ISO 标准——IEC 27001:2005

信息安全管理体系——

规范与使用指南

Reference number
ISO/IEC 27001:2005(E)

0 简介

0.1 总则

本国际标准的目的是提供建立、实施、运作、监控、评审、维护和改进信息安全管理体系（ISMS）的模型。采用 ISMS 应是一个组织的战略决定。组织 ISMS 的设计和实施受业务需求和目标、安全需求、应用的过程及组织的规模、结构的影响。上述因素和他们的支持系统预计会随事件而变化。希望根据组织的需要去扩充 ISMS 的实施，如，简单的环境是用简单的 ISMS 解决方案。

本国际标准可以用于内部、外部评估其符合性。

0.2 过程方法

本国际标准鼓励采用过程的方法建立、实施、运作、监控、评审、维护和改进一个组织的 ISMS 的有效性。

一个组织必须识别和管理许多活动使其有效地运行。通过利用资源和管理，将输入转换为输出的活动，可以被认为是一个过程。通常，一个过程的输出直接形成了下一个过程的输入。

组织内过程体系的应用，连同这些过程的识别和相互作用及管理，可以称之这“过程的方法”。

在本国际标准中，信息安全管理的过程方法鼓励用户强调以下方面的重要性：

a) 了解组织信息安全需求和建立信息安全策略和目标的需求；

b) 在组织的整体业务风险框架下，通过实施及运作控制措施管理组织的信息安全风险；

c) 监控和评审 ISMS 的执行和有效性；

d) 基于客观测量的持续改进。

本国际标准采用了“计划-实施-检查-改进”（PDCA）模型去构架全部 ISMS 流程。图 1 显示 ISMS 如何输入相关方的信息安全需求和期望，经过必要的处理，产生满足需求和期望的产品信息安全输出，图 1 阐明与条款 4、5、6、7、8 相关。

采用 PDCA 模型将影响 OECD《信息系统和网络的安全治理》（2002）中陈述的原则，

0 Introduction

0.1 General

This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization’s ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.

This International Standard can be used in order to assess conformance by interested internal and external parties.

0.2 Process approach

This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

An organization needs to identify and manage many activities in order to functior effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a “process approach”.

The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

a) understanding an organization’s information security requirements and the need to establish policy and objectives for information security;

b) implementing and operating controls to manage an organization's information security risks in the context of the organization’s overall business risks;

c) monitoring and reviewing the performance and effectiveness of the ISMS; and

d) continual improvement based on objective measurement.

This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations. Figure 1 also illustrates the links in the processes presented in Clauses 4, 5, 6, 7 and 8.

The adoption of the PDCA model will also reflect the principles as set out in the

本国际标准提供一个健壮的模型去实施指南中的控制风险评估、安全设计和实施、安全管理和再评估的原则。

例 1

要求可以是违背信息安全不会给组织带来严重经济损失或干扰。

例 2

期望可以是指假设发生了严重的事件--可能是组织的电子商务网站遭受了黑客攻击—那么就必须有训练有素的人员通过适当的程序尽量减少其影响。

0.3 与其他管理系统的兼容性

为了增强一致性，并与相关的管理标准整合实施和运作，本国际标准与BS EN ISO 9001：2000 和BSEN ISO 14001：2004相互协调。一个设计合理的管理系统能够满足所有标准的需求。

表C.1 展示了本国际标准与ISO 9001：2000和ISO 14001：2004之间的关系。

本国际标准设计上就考虑把 ISMS 与其他相关的管理系统进行整合；

OECD Guidelines (2002)1) governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

EXAMPLE 1

A requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization.

EXAMPLE 2

An expectation might be that if a serious incident occurs — perhaps hacking of an organization’s eBusiness web site — there should be people with sufficient training in appropriate procedures to minimize the impact.

0.3 Compatibility with other management systems

This International Standard is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can thus satisfy the requirements of all these standards. Table C.1 illustrates the relationship between the clauses of this International Standard, ISO 9001:2000 and ISO 14001:2004.

This International Standard is designed to enable an organization to align or integrate its ISMS with related management system requirements.

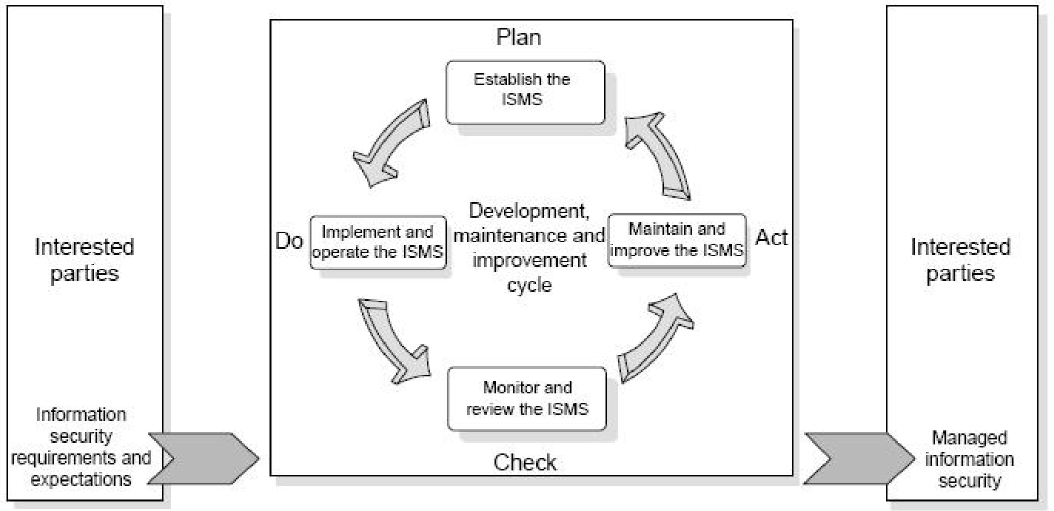
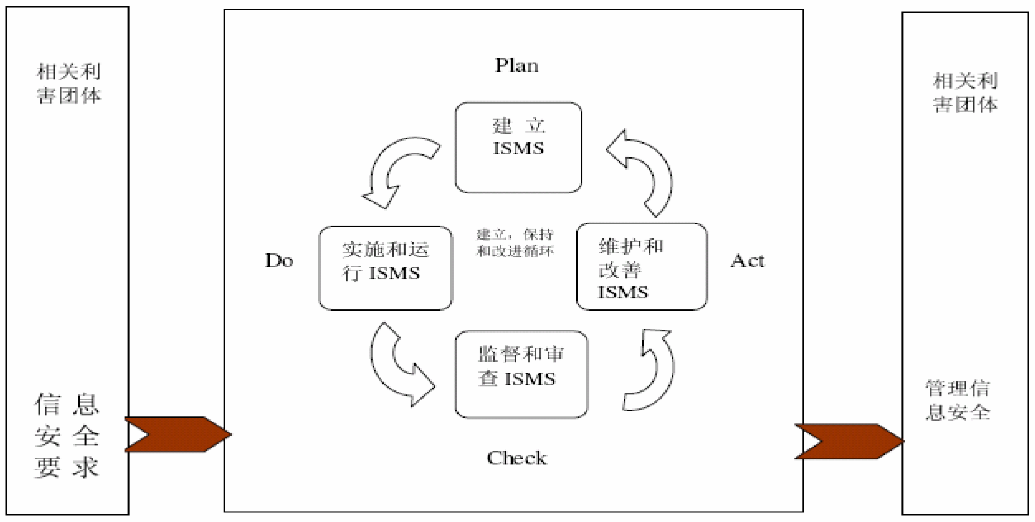

Interested parties
Information security requirements and expectations
Plan
Establish the ISMS
Do
Implement and operate the ISMS
Development, maintenance and improvement cycle
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested parties
Managed information security

Figure 1 — PDCA model applied to ISMS processes



应用于 ISMS 过程的 PDCA 模式

Plan(establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives.
Do(implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check(monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act(maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

计划(建立 ISMS)	根据组织的整体策略和目标，建立与管理风险相关的 ISMS 策略、目标、过程和程序，改进信息安全达到期望的结果。
实施(实施和运行 ISMS)	实施和运作 ISMS 的策略、控制措施和程序。
检查(监控和审核 ISMS)	针对于 ISMS 策略、目标、实践经验进行评估、测量，并报告结果给管理层评审。
改进(维护和改进 ISMS)	根据内部 ISMS 审核、管理评审的结果及其他相关信息，采取纠正和预防措施，实现 ISMS 的持继改进。

1 范围	**1 Scope**
1.1 概要 本国际标准覆盖了所有类型的组织（如业务企业、政府机构、非盈利机构），在组织的整体业务风险环境下，本国际标准定义了建立、实施、运行、监控、评审、维护和改进一个文件化的 ISMS。它定义了一个独立组织或组织的一部分实施安全控制的需求。 ISMS 的设计提供了充分、适当的安全控制，充分保护信息资产并给与客户和其他利益相关方信心。 注 1：在本国际标准中的术语‘business’被认为对于组织存在的目的非常关键的活动。 注 2：ISO/IEC 17799 为设计控制措施提供实施指南。 **1.2 应用** 本标准规定所有要求是通用的,旨在适用于各种类型、不同规模和不同性质的组织。当组织宣布符合本国际标准，对于条款 4,5,6,7 和 8 要求的删减是不能接受。 需证明任何控制的删减满足风险接受的准则，必须证明是正当的并需要提供证据证明相关风险被责任人适当的接受。当由于组织的性质和业务本标准中的要求不能使用相关控制，要求可以考虑删减，除非删减不影响组织满足风险评估和适用的法律要求的能力和/或责任，否则不能声称符合本标准。 注：如果组织已经运行业务管理系统（如 ISO9001 或 ISO14001），那将更容易满足本国际标准的需求。	**1.1 General** This International Standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations). This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization’s overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. NOTE 1: References to ‘business’ in this International Standard should be interpreted broadly to mean those activities that are core to the purposes for the organization’s existence. NOTE 2: ISO/IEC 17799 provides implementation guidance that can be used when designing controls. **1.2 Application** The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size and nature. Excluding any of the requirements specified in Clauses 4, 5, 6, 7, and 8 is not acceptable when an organization claims conformity to this International Standard. Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons. Where any controls are excluded, claims of conformity to this International Standard are not acceptable unless such exclusions do not affect the organization’s ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable legal or regulatory requirements. NOTE: If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within this existing management system.
2 引用标准 下列标准引用的条文在本标准中同样引用。因为时间的原因，引用标准处于编辑状态。为了更新引用，应考虑参考文档最新版本。 ISO/IEC 17799:2005 信息技术—安全技术--信息安全管理实施指南	**2 Normative references** The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies. ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

3 名词和定义

从本国际标准的目的出发，以下名词和定义适用。

3.1 资产

对组织而言具有价值的事物。

[BS ISO/IEC 13335-1:2004]

3.2 可用性

保证被授权的使用者需要时能够访问信息及相关资产。

[BS ISO/IEC 13335-1:2004]

3.3 保密性

信息不被未授权的个人、实体、流程访问披露。

[BS ISO/IEC 13335-1:2004]

3.4 信息安全

保护信息的保密性、完整性、可用性及其他属性，如：真实性、可确认性、不可否认性和可靠性。

[BS ISO/IEC 17799:2005]

3.5 信息安全事件

系统、服务或网络状态发生的事件违背了信息安全策略，或使安全措施失效，或以前末知的与安全相关的情况

[BS ISO/IEC TR 18044:2004]

3.6 信息安全事故

单个或一系列的意外信息安全事件可能严重影响业务运作并威胁信息安全.

[BS ISO/IEC TR 18044:2004]

3.7 信息安全管理体系（ISMS）

是整个管理体系的一部分，建立在业务风险的方法上，以开发、实施、运行、评审、维护和改进信息安全。

注：管理系统包括组织架构、策略、策划、职责、实践、程序、流程和资源。

3.8 完整性

保护资产的准确和完整。

[BS ISO/IEC 13335-1:2004]

3.9 剩余风险

经过风险处理后仍保留的风险。

[BS ISO/IEC Guide 73:2002]

3.10 风险接受

接受风险的决策。

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 asset

anything that has value to the organization.

[ISO/IEC 13335-1:2004]

3.2 availability

the property of being accessible and usable upon demand by an authorized entity.

[ISO/IEC 13335-1:2004]

3.3 confidentiality

the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

[ISO/IEC 13335-1:2004]

3.4 information security

preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

[ISO/IEC 17799:2005]

3.5 information security event

an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

[ISO/IEC TR 18044:2004]

3.6 information security incident

a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

[ISO/IEC TR 18044:2004]

3.7 information security management system ISMS

that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.8 integrity

the property of safeguarding the accuracy and completeness of assets.

[ISO/IEC 13335-1:2004]

3.9 residual risk

the risk remaining after risk treatment.

[ISO/IEC Guide 73:2002]

3.10 risk acceptance

decision to accept a risk.

[ISO/IEC Guide 73:2002]

3.11 risk analysis

[ISO Guide 73:2002]

3.11 风险分析

系统化地使用信息识别来源和估计风险。

[ISO Guide 73:2002]

3.12 风险评估

风险分析和风险评价的整个过程。[ISO Guide 73:2002]

3.13 风险评价

比较估计风险与给出的风险标准，确定风险严重性的过程。

[ISO Guide 73:2002]

3.14 风险管理

指导和控制组织风险的联合行动。

[ISO Guide 73:2002]

注：典型风险管理包括风险评估、风险处置、风险接受和风险沟通。

3.15 风险处理

选择和实施措施以更改风险处理过程。

[ISO Guide 73:2002]

注：本标准中术语“控制措施”等同于“措施”。

3.16 适用性声明

描述与使用组织的 ISMS 范围的控制目标和控制措施。

注：控制目标和控制措施是建立在风险评估、风险处理过程、法律法规的要求、合同要求、组织对信息安全要求的结论和结果基础上。

systematic use of information to identify sources and to estimate the risk.

[ISO/IEC Guide 73:2002]

3.12 risk assessment

overall process of risk analysis and risk evaluation.

[ISO/IEC Guide 73:2002]

3.13 risk evaluation

process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

[ISO/IEC Guide 73:2002]

3.14 risk management

coordinated activities to direct and control an organization with regard to risk.

[ISO/IEC Guide 73:2002]

3.15 risk treatment

process of selection and implementation of measures to modify risk.

[ISO/IEC Guide 73:2002]

NOTE: In this International Standard the term ‘control’ is used as a synonym for ‘measure’.

3.16 statement of applicability

documented statement describing the control objectives and controls that are relevant and applicable to the organization’s ISMS.

NOTE: Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization’s business requirements for information security.

4 信息安全管理体系

4.1 总要求

组织应在组织整体业务活动和风险的环境下建立、实施、运作、监控、评审、维护和改进文件化的 ISMS。本标准应用了图 1 所示的 PDCA 模型。

4.2 建立和管理 ISMS

4.2.1 建立 ISMS

组织应：

a) 根据业务的性质、组织、位置、资产和技术定义 ISMS 范围和界限，以及被排除范围的详细理由；

b) 根据组织的业务性质、组织、位置、资产和技术定义 ISMS 策略，策略应：

1) 包括建立目标框架和信息安全活动建立整体的方向和原则；
2) 考虑业务及法律法规的要求，及合同的安全义务；
3) 建立组织战略和风险管理，建立和维护信息安全管理体系；
4) 建立风险评价标准；[见 4.2.1c]
5) 经管理层批准；

注：根据国际标准的目的，信息安全管理体系的策略应该包含信息安全策略，这些策略可在一个文件中描述。

c) 定义组织风险评估的方法；

1) 识别适用于 ISMS 及已识别的信息安全、法律和法规要求的风险评估方法；
2) 开发接受风险的准则和识别可接受风险水平；[见 5.1f]

风险评估方法的选择应确保风险评估结果具有可重复性和可比较性。

注：有许多不同风险评估方法。风险评估方法的例子详细讨论在 ISO/IEC TR 13335-3，《信息技术-IT 安全管理指南-IT 安全管理技术》。

d) 识别风险；

1) 识别ISMS范围内资产及其责任人[2])
2) 识别资产的威胁；
3) 识别可能被威胁利用的脆弱性；
4) 识别资产保密性、完整性和可用性损失的

4 Information security management systems

4.1 General requirements

The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organization's overall business activities and risk it faces. For the purposes of this international standard the process used is based on the PDCA model shown in Figure 1.

4.2 Establishing and managing the ISMS

4.2.1 Establish the ISMS

The organization shall do the follow.

a) Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope(see1.2).

b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology that:

1) Includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security;
2) Takes into account business and legal or regulatory requirements, and contractual security obligations;
3) Aligns with organization's strategic risk management context in which the establishment and maintenance of the ISMS will take place;
4) Establishes criteria against which risk will be evaluated [see 4.2.1c];and
5) Has been approved by management.

NOTE：For the purposes of this International Standard, the ISMS policy is considered as a superset of the information security policy. These policies can be described in one document.

c) Define the risk assessment approach of the organization

1) Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.
2) Develop criteria for accepting the risks and identify the acceptable levels of risk[see5.1f]].

The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results.

NOTE: There are different methodologies for risk assessment. Examples of risk assessment methodologies are discussed in ISO/IEC TR 13335-3, Information technology- Guidelines for the management of IT Security-Techniques for the management of IT security.

d) Identify the risks

1) Identify the assets within the scope of the ISMS, and the owners[2]) of these assets.
2) Identify the threats to those assets.
3) Identify the vulnerabilities that might be exploited by the threats.

影响；

3) 术语‘责任人’定义了个人或实体经过管理层的批准，有责任去控制产品、开发、维护、使用和保证资产安全。术语‘责任人’并不意味着其真正拥有资产。

e) 分析和评估风险；

1) 评估安全失效带来的业务影响，考虑资产失去保密性、完整性和可用性的潜在后果；

2) 评估资产的主要威胁、脆弱点和影响以及已经实施的安全控制措施，评估安全失效发生的现实可能性；

3) 估计风险等级；

4) 根据在4.2.1c)中建立的准则，进行衡量风险是可接收，还是需要处理；

f) 识别和评价处置风险的选项；

可选措施：

1) 应用适当的控制措施；

2) 在确切满足组织策略和风险接受准则的前提下，有意识地、客观地接受风险；[见4.2.1]

3) 回避风险；

4) 将相关业务风险转嫁他方，如：保险公司、供应商等；

g) 选择风险处置的控制目标和控制措施；

选择合适的控制目标和控制措施，以满足风险评估和风险处理过程的要求。选择方法应考虑可接收的风险(见 4.2.1c)2))以及法律、法规与合同的要求。

附录 A 中列出控制目标和控制措施，作为本流程的一部分，适用于被识别要求。

注：附录 A 包含适用于通用组织全面的控制目标和控制措施列表，本国标准用户直接从附录 A 中选择控制措施，确保没有重要控制选项被忽略。

h) 管理层批准建议的残余风险；

i) 获得管理层授权实施和运作 ISMS；

j) 准备适用性声明；

适用性声明应被准备并包含下列内容：

1) 从4.2.1(g)选择控制目标和控制措施以及被选择的原因；

2) 正在实施控制目标和控制措施；

3) 附件 A 中被排除的控制目标和控制

4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

[2]) The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ‘owner’ does not mean that the person actually has any property rights to the asset.

e) Analysis and evaluate the risks

1) Assess the business impacts upon the organization that might result from a security failure, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets.

2) Assess the realistic likelihood of security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls currently implemented.

3) Estimate the levels of risks

4) Determine whether the risk are acceptable or requires treatment using the criteria for accepting risks established in 4.2.1c).

f) Identify and evaluate options for the treatment of risks。

Possible actions include:

1) Applying appropriate controls;

2) Knowingly and objectively accepting risks, providing they clearly satisfy the organization’s policies and the criteria for accepting risk[see 4.2.1c];

3) Avoiding risks; and

4) Transferring the associated business risks to other parties, e.g. insures, suppliers.

g) Select control objectives and controls for the treatment of risks

The control objectives and controls shall be selected and implement to meet the requirement identified by risk assessment and risk treatment process. This selection shall take account of the criteria for accepting risk (see 4.2.1c)2)) as well as legal, regulatory and contractual requirements.

The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover the identified requirements.

NOTE: Annex A contains a comprehensives list of control objectives and controls that have been found to be commonly relevant in organizations. User of this international Standard are directed to Annex A as a starting point for control selection to ensure that no important control options are overlooked.

h) Obtain management approval of the proposed residual risks

i) Obtain management authorization to implement and operate the ISMS.

j) Prepare a statement of applicability

A statement of Applicability shall be prepared that includes the following:

1) The control objectives and control selected in 4.2.1g) and the reasons for their selection;

2) the control objectives and controls currently implemented (see 4.2.1e2)); and

3) the exclusion of any controls objectives and controls in Annex A and the justification for their exclusion.

措施应解释其被排除的理由；

注：适用性声明提供了一份考虑风险处理结果的摘要，被排除的选项需反复确认以保证不会忽略任何控制。

4.2.2 实施和运作 ISMS

组织应：

a) 阐述风险处理计划，它为信息安全风险管理指出适当的管理措施、资源、职责、优先级；-[见条款 5]

b) 实施风险处置计划以达到识别的控制目标，包括对资金需求及安全角色和职责分配；

c) 实施在 4.2.1(g)选择的控制措施以达到控制目标；

d) 定义如何测量所选控制措施的有效性，检测方式如何被用于评估控制措施的有效性，产生可比较的、可重复的结果；[见 4.2.3c].

注：通过测量控制措施的有效性，允许管理者和职员去决定如何很好的控制以达到计划的控制目标。

e) 实施培训和意识[见 5.2.2]；

f) 管理信息安全管理系统运作；

g) 管理信息安全管理系统资源[见 5.2]；

h) 实施程序及其他及时检测的控制措施，并响应安全事故；[见 4.2.3a].

4.2.3 监控和评审 ISMS

组织应：

a) 执行监控、评审程序和其他控制措施：

1) 及时检测过程结果中的错误；

2) 及时识别失败的和成功的安全违规和事故；

3) 使管理层决定将安全活动授权，或由信息技术实施的安全活动是否按期望实施；

4) 使用通知提示帮助检测安全事件，从而避免安全事故的发生；

5) 确定解决安全违规的行动是否有效；

b) 定期评审 ISMS 的有效性（包括符合安全策略和目标，及安全控制措施评审）考虑安全评审、事故、有效测量的结果及来自所有利益相关方的建议和反馈；

c) 测量控制措施的有效性，验证已经达到安

NOTE: The Statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusion provides a cross-check that no controls have been inadvertently omitted.

4.2.2 Implement and operate the ISMS

The organization shall do the following.

a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks (see 5).

b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.

c) Implement controls selected in 4.2.1g) to meet the control objectives.

d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3c)).

NOTE: Measuring the effectiveness of controls allows managers and staff to determine how well controls achieve planned control objectives.

e) Implement training and awareness programmes(see 5.2.2).

f) Manage operations of the ISMS.

g) Manage resources for the ISMS(see 5.2).

h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents. (see 4.2.3a)).

4.2.3 Monitor and review the ISMS

The organization shall do the following.

a) Execute monitoring and reviewing procedures and other controls to:

1) Promptly detect errors in the results of processing;

2) promptly Identify failed and successful security breaches and incidents;

3) Enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;

4) Help detect security events and thereby prevent security incidents by the use of indicators; and

5) Determine whether the actions taken to resolve a breach of security were effective.

b) Undertake regular reviews of the effectiveness of the ISMS(including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.

c) Measure the effectiveness of controls to verify that security requirements

全要求；

d) 按计划定期评审风险评估、残余风险和可接受风险的水平，考虑以下变化：

1） 组织；

2） 技术；

3） 业务目标和过程；

4） 已识别威胁；

5） 已实施控制的有效性；

6） 外部事件，如：法律、法规、合同责任及社会环境发生的变化；

e) 在计划的时间段内实施内部 ISMS 审核（见条款 6）；

注：内部审核，也称为第一方审核，根据组织本身的内部目标来进行实施；

f) 定期进行 ISMS 管理评审以保证信息安全管理体系范围仍然充分，识别 ISMS 过程中的改进措施；（见条款 7.1）

g) 更新安全计划，考虑监控和评审活动的发现；

h) 记录能够影响 ISMS 的有效性或性能的措施和事件；［见 4.3.3］

4.2.4 维护和改进 ISMS

组织应定期进行：

a) 实施 ISMS 已识别的改进措施；

b) 按照 8.2 和 8.3 采取合适的纠正和预防行动。应用从其他组织和组织内学到安全经验；

c) 与相关人员沟通措施和改进，沟通的详细程度与环境相适宜，必要时，应约定如何进行；

d) 确保改进行动达到预期目标；

4.3 文件要求

4.3.1 总则

文件应包括管理层决策的记录，确保措施可以追溯到管理层决策和策略，确保记录结果是可重复；

重要的是能够证明所选择的控制措施与风险评估和风险处理过程的结果之间的关系，以及追溯到信息安全管理策略和目标。

ISMS 文件应包括：

a) 文件化的安全策略文件和控制目标；

b) ISMS 范围；［见 4.2.1c］

have been met.

d) Review risk assessment at planned intervals and review the residual risks and identified acceptable levels of risks, taking into account changes to:

1) The organization;

2) Technology;

3) Business objectives and processes;

4) Identified threat;

5) Effectiveness of the implemented controls; and

6) External events, such as changes to the legal or regulatory environment, changed contractual obligations, and changes in social climate.

e) Conduct internal ISMS audits at planned intervals(see 6).

NOTE: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself for internal purposes.

f) Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified(see 7.1).

g) Update security plans to take into account the findings of monitoring and reviewing activities.

h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS(see 4.3.3).

4.2.4 Maintain and improve the ISMS

The organization shall regulatory do the following.

a) Implement the identified improvements in the ISMS.

b) Take appropriate corrective and preventive actions in accordance with 8.2 and 8.3. Apply the lessons learnt from the security experiences of other organizations and those of the organization itself.

c) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstance and , as relevant, agree on how to proceed..

d) Ensure that the improvements achieve their intended objectives.

4.3 Documentation requirements

4.3.1 General

Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and ensure that the recorded results are reproducible.

It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.

The ISMS documentation shall include :

a) Document statements of the ISMS policy [see 4.2.1b] and objectives.

b) The scope of the ISMS [see 4.2.1c]

c) ISMS 的支持性程序及控制措施；

d) 风险评估方法的描述；［见 4.2.1c］

e) 风险评估报告；［见 4.2.1c］到［4.2.1g］

f) 风险处置计划；［见 4.2.2b］

g) 组织为确保其信息安全过程有效规划、运作和控制以及规定如何测量控制措施的有效性所需要的程序文件；［见 4.2.3c］

h) 本标准要求的记录；［见 4.3.3］

i) 适用性声明；

信息安全管理体系需要的全部文档应该是有效的。

注 1：当本国际标准中出现“文件的程序”，这意味着建立、文件化、实施和维护该程序。

注 2：信息安全管理体系文档的范围不同的组织是不相同的，依据：

----组织的大小和业务活动的类型；

----被管理的系统和安全的需求的复杂性和范围；

注 3:文档和记录可以在任何形式或任何介质的；

4.3.2 文件控制

应保护和控制 ISMS 要求的文件。应建立文件化的程序确定所需管理措施：

a)文件发布前得到批准，以确保文件的充分性；

b)必要时对文件进行评审与更新，并再次批准；

c)确保文件的更改和现行修订状态得到识别；

d)确保在使用处可获得适用文件的有关版本；

e)确保文件保持清晰、易于识别；

f)确保需要文档的人可以获得有效文档，根据他们的分类进行传输、存储和最终的销毁；

g)确保外来文件得到识别；

h)确保文件的发放是受控的；

i)防止作废文件的非预期使用；

j)若因任何原因而保留作废文件时，对这些文件进行适当的标识；

4.3.3 记录控制

应建立并保持纪录，以提供符合要求和信息安全管理体系的有效运行的证据。应当保护和控制记录。信息安全管理体系应考虑任何有关的法律、法规和合同责任的要求。记录应保持清

c) procedures and controls in support of the ISMS

d) A description of the risk assessment methodology(see 4.2.1c));

e) Risk assessment report [see 4.2.1c]] to 4.2.1g)].

f) Risk treatment plan [see 4.2.2b].

g) Documented procedures needed by the organization to ensure the effective planning, operation and control of its information security process and describe how to measure the effectiveness of controls(see 4.2.3c)).

h) Records required by this International Standard(see 4.3.3).

i) The Statement of Applicability.

All documentation shall be made available as required by the ISMS policy.

NOTE 1: where the term “documented procedure” appears within this International standard, this means that the procedure is established, documented, implemented and maintained.

NOTE 2: the extent of the ISMS documentation can differ from one organization to another owing to:

----the size of the organization and the type of its activities; and

----the scope and complexity of the security requirements and the system being managed;

NOTE 3:documents and records may be in any form or type of medium.

4.3.2 Control of documents

Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:

a) Approve documents for adequacy prior to issue;

b) Review and update documents as necessary and re-approve documents;

c) Ensure that changes and the current revision status of documents are identified;

d) Ensure that relevant version of applicable documents are available at points of use;

e) Ensure that documents remain legible and readily identifiable;

f) Ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification;

g) Ensure that documents of external origin are identified;

h) Ensure that the distribution of documents is controlled;

i) Prevent the unintended use of obsolete documents; and

j) Apply suitable identification to them if they are retained for any purpose.

4.3.3 Control of records

Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be protected and controlled. The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. Records shall remain legible, readily

晰、易于识别和检索。记录的标识、储存、保护、检索、保存期限和处置所需的控制应被文件化并实施。

应保留 4.2 列出的过程执行记录和所有与信息安全管理体系有关的安全事故发生的纪录。

举例

记录的例子如：访问者的签名簿，审核记录和完整的授权访问记录。

identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of the records shall be documented and implemented.

Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of security incidents related to the ISMS.

EXAMPLE

Examples of records are a visitor's book, audit records and completed access authorization forms.

5 管理职责

5.1 管理承诺

管理层应提供其承诺建立、实施、运行、监控、评审、维护和改进信息安全管理体系的证据，包括：

a) 建立信息安全策略；

b) 确保建立信息安全目标和计划；

c) 为信息安全确立角色和责任；

d) 向组织传达达到信息安全目标和符合信息安全策略、法律责任的重要性及持续改进的需要；

e) 提供足够的资源以建立、实施，监控、评审、维护和改进信息安全管理体系［见 5.2.1］；

f) 确定可接受风险准则和可接收风险等级；

g) 确保信息安全管理体系内部评审的实施；［见 6］

h) 进行信息安全管理体系的管理评审［见条款 6］；

5.2 资源管理

5.2.1 提供资源

组织将确定和提供所需的资源，以：

建立、实施、运行、监控、评审和维护信息安全管理体系；

确保信息安全程序支持业务需求；

识别和强调法律和法规要求及合同安全责任；

正确地应用所有实施的控制措施维护足够的安全；

必要时，进行评审，并对评审的结果采取适当措施；

需要时，改进信息安全管理体系的有效性；

5.2.2 培训、意识和能力

组织应确保在信息安全管理体系承担责任的人员应能够胜任要求的任务。组织应：

a) 确定从事影响信息安全管理体系的人员所必要的能力；

b) 提供培训和采取其他措施（聘用有能力的

5 Management responsibility

5.1 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a) Establishing an ISMS policy;

b) Ensuring that ISMS objectives and plans are established;

c) Establishing roles and responsibilities for information security;

d) Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;

e) Providing sufficient resources to establish, implement, monitor, review, maintain and improve the ISMS(see 5.2.1);

f) Deciding the criteria for accepting risk and the acceptable levels of risk;

g) Ensuring that internal ISMS audits are conducted (see 6); and

h) Conducting management reviews of the ISMS (see 7).

5.2 Resource management

5.2.1 Provision of resources

The organization shall determine and provide the resources needed to:

a) Establish, implement, operate, monitor, review, maintain and improve an ISMS;

b) Ensure that information security procedures support the business requirements;

c) Identify and address legal and regulatory requirements and contractual security obligations;

d) Maintain adequate security by correct application of all implemented controls;

e) Carry out reviews when necessary, and to react appropriately to the results of these reviews; and

f) Where required , improve the effectiveness of the ISMS.

5.2.2 Training, awareness and competency

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

a) Determining the necessary competencies for personnel performing work effecting the ISMS;

人员）满足这些需求； c） 评价提供的培训和所采取行动的有效性； d） 保持教育、培训、技能、经验和资格的纪录［ 见 4．3．3］； 组织应确保所有相关的人员认识到他们信息安全活动的相关性和重要性，以及他们如何为实现信息安全管理体系目标做出贡献。	b) Providing training or taking other actions(e.g. employing competent personnel) to satisfy these needs; c) Evaluating the effectiveness of the actions takes; and d) Maintaining records of education,, training , skills, experience and qualifications(see 4.3.3). The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.
6 信息安全管理体系内部审核 组织应按计划的时间定期进行内部信息安全管理体系审核，以确定信息安全管理体系的控制目标、控制措施、安全管理体系的过程和程序是否： a） 符合本国际标准和相关法律法规的要求； b） 符合已识别的信息安全要求； c） 得到有效地实施和维护； d） 按期望执行； 应策划审核活动，考虑审核过程和区域的状况及重要性，以及前次审核的结果。应确定审核的准则、范围、频次和方法。选择审核员及进行审核应确保审核过程的客观和公正。审核员不应审核自己的工作。 应定义文件化的程序，以规定策划和指导审核、报告结果和维护记录［见 4.3.3］的责任及要求。 负责被审核区域的管理者应确保立即采取措施消除发现的不符合及其原因。跟踪应包括采取措施的验证和验证结果的报告［见条款 8］。 注：在 ISO19011:2002 中，针对于质量/环境管理系统审核的策略，可能为内部信息安全检查管理审核提供有帮助的指导。	**6 Internal ISMS audits** The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS; a) Conform to the requirements of this international Standard and relevant legislation or regulations; b) Conform to the identified information security requirements; c) Are effectively implemented and maintained; and d) Perform as expected. An audit programme shall be planned, taking into consideration the status and importance of the process and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work. The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records(see 4.3.3) shall be defined in a documented procedure. The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification result (see 8). NOTE: ISO19011:2002, Guidelines for quality and/or environmental management systems auditing, may provide helpful guidance for carrying out the internal ISMS audits.
7 信息安全管理体系管理评审 **7．1 总则** 管理层应按计划的时间定期（至少一年一次）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。评审应包括评价信息安全管理体系改进机会和变更需要，包括信息安全策略和信息安全目标。 评审结果应清楚地写入文件，应保持管理评审的纪录［见 4.3.3］	**7 Management review of the ISMS** **7.1 General** Management shall review the organization's ISMS at planned intervals(at least once a year) to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. The results of the reviews shall be clearly documented and records shall be maintained(see 4.3.3).

7．2 评审输入 管理评审输入应包括以下方面的信息： a）信息安全管理体系审核和评审结果； b）相关方反馈； c）可以用于组织改进其信息安全管理体系业绩和有效性的技术、产品或程序； d）预防和纠正措施的实施情况； e）上次风险评估未充分强调的脆弱性或威胁； f）有效的测量结果； g）上次管理评审所采取措施的跟踪验证； h）任何可能影响信息安全管理体系的变更； i）改进建议； **7．3 评审输出** 管理评审输出应包括以下方面有关的任何决定和措施： a）信息安全管理体系有效性的改进； b）更新风险评估和风险处理计划； c）修改影响信息安全的程序和控制措施，必要时，以反映内部或外部可能影响信息安全管理体系的事件，包括以下的变更： 1）业务要求； 2）安全要求； 3）影响现有业务过程的业务要求； 4）法规或法律要求； 5）合同责任； 6）风险的等级和／或可接受风险的水平； d）资源需求； e） 改进测量控制措施有效性的方式；	**7.2 Review input** The input to a management review shall include: a) Result of ISMS audits and reviews; b) Feedback from interested parties; c) Techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness; d) Status of preventive and corrective actions; e) Vulnerabilities or threats not adequately addressed in the previous risk assessments; f) Results from effectiveness measurements; g) Follow-up actions from previous management reviews; h) Any changes that could affect the ISMS;and i) Recommendations for improvement. **7.3 Review output** The output from the management review shall include any decisions and actions related to the following. a) Improvement of the effectiveness of the ISMS. b) Update of the risk assessment and risk treatment plan. c) Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to: 1) Business requirements; 2) Security requirements; 3) Business processes effecting the existing business requirements; 4) Regulatory or legal environment; 5) Contractual obligations; and 6) Levels of risk and /or criteria for accepting risks. d) Resource needs. e) Improvement to how the effectiveness of controls is being measured.
8 ISMS 改进 **8.1 持续改进** 组织应通过使用安全策略、安全目标、审核结果、监控事件的分析、纠正和预防行动和管理评审的信息持续改进 ISMS 的有效性[见 7]。 **8.2 纠正措施** 组织应采取措施，消除与实施和运行信息安全管理体系有关的不合格的原因，防止再发生。应为纠正措施编制形成文件的程序，确定以下要求： a）识别信息安全管理体系的不符合； b）确定不符合原因； c）评价确保不符合不再发生所需措施；	**8 ISMS improvement** **8.1 continual improvement** The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objective, audit results, analysis of monitored events, corrective and preventive actions and management review(see 7). **8.2 Corrective action** The organization shall take action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence. The documented procedures for corrective action shall define requirement for: a) Identifying nonconformities ; b) Determine the causes of nonconformities; c) Evaluating the need for action to ensure that nonconformities do no recur ;

d）确定和实施所需纠正措施； e）记录所采取措施的结果[见4.3.3] ； f）评审所采取的纠正措施； **8.3 预防措施** 组织应采取措施，以消除与信息管理体系要求潜在不符合的原因，避免再次发生。预防措施应于潜在问题的影响程度相适应。应为预防措施编制形成文件的程序，以确定以下方面要求： a）识别潜在不符合及其原因； b）评估预防不符合发生所需的措施； c）确定和实施所需预防措施： d）记录所采取措施结果[见4.3.3]； e）评审所采取的预防措施； 组织应识别变化的风险和识别关注于重要变化风险的预防措施的要求。 纠正措施的优先权应以风险评估结果为基础确定。 注：预防不合格的措施总是比纠正措施更节约成本。	d) Determining and implementing the corrective action needed; e) Recording results of action taken(see 4.3.3); and f) Review of corrective action taken. **8.3 Preventive action** The organization shall determine action to eliminate the cause of potential nonconformities in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for: a) Identifying potential nonconformities and their causes; b) Evaluating the need for action to prevent occurrence of nonconformities; c) Determining and implementing preventive action needed; d) Recording results of action taken(see 4.3.3); and e) Reviewing of preventive action taken; The organization shall Identify changed risks and identify preventive action requirements focusing attention on significantly changed risks. The priority of preventive actions shall be determined based on the results of the risk assessment. NOTE:Action to prevent nonconformities is often more cost-effective than corrective action.

附录 A（引用） **控制目标和控制措施** 从A.5到A.15列出的控制目标和控制措施是直接引用并与BS ISO/IEC 17799：2005条款5到15一致。在表中的控制目标与控制措施并不详尽，组织可能考虑另外必要的控制目标和控制措施。在这些表中选择控制目标和控制措施是条款4.2.1规定的信息安全管理体系过程的一部分。 ISO／IEC 17799：2005条款5至15提供最佳惯例的实施建议和指南以支持A.5到A.15规范的控制措施。	**Annex A (normative)** **Control objectives and controls** The control objectives and controls listed in table **A.1** are directly derived from and aligned with those listed in BS ISO/IEC 17799:2005 Clauses **5** to **15**. The lists in tables **A.1** are not exhaustive and an organization may consider that additional control objectives and controls are necessary. Control objectives and controls from these tables shall be selected as part of the ISMS process specified in **4.2.1**. ISO/IEC 17799:2005 Clauses **5** to **15** provide implementation advice and guidance on best practice in support of the controls specified in **A.5** to **A.15**.

A.5 信息安全策略	***A.5 Information security policy***
A.5.1 信息安全策略 控制目标：为信息安全提供符合业务需求和相关法律、法规，提供管理方向和支持；	**A.5.1 *Information security policy*** *Objective*: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations
A.5.1.1 信息安全策略文件 控制措施 信息安全策略文件应经过管理层批准，向所有员工和相关外部部团体发布和沟通； A.5.1.2 信息安全策略评审 控制措施 应按计划的时间间隔或在发生重大的变化时评审策略文件，确保策略的持续性、稳定性、充分性和有效性；	A.5.1.1 Information security policy document *Control* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties. A.5.1.2 Review of the information security policy *Control* The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
A.6 信息安全组织	**A.6 Organization of information security**
A.6.1 内部组织 控制目标：在组织内部管理信息安全；	***A.6.1 Internal organization*** *Objective:* To manage information security within the organization.
A.6.1.1 信息安全管理承诺 控制措施 管理者通过清晰的方向、可见的承诺、详细的分工、信息安全职责的沟通，去积极支持安全； A.6.1.2 信息安全协作 控制措施 信息安全活动应由组织相关部门及相关角色和职能的代表共同协作实施； A.6.1.3 信息安全责任划分 控制措施 应明确定义所有信息安全职责； A.6.1.4 信息处理设施授权过程 控制措施 应建立和实施对于新的信息处理设施的管理授权过程； A.6.1.5 保密协议 控制措施 根据影响组织信息保护的需求，保密或不泄露协议的需求应被定义和定期评审； A.6.1.6 与监管机构的联系 控制措施 与相关监管机构应维持适当联系； A.6.1.7 与特殊利益团体的联系 控制措施 与特殊利益团体、其他专业安全协会或行业协会应维持适当联系；	A.6.1.1 Management commitment to information security *Control* Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. A.6.1.2 Information security coordination *Control* Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions. A.6.1.3 Allocation of information security responsibilities Control All information security responsibilities shall be clearly defined. A.6.1.4 Authorization process for information processing facilities *Control* A management authorization process for new information processing facilities shall be defined and implemented. A.6.1.5 Confidentiality agreements *Control* Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified and regularly reviewed. A.6.1.6 Contact with authorities *Control* Appropriate contacts with relevant authorities shall be maintained. A.6.1.7 Contact with special interest groups *Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A.6.1.8 信息安全独立审查 控制措施 组织管理信息安全的方法及其实施（如：信息安全控制目标、控制措施、策略、流程、和程序）应在计划周期内或当重大变化发生时进行独立审查；	A.6.1.8 Independent review of information security *Control* 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.
A.6.2 外部组织 控制目标：维护组织信息及信息处理设施被外部组织访问、处理、沟通或管理时的安全；	***A.6.2 External parties*** *Objective:* To maintain the security of the organization’s information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
A.6.2.1 识别外部组织风险 控制措施 应识别外部组织业务过程的信息及信息处理设施的风险，并在允许访问前实施适当的控制； A.6.2.2 当与客户接触时强调安全 控制措施 应在允许客户访问组织的信息或资产之前强调所有识别的安全需求； A.6.2.3 在第三方协议中强调安全 控制措施 在与第三方合约中应包含所有的安全要求，如访问、处理、沟通、管理组织的信息或信息处理设施，或增加信息处理设施的产品和服务；	A.6.2.1 Identification of risks related to external parties Control The risks to the organization’s information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access. A. 6.2.2 Addressing security when dealing with customers Control All identified security requirements shall be addressed before giving customers access to the organization’s information or assets. A. 6.2.3 Addressing security in third party agreements Control Agreements with third parties involving accessing, processing, communicating or managing the organization’s information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.
A.7 资产管理	**A.7 Asset management**
A.7.1 资产的责任 控制目标：实现和维持组织资产的适当保护；	***A.7.1 Responsibility for assets*** Objective: To achieve and maintain appropriate protection of organizational assets.
A.7.1.1 资产清单 控制措施 应清楚的识别所有的资产，并编制和维持所有重要资产清单； A.7.1.2 资产所有权 控制措施 所有信息和信息处理设施相关资产应指定其组织内的拥有者[3])； A.7.1.3 资产的合理使用 控制措施 应识别信息和信息处理设施相关资产的合理使用准则，形成文件并实施；	A.7.1.1 Inventory of assets Control All assets shall be clearly identified and an inventory of all important assets drawn up and maintained. A.7.1.2 Ownership of assets Control All information and assets associated with information processing facilities shall be ‘owned’ 3) by a designated part of the organization. A.7.1.3 Acceptable use of assets Control Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.
3)解释：术语“拥有者”定义了经过管理层批准的个人或实体，有责任去控制生产、开发、维护、使用安全资产，术语“拥有者”并不代表其真正的拥有资产。	3) Explanation: The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ‘owner’ does not mean that the person actually has property rights to the asset.

A.7.2 信息分类 控制目标：确保信息资产受到适当程度保护	***A.7.2 Information classification*** Objective: To ensure that information receives an appropriate level of protection.
A.7.2.1 分类原则 控制措施 信息分类应根据其本身价值、法律需求和对于组织的敏感性和重要性； A.7.2.2 信息标识及处置 控制措施 应制定一套符合组织所采用分类方案的信息标识及处置的程序，并实施；	A.7.2.1 Classification guidelines Control Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization. A.7.2.2 Information labeling and handling Control An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
A.8 人力资源的安全	**A.8 Human resources security**
***A.8.1 雇用之前*[4]）** 控制目标：确保员工、合同人员和第三方人员理解他们的责任，以及他们适用的角色，减少偷窃、诈欺或设施误用所造成的风险；	***A.8.1 Prior to employment*** [4]) Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
A.8.1.1 角色和职责 控制措施 根据组织信息安全策略，应定义员工、合同人员及第三方人员的安全角色与职责，并形成文件化； A.8.1.2 人员筛选 控制措施 根据相关法律、法规、道德规范，对员工、合同人员及第三方人员的应聘人员进行背景调查，调查应符合业务需求、访问信息的类别及已知风险； A.8.1.3 雇用条款和条件 控制措施 作为合同的一部分，员工、合同人员及第三方人员应统一并签订他们的雇用合同条款和条件，这些条款和条件应规定他们和组织对于信息安全的责任；	A.8.1.1 Roles and responsibilities Control Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization’s information security policy. A.8.1.2 Screening Control Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. A.8.1.3 Terms and conditions of employment Control As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization’s responsibilities for information security.
A.8.2 雇用中 控制目标：确保员工、合同方和第三方用户清楚信息安全威胁和相关事宜、他们的责任和义务并准备在他们日常工作中支持组织信息安全策略，以减少人为错误的风险；	***A.8.2 During employment*** Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
A.8.2.1 管理职责 控制措施 管理层应要求员工、合同方和第三方用户应用符合组织建立的安全策略和程序的安全； A.8.2.2 信息安全意识、教育与培训 控制措施	A.8.2.1 Management responsibilities Control Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. A.8.2.2 Information security awareness, education and training Control

组织内所有员工、相关合同人员及第三方人员应接受适当的意识培训，并定期更新与他们工作相关的组织策略及程序； A.8.2.3 惩戒过程 控制措施 应建立一个正式的员工违反安全的惩戒过程；	All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. A.8.2.3 Disciplinary process Control There shall be a formal disciplinary process for employees who have committed a security breach.
4)解释：	4) Explanation: The word ‘employment’ is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.
A.8.3 **雇用终止和变更** 控制目标：确保员工、合同人员及第三方人员离开组织和变更雇用关系有序地进行；	***A.8.3 Termination or change of employment*** Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.
A.8.3.1 终止责任 控制措施 应清晰的定义和分配执行雇用合同终止或变更的责任； A.8.3.2 资产归还 控制措施 在终止雇用、合同或协议时，所有员工、合同人员及第三方人员应归还所使用的全部组织资产； A.8.3.1 删除访问权限 控制措施 在终止雇用、合同、协议时，应删除所有员工、合同人员及第三方人员对于信息和信息处理设施的访问权限，或根据变化调整；	A. 8.3.1 Termination responsibilities Control Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned. A. 8.3.2 Return of assets Control All employees, contractors and third party users shall return all of the organization’s assets in their possession upon termination of their employment, contract or agreement. A. 8.3.3 Removal of access rights Control The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
A.9 物理和环境安全	**A.9 Physical and environmental security**
A.9.1 安全区域 控制目标：防止对组织办公场所及信息未经授权物理访问、破坏及干扰；	***A.9.1 Secure areas*** Objective: To prevent unauthorized physical access, damage and interference to the organization’s premises and information.
A.9.1.1 物理安全边界 控制措施 组织应有安全边界（如墙、门禁系统控制或人工接待台）以保护包含信息和信息处理设施的区域； A.9.1.2 物理进入控制 控制措施 安全区域应有适当的进入控制保护，以确保只有经授权人员可以进入； A.9.1.3 办公室、房间及设施和安全 控制措施 应设计和实施保护办公室、房间及所及设备的	A.9.1.1 Physical security perimeter Control Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities. A. 9.1.2 Physical entry controls Control Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. A. 9.1.3 Securing offices, rooms and facilities Control Physical security for offices, rooms, and facilities shall be designed and applied

物理安全； A.9.1.4 防范外部和环境威胁 控制措施 应设计和实施针对于火灾、洪水、地震、爆炸、骚乱等其他天灾或人为灾难的物理保护措施； A.9.1.5 在安全区域工作 控制措施 应设计和实施在安全区域中工作有物理保护和指南； A.9.1.6 公共访问和装卸区域 控制措施 访问区域如装卸区域，及其他未经授权人员可能进入办公场所的地点应加以控制，如有可能话，信息处理设施应隔离以防止未授权的访问；	A. 9.1.4 Protecting against external and environmental threats Control Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied. A. 9.1.5 Working in secure areas Control Physical protection and guidelines for working in secure areas shall be designed and applied. A. 9.1.6 Public access, delivery and loading areas Control 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.
A.9.2 设备安全 控制目标：预防资产遗失、损害、偷窃或损失和干扰企业业务活动；	***A.9.2 Equipment security*** Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization’s activities.
A.9.2.1 设备安置及保护 控制措施 应妥善安置及保护设备，以减少来自环境的威胁与危害以及未经授权访问 A.9.2.2 支持设施 控制措施 应保护设备免于电力中断及其它因支持设施失效导致中断； A.9.2.3 电缆安全 控制措施 应保护传输数据或支持信息服务的电力及通讯电缆，免遭中断或破坏 A.9.2.4 设备维护 控制措施 应正确维护设备，以确保其持续的可用性及完整性； A.9.2.5 管辖区域外设备安全 控制措施 应对组织办公区域外的设备实施安全防护，并考虑在组织外工作的不同风险； A.9.2.6 设备报废或重用 控制措施 应检查包括存储介质的所有设备，在报废前，确保任何敏感数据和授权软件被删除或被安全重写； A.9.2.7 财产转移	A.9.2.1 Equipment siting and protection Control Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. A. 9.2.2 Supporting utilities Control Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. A. 9.2.3 Cabling security Control Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. A. 9.2.4 Equipment maintenance Control Equipment shall be correctly maintained to ensure its continued availability and integrity. A. 9.2.5 Security of equipment offpremises Control Security shall be applied to off-site equipment taking into account the different risks of working outside the organization’s premises. A. 9.2.6 Secure disposal or re-use of equipment Control All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. A. 9.2.7 Removal of property

控制措施 未经授权，设备、信息及软件不得带出办公场所；	Control Equipment, information or software shall not be taken off-site without prior authorization.
A.10 通讯与操作管理	**A.10 Communications and operations management**
A.10.1 操作程序及职责 控制目标：确保信息处理设施正确及安全的操作；	***A.10.1 Operational procedures and responsibilities*** Objective: To ensure the correct and secure operation of information processing facilities.
A.10.1.1 文件化的操作程序 控制措施 作业程序应以文件化及维护,并确保需要的用户可以获得； A.10.1.2 变更管理 控制措施 对信息处理设施及系统的变更应加以控制 A.10.1.3 职责分离 控制措施 应分离职责与责任区域以降低非授权更改或误用信息或服务的机会 A.10.1.4 开发、测试与运营设施的分离 控制措施 开发及测试设备应与运营设备分离。减少未授权访问和对操作系统变更的风险；	A.10.1.1 Documented operating procedures Control Operating procedures shall be documented, maintained, and made available to all users who need them. A. 10.1.2 Change management Control Changes to information processing facilities and systems shall be controlled. A. 10.1.3 Segregation of duties Control Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. A. 10.1.4 Separation of development, test and operational facilities Control Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.
A.10.2 第三方服务交付管理 控制目标：实施和维护信息安全的适当水平，确保第三方交付的服务符合协议要求；	***A.10.2 Third party service delivery management*** Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
A.10.2.1 服务交付 控制措施 应确保包含在第三方服务交付协议中的安全控制、服务定义、交付级别应由第三方去实施、运营和维护； A.10.2.2 第三方服务的监督和评审 控制措施 由第三方提供的服务、报告和记录应定期监控和评审，应有规律的进行审核； A.10.2.3 第三方服务的变更管理 控制措施 服务提供的改变，包括维护、改进存在的信息安全策略、程序和控制措施应被管理，考虑业务系统和过程的关键性并再次评估风险；	A.10.2.1 Service delivery Control It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. A. 10.2.2 Monitoring and review of third party services Control The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly. A. 10.2.3 Managing changes to third party services Control Changes to the provision of services, including maintaining and Improving，existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
A.10.3 系统规划和验收 控制目标：最小系统失败的风险；	***A.10.3 System planning and acceptance*** Objective: To minimize the risk of systems failures.

A.10.3.1 容量管理 控制措施 应监控、调整资源的使用，并反映将来容量的要求，以确保系统性能； A.10.3.2 系统验收 控制措施 应建立新信息系统、系统升级及新版本的验收标准，并且在开发过程中和验收前对系统进行适当的测试	A. 10.3.1 Capacity management Control The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. A. 10.3.2 System acceptance Control Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
A.10.4 防范恶意代码和移动代码 控制目标：保护软件和信息的完整性	***A.10.4 Protection against malicious and mobile code*** Objective: To protect the integrity of software and information.
A.10.4.1 控制恶意代码 控制措施 应实施恶意代码检测、预防及恢复，以及适当的用户意识程序； A.10.4.2 控制移动代码 控制措施 配置管理应确保被授权的移动代码按照明确定义的安全策略运行，防止未授权移动代码的执行；	A.10.4.1 Controls against malicious code Control Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented. A.10.4.2 Controls against mobile code Control Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.
A.10.5 备份 控制目标：维护信息和信息处理设施的完整性和有效性；	***A.10.5 Back-up*** Objective: To maintain the integrity and availability of information and information processing facilities.
A.10.5.1 信息备份 控制措施 根据已定义的备份策略备份信息和软件，并定期测试；	A.10.5.1 Information back-up Control Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.
A.10.6 网络安全管理 控制目标：确保网络中信息以及支持性基础设施得到保护；	***A.10.6 Network security management*** Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.
A.10.6.1 网络控制 控制措施 应确保网络充分的管理和控制，以防范威胁、保护使用网络的系统和应用维护安全，包括传输的信息； A.10.6.2 网络服务安全 控制措施 应识别所有网络服务的安全特性、服务级别和管理要求，并包括在网络服务协议中，无论网络服务是内部提供还是外包；	A.10.6.1 Network controls Control Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. A.10.6.2 Security of network services Control Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
A.10.7 介质处置 控制目标：防止资产的未授权暴露、修改、删除或破坏，使业务活动中断；	***A.10.7 Media handling*** Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.
A.10.7.1 可移动介质管理	A.10.7.1 Management of removable media

控制措施 应建立可移动介质的管理程序； A. 10.7.2 媒体销毁 控制措施 当介质不在需要时，按照正式程序进行可靠的、安全的处置； A.10.7.3 信息处理程序 控制措施 应建立信息的处理及储存程序，以防范信息未授权的泄漏或误用； A.10.7.4 系统文档安全 控制措施 应保护系统文件以防未经授权的访问；	Control There shall be procedures in place for the management of removable media. A. 10.7.2 Disposal of media Control Media shall be disposed of securely and safely when no longer required, using formal procedures. A. 10.7.3 Information handling procedures Control Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse. A. 10.7.4 Security of system documentation Control System documentation shall be protected against unauthorized access.
A.10.8 信息交换 控制目标：在保持组织间或组织和外部组织之间交换时信息和软件的安全；	***A.10.8 Exchange of information*** Objective: To maintain the security of information and software exchanged within an organization and with any external entity.
A.10.8.1 信息交换策略和程序 控制措施 应建立正式的交换策略、程序和控制措施，以保护所有类型的通信设施交换信息的安全； A.10.8.2 交换协议 控制措施 应建立组织和外部组织之间的信息和软件交换的协议； A.10.8.3 物理介质传输 控制措施 在组织物理边界之外进行运输的过程中，应保护包含信息的介质免受未授权的访问、误用或损坏； A.10.8.4 电子消息 控制措施 应适当保护电子消息的信息； A.10.8.5 业务信息系统 控制措施 应开发和实施策略和程序，保护业务信息系统互联的信息；	A.10.8.1 Information exchange policies and procedures Control Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities. A. 10.8.2 Exchange agreements Control Agreements shall be established for the exchange of information and software between the organization and external parties. A. 10.8.3 Physical media in transit Control Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries. A. 10.8.4 Electronic messaging Control Information involved in electronic messaging shall be appropriately protected. A. 10.8.5 Business information systems Control Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.
A.10.9 电子商务服务 控制目标：确保电子商务服务的安全及他们的安全使用；	***A.10.9 Electronic commerce services*** Objective: To ensure the security of electronic commerce services, and their secure use.
A.10.9.1 电子商务 控制措施 应保护电子商务中通过公共网络传输的信息，以避免欺诈行为、合同争议、未授权的泄露和修改；	A.10.9.1 Electronic commerce Control Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

A.10.9.2 在线交易 控制措施 应保护在线处理的信息，避免不完整的传输、路由错误、未授权的消息修改、未授权的泄露、未授权的信息复制和回复；	A. 10.9.2 On-line transactions Control Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.10.9.3 公共可用信息 控制措施 应保护公共可用系统中信息的完整性，并防止未授权的修改；	A. 10.9.3 Publicly available Information Control The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
A.10.10 监督 控制目标：检测未授权的信息处理活动；	***A.10.10 Monitoring*** Objective: To detect unauthorized information processing activities.
A. 10.10.1 审核日志 控制措施 审核日志记录了用户的活动、意外和信息安全事件日志，并按照约定的期限进行保留，以支持未来的调查和访问控制监控；	A. 10.10.1 Audit logging Control Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
A. 10.10.2 监控系统的使用 控制措施 应建立监控信息处理设施使用的程序，并定期审核监控的结果；	A. 10.10.2 Monitoring system use Control Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
A. 10.10.3 日志信息保护 控制措施 防止篡改和未授权访问日志设备和日志信息；	A. 10.10.3 Protection of log information Control Logging facilities and log information shall be protected against tampering and unauthorized access.
A. 10.10.4 管理员和操作员日志 控制措施 应记录系统管理员和系统操作员的活动；	A. 10.10.4 Administrator and operator logs Control System administrator and system operator activities shall be logged.
A. 10.10.5 错误日志 控制措施 故障应被记录、分析和采取适当的措施；	A. 10.10.5 Fault logging Control Faults shall be logged, analyzed, and appropriate action taken.
A. 10.10.6 时钟同步 控制措施 在组织或安全域内的所有相关信息处理系统的时钟应按照约定的正确时间源保持同步；	A. 10.10.6 Clock synchronization Control The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.
A.11 访问控制	**A.11 Access control**
A.11.1 访问控制的业务需求 控制目标：控制对信息的访问；	***A.11.1 Business requirement for access control*** Objective: To control access to information.
A.11.1.1 访问控制策略 控制措施 应建立文件化访问控制策略，并根据业务和安全要求对访问策略进行评审；	A.11.1.1 Access control policy Control An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
A.11.2 用户访问管理 控制目标：确保授权的用户访问和预防非授权	***A.11.2 User access management*** Objective: To ensure authorized user access and to prevent unauthorized access to

访问信息系统；	information systems.
A.11.2.1 用户注册 控制措施 应有正式的用户注册及撤销注册程序，以允许和撤销对于所有信息系统及服务的访问； A.11.2.2 特权管理 控制措施 应限制及控制特权的分配及使用； A.11.2.3 用户口令管理 控制措施 应通过正式管理流程控制口令的分配； A.11.2.4 用户访问权限的评审 控制措施 管理层应定期执行正式流程评审用户的访问权限；	A.11.2.1 User registration Control There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. A.11.2.2 Privilege management Control The allocation and use of privileges shall be restricted and controlled. A.11.2.3 User password management Control The allocation of passwords shall be controlled through a formal management process. A.11.2.4 Review of user access rights Control Management shall review users' access rights at regular intervals using a formal process.
A.11.3 用户责任 控制目标：防止未经授权用户的访问，威胁或偷窃信息和信息处理设备；	***A.11.3 User responsibilities*** Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.
A.11.3.1 口令使用 控制措施 应要求用户在选择及使用密码时，遵循良好的安全惯例； A.11.3.2 无人值守的用户设备 控制措施 用户应确保无人值守使用者的设备得到适当的保护； A.11.3.4 清除桌面及屏幕策略 控制措施 应采用清除桌面纸张和可移动存储介质，及清除信息处理设备屏幕策略；	A. 11.3.1 Password use Control Users shall be required to follow good security practices in the selection and use of passwords. A.11.3.2 Unattended user equipment Control Users shall ensure that unattended equipment has appropriate protection. A.11.3.3 Clear desk and clear screen policy Control A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
A.11.4 网络访问控制 控制目标：避免未授权的访问网络服务；	***A.11.4 Network access control*** Objective: To prevent unauthorized access to networked services.
A.11.4.1 网络服务使用政策 控制措施 用户应只能访问已获明确授权使用的服务； A.11.4.2 外部连接用户的鉴别 控制措施 应使用适当的鉴别控制远程用户的访问； A.11.4.3 网络设备的识别 控制措施 应考虑把自动设备识别作为鉴别特定区域和设备的连接鉴别的方法；	A. 11.4.1 Policy on use of network services Control Users shall only be provided with access to the services that they have been specifically authorized to use. A. 11.4.2 User authentication for external connections Control Appropriate authentication methods shall be used to control access by remote users. A. 11.4.3 Equipment identification in networks Control Automatic equipment identification shall be considered as a means to authenticate

A.11.4.4 远程诊断和配置端口保护 控制措施 应控制对诊断和配置端口的物理和逻辑访问； A.11.4.5 网内隔离 控制措施 应在网络中以分组方式隔离信息服务、用户及信息系统； A.11.4.6 网络连接控制 控制措施 在公共网络中，尤其是扩展到组织边界之外的网络，应限制用户连接网络的能力，并与访问控制策略和业务应用程序的要求一致；[见 11.1] A.11.4.7 网络路由控制 控制措施 应对网络进行路由控制，以确保信息联接及信息流不违反业务应用程序的访问控制政策；	connections from specific locations and equipment. A. 11.4.4 Remote diagnostic and configuration port protection Control Physical and logical access to diagnostic and configuration ports shall be controlled. A. 11.4.5 Segregation in networks Control Groups of information services, users, and information systems shall be segregated on networks. A. 11.4.6 Network connection control Control For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1). A. 11.4.7 Network routing control Control Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
A.11.5 操作系统访问控制 控制目标：防止对操作系统的未授权访问	***A.11.5 Operating system access control*** Objective: To prevent unauthorized access to operating systems.
A.11.5.1 安全登录程序 控制措施 应通过安全登录程序控制对操作系统的访问； A.11.5.2 用户标识和鉴别 控制措施 所有用户应有唯一的识别码（用户 ID）且仅供本人的使用，应使用适当的鉴别技术来证实用户的身份； A.11.5.3 口令管理系统 控制措施 应使用交互式口令管理系统，确保口令质量； A.11.5.4 系统设施的使用 控制措施 应限制并严格控制系统设施的使用和应用系统控制的使用； A.11.5.5 会话超时 控制措施 在规定时间内，不活动的会话会被中断； A.11.5.6 联机时间限制 控制措施 应使用联机时间的限制，为高风险的应用程序	A.11.5.1 Secure log-on procedures Control Access to operating systems shall be controlled by a secure log-on procedure. A. 11.5.2 User identification and authentication Control All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user. A. 11.5.3 Password management System Control Systems for managing passwords shall be interactive and shall ensure quality passwords. A. 11.5.4 Use of system utilities Control The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. A. 11.5.5 Session time-out Control Inactive sessions shall shut down after a defined period of inactivity. A. 11.5.6 Limitation of connection time Control Restrictions on connection times shall be used to provide additional security for high-risk applications.

提供额外的安全；	
A.11.6 应用系统和信息访问控制 控制目标：防止对应用系统中信息的未授权访问;	***A.11.6 Application and information access control*** Objective: To prevent unauthorized access to information held in application systems.
A.11.6.1 信息访问限制 控制措施 用户和支持人员对于信息及应用系统的功能的访问应依照访问控制策略加以限制； A.11.6.2 敏感系统隔离 控制措施 敏感系统应使用隔离的计算环境;	A.11.6.1 Information access restriction Control Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy. A.11.6.2 Sensitive system isolation Control Sensitive systems shall have a dedicated (isolated) computing environment.
A.11.7 移动计算和远程工作 控制目标：确保使用移动计算及远程工作设施的信息安全;	***A.11.7 Mobile computing and teleworking*** Objective: To ensure information security when using mobile computing and teleworking facilities.
A.11.7.1 移动计算和通讯 控制措施 应建立正式的政策并实施适当的措施，以防范使用移动计算和通讯设施的风险； A.11.7.2 远程工作 控制措施 应开发和实施远程工作的策略、操作计划和程序；	A.11.7.1 Mobile computing and communications Control A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities. A.11.7.2 Teleworking Control A policy, operational plans and procedures shall be developed and implemented for teleworking activities.
A.12 信息系统采集、开发及维护	**A.12 Information systems acquisition, development and maintenance**
A.12.1 信息系统安全要求 控制目标：确保安全成为信息系统的内置部分；	***A.12.1 Security requirements of information systems*** Objective: To ensure that security is an integral part of information systems.
A.12.1.1 安全要求分析及规范 控制措施 新的信息系统或对现有信息系统的更新的业务要求中应规定安全控制的要求；	A.12.1.1 Security requirements analysis and specification Control Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.
A.12.2 应用程序中的正确处理 控制目标：防止应用程序中的信息错误、遗失、修改及误用；	***A.12.2 Correct processing in applications*** Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications
A.12.2.1 输入数据验证 控制措施 应验证应用程序输入数据，以确保是正确且适当的； A.12.2.2 内部处理控制 控制措施 验证检查应成为系统的一部分，以检测数据处理过程中的错误； A.12.2.3 消息完整性	A.12.2.1 Input data validation Control Data input to applications shall be validated to ensure that this data is correct and appropriate. A.12.2.2 Control of internal processing Control Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. A.12.2.3 Message integrity

控制措施 应识别应用系统中确保鉴别和保护信息完整性的要求，并识别和实施适当的控制措施； A.12.2.4 输出数据验证 控制措施 应确认应用系统输出的数据，以确保储存的信息处理流程是正确的，并与环境相适宜；	Control Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented. A.12.2.4 Output data validation Control Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
A.12.3 加密控制 控制目标：使用加密方法去保护信息的机密性、真实性或完整性;	***A.12.3 Cryptographic controls*** Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.
A.12.3.1 使用加密控制的策略 控制措施 为了保护信息应开发和实施加密控制措施的策略； A.12.3.2 密钥管理 控制措施 应进行密钥管理，以支持组织的密码技术的运用；	A.12.3.1 Policy on the use of cryptographic controls Control A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management Control Key management shall be in place to support the organization’s use of cryptographic techniques.
A.12.4 系统文档安全 控制目标：确保系统文件安全；	***A.12.4 Security of system files*** Objective: To ensure the security of system files.
A.12.4.1 操作软件控制 控制措施 应建立程序对操作系统软件安装进行控制； A.12.4.2 系统测试数据的保护 控制措施 测试数据应仔细的选择，并加以保护及控制 A.12.4.3 源代码库的访问控制 控制措施 应限制访问源代码库；	A.12.4.1 Control of operational software Control There shall be procedures in place to control the installation of software on operational systems. A.12.4.2 Protection of system test data Control Test data shall be selected carefully, and protected and controlled. A.12.4.3 Access control to program source code Control Access to program source code shall be restricted.
A.12.5 开发及支持过程的安全 控制目标:维持应用系统的软件及信息的安全;	***A.12.5 Security in development and support processes*** Objective: To maintain the security of application system software and information.
A.12.5.1 变更控制程序 控制措施 应使用正式的变更控制程序，严格地控制变更的实施； A.12.5.2 操作系统变更的技术审查 控制措施 当操作系统发生变更后，应评审和测试关键的业务应用系统，确保对组织的运作和安全没有负面影响； A.12.5.3 软件包变更限制 控制措施	A.12.5.1 Change control procedures Control The implementation of changes shall be controlled by the use of formal change control procedures. A.12.5.2 Technical review of applications after operating system changes Control When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. A.12.5.3 Restrictions on changes to software packages Control

不鼓励对软件包的变更，对必要的更改需严格控制； A.12.5.4 信息泄露 控制措施 防止信息泄露的机会； A.12.5.5 软件外包开发 控制措施 组织应监督和控制软件外包开发；	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled. A.12.5.4 Information leakage Control Opportunities for information leakage shall be prevented. A.12.5.5 Outsourced software Development Control Outsourced software development shall be supervised and monitored by the organization.
A.12.6 技术漏洞管理 控制目标:减少由公开的技术漏洞产生的风险;	***A.12.6 Technical Vulnerability Management*** Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.
A.12.6.1 控制技术漏洞 控制措施 应及时的获得信息系统的技术漏洞，对漏洞进行评估，并采取适当的措施去处理相关风险；	A.12.6.1 Control of technical Vulnerabilities Control Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
A.13 信息安全事故的管理	**A.13 Information security incident management**
A.13.1 报告安全事件和弱点 控制目标：确保与信息系统相关信息安全事件和弱点的沟通，并及时采取纠正措施；	***A.13.1 Reporting information security events and weaknesses*** Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
A.13.1.1 信息安全事件报告 控制措施 应及时的通过适当管理渠道报告信息安全事件； A.13.1.2 报告信息安全弱点 控制措施 应要求使用信息系统和服务的所有员工、合同人员及第三方人员记录和报告在系统和服务中观察或可疑的弱点；	A.13.1.1 Reporting information security events Control Information security events shall be reported through appropriate management channels as quickly as possible. A.13.1.2 Reporting security weaknesses Control All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
A.13.2 信息安全事故的管理和改进 控制目标：确保持续、有效的方法管理信息安全事故管理;	***A.13.2 Management of information security incidents and improvements*** Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.
A.13.2.1 职责和程序 控制措施 应建立管理层的职责和程序，确保快速、有效、有序的响应信息安全事故； A.13.2.2 从安全事故中学习 控制措施 应建立合适的机制去量化和监控信息安全事故的类型、数量和价值； A.13.2.3 收集证据	A.13.2.1 Responsibilities and procedures Control Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents. A.13.2.2 Learning from information security incidents Control There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. A.13.2.3 Collection of evidence

控制措施 事故发生后，在法律上采取追踪个人或组织的行为（无论是民法或刑法），应收集、保留证据并以符合相关法律规定的形式呈现证据。	Control Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
A.14 业务连续性管理	**A.14 Business continuity management**
A.14.1 业务连续管理信息的安全方面 控制目标：防止业务运作中断并且保护关键业务流程免于信息系统的重大失效或灾难的影响，并确保及时恢复；	***A.14.1 Information security aspects of business continuity management*** Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
A.14.1.1 包含信息安全的业务连续性管理过程 控制措施 应在组织内开发和维护业务连续性管理过程，该过程陈述组织业务连续性对信息安全要求； A.14.1.2 业务连续性及风险评估 控制措施 应识别能导致业务过程中断的事件，及事件发生的可能性、中断的影响及信息安全后果； A.14.1.3 开发和实施包括信息安全的持续计划 控制措施 应开发和实施计划去维护和恢复运作，在关键业务过程中断、失败时，仍能确保信息在需要级别上和需要的时间里保持有效性； A.14.1.4 业务连续计划架构 控制措施 应维持一个单一的业务连续运作计划框架，以确保所有计划的一致性，且鉴别测试与维护的优先次序； A.14.1.5 业务连续计划的测试、维护与再评估 控制措施 应定期测试和更新业务连续计划，以确保更新及有效性；	A.14.1.1 Including information security in the business continuity management process Control A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity. A.14.1.2 Business continuity and risk assessment Control Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security. A.14.1.3 Developing and implementing continuity plans including information security Control Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. A.14.1.4 Business continuity planning framework Control A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. A.14.1.5 Testing, maintaining and reassessing Business continuity plans Control Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.
A. 15 符合性	**A.15 Compliance**
A.15.1 法律要求的符合性 控制目标：避免违反任何法律、法令、法规或合同要求，及任何安全要求；	***A.15.1 Compliance with legal requirements*** Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
A. 15.1.1 识别适用的法律法规	A.15.1.1 Identification of applicable legislation

控制措施 应清楚的定义所有相关法律、法规与合同的要求及组织的符合要求的方法并形成文件，并针对每个信息系统和组织进行更新； A. 15.1.2 知识产权（IPR） 控制措施 应实施适当的程序，确保使用有知识产权的资料和专利软件产品是符合法律、法规和合同要求； A.15.1.3 保护组织记录 控制措施 根据法律、法规、合同和业务要求，应防止组织的重要纪录遗失、破坏及篡改； A.15.1.4 个人信息的隐私及数据保护 控制措施 根据法律、法规或合同要求，保护数据和个人隐私； A.15.1.5 防范信息处理设施的误用 控制措施 应阻止用户把信息处理设施用于未授权的目的； A.15.1.6 加密控制法规 控制措施 使用密码控制应确保遵守相关协议、法律及规定；	Control All relevant statutory, regulatory and contractual requirements and the organization’s approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization. A.15.1.2 Intellectual property rights (IPR) Control Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. A.15.1.3 Protection of organizational records Control Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements. A.15.1.4 Data protection and privacy of personal information Control Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. A.15.1.5 Prevention of misuse of information processing facilities Control Users shall be deterred from using information processing facilities for unauthorized purposes. A.15.1.6 Regulation of cryptographic controls Control Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
A.15.2 符合安全策略、标准和技术的适应性 目标：确保系统符合组织的安全策略和标准；	***A.15.2 Compliance with security policies and standards, and technical compliance*** Objective: To ensure compliance of systems with organizational security policies and standards.
A.15.2.1 符合安全策略和标准 控制措施 管理者应确保在其职责范围内的所有安全程序被正确实施，以符合安全策略和标准； A.15.2.2 技术符合性检查 控制措施 应定期检查信息系统与安全实施标准的符合程度；	A.15.2.1 Compliance with security policies and standards Control Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. A.15.2.2 Technical compliance checking Control Information systems shall be regularly checked for compliance with security implementation standards.
A.15.3 信息系统审核的考虑因素 目标：最大化信息系统审核的有效性，最小化来自信息系统审核的影响；	***A.15.3 Information systems audit considerations*** Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.
A.15.3.1 信息系统审核控制	A.15.3.1 Information systems audit controls

控制措施	Control
应谨慎的策划对操作系统检查所涉及的审核要求和活动并获得许可，将业务过程中断风险降至最小；	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
A.15.3.2 信息系统审核工具保护	A.15.3.2 Protection of information systems audit tools
控制措施	Control
应限制对信息系统审计工具的访问，以防止可能的误用或损坏；	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.