

ISO 标准——IEC 27001:2013

信息安全管理体系—— 要求

仅供培训使用

Reference number
ISO/IEC 27001:2013(E)



1 范围	1 Scope
本国际标准规定了在组织背景下建立、实施、维护和持续改进信息安全管理体系。本标准还包括信息安全风险评估和处置要求，可裁剪以适用于组织。本国际标准的要求是通用的，适用于所有的组织，不考虑类型、规模和特征。当组织声称符合本国际标准时，任何条款4-10的排除是不可接受的。	This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. 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.
2 规范性引用文件 下列参考文件是本文件的标准参考，也是应用本文件必不可缺的。对于标注日期的引用文件，仅适用于引用版本。对于不标注日期的引用文件，适用于最新版本的引用文件。 ISO/IEC 27000，信息技术—安全技术—信息安全管理体系—简介和词汇表。	2 Normative references 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. ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary
3 术语和定义 ISO 27000的术语和定义适用于本文件	3 Terms and definitions For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

<p>4. 组织环境</p> <p>4.1 理解组织及其环境</p> <p>组织应当确定与信息安全管理体目的相关联及影响其实现预期结果能力的外部及内部环境。</p> <p>注：确定这些问题参考 ISO31000:2009 中 5.3 条款的建立组织外部和内部环境；</p> <p>4.2 理解相关方的需求和期望</p> <p>组织应确定：</p> <p>a) 信息安全管理体的利益相关方；</p> <p>b) 这些利益相关方的信息安全相关要求；</p> <p>注：利益相关方的要求可能包括法律、法规要求和合同责任。</p> <p>4.3 确定信息安全管理体范围</p> <p>组织应确定信息安全管理体的边界和应用性，以建立其范围。</p> <p>当确定此范围时，组织应考虑：</p> <p>a) 4.1 所提及的外部 and 内部问题；</p> <p>b) 4.2 所提及的要求；</p> <p>c) 接口和组织执行的活动之间的依赖关系，以及其他组织执行的活动。</p> <p>范围应成为文件化信息。</p> <p>4.4 信息安全管理体</p> <p>组织应按照本国际标准的要求建立、实施、维护和持续改进信息安全管理体。</p>	<p>4 Context of the organization</p> <p>4.1 Understanding the organization and its context</p> <p>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.</p> <p>NOTE: Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009.</p> <p>4.2 Understanding the needs and expectations of interested parties</p> <p>The organization shall determine:</p> <p>a) interested parties that are relevant to the information security management system; and</p> <p>b) the requirements of these interested parties relevant to information security.</p> <p>NOTE: The requirements of interested parties may include legal and regulatory requirements and contractual obligations.</p> <p>4.3 Determining the scope of the information security management system</p> <p>The organization shall determine the boundaries and applicability of the information security management system to establish its scope.</p> <p>When determining this scope, the organization shall consider:</p> <p>a) the external and internal issues referred to in 4.1;</p> <p>b) the requirements referred to in 4.2; and</p> <p>c) interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations.</p> <p>The scope shall be available as documented information.</p> <p>4.4 Information security management system</p> <p>The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.</p>
<p>5. 领导力</p> <p>5.1 领导力和承诺</p> <p>最高管理者应当展示关注信息安全管理体的领导力和承诺，通过：</p> <p>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兼容；</p> <p>b) 确保信息安全管理体要求融合到组织的流程中；</p>	<p>5 Leadership</p> <p>5.1 Leadership and commitment</p> <p>Top management shall demonstrate leadership and commitment with respect to the information security management system by:</p> <p>a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;</p> <p>b) ensuring the integration of the information security management</p>

<ul style="list-style-type: none"> c) 确保信息安全体系所需要的资源; d) 沟通有效信息安全管理的重要性,并符合信息安全管理体系的要求; e) 确保信息安全管理体系达到预期的成果; f) 指导和支持员工对信息安全管理体系的有效性做出贡献; g) 促进持续改进; h) 支持其他相关管理角色来展示其领导力,当适用其职责范围时。 	<p>system requirements into the organization's processes;</p> <ul style="list-style-type: none"> c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and 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.
<p>5.2 方针</p> <p>最高管理层应建立一个信息安全方针:</p> <ul style="list-style-type: none"> a) 与组织的目标相关适应; b) 包括信息安全目标 (见 6.2), 或提供制定信息安全目标的框架; c) 包括满足适用信息安全要求的承诺; d) 包括信息安全管理体系持续改进的承诺; <p>信息安全方针应:</p> <ul style="list-style-type: none"> e) 成为文件化的信息; f) 在组织内部沟通; g) 适当时, 提供给利益相关方; 	<p>5.2 Policy</p> <p>Top management shall establish an information security policy that:</p> <ul style="list-style-type: none"> 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; and d) includes a commitment to continual improvement of the information security management system. <p>The information security policy shall:</p> <ul style="list-style-type: none"> e) be available as documented information; f) be communicated within the organization; and g) be available to interested parties, as appropriate.
<p>5.3 组织角色、职责和权限</p> <p>最高管理层应确保信息安全相关角色的职责和权限的分配和沟通。</p> <p>最高管理层应指定责任和授权, 以:</p> <ul style="list-style-type: none"> a) 确保信息安全管理体系符合本国际标准的要求; b) 将信息安全管理体系绩效报告给最高管理层; <p>注: 最高管理层可以为组织内信息安全管理体系绩效报告指派职责和授权。</p>	<p>5.3 Organizational roles, responsibilities and authorities</p> <p>Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.</p> <p>Top management shall assign the responsibility and authority for:</p> <ul style="list-style-type: none"> 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. <p>NOTE: Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organization.</p>
<p>6. 策划</p> <p>6.1 针对风险和机会所采取的措施</p> <p>6.1.1 总则</p> <p>当进行信息安全管理体系策划时, 组织应</p>	<p>6 Planning</p> <p>6.1 Actions to address risks and opportunities</p> <p>6.1.1 General</p> <p>When planning for the information security management system, the organization</p>

<p>当考虑在 4.1 条款中提到事宜及 4.2 条款中规定的要求，并确定需要关注的风险和机会，以：</p> <ul style="list-style-type: none"> a) 确保信息安全管理体系能够实现其预期结果 b) 预防或降低不希望得到的影响 c) 实现持续改进 <p>组织应当计划：</p> <ul style="list-style-type: none"> d) 针对这些风险和机会所采取的措施，以及 e) 如何 <ul style="list-style-type: none"> 1) 将这些措施整合进信息安全管理体系过程之中， 2) 评价这些措施的有效性 <p>6.1.2 信息安全风险评估</p> <p>组织应定义和应用信息安全风险评估流程，以：</p> <ul style="list-style-type: none"> a) 建立和维护信息安全标准，包括 <ul style="list-style-type: none"> 1) 风险接受准则； 2) 执行信息安全风险评估准则； b) 确保可重复的信息安全风险评估生成一致、有效和可比较的结果 c) 识别信息安全风险 <ul style="list-style-type: none"> 1) 应用信息安全风险评估流程，识别 ISMS 范围内信息保密性、完整性和可用性损失的风险； 2) 识别风险所有者； d) 风险信息安全风险评估 <ul style="list-style-type: none"> 1) 评估在 6.1.2 c) 1) 中识别风险导致的潜在后果 2) 评估在 6.1.2 c) 1) 中识别风险发生性的可能性 3) 确定风险等级 e) 评估信息安全风险 <ul style="list-style-type: none"> 1) 风险分析结果与 6.1.2 a) 中建立的风险准则进行比较 2) 为风险处理，建立风险优先级和分析 <p>组织应保留文件化的信息安全风险评估流程信息</p>	<p>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:</p> <ul style="list-style-type: none"> a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement. <p>The organization shall plan:</p> <ul style="list-style-type: none"> d) actions to address these risks and opportunities, and e) how to <ul style="list-style-type: none"> 1) integrate and implement the actions into its information security management system processes; and 2) evaluate the effectiveness of these actions. <p>6.1.2 Information security risk assessment</p> <p>The organization shall define and apply an information security risk assessment process that:</p> <ul style="list-style-type: none"> a) establishes and maintains information security criteria that include: <ul style="list-style-type: none"> 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) Identify the information security risks. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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) Evaluate the information security risks. <ul style="list-style-type: none"> 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. <p>The organization shall retain documented information about the information security risk assessment process.</p>
---	--

<p>6.1.3 信息安全风险处置</p> <p>组织应定义和应用信息安全风险处置流程，以：</p> <ul style="list-style-type: none"> a) 选择适当的信息安全风险处置选项，考虑风险评估结果； b) 确定实施所选信息安全风险处置选项所需的所有控制措施； <p>注：组织可设计所需的控制措施，或从任何来源中识别它们</p> <ul style="list-style-type: none"> c) 比较6.1.3 b)中与附录A中的措施项，确认没有忽略必要的控制项； <p>注1：附录A包含控制目标和控制措施的完整列表。本国际标准用户应确保附录A的重要控制措施没有被忽略</p> <p>注2：控制目标隐含在所选择的控制项中。附录A中的控制目标和控制措施并不全面，可能还需要额外的控制目标和控制措施。</p> <ul style="list-style-type: none"> d) 制作适用性声明，包括必要的控制措施（见6.1.3 b)和c)）和选择的理由，无论实施与否，应说明删减附录A中控制措施的理由； e) 制定信息安全风险处置计划； f) 获得风险所有者批准信息安全风险处置计划和残余信息安全风险接受标准； <p>组织应保留信息安全风险处置过程的文件化信息。</p> <p>注：本国际标准中信息安全风险评估和处置过程与ISO31000中的原则和通用指南一致。</p> <p>6.2 信息安全目标及实现其目标的策划</p> <p>组织应当在相关职能及层次上建立信息安全目标。</p> <p>信息安全目标应：</p> <ul style="list-style-type: none"> a) 与信息安全方针保持一致； b) 是可测量的（如果可行）； c) 考虑适用的信息安全要求，以及风险评估和风险处置的结果； d) 是可沟通的； 	<p>6.1.3 Information security risk treatment</p> <p>The organization shall define and apply an information security risk treatment process to:</p> <ul style="list-style-type: none"> 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; <p>NOTE: Organizations can design controls as required, or identify them from any source.</p> <ul style="list-style-type: none"> 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; <p>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 important control are overlooked</p> <p>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 also be needed.</p> <ul style="list-style-type: none"> 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 in Annex A; e) formulate an information security risk treatment plan; and f) obtain risk owner's approval of the information security risk treatment plan and the acceptance of the residual information security risks. <p>The organization shall retain documented information about the information security risk treatment process.</p> <p>NOTE: The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000.</p> <p>6.2 Information security objectives and planing to achieve them</p> <p>The organization shall establish information security objectives at relevant functions and levels.</p> <p>The information security objectives shall:</p> <ul style="list-style-type: none"> 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 treatment results; d) be communicated, and
---	--

<p>e) 能适时更新;</p> <p>组织应当保持信息安全目标的文件化信息。</p> <p>当对实现其信息安全目标进行策划时, 组织应当确定:</p> <p>f) 将要做什么</p> <p>g) 将需要什么资源</p> <p>h) 将由谁来做</p> <p>i) 将在何时完成</p> <p>j) 将如何对结果进行评价</p>	<p>e) be updated as appropriate.</p> <p>The organization shall retain documented information on the information security objectives.</p> <p>When planning how to achieve its information security objectives, the organization shall determine:</p> <p>f) what will be done;</p> <p>g) what resources will be required;</p> <p>h) who will be responsible;</p> <p>i) when it will be completed; and</p> <p>j) how the results will be evaluated.</p>
<p>7. 支持</p> <p>7.1 资源</p> <p>组织应确定和提供信息安全管理体的建立、实施、维护和持续改进所需的资源。</p> <p>7.2 能力</p> <p>组织应:</p> <p>a) 确定影响组织信息安全绩效的员工在 ISMS 管控中工作的必备能力;</p> <p>b) 确保这些员工在适当的培育、培训和经验的基础上是能胜任的;</p> <p>c) 适当时, 采取行动获取所需能力, 并评估所采取行动的有效性;</p> <p>d) 保留适当文件化信息作为证据;</p> <p>注: 适当的行动可能包括, 如提供培训、指导、重新指派现有员工、或聘用或外包有能力的员工。</p> <p>7.3 意识</p> <p>在组织控制中工作的人员应了解:</p> <p>a) 信息安全方针;</p> <p>b) 信息安全管理体有效性的贡献, 包括提高信息安全绩效的收益;</p> <p>c) 不符合信息安全管理体要求的影响;</p> <p>7.4 沟通</p> <p>组织应当确定与信息安全管理体相关内部和外部沟通需求, 包括:</p> <p>a) 需要沟通内容</p> <p>b) 何时进行沟通</p>	<p>7 Support</p> <p>7.1 Resources</p> <p>The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.</p> <p>7.2 Competence</p> <p>The organization shall:</p> <p>a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;</p> <p>b) ensure that these persons are competent on the basis of appropriate education, training, or experience;</p> <p>c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and</p> <p>d) retain appropriate documented information as evidence of competence.</p> <p>NOTE: Applicable actions may include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.</p> <p>7.3 Awareness</p> <p>Persons doing work under the organization's control shall be aware of:</p> <p>a) the information security policy;</p> <p>b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and</p> <p>c) the implications of not conforming with the information security management system requirements.</p> <p>7.4 Communication</p> <p>The organization shall determine the need for internal and external communications relevant to the information security management system including:</p> <p>a) on what to communicate;</p>

<ul style="list-style-type: none"> c) 与谁进行沟通 d) 谁应该沟通 e) 有效沟通的流程 	<ul style="list-style-type: none"> b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected.
<p>7.5 文件化信息</p>	<p>7.5 Documented information</p>
<p>7.5.1 总则</p>	<p>7.5.1 General</p>
<p>组织的信息安全管理体系应包括：</p>	<p>The organization's information security management system shall include:</p>
<ul style="list-style-type: none"> a) 本国际标准所需要的文件化信息； b) 组织确定信息安全管理体系有效性所需要的信息； 	<ul style="list-style-type: none"> 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.
<p>注：不同组织的信息安全管理体系文件化信息的程度取决于：</p>	<p>NOTE: The extent of documented information for an information security management system can differ from one organization to another due to:</p>
<ul style="list-style-type: none"> 1) 组织的规模、其活动类型、流程、产品和服务； 2) 流程及其他交互的复杂性； 3) 人员的能力； 	<ul style="list-style-type: none"> 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.
<p>7.5.2 创建和更新</p>	<p>7.5.2 Creating and updating</p>
<p>当创建和更新文件化信息时，组织应确保适当的：</p>	<p>When creating and updating documented information the organization shall ensure appropriate:</p>
<ul style="list-style-type: none"> a) 识别和描述（如标题、日期、作者或参考号码）； b) 格式（如语言、软件版本、图形）和媒体（如纸张、电子）； c) 评估和批准适当性和充分性。 	<ul style="list-style-type: none"> a) identification and description (e.g. a title, date, author, or reference number); b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c) review and approval for suitability and adequacy.
<p>7.5.3 文件化信息控制</p>	<p>7.5.3 Control of documented information</p>
<p>信息安全管理体系和本国际标准所要求的文件化信息应被管控，以确保：</p>	<p>Documented information required by the information security management system and by this International Standard shall be controlled to ensure:</p>
<ul style="list-style-type: none"> a) 需要时，文件是可用和适用的； b) 得到充分的保护（如保密性丧失、不当使用、或完整性丧失）； 	<ul style="list-style-type: none"> 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).
<p>对于文件化信息的控制，组织应制定下列活动（如适用）：</p>	<p>For the control of documented information, the organization shall address the following activities, as applicable:</p>
<ul style="list-style-type: none"> c) 分配、访问、检索和使用； d) 存储和保存，包括易读性的保存； 	<ul style="list-style-type: none"> c) distribution, access, retrieval and use; d) storage and preservation, including the preservation of legibility;

<p>e) 变更管理（如版本控制）； f) 保留和处置；</p> <p>组织信息安全管理体的规划和运作所需的外来文件化信息，应被适当的识别和管理；</p> <p>注：访问表示有权查看文件化信息，或获得权限或授权以查看和变更文件化信息等；</p>	<p>e) control of changes (e.g. version control); and f) retention and disposition.</p> <p>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.</p> <p>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.</p>
<p>8. 运行</p> <p>8.1 运行策划和控制</p> <p>组织应策划、实施和控制满足信息安全要求的流程，并实施在 6.1 中规定的措施。组织还应实施计划，以实现信息安全在 6.2 中确定的目标。</p> <p>组织应保存相关文件化信息，以保证流程已经按照计划实施。</p> <p>组织应控制计划变更，评审非计划变更的后果，如需要，采取适当措施减轻不良影响；</p> <p>组织应确保外包活动被确定和受控。</p> <p>8.2 信息安全风险评估</p> <p>组织应在定期或发生重大变化时执行信息安全风险评估，将 6.1.2 中建立的标准纳入考虑范围。</p> <p>组织应保留信息安全风险评估结果的相关文件化信息。</p> <p>8.3 信息安全风险处置</p> <p>组织应实施信息安全风险处置计划。</p> <p>组织应保留信息安全风险处置结果的文件化信息。</p>	<p>8 Operation</p> <p>8.1 Operational planning and control</p> <p>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.</p> <p>The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.</p> <p>The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.</p> <p>The organization shall ensure that outsourced processes are determined and controlled.</p> <p>8.2 Information security risk assessment</p> <p>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).</p> <p>The organization shall retain documented information of the results of the information security risk assessments.</p> <p>8.3 Information security risk treatment</p> <p>The organization shall implement the information security risk treatment plan.</p> <p>The organization shall retain documented information of the results of the information security risk treatment.</p>
<p>9. 绩效评价</p> <p>9.1 监视、测量、分析和评价</p> <p>组织应评估信息安全绩效和信息安全管理体系的有效性。</p> <p>组织应当确定：</p> <p>a) 什么需要监控和测量，包括信息安全流程和控制</p>	<p>9 Performance evaluation</p> <p>9.1 Monitoring, measurement, analysis and evaluation</p> <p>The organization shall evaluate the information security performance and the effectiveness of the information security management system.</p> <p>The organization shall determine:</p> <p>a) what needs to be monitored and measured, including information security processes and controls;</p>

<p>b) 采用什么适宜方法来进行监控、测量、分析和评价，以确保结果有效 注：生成可比较和可重复结果的所选方法被认为是有效的</p> <p>c) 何时应当进行监控和测量</p> <p>d) 何时应当对监控和测量结果进行分析和评价</p> <p>e) 谁分析和评估结果</p> <p>组织应当保持适当的文件化信息作为监控和测量结果的证据。</p>	<p>b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; NOTE: The methods selected should produce comparable and reproducible results to be considered valid.</p> <p>c) when the monitoring and measuring shall be performed;</p> <p>d) who shall monitor and measure;</p> <p>e) when the results from monitoring and measurement shall be analysed and evaluated; and</p> <p>f) who shall analyse and evaluate these results.</p> <p>The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.</p>
<p>9.2 内部审核</p> <p>组织应当按照计划的时间间隔进行内部审核，以确定信息安全管理体系统：</p> <p>a) 符合</p> <p>1) 组织自身信息安全管理体系统的要求；</p> <p>2) 本国际标准的要求</p> <p>b) 有效的实施和维护； 组织应：</p> <p>c) 计划、建立、实施和维护审核方案，包括频率、方法、职责、规划要求和报告。审核方案应考虑相关过程和以往审核结果的重要性；</p> <p>d) 定义每次审核准则和范围；</p> <p>e) 选择审核员工和执行审核，确保审核过程的客观和公正；</p> <p>f) 确保审核结果报告提交相关管理层；</p> <p>g) 保留审核方案和审核结果的文件化信息；</p>	<p>9.2 Internal audit</p> <p>The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:</p> <p>a) conforms to</p> <p>1) the organization's own requirements for its information security management system; and</p> <p>2) the requirements of this International Standard;</p> <p>b) is effectively implemented and maintained.</p> <p>The organization shall:</p> <p>c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;</p> <p>d) define the audit criteria and scope for each audit;</p> <p>e) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;</p> <p>f) ensure that the results of the audits are reported to relevant management; and</p> <p>g) retain documented information as evidence of the audit programme(s) and the audit results.</p>
<p>9.3 管理评审</p> <p>管理者应按计划的时间间隔（至少每年 1 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。</p> <p>管理评审应考虑：</p> <p>a) 以往管理评审措施的状态；</p> <p>b) 信息安全管理体系统相关的内外部变化；</p> <p>c) 信息安全绩效的反馈，包括：</p>	<p>9.3 Management review</p> <p>Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.</p> <p>The management review shall include consideration of:</p> <p>a) the status of actions from previous management reviews;</p> <p>b) changes in external and internal issues that are relevant to the information security management system;</p> <p>c) feedback on the information security performance, including</p>

<p>1) 不符合和纠正措施; 2) 监控和测量结果; 3) 审核结果; 4) 信息安全目标的实现; d) 相关方反馈; e) 风险评估结果和风险处置计划的状态; f) 持续改进的机会;</p> <p>管理评审的输出应包括持续改进机会和任何信息安全管理体系变更所需的相关决定; 组织应保留管理评审结果的文件化信息作为证据;</p>	<p>trends in:</p> <p>1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 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.</p> <p>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.</p> <p>The organization shall retain documented information as evidence of the results of management reviews.</p>
<p>10. 改进 10.1 不合格和纠正措施 当出现不符合项时, 组织应:</p> <p>a) 对不符合项作出反应, 适用时:</p> <p>1) 采取措施控制和纠正; 2) 处理后果;</p> <p>b) 评估采取措施的必要性, 以消除不符合项的原因, 使其不再发生或在其他地方发生, 通过:</p> <p>1) 评审不符合项; 2) 确定不符合原因; 3) 确定类似不符合性存在, 或发生的可能;</p> <p>c) 实施所需的任何措施; d) 评审已采取纠正措施的有效性; e) 如需要, 变更信息安全管理体系;</p> <p>纠正措施应适当的影响不符合项; 组织应保留文件化信息, 作为下列证据:</p> <p>f) 不符合项的特征和任何后续采取的措施; g) 任何纠正措施的结果;</p> <p>10.2 持续改进 组织应持续提高信息安全管理体系的适宜性、充分性和有效性;</p>	<p>10 Improvement 10.1 Nonconformity and corrective action When a nonconformity occurs, the organization shall:</p> <p>a) react to the nonconformity, and as applicable:</p> <p>1) take action to control and correct it; and 2) deal with the consequences;</p> <p>b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:</p> <p>1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur;</p> <p>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.</p> <p>Corrective actions shall be appropriate to the effects of the nonconformities encountered.</p> <p>The organization shall retain documented information as evidence of:</p> <p>f) the nature of the nonconformities and any subsequent actions taken, and g) the results of any corrective action.</p> <p>10.2 Continual improvement The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.</p>

<p>附录 A（引用）</p> <p>控制目标和控制措施</p> <p>表 A-1 所列的控制目标和控制措施是直接源自并与 ISO/IEC 17799:2005 第 5 到 15 章一致。表 A.1 中的清单并不详尽，一个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 ISMS 过程的一部分。</p> <p>ISO/IEC 17799:2005 第 5 至 15 章提供了最佳实践的实施建议和指南，以支持 A.5 到 A.15 列出的控制措施。</p>	<p>Annex A (normative)</p> <p>Reference control objectives and controls</p> <p>The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC DIS 27002:2013 Clauses 5 to 18 and are to be used in context with Clause 6.1.3.</p>
--	---

A. 5 安全方针	A.5 Information security policies
A. 5.1 管理信息安全方向 控制目标：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 Management direction for information security Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
A. 5.1.1 信息安全方针 控制措施 一系列信息安全方针应被定义、并由管理者批准、发布并传达给员工和外部相关方。	A.5.1.1 Policies for information security Control A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties
A. 5.1.2 信息安全方针评审 控制措施 宜按计划的时间间隔或当重大变化发生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。	A.5.1.2 Review of the policies for information security Control The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their 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：建立管理架构，启动和控制信息安全在组织内的实施；	A.6.1 Internal organization Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization
A. 6.1.1 信息角色和职责 控制措施 所有信息安全职责应被定义和分配；	A.6.1.1 Information security roles and responsibilities Control All information security responsibilities shall be defined and allocated
A. 6.1.2 责任分割 控制措施 冲突责任及职责范围加以分割，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.6.1.2 Segregation of duties Control Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A. 6.1.3 与政府部门的联系 控制措施 应保持与政府相关部门的适当联系；	A.6.1.3 Contact with authorities Control Appropriate contacts with relevant authorities shall be maintained
A. 6.1.4 与特定利益集团的联系 控制措施 应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.6.1.4 Contact with special interest groups Control Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained
A. 6.1.5 项目管理中的信息安全 控制措施 无论项目类型，项目管理中均应描述信息安全；	A.6.1.5 Information security in project management Control Information security shall be addressed in project management, regardless of the type of the project
A. 6.2 移动设备和远程工作 控制目标：确保使用移动设备的使用及远程工作的安全；	A.6.2 Mobile devices and teleworking Objective: To ensure the security of teleworking and use of mobile devices
A. 6.2.1 移动设备策略 控制措施 应采用策略和相应的安全测量，以防范使用移动设备时所造成的风险；	A.6.2.1 Mobile device policy Control A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices

<p>A. 6.2.2 远程工作</p> <p>控制措施</p> <p>应实施策略和相应的安全测量，以防保护信息的访问、处理和存储在远程站点；</p>	<p>A.6.2.2 Teleworking</p> <p>Control</p> <p>A policy and supporting security measures shall be implemented to protect information accessed, processed or stored on teleworking sites</p>
<p>A.7 人力资源安全</p>	<p>A.7 Human resource security</p>
<p>A.7.1 任用之前</p> <p>控制目标：建立管理框架，以启动和控制组织内信息安全的实施；</p>	<p>A.7.1 Prior to employment</p> <p>Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.</p>
<p>A.7.1.1 审查</p> <p>控制措施</p> <p>所有任用候选者的背景验证检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> <p>A.7.1.2 任用条款和条件</p> <p>控制措施</p> <p>与员工和合同方的合同应声明他们和组织的信息安全职责；</p>	<p>A.7.1.1 Screening</p> <p>Control</p> <p>Background verification checks on all candidates for employment 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</p> <p>A.7.1.2 Terms and conditions of employment</p> <p>Control</p> <p>The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security</p>
<p>A.7.2 任用中</p> <p>控制目标：确保雇员和合同方知悉和实施他们信息安全职责；</p>	<p>A.7.2 During employment</p> <p>Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities</p>
<p>A.7.2.1 管理职责</p> <p>控制措施</p> <p>管理者应要求所有雇员和合同方按照组织已建立的方针策略和程序对安全尽心尽力；</p> <p>A.7.2.2 信息安全意识、教育和培训</p> <p>控制措施</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和培训，以及组织方针策略及程序的定期更新培训；</p> <p>A.7.2.3 纪律处理过程</p> <p>控制措施</p> <p>应有一个正式和已传达的纪律处理过程，对于安全违规的雇员采取行动；</p>	<p>A.7.2.1 Management Responsibilities</p> <p>Control</p> <p>Management shall require all employees and contractors users to apply information security in accordance with established policies and procedures of the organization</p> <p>A.7.2.2 Information security awareness, education and training</p> <p>Control</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>A.7.2.3 Disciplinary process</p> <p>Control</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>A.7.3 任用的终止或变化</p> <p>控制目标：保护组织的利益，作为改变或终止任用关系流程的一部分；</p>	<p>A.7.3 Termination and change of employment</p> <p>Objective: To protect the organization's interests as part of the process of changing or terminating employment</p>
<p>A.7.3.1 作用职责的终止或改变</p> <p>控制措施</p> <p>任用终止或任用变更后，仍保持有效的信息安全责任和职责应被定义和传达到雇员或合同方，并强制执行；</p>	<p>A.7.3.1 Termination or change of employment responsibilities</p> <p>Control</p> <p>Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced</p>

A.8 资产管理	A.8 Asset management
A.8.1 资产职责 控制目标：识别组织资产，定义适当的保护职责	A.8.1 Responsibility for assets Objective: To identify organizational assets and define appropriate protection responsibilities.
A.8.1.1 资产清单 控制措施 应识别信息和信息处理设施相关的资产，编制并维护所有资产的清单；	A.8.1.1 Inventory of assets Control Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained
A.8.1.2 资产责任人 控制措施 资产清单中维护的资产应有责任人；	A.8.1.2 Ownership of assets Control Assets maintained in the inventory shall be owned
A.8.1.3 资产的可接受使用 控制措施 与信息处理设施有关的信息和资产可接受使用规则应被确定、形成文件并加以实施；	A.8.1.3 Acceptable use of Assets Control Rules for the acceptable use of information and assets associated with information and information processing facilities shall be identified, documented and implemented
A.8.1.4 资产的归还 控制措施 所有的雇员和外部人员在终止任用、合同或协议时，应归还他们使用的所有组织资产；	A.8.1.4 Return of assets Control All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement
A.8.2 信息分类 控制目标：根据信息对组织的重要性，确保受到适当级别的保护	A.8.2 Information classification Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization
A.8.2.1 分类指南 控制措施 信息应按照未授权泄露或篡改的法律要求、价值、敏感性和关键性予以分类；	A.8.2.1 Classification of Information Control Information shall be classified in terms of legal requirements, value, criticality, sensitivity to unauthorized disclosure or modification.
A.8.2.2 信息的标记 控制措施 应按照组织所采纳的信息分类机制建立和实施一组合适的信息标记程序；	A.8.2.2 Labeling of information Control An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization
A.8.2.3 资产的处理 控制措施 应按照组织所采纳的信息分类机制建立和实施资产处理程序；	A.8.2.3 Handling of assets Control Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization
A.8.3 介质处理 控制目标：防止未泄露、修改、移动或销毁存储在介质上的信息	A.8.3 Media handling Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media
A.8.3.1 可移动介质的管理 控制措施 应按照组织所采纳的信息分类机制实施可移动介质的管理规程；	A.8.3.1 Management of removable media Control Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization
A.8.3.2 介质的报废处置	A.8.3.2 Disposal of media

<p>控制措施</p> <p>不再需要的介质，应使用正式的规程安全地处置；</p> <p>A. 8. 3. 3 运输中的物理介质</p> <p>控制措施</p> <p>包含信息的介质应防止未授权的访问、不当使用或毁坏；</p>	<p>Control</p> <p>Media shall be disposed of securely when no longer required, using formal procedures</p> <p>A.8.3.3 Physical media transfer</p> <p>Control</p> <p>Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.</p>
A. 9 访问控制	A.9 Access control
<p>A. 9. 1 访问控制的业务要求</p> <p>控制目标：控制对信息和信息处理设施的访问；</p>	<p>A.9.1 Business requirements of access control</p> <p>Objective: To limit access to information and information processing facilities</p>
<p>A. 9. 1. 1 访问控制策略</p> <p>控制措施</p> <p>访问控制策略应建立、形成文件，并基于业务和信息安全要求进行评审；</p> <p>A. 9. 1. 访问网络和网络服务的策略</p> <p>控制措施</p> <p>用户应仅能访问已获专门授权使用的网络和网络服务；</p>	<p>A.9.1.1 Access control policy</p> <p>Control</p> <p>An access control policy shall be established, documented and reviewed based on business and information security requirements</p> <p>A.9.1.2 Access to network and network services</p> <p>Control</p> <p>Users shall only be provided with access to the network and network services that they have been specifically authorized to use</p>
<p>A. 9. 2 用户访问管理</p> <p>控制目标：确保授权用户访问系统和服务，并避免未授权访问</p>	<p>A.9.2 User access management</p> <p>Objective: To ensure authorized user access and to prevent unauthorized access to systems and services</p>
<p>A. 9. 2. 1 用户注册和注销</p> <p>控制措施</p> <p>应实施正式用户注册和注销规程，确保访问权限分配</p> <p>A. 9. 2. 2 提供用户访问</p> <p>控制措施</p> <p>应实施正式提供用户访问规程，为所有系统和所有用户类型分派和撤销访问权限；</p> <p>A. 9. 2. 3 特权访问权限管理</p> <p>控制措施</p> <p>应限制和控制特权访问权限的分配和使用；</p> <p>A. 9. 2. 4 管理用户的秘密验证信息</p> <p>控制措施</p> <p>通过正式管理规程控制秘密验证信息的分配；</p> <p>A. 9. 2. 5 用户访问权的复查</p> <p>控制措施</p> <p>资产所有者应定期对用户的访问权进行复查；</p> <p>A. 9. 2. 6 撤销或调整访问权</p> <p>控制措施</p> <p>所有雇员和外部用户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，</p>	<p>A.9.2.1 User registration and de-registration</p> <p>Control</p> <p>A formal user registration and de-registration procedure shall be implemented to enable assignment of access rights.</p> <p>A.9.2.2 User access provisioning</p> <p>Control</p> <p>A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.</p> <p>A.9.2.3 Management of privileged access rights</p> <p>Control</p> <p>The allocation and use of privileged access rights shall be restricted and controlled.</p> <p>A.9.2.4 Management of secret authentication information of users</p> <p>Control</p> <p>The allocation of secret authentication information shall be controlled through a formal management process</p> <p>A.9.2.5 Review of user access Rights</p> <p>Control</p> <p>Asset owners shall review users' access rights at regular intervals</p> <p>A.9.2.6 Removal or adjustment of access rights</p> <p>Control</p> <p>The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their</p>

或在变化时调整;	employment, contract or agreement, or adjusted upon change
A. 9.3 用户职责 控制目标: 确保用户保护他们验证信息	A.9.3 User responsibilities Objective: To make users accountable for safeguarding their authentication information
A. 9.3.1 使用秘密验证信息 控制措施 使用秘密验证信息时, 应要求用户遵守组织安全实施;	A.9.3.1 Use of secret authentication information Control Users shall be required to follow the organization's security practices in the use of secret authentication information
A. 9.4 系统和应用访问控制 控制目标: 避免未经授权访问系统和应用	A.9.4 System and application access control Objective: To prevent unauthorized access to systems and applications
A. 9.4.1 信息访问限制 控制措施 对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; A. 9.4.2 安全登录流程 控制措施 当需要访问控制策略时, 系统和应用的访问应有安全登录流程的控制 A. 9.4.3 口令管理系统 控制措施 口令管理系统应是交互式的, 并确保优质的口令; A. 9.4.4 系统实用工具的使用 控制措施 可能超越系统和应用程序控制的实用工具的使用应加以限制并严格控制; A. 9.4.5 对程序源代码的访问控制 控制措施 应限制访问程序源代码;	A.9.4.1 Information access Restriction Control Access to information and application system functions shall be restricted in accordance with the access control policy A.9.4.2 Secure log-on Procedures Control Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure A.9.4.3 Password management System Control Passwords management systems shall be interactive and shall ensure quality passwords A.9.4.4 Use of privileged utility Programs Control The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled A.9.4.5 Access control to program source code Control Access to program source code shall be restricted
A. 10 密码	A.10 Cryptography
A. 10.1 密码控制 控制目标: 确保适当和有效的使用密码方法保护信息的保密性、真实性或完整性;	A.10.1 Cryptographic controls Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information
A. 10.1.1 使用密码控制的策略 控制措施 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 密钥管理 控制措施 应开发密钥的使用、保护和生命周期的策略, 并在整个生命周期中实施	A.10.1.1 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.10.1.2 Key management Control A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle
A. 11 物理环境安全	A.11 Physical and environmental security
A. 11.1 安全区域 控制目标: 防止对组织信息这和信息处理设施	A.11.1 Secure areas Objective: To prevent unauthorized physical access, damage and interference to

的未授权物理访问、损坏和干扰；	the organization's information and information processing facilities
<p>A. 11.1.1 物理安全边界</p> <p>控制措施</p> <p>应定义和使用安全边界，来保护包含敏感或关键信息和信息处理设施的区域；</p> <p>A. 11.1.2 物理入口控制</p> <p>控制措施</p> <p>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；</p> <p>A. 11.1.3 办公室、房间和设施的安全保护</p> <p>控制措施</p> <p>应为办公室、房间和设施设计并采取物理安全措施；</p> <p>A. 11.1.4 外部和环境威胁的安全防护</p> <p>控制措施</p> <p>为防止自然灾害、恶意攻击或意外事件，应设计和采取物理保护措施；</p> <p>A. 11.1.5 在安全区域工作</p> <p>控制措施</p> <p>应设计和运用用于安全区域工作的流程；</p> <p>A. 11.1.6 交接区安全</p> <p>控制措施</p> <p>访问点（例如交接区）和未授权人员可进入办公场所的其他点应加以控制，如果可能，要与信息处理设施隔离，以避免未授权访问；</p>	<p>A.11.1.1 Physical security Perimeter</p> <p>Control</p> <p>Security perimeters shall be defined and used to protect areas that contain either sensitive or or critical information and information processing facilities</p> <p>A.11.1.2 Physical entry controls</p> <p>Control</p> <p>Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access</p> <p>A.11.1.3 Securing office, room and facilities</p> <p>Control</p> <p>Physical security for offices, rooms and facilities shall be designed and Applied</p> <p>A.11.1.4 Protecting against external end environmental threats</p> <p>Control</p> <p>Physical protection against natural disasters, malicious attack or accidents shall be designed and applied</p> <p>A.11.1.5 Working in secure areas</p> <p>Control</p> <p>Procedure for working in secure areas shall be designed and applied</p> <p>A.11.1.6 Delivery and loading areas</p> <p>Control</p> <p>Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access</p>
<p>A. 11.2 设备安全</p> <p>控制目标：防止资产的丢失、损坏、失窃或危及资产安全以及组织运营的中断；</p>	<p>A.11.2 Equipment</p> <p>Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations</p>
<p>A. 11.2.1 设备安置和保护</p> <p>控制措施</p> <p>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</p> <p>A. 11.2.2 支持性设施</p> <p>控制措施</p> <p>应保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断；</p> <p>A. 11.2.3 布缆安全</p> <p>控制措施</p> <p>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；</p> <p>A. 11.2.4 设备维护</p> <p>控制措施</p> <p>设备应予以正确地维护，以确保其持续的可用性和完整性；</p>	<p>A.11.2.1 Equipment siting and protection</p> <p>Control</p> <p>Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access</p> <p>A.11.2.2 Supporting utilities</p> <p>Control</p> <p>Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities</p> <p>A.11.2.3 Cabling security</p> <p>Control</p> <p>Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage</p> <p>A.11.2.4 Equipment maintenance</p> <p>Control</p> <p>Equipment shall be correctly maintained to ensure its continued availability and integrity</p>

<p>A. 11.2.5 资产的移动 控制措施 设备、信息或软件在授权之前不应带出组织场所；</p> <p>A. 11.2.6 组织场所外的设备安全 控制措施 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；</p> <p>A. 11.2.7 设备的安全处置或再利用 控制措施 包含储存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；</p> <p>A. 11.2.8 无人值守的用户设备 控制措施 用户应确保无人值守的用户设备有适当的保护；</p> <p>A. 11.2.9 清空桌面和屏幕策略 控制措施 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；</p>	<p>A.11.2.5 Removal of assets Control Equipment, information or software shall not be taken off-site without prior authorization</p> <p>A.11.2.6 Security of equipment and assets off-premises Control Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises</p> <p>A.11.2.7 Security disposal or re-use of equipment Control 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</p> <p>A.11.2.8 Unattended user Equipment Control Users shall ensure that unattended equipment has appropriate protection</p> <p>A.11.2.9 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</p>
<p>A. 12 运营安全</p>	<p><i>A.12 Operations security</i></p>
<p>A. 12.1 操作程序及职责 控制目标：确保正确、安全的操作信息处理设施；</p>	<p><i>A.12.1 Operational procedures and responsibilities</i> Objective: To ensure correct and secure operations of information processing facilities</p>
<p>A. 12.1.1 文件化的操作程序 控制措施 操作程序应形成文件、保持并对所有需要的用户可用；</p> <p>A. 12.1.2 变更管理 控制措施 对于影响信息安全的组织、业务流程、信息处理设施和系统的变更应加以控制；</p> <p>A. 12.1.3 容量管理 控制措施 资源的使用应加以监视、调整，并应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> <p>A. 12.1.4 开发、测试和运行设施分离 控制措施 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>	<p>A.12.1.1 Documented operating Procedures Control Operating procedures shall be documented and made available to all users who need them</p> <p>A.12.1.2 Change management Control Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled</p> <p>A.12.1.3 Capacity management Control The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance</p> <p>A.12.1.4 Separation of development, testing and operational environments Control Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment</p>
<p>A. 12.2 防范恶意代码 控制目标：确保信息和信息处理设施不受恶意</p>	<p><i>A.12.2 Protection from malware</i> Objective: To ensure that information and information processing facilities are</p>

软件侵害	protected against malware
A. 12. 2. 1 控制恶意代码 控制措施 应实施恶意代码的监测、预防和恢复的控制措施，以及适当的用户意识；	A.12.2.1 Controls against Malware Control Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness
A. 12. 3 备份 控制目标：防止数据的丢失；	A.12.3 Backup Objective: To protect against loss of data
A. 12. 3. 1 信息备份 控制措施 应按照协商的备份策略，定期备份和测试信息、软件和系统影像；	A.12.3.1 Information backup Control Backup copies of information, software and system images shall be taken and tested regularly in accordance with the agreed backup policy
A. 12. 4 日志和监视 控制目标：记录事件和生成证据；	A.12.4 Logging and monitoring Objective: To record events and generate evidence
A. 12. 4. 1 事件记录 控制措施 应产生记录用户活动、异常、故障和信息安全事态的审核日志，并保持和定期评审； A. 12. 4. 2 日志信息的保护 控制措施 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； A. 12. 4. 3 管理员和操作员日志 控制措施 系统管理员和系统操作员活动应记入日志，日志应被保护并定期评审； A. 12. 4. 4 时钟同步 控制措施 一个组织或安全域内的所有相关信息处理系统的时钟应使用单个时间源进行同步；	A.12.4.1 Event logging Control Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed A.12.4.2 Protection of log Information Control Logging facilities and log information shall be protected against tampering and unauthorized access A.12.4.3 Administrator and Operator logs Control System administrator and system operator activities shall be logged, and the logs protected and regularly reviewed A.12.4.4 Clock Synchronisation Control The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source
A. 12. 5 控制操作软件 控制目标：确保运行系统的完整性；	A.12.5 Control of operational software Objective: To ensure the integrity of operational systems
A. 12. 5. 1 运行系统软件的安装 控制措施 应实施流程对运行系统软件安装进行控制；	A.12.5.1 Installation of software on operational systems Control Procedures shall be implemented to control the installation of software on operational systems
A. 12. 6 技术脆弱性管理 控制目标：避免技术脆弱性的暴露；	A.12.6 Technical vulnerability management Objective: To prevent exploitation of technical vulnerabilities
A. 12. 6. 1 技术脆弱性的控制 控制措施 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； A. 12. 6. 2 软件安装的限制 控制措施	A.12.6.1 Management of technical vulnerabilities Control 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 taken to address the associated risk A.12.6.2 Restrictions on software installation Control

应建立和实施规则，控制用户安装软件	Rules governing the installation of software by users shall be established and implemented
A. 12. 7 信息系统审核考虑 目标：审计活动对运行系统干扰最小化；	A.12.7 Information systems audit considerations Objective: To minimize the impact of audit activities on operational systems
A. 12. 7. 1 信息系统审计控制措施 控制措施 涉及对运行系统验证的审计要求和活动，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；	A.12.7.1 Information systems audit controls Control Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes
A. 13 通信安全	A.13 Communications security
A. 13. 1 网络安全管理 控制目标：确保网络和其支持信息处理设施中信息的保护；	A.13.1 Network security management Objective: To ensure the protection of information in networks and its supporting information processing facilities
A. 13. 1. 1 网络控制 控制措施 应充分管理和控制网络，以保护系统和应用中的信息； A. 13. 1. 2 网络服务的安全 控制措施 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； A. 13. 1. 3 网络隔离 控制措施 应在网络中隔离信息服务、用户及信息系统；	A.13.1.1 Network controls Control Networks shall be managed and controlled to protect information in systems and applications A.13.1.2 Security of network Services Control 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 A.13.1.3 Segregation in Networks Control Groups of information services, users and information systems shall be segregated on networks
A. 13. 2 信息传输 控制目标：维护组织与任何外部实体的信息传输安全；	A.13.2 Information transfer Objective: To maintain the security of information transferred within an organization and with any external entity
A. 13. 2. 1 信息交换策略和规程 控制措施 应有正式的传输策略、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 交换协议 控制措施 协议应描述组织与外部方之间商业信息的安全传输； A. 13. 2. 3 电子消息发送 控制措施 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 保密性协议 控制措施 应识别并定期评审反映组织信息保护需要的	A.13.2.1 Information transfer policies and procedures Control 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 A.13.2.2 Agreements on information transfer Control Agreements shall address the secure transfer of business information between the organization and external parties A.13.2.3 Electronic messaging Control Information involved in electronic messaging shall be appropriately Protected A.13.2.4 Confidentiality or non-disclosure agreements Control Requirements for confidentiality or non-disclosure agreements reflecting the

保密性或不泄露协议的要求；	organization's needs for the protection of information shall be identified, regularly reviewed and documented
A. 14 系统获取、开发和维护	A.14 System acquisition, development and maintenance
A. 14.1 信息系统的安全要求 控制目标：确保安全是信息系统整个生命周期的一个有机组成部分。包括通过公用网络提供服务的不要求；	A.14.1 Security requirements of information systems Objective: To ensure that security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks
A. 14.1.1 安全要求分析和说明 控制措施 在新的信息系统或增强已有信息系统的业务要求陈述中，应规定对安全控制措施的要求； A. 14.1.2 保护公共网络上的应用服务 控制措施 通过公共网络传输应用服务的信息应被保护，以免遭受欺诈、合同纠纷和未经授权的披露和篡改； A. 14.1.3 保护应用服务交易 控制措施 应用服务交易的信息应加以保护，以防止不完整的传输、路由错误、未经授权信息修改、未经授权披露、未经授权信息复制或重放；	A.14.1.1 Information security requirements analysis and specification Control The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems. A.14.1.2 Securing applications services on public networks Control Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification A.14.1.3 Protecting application services transactions Control 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
A. 14.2 开发和支持过程中的安全 控制目标：确保在信息系统开发生命周期中的信息安全设计和实施；	A.14.2 Security in development and support processes Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems
A. 14.2.1 安全开发策略 控制措施 应制定及应用组织内软件和系统开发规则； A. 14.2.2 变更控制规程 控制措施 应使用正式的变更控制规程控制开发生命周期内的系统变更 A. 14.2.3 操作系统变更后应用的技术评审 控制措施 当操作系统发生变更后，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和安全没有负面影响； A. 14.2.4 软件包变更的限制 控制措施 应对软件包的修改进行劝阻，限制必要的变更，且对所有的变更加以严格控制； A. 14.2.5 安全系统创建原则 控制措施 应建立、文件化、维护制造安全系统的原则，	A.14.2.1 Secure development Policy Control Rules for the development of software and systems shall be established and applied to developments within the organization A.14.2.2 Change control Procedures Control Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures A.14.2.3 Technical review of applications after operating platform changes Control 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 A.14.2.4 Restrictions on changes to software packages Control Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled A.14.2.5 Secure system engineering principles Control Principles for engineering secure systems shall be established, documented,

<p>并应用到任何信息系统实施；</p> <p>A. 14. 2. 6 安全开发环境</p> <p>控制措施</p> <p>组织应建立并适当的保护安全开发环境，并覆盖整个系统开发生命周期；</p> <p>A. 14. 2. 7 外包软件开发</p> <p>控制措施</p> <p>组织应管理和监视外包软件的开发；</p> <p>A. 14. 2. 8 系统安全测试</p> <p>控制措施</p> <p>开发过程中，应测试安全功能；</p> <p>A. 14. 2. 9 系统验收测试</p> <p>控制措施</p> <p>在建立新系统、升级系统和更新版本时，建立验收测试程序和 related 标准；</p>	<p>maintained and applied to any information system implementation efforts</p> <p>A.14.2.6 Secure development environment</p> <p>Control</p> <p>Organizations shall establish and appropriately protect secure development environment for system development and integration efforts that covers the entire system development lifecycle</p> <p>A.14.2.7 Outsourced Development</p> <p>Control</p> <p>The organization shall supervise and monitor the activity of outsourced system development</p> <p>A.14.2.8 System security testing</p> <p>Control</p> <p>Tests of the security functionality shall be carried out during development</p> <p>A.14.2.9 System acceptance Testing</p> <p>Control</p> <p>Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions</p>
A. 14. 3 测试数据	A.14.3 Test data
控制目标：确保保护用于测试的数据；	Objective: To ensure the protection of data used for testing
A. 14. 3. 1 系统测试数据的保护	A.14.3.1 Protection of test data
控制措施	Control
测试数据应认真地加以选择、保护和控制；	Test data shall be selected carefully, protected and controlled
A. 15 供方关系	A.15 Supplier relationships
A. 15. 1 供方关系的信息安全	A.15.1 Information security in supplier relationships
控制目标：确保保护供方访问的组织资产的安全；	Objective: To ensure protection of the organization's asset that is accessible by suppliers
A. 15. 1. 1 供方关系的信息安全策略	A.15.1.1 Information security policy for supplier relationships
控制措施	Control
减少供方访问组织资产相关风险的信息安全要求应与供方协商，并记录；	Information security requirements for mitigating the risks associated with supplier access to organization's asset shall be agreed with the supplier and documented.
A. 15. 1. 2 供方协议中描述安全	A.15.1.2 Addressing security within supplier agreements
控制措施	Control
应建立所有相关信息安全要求，并与可能为组织信息进行访问、处置、存储、沟通或提供 IT 基础设施组件的每个供应商进行协商；	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
A. 15. 1. 3 信息和通讯技术供应链	A.15.1.3 Information and communication technology supply chain
控制措施	Control
与供应商的协议应包括信息和沟通技术服务和产品供应链相关的信息安全风险；	Agreements with suppliers shall include requirements to address the information security risks associated with Information and Communications Technology services and product supply chain
A. 15. 2 供方服务交付管理	A.15.2 Supplier service delivery management
控制目标：根据供应商协议，维护信息安全和交付的服务水平；	Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements
A. 15. 2. 1 供方服务的监控和评审	A.15.2.1 Monitoring and review of supplier services

<p>控制措施</p> <p>组织应定期监控、评审和审计供方服务交付；</p> <p>A. 15. 2. 2 供方服务的变更管理</p> <p>控制措施</p> <p>应管理供方服务提供的变更，包括保持和改进现有的信息安全方针政策、规程和控制措施，要考虑业务系统和涉及过程的关键程度及风险的再评估；</p>	<p>Control</p> <p>Organizations shall regularly monitor, review and audit supplier service delivery</p> <p>A.15.2.2 Managing changes to supplier services</p> <p>Control</p> <p>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</p>
A. 16 信息安全事件管理	A.16 Information security incident management
<p>A. 16. 1 信息安全事件和改进的管理</p> <p>控制目标：确保采用一致和有效的方法对信息安全事件进行管理，包括安全事态和弱点的沟通；</p>	<p>A.16.1 Management of information security incidents and improvements</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>A. 16. 1. 1 职责和规程</p> <p>控制措施</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> <p>A. 16. 1. 2 报告信息安全事态</p> <p>控制措施</p> <p>信息安全事态应该尽可能快地通过适当的管理渠道进行报告；</p> <p>A. 16. 1. 3 报告安全弱点</p> <p>控制措施</p> <p>应要求使用信息系统和服务的雇员和合同人员记录并报告他们观察到的或怀疑的任何系统或服务的安全弱点；</p> <p>A. 16. 1. 4 信息安全事态评估和决策</p> <p>控制措施</p> <p>信息安全事态应被评估，应决定是否属于信息安全事件；</p> <p>A. 16. 1. 5 信息安全事件响应</p> <p>控制措施</p> <p>信息安全事件应根据文件化流程进行响应；</p> <p>A. 16. 1. 6 对信息安全事件的总结</p> <p>控制措施</p> <p>从分析和解决信息安全事件所获得的知识，应用于减少未来事件发生的可能性或影响；</p> <p>A. 16. 1. 7 证据的收集</p> <p>控制措施</p> <p>组织应定义和应用程序，以识别、收集、获取和保存可作为证据的信息；</p>	<p>A.16.1.1 Responsibilities and Procedures</p> <p>Control</p> <p>Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents</p> <p>A.16.1.2 Reporting information security events</p> <p>Control</p> <p>Information security events shall be reported through appropriate management channels as quickly as possible</p> <p>A.16.1.3 Reporting information security weaknesses</p> <p>Control</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>A.16.1.4 Assessment and decision of information security events</p> <p>Control</p> <p>Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents</p> <p>A.16.1.5 Response to information security incidents</p> <p>Control</p> <p>Information security incidents shall be responded to in accordance with the documented procedures</p> <p>A.16.1.6 Learning from information security incidents</p> <p>Control</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>A.16.1.7 Collection of evidence</p> <p>Control</p> <p>The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence</p>
A. 17 业务连续性管理的信息安全方面	A.17 Information security aspects of business continuity

	management
A. 17.1 信息安全连续性 控制目标：信息安全连续性应嵌入组织的业务连续性管理体系；	A.17.1 Information security continuity Objective: Information security continuity shall be embedded in organization's business continuity management system.
A. 17.1.1 规划信息安全连续性 控制措施 组织应确定在不利情况下信息安全和信息安全连续性要求，如危机或灾难；	A.17.1.1 Planning information security continuity Control 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
A. 17.1.2 实施信息安全连续性 控制措施 组织应建立、记录、实施和维护流程、程序、控制措施，以确保在不利情况下保证要求的信息安全的连续性等级；	A.17.1.2 Implementing information security continuity Control The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation
A. 17.1.3 验证、评审和评估信息安全连续性 控制措施 组织应定期验证已建立和实施的的信息安全连续性控制措施，以确保在不利情况下是有效的和生效的；	A.17.1.3 Verify, review and evaluate information security continuity Control 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
A. 17.2 冗余 控制目标：确保信息处理设施的可用性；	A.17.2 Redundancies Objective: To ensure availability of information processing facilities
A. 17.2.1 信息处理设施的可用性 控制措施 信息处理设施应实现冗余，以满足可用性要求；	A.17.2.1 Availability of information processing facilities Control Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements
A. 18 合规性	A.18 Compliance
A. 18.1 符合法规和合同要求 控制目标：避免违反信息安全相关法律、法规或合同责任，以及任何安全要求；	A.18.1 Compliance with legal and contractual requirements Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements
A. 18.1.1 适用法律和合同要求的识别 控制措施 对每一个信息系统和组织而言，所有相关的法令、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.18.1.1 Identification of applicable legislation and contractual requirements Control All relevant 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
A. 18.1.2 知识产权（IPR） 控制措施 应实施适当的程序，以确保在使用具有知识产权的材料和具有所有权的软件产品时，符合法律、法规和合同的要求；	A.18.1.2 Intellectual property rights Control 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
A. 18.1.3 保护组织的记录 控制措施 根据法令、法规、合同和业务的要求，应防止记录遗失、毁坏和伪造、未授权访问和未授权	A.18.1.3 Protection of records Control Records shall be protected from loss, destruction, falsification unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual

<p>发布；</p> <p>A. 18. 1. 4 隐私和保护个人身份信息</p> <p>控制措施</p> <p>隐私和保护个人身份信息应确保遵守相关的法律法规的要求；</p> <p>A. 18. 1. 5 密码控制措施的规则</p> <p>控制措施</p> <p>使用密码控制措施应遵从相关的协议、法律和法规；</p>	<p>and business requirements</p> <p>A.18.1.4 Privacy and protection of personally identifiable information</p> <p>Control</p> <p>Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulations where applicable</p> <p>A.18.1.5 Regulation of cryptographic controls</p> <p>Control</p> <p>Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations</p>
<p>A. 18. 2 信息安全审查</p> <p>控制目标：确保根据组织策略和程序运行和实施信息安全；</p>	<p>A.18.2 Information security reviews</p> <p>Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures</p>
<p>A. 18. 2. 1 信息安全的独立评审</p> <p>控制措施</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、过程和程序）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> <p>A. 18. 2. 2 符合安全策略和标准</p> <p>控制措施</p> <p>管理人员应定期评审其职责范围内的信息处理和规程符合安全策略、标准和其他安全要求；</p> <p>A. 18. 2. 3 技术符合性评审</p> <p>控制措施</p> <p>信息系统应被定期评审是否符合组织信息安全策略和标准；</p>	<p>A.18.2.1 Independent review of information security</p> <p>Control</p> <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 occur</p> <p>A.18.2.2 Compliance with security policies and standards</p> <p>Control</p> <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>A.18.2.3 Technical compliance review</p> <p>Control</p> <p>Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards</p>

Bibliography

- [1] ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls
- [2] ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance
- [3] ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement
- [4] ISO/IEC 27005, Information technology — Security techniques — Information security risk management
- [5] ISO 31000:2009, Risk management — Principles and guidelines
- [6] ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012