  应对软件包的修改进行劝阻，只限于必要的变更，且对所有的变更加以严格控制。

		严格控制。
A.14.2.5	Secure system engineering principles 安全系统工程原则	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development efforts. 工程安全系统原则应被建立、形成文档，并应用到任何信息系统开发工作中。
A.14.2.6	Secure development environment 安全开发环境	Organizations shall establish and appropriately protect secure development environment for system development and integration efforts that covers the entire system development lifecycle. 应在整个系统开发生命周期的系统开发和集成工作中，建立并适当保护开发环境的安全。
A.14.2.7	Outsourced development 外包开发	The organization shall supervise and monitor the activity of outsourced system development. 组织应监督、监视系统开发外包活动。
A.14.2.8	System security testing 系统安全测试	Tests of the security functionality shall be carried out during development. 在开发过程中，应进行安全功能测试。
A.14.2.9	System acceptance testing 系统验收测试	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions. 应建立新建信息系统、系统更新、版本升级验收测试规程和相关标准。
<b>A.14.3 Test data</b> <b>测试数据</b> Objective: To ensure the protection of data used for testing. 目标：确保测试数据的安全。		
A.14.3.1	Protection of test data 保护测试数据	Test data shall be selected carefully, protected and controlled. 测试数据应认真地加以选择、保护和控制。
<b>A.15 Supplier relationships</b> <b>供应关系</b>		
<b>A.15.1 Security in supplier relationship</b> <b>供应关系安全</b> Objective: To ensure protection of the organization's information that is accessible by suppliers. 目标：确保组织中被供应商访问信息的安全。		

A.15.1.1	Information security policy for supplier relationships 供应关系信息安全策略	Information security requirements for mitigating the risks associated with supplier access to organization's assets shall be agreed with the supplier and documented.  用于减轻供应商访问组织的资产相关风险的信息安全要求应形成文档并与供应商达成一致。
A.15.1.2	Addressing security within supplier agreements 处理供应商协议中的安全问题	All relevant information security requirements shall be established and agreed with each supplier that may have access to, process, store, communicate or provide IT infrastructure components for the organization's information.  应与每个可能访问、处理、存储组织信息，与组织进行通信或为组织提供 IT 基础设施组件的供应商建立并协商所有信息安全相关要求。
A.15.1.3	Information and communication technology supply chain 信息和通信技术供应链	Agreements with suppliers shall include requirements to address the information security risks associated with Information and Communications Technology services and product supply chain.  供应商协议应包括信息、通信技术服务和产品供应链的相关信息安全风险。
<b>A.15.2 Supplier service delivery management</b> <b>供应商服务交付管理</b> Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements. 确保信息安全和交付水平与供应商协议保持一致。		
A.15.2.1	Monitoring and review of supplier services 供应商服务的监视和评审	Organizations shall regularly monitor, review and audit supplier service delivery.  组织应定期监视、评审、审计供应商服务交付。
A.15.2.2	Managing changes to supplier services 供应商服务的变更管理	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.  应管理供应商提供服务的变更，包括保持和改进现有的信息安全策略、规程和控制措施，并考虑到业务系统和涉及过程的关键程度及风险的再评估。
<b>A.16 Information security incident management</b> <b>信息安全事件管理</b>		



<p>A.16.1 Management of information security incidents and improvements</p> <p>信息安全事件和改进的管理</p> <p>Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.</p> <p>目标：确保对信息安全事件进行持续、有效地管理，包括信息安全事态和弱点的沟通。</p>		
A.16.1.1	<p>Responsibilities and procedures</p> <p>职责和规程</p>	<p>Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.</p> <p>应建立管理职责和规程，以确保快速、有效和有序地响应信息安全事件。</p>
A.16.1.2	<p>Reporting information security events</p> <p>报告信息安全事态</p>	<p>Information security events shall be reported through appropriate management channels as quickly as possible.</p> <p>应通过适当的管理途径尽快地报告信息安全事态。</p>
A.16.1.3	<p>Reporting information security weaknesses</p> <p>报告信息安全弱点</p>	<p>Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.</p> <p>应要求使用组织信息系统和服务的所有雇员和合同方记录并报告他们观察到的或怀疑的任何系统或服务的信息安全弱点。</p>
A.16.1.4	<p>Assessment and decision of information security events</p> <p>信息安全事态评估与决策</p>	<p>Information security events shall be assessed and decided if they shall be classified as information security incidents.</p> <p>Information security events shall be assessed and decided if they shall be classified as information security incidents.</p> <p>应对信息安全事态进行评估，以决定他们是否被归类为信息安全事件。</p>
A.16.1.5	<p>Response to information security incidents</p> <p>信息安全事件响应</p>	<p>Information security incidents shall be responded to in accordance with the documented procedures.</p> <p>应按照文件化规程来响应信息安全事件。</p>
A.16.1.6	<p>Learning from information security incidents</p> <p>对信息安全事件的总结</p>	<p>Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.</p> <p>分析和解决信息安全事件积累的知识应用来减少未来事件的可能性或影响。</p>
A.16.1.7	<p>Collection of evidence</p> <p>证据的收集</p>	<p>The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information,</p>

		<p>which can serve as evidence.</p> <p>组织应建立和应用规程以识别、收集、采集和保存可以作为证据的信息。</p>
<p>A.17 Information security aspects of business continuity management</p> <p>业务连续性管理的信息安全方面</p>		
<p>A.17.1 Information security continuity</p> <p>信息安全连续性</p> <p>Objective: Information security continuity shall be embedded in organization's business continuity management systems.</p> <p>目标：信息安全的连续性应嵌入组织的业务连续性管理体系。</p>		
A.17.1.1	<p>Planning information security continuity</p> <p>策划信息安全连续性</p>	<p>The organization shall determine its requirements for information security and continuity of information security management in adverse situations, e.g. during a crisis or disaster.</p> <p>组织应明确在不利情况下（如危机或灾难时）信息安全和信息安全管理连续性的要求。</p>
A.17.1.2	<p>Implementing information security continuity</p> <p>实施信息安全连续性</p>	<p>The organization shall establish, document, implement and maintain processes, procedures and controls to guarantee the required level of continuity for information security during an adverse situation.</p> <p>组织应建立，记录，实施，维护流程、程序和控制，以确保满足不利的情况下信息安全连续性所要求的级别。</p>
A.17.1.3	<p>Verify, review and evaluate information security continuity</p> <p>验证、评审和评价信息安全连续性</p>	<p>The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.</p> <p>组织应定期验证已建立并实施的信息安全连续性控制，以确保它们在不利条件下是适当并有效的。</p>
<p>A.17.2 Redundancies</p> <p>冗余</p> <p>Objective: To ensure availability of information processing facilities.</p> <p>目标：确保信息处理设施的可用性。</p>		
A.17.2.1	<p>Availability of information processing facilities</p> <p>信息处理设施的可用性</p>	<p>Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.</p> <p>信息处理设施应具备足够的冗余，以满足可用性要求。</p>

<b>A.18 Compliance</b> 符合性		
<b>A.18.1 Compliance with legal and contractual requirements</b> 符合法律与合同要求 Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. 目标：避免违反任何信息安全相关的法律、法令、法规或合同义务以及任何安全要求。		
A.18.1.1	Identification of applicable legislation and contractual requirements 可用法律与合同要求的识别	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization. 对每一个信息系统和组织而言，所有相关的法律、法规和合同要求，以及为满足这些要求组织所采用的方法，应加以明确地定义、形成文件并保持更新。
A.18.1.2	Intellectual property rights 知识产权	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. 应实施适当的规程、以确保在涉及知识产权和使用具有所有权的软件产品时，符合法律、法规和合同的要求。
A.18.1.3	Protection of records 保护记录	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with statutory, regulatory, contractual and business requirements. 应防止记录的遗失、毁坏、伪造、未授权的访问与发布，以满足法令、法规、合同和业务的要求。
A.18.1.4	Privacy and protection of personally identifiable information 隐私和个人身份信息保护	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable. 应依照相关的法律、法规的要求，确保隐私和个人身份信息的保护。
A.18.1.5	Regulation of cryptographic controls 密码控制措施的规则	Cryptographic controls shall be used in compliance with all relevant agreements legislation and regulations. 使用密码控制措施应遵从相关的协议、法律和法规。
<b>A.18.2 Information security reviews</b>		

## 信息安全评审

Objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures

目标：确保信息安全依照组织策略和规程进行实施并运行。

A.18.2.1	Independent review of information security 信息安全的独立评审	<p>The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes to the security implementation occur.</p> <p>组织管理信息安全的方法及其实施（例如信息安全的控制目标、控制措施、策略、过程和规程）应按计划的时间间隔进行独立评审，当安全实施发生重大变化时，也要进行独立评审。</p>
A.18.2.2	Compliance with security policies and standards 符合安全策略和标准	<p>Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.</p> <p>管理层应定期评审信息处理和程序符合他们的责任范围内适当的安全策略、标准和任何其他安全要求。</p>
A.18.2.3	Technical compliance review 技术符合性评审	<p>Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards.</p> <p>信息系统应被定期核查是否符合信息安全策略和标准。</p>