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，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。

.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；

1 范围

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

本标准规定的所有要求是通用的,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 的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。

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

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

保证信息对于未被授权的访问是无效的。

[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

发生的系统、服务或网络状态的事件违背了信息安全策略，或使用安全措施失效，或以前未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的影响业务运作并威胁信息的安全.

[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

保护信息的准确和完整。

[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。

[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。

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 的范围和界限，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 的策略，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) 建立风险评价的标准和风险评估定义的结构；[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，这些策略能在一个文件中描述。

c) 定义组织的风险评估的方法；

1) 识别适用于 ISMS 及已识别的信息安全、法律和法规的要求的风险评估的方法；

2) 开发接受风险的准则和识别可接受风险的水平；[见 5.1f]

选择的风险评估方法应确保风险评估的结果具有可重复性和可比较性。

注：有许多不同的风险评估的方法。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 的范围内的资产及其责任人 [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、使用和保证资产的安全。术语‘责任人’并不意味着其真正的拥有资产。

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) 估计风险的等级；

4) 根据在 4.2.1c)中建立的准则，进行衡量风险是可接收的，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。

注：附件 A 中列出的控制目标和控制措施，作为本标准的一部分，并不是所有的控制目标和措施，组织可能选择另加的控制措施。

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)选择的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的运作；

g) 管理信息安全管理系统的资源[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，及安全控制措施的评审）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的范围仍然充分，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 的有效性或执行的措施和事件；[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) 确保改进行动达到了预期的目标；

4.3 文件要求

4.3.1 总则

文件化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，确保记录的结果是可重复的；

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]
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的有效规划、动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

ISMS 要求的文件应保护和控制。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。

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：

a) 建立、实施、运行、监控、评审和维护信息安全管理体系；

b) 确保信息安全程序支持业务需求；

c) 识别和强调法律和法规要求及合同安全责任；

d) 正确地应用所有实施的控制措施维护足够的安全；

e) 必要时，进行评审，并对评审的结果采取适当措施；

f) 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。

5 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。

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的机会和变更的需要，包括信息安全策略和信息安全目标。

评审的结果因清楚地写入文件，应保持管理评审的纪录［见 4.3.3］

7．2 评审输入

管理评审的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的结果；

b）相关方的反馈；

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）改进的建议；

7．3 评审输出

管理评审的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 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，确定以下的要求：

a）识别信息安全管理体系的不符合；

b）确定不符合的原因；

c）评价确保不符合不再发生所需的措施；

d) 确定和实施所需的纠正措施；

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，以防上其发生。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，以确定以下方面的要求：

a）识别潜在的不符合及其原因；

b) 评估预防不符合发生所需的措施；

c）确定和实施所需的预防措施：

d）记录所采取措施的结果[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的结果为基础确定。

注：预防不合格的措施总是比纠正措施更节约成本。

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。

A.5 信息安全策略

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.5.1.1 信息安全策略文件

控制措施

信息安全的策略文件应经过管理层批准，向所有员工和相关外部团体发布和沟通；

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.6 信息安全组织

A.6.1 内部组织

控制目标：在组织内部管理信息安全；

A.6.1.1 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的职责；

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的联系；

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的联系；

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）应在计划的周期内或当重大变化发生时进行独立审查；

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.6.2.1 识别外部组织的风险

控制措施

应识别外部组织的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 当与客户接触的时候强调安全

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.7 资产管理

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.7.1.1 资产的清单

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的清单；

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的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；

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。

A.7.2 信息分类

控制目标：确保信息资产受到适当程度的保护

A.7.2.1 分类原则

控制措施

信息的分类应根据其本身的价值、法律的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的分类方案的信息标识及处置的程序，并实施；

A.8 人力资源的安全

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.8.1.1 角色和职责

控制措施

根据组织的信息安全策略，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的条款和条件，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.8.2 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的威胁和相关事宜、他们的责任和义务并准备在他们日常的工作中支持组织的信息安全策略，以减少人为错误的风险；

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应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

组织内的所有员工、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；

4)解释：

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.8.3.1 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，所有的员工、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.9 物理和环境安全

A.9.1 安全区域

控制目标：防止对组织办公场所及信息的未经授权物理访问、破坏及干扰；

A.9.1.1 物理安全边界

控制措施

组织应有安全的边界（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，以确保只有经授权的人员可以进入；

A.9.1.3 办公室、房间及所及设施的安全

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.9.1.5 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.9.2 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.9.2.1 设备的安置及保护

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的访问

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

控制措施

未经授权，设备、信息及软件不得带出办公室；

A.10 通讯与操作管理

A.10.1 操作程序及职责

控制目标：确保信息处理设施的正确及安全操作；

A.10.1.1 文件化的操作程序

控制措施

作业程序应加以文件化及维护,并确保所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.10.2 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.10.2.1 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 第三方的服务的监督和评审

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.10.3 系统规划和验收

控制目标：最小系统失败的风险;

A.10.3.1 容量管理

控制措施

应监控、调整资源的使用，并反应将来容量的要求，以确保系统的性能； 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.10.4 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.10.4.1 控制恶意代码 控制措施 应实施恶意代码的检测、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运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.10.5 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.10.5.1 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.10.6 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.10.6.1 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 网络服务的安全 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的；
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.10.7.1 可移动介质的管理 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；
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.10.8.1 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.10.9 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.10.9.1 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.10.9.2 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.10.9.3 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.10.10 监督

控制目标：检测未授权的信息处理活动；

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. 10.10.2 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. 10.10.3 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. 10.10.4 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. 10.10.5 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. 10.10.6 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.11 访问控制

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.11.1.1 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.11.2 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访问信息系统；

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

应通过正式的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.11.3 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.11.3.1 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.11.4 网络访问控制

控制目标：避免未授权的访问网络服务；

A.11.4.1 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.11.4.4 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；

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.11.5.1 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

在规定的时间内，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的访问;

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.11.7 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.11.7.1 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.12 信息系统采集、开发及维护

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.12.1.1 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.12.2 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.12.2.1 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

验证的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

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，以确保储存的信息的处理流程是正确的，并与环境相适宜；

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.12.3.1 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.12.4 系统文档安全

控制目标：确保系统文件的安全；

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.12.5 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.12.5.1 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
不鼓励对软件包的变更，对必要的更改严格控制；

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；

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.12.6.1 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.13 信息安全事故的管理

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.13.1.1 信息安全事件报告
控制措施
应及时的通过适当的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.13.2 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.13.2.1 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

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。

A.14 业务连续性管理

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.14.1.1 包含信息安全的业务持续运作的管理过程

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 业务持续计划架构

控制措施

应维持一个单一的业务持续运作计划框架，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 业务持续计划的测试、维护与再评估

控制措施

应定期测试和更新业务持续计划，以确保更新及有效性；

A. 15 符合性

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. 15.1.1 识别适用的法律法规

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；
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.15.2.1 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.15.3 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.15.3.1 信息系统审核控制 控制措施 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； A.15.3.2 信息系统审核工具保护 控制措施 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；