国际标准

ISO/IEC 27001

第 二 版

2013-10-01

信息技术-安全技术-信息安全管理体系-要求

Information technology -Security techniques-Information security management systems-Requirements

科飞 COFLY

科飞管理咨询公司

目　　录

前　言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成世界范围内的标准化专门体系。国家机构作为 ISO 或 IEC 的成员，通过由处理特定技术领域的相应组织所建立的技术委员会参与开发国际标准。ISO 和 IEC 的技术委员会在共同关心的领域合作。其他的国际性组织，官方或非官方的，也与 ISO 和 IEC 联系，参与部分工作。在信息技术领域，ISO/IEC 建立了联合技术委员会，IEO/IEC JTC 1。

国际标准依据 ISO/IEC 指南第 2 部分起草。

联合技术委员会的主要任务是起草国际标准。被联合技术委员会接受的国际标准草案，将提交过国家机构进行投票。成为国际标准公开发布，则需要至少 75%的国家机构投赞成票。

应注意本标准的某些内容可能涉及专利。ISO 和 IEC 不负责识别任何专利。

ISO/IEC 27001 是由 JTC 1/SC27（信息安全分技术委员会）所制定。

本次第二版是对第一版进行技术修订，并取代第一版。

译者注：本标准供内部咨询师学习用，本文件持有人不得以任何方式复制和外传，由于时间仓促，难免在翻译过程中产生差异和谬误，咨询过程以英文版 ISO/IEC 27001:2013(E)为准。

科飞咨询公司　2013-11-20

0 引言

0.1 总则

本国际标准提供建立、实施、保持和持续改进 ISMS 的要求。采用 ISMS 当应是一个组织的战略一项决策。组织 ISMS 的设计和实施受其业务需求和目标、安全要求、 所采用的过程及组织的规模和结构的影响。上述因素可能会随时间而变化。

ISMS 通过使用风险管理过程来保护信息的保密性，完整性和可用性，给相关方带来风险得到适当管理的信心。

重要的是，ISMS 是组织结构过程和整体管理架构的一部分，在设计流程、信息系统、控制措施时都应考虑信息安全。ISMS 的实施应与组织的需求相对应。

本标准可用于内外部相关方评估组织满足自身信息安全要求的能力。

本国际标准中要求的顺序并不反映它们的重要程度或暗示它们的实施顺序。列举项仅供参考。

ISO/IEC 27000 提供了 ISMS 的概述和术语表，并可参考 ISMS 系列标准(包括 ISO/IEC 27003[2]，ISO/IEC 27004[3]，ISO/IEC 27005[4]）中的术语和定义。

0.2 与其它管理体系标准的兼容性

本国际标准采用 ISO/ IEC 导则第 1 部分中的附件 SL 中所定义的整体结构层次，相同的副条款标题，相同的文本，通用术语和核心定义。因此与其他遵循附录 SL 的管理体系标准相兼容。

附件 SL 中定义的这种通用方法，在组织利用一个管理体系来满足两个或两个以上管理体系标准要求时是很有用的。

信息技术-安全技术-信息安全管理体系-要求

1 范围

本标准规定了在组织环境下建立、实施、保持和持续改进 ISMS 的要求。本标准还包括根据组织要求而进行信息安全风险评估和处置的要求。本标准所规定的要求是通用性的，适用于各种规模、类型和特性的组织。组织声称符合本标准时，对于条款 4 到条款 10 的要求不能删剪。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注明日期的引用文件，只有引用的版本适用于本标准。凡是不注日期的引用文件，其最新版本的参考文件（包括任何修改）适用于本标准。

ISO/IEC 27000，信息技术-安全技术-信息安全管理体系-概览和词汇

3 术语和定义

ISO/IEC 27000 中的术语和定义适用于本标准。

4 组织的环境

4.1 了解组织及其环境

组织应确定与 ISMS 目的以及影响达成预期效果的内外部问题。

注：确定这些问题可参考 ISO 31000:2009[5]条款 5.3 中所提及的建立组织的外部和内部环境。

4.2 理解相关方的需求和期望

组织应确定：

a) ISMS 的相关方；以及

b) 这些相关方的信息安全相关要求。

注：相关方的要求可能包括法律法规的要求以及合同义务。

4.3 确定 ISMS 的范围

组织应确定 ISMS 的边界和适用性，以建立其范围。

在确定范围时，组织应考虑：

a) 4.1 提及的外部和内部的问题；

b) 4.2 提及的要求；以及

c) 组织内的活动以及由其他组织执行的活动间的接口和依赖关系。

范围应形成文件化的信息。

4.4 信息安全管理体系（ISMS）

组织应按照本标准的要求建立、实施、保持和持续改进 ISMS。

5 领导作用

5.1 领导作用和承诺

最高管理者应通过以下活动，对 ISMS 的领导和承诺提供证据：

a) 确保信息安全方针和信息安全目标的制定，并与组织的战略方向相一致；

b) 确保将 ISMS 的要求融合到组织的工作流程中；

c) 确保提供 ISMS 所需要的资源；

d) 传达信息安全管理有效执行并符合 ISMS 要求的重要性；

e) 确保 ISMS 达到其预期的效果；

f) 指导和支持员工对 ISMS 做出有效的贡献；

g) 促进持续改进；

h) 支持其他相关管理角色在其职责范围内证实其领导作用。

5.2 方针

最高管理者应建立信息安全方针：

a) 与组织的目标相适应；

b) 包括信息安全目标（见 6.2），或为建立信息安全目标提供框架；

c) 包括满足与信息安全相关的合理要求的承诺；

d) 包括 ISMS 持续改进的承诺。

信息安全的方针应：

e) 形成文件化的信息；

f) 在组织内沟通；以及

g) 适用时，提供给相关方。

5.3 组织的角色、责任和授权

最高管理者应确保与信息安全相关角色的职责和权限的分配和并得到沟通。

最高管理者应为以下活动分配责任和权限：

a) 确保 ISMS 符合本国际标准的要求；

b) 将 ISMS 的绩效报告给最高管理者。

注：最高管理者可以授权组织内的其他人员负责 ISMS 的绩效报告。

6 策划

6.1 处理风险的行动和机会

6.1.1 总则

当规划组织的 ISMS 时，应当考虑条款 4.1 所提及的问题和条款 4.2 所提及的要求，并确定需要处理的风险和机会：

a) 确保 ISMS 可实现预期的结果；

b) 防止或减少不良影响；以及

c) 实现持续改进。

组织应策划：

d) 处理这些风险和机合的行动；以及

e) 如何

1)整合和实施这些行动，并纳入 ISMS 过程中；

2)评估这些行动的有效性。

6.1.2 信息安全风险评估

组织应确定并应用信息安全风险评估过程：

a) 建立和保持信息安全风险的准则，包括：

1) 风险接受准则；

2) 信息安全风险评估的实施准则；

b) 确保重复使用信息安全风险评估过程能产生一致的，有效的和可比较的结果；

c) 识别信息安全风险：

1) 应用信息安全风险评估过程，以识别 ISMS 范围内的信息丧失保密性、完整性和可用性的风险；以及

2) 识别风险的所有者；

d) 分析信息安全风险：

1) 评估 6.1.2 c）1）所识别风险如果发生后的潜在后果；

2) 评估 6.1.2 c）1）所识别风险发生的可能性；

3) 确定风险等级；

e) 评价信息安全风险：

1) 参照 6.1.2 a）所建立风险准则比较风险分析的结果；以及

2) 确定已分析风险的处置优先次序。

组织应保留信息安全风险评估过程中的文件化信息。

6.1.3 信息安全风险处置

组织应定义并利用信息安全风险处置过程，以：

a) 考虑风险评估的结果，选择合适的信息安全风险处理方法；

b) 确定所选择的信息安全风险处置措施是必要的；

注：组织可以设计所需的控制项，或从任何来源中识别。

c) 将 6.1.3 b)所确定的控制措施中与附件 A 中的控制措施进行比较，以确认没有遗漏必要的控制措施；

注 1：附件 A 中包含控制目标和控制措施的完整列表。本国际标准的用户应注意附件 A，以确保没有重要的控制措施被忽略。

注 2：控制目标应隐含在所选择的控制措施中。附件 A 所列的控制目标和控制措施并不是所有的控制目标和控制措施，可能还需要额外的控制目标和控制措施。

d) 制定适用性声明，包含从附录 A 中所选择的必要控制措施（见 6.1.3 b)和 c)）和理由（无论是否实施），以及对附件 A 中控制措施的删减及理由；

e) 制定信息安全风险处置计划；

f) 风险处置方案和残余风险应得到风险所有者的批准。

组织应保留信息安全风险的处理过程中的文件化信息。

注：本标准的信息安全风险评估和处置过程与国际标准 ISO 31000[5]规定的原则和通用指南相一致。

6.2 信息安全目标及达成计划

组织应在相关职能层级制定信息安全目标。

信息安全目标应：

a)与信息安全方针一致；

b)是可衡量的（如果可行）；

c)考虑到适用的信息安全要求，以及风险评估和处置结果；

d)是可沟通的；以及

e)适时更新。

组织应保留信息安全目标相关的文件化信息。

当策划如何实现信息安全目标时，组织应确定：

f)需要做什么；

g)需要哪些资源；

h)谁负责；

i)何时完成；

j)如何评估结果。

7 支持

7.1 资源

组织应确定并提供 ISMS 的建立、实施、保持和持续改进所需的资源。

7.2 能力

组织应：

a) 确定影响组织信息安全绩效的控制措施所需要的员工技能；

b) 确保相关人员得到适当的教育，培训后能够胜任，或具有相关工作经验；

c) 在适当情况下，采取行动以获得必要的能力，并评估所采取行动的有效性；

d) 保留适当的文件化信息作为证据。

注：适用的行动可能包括，例如：提供培训、指导，或重新分配现有雇员、主管人员的聘用合同。

7.3 意识

在组织控制下工作的人员应了解：

a) 信息安全方针；

b) 他们对 ISMS 有效性的贡献，包括提高信息安全绩效的收益；

c) 违背 ISMS 要求所带来的影响。

7.4 沟通

组织应确定 ISMS 内外部相关沟通需求：

a) 沟通的内容；

b) 沟通的时机；

c) 沟通的人员；

d) 谁应该沟通；以及

e) 有效沟通的过程。

7.5 文件化信息

7.5.1 总则

组织的 ISMS 应包括：

a) 本国际标准所需要的文件化信息；

b) 由组织定义的记录 ISMS 有效性的必要的文件化信息。

注意：不同组织的 ISMS 文件化信息的多少与详略程度取决于：

1) 组织的规模、活动的类型、过程、产品和服务；

2) 过程及其相互作用的复杂性；

3) 人员的能力。

7.5.2 建立和更新

当建立和更新文件化信息时，组织应确保适当的：

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）和媒质（如纸张，电子）；

c) 适当和足够的审查和批准。

7.5.3 文件化信息的控制

ISMS 与本标准要求的文件化信息应被控制，以确保：

a) 当文件化信息被需要时是可用且适用的；

b) 得到充分的保护（以防止，例如保密性丧失、使用不当、完整性丧失等）。

对于文件化信息的控制，组织应制定以下活动：

a) 分配，访问，检索和使用；

b) 存储和保存，包括易读性的保存；

c) 变更管理（例如版本控制）；

d) 保留和处置。

组织 ISMS 的规划和运作所需要的外来文件化信息，应被适当识别和管理。

注：访问表示有权查看文件化信息，或获得授权以查看和更改文件化信息等。

8 运行

8.1 运行策划及控制

组织应策划、实施和控制满足信息安全要求所需的过程，并实施在 6.1 中所确定的行动。组织还应当实施计划，以实现信息安全在 6.2 中确定的目标。

组织应保存相关的文件化信息，以保证过程已按照计划实施。

组织应控制计划的变更，同时对非预期变更进行评审，并采取适当措施以减轻任何不良影响。

组织应确保外包过程被确定并受控。

8.2 信息安全风险评估

组织应按策划的时间间隔或发生重大变化时进行信息安全风险评估，并考虑 6.1.2 a) 中所建立的准则。

组织应保留信息安全风险评估结果的相关文件化信息。

8.3 信息安全风险处置

组织应实施信息安全风险处置计划。

组织应保留信息安全风险处置结果的文件化信息。

9 绩效评价

9.1 监视，测量，分析和评价

组织应评估信息安全绩效和 ISMS 的有效性。

组织应确定：

a) 需要进行监视和测量的内容，包括信息安全过程和控制措施；

b) 监视、测量、分析和评价的方法，以确保结果有效；

注：选择被认为是有效的方法应该可以产生可比较的和可再现的结果。

c) 监视和测量时机；

d) 监视和测量的人员；

e) 对监视和测量的结果进行分析和评估的时机；

f) 对结果分析和评估的人员。

组织应保留适当的监视和测量结果的文件化信息作为证据。

9.2 内部审核

组织应按策划的时间间隔进行内部审核，根据提供的信息判断 ISMS 是否：

a) 符合

1) 组织自身 ISMS 的要求；

2) 本标准的要求；

b) 得到有效实施和保持。

组织应：

c) 策划、建立、实施并保持审核方案，其中包括频率、方法、职责、计划要求和报告。审核方案应考虑相关过程的重要程度和以往审核结果；

d) 定义每次审核的准则和范围；

e) 选择审核员并执行审核，审核应确保审核过程的客观性和公正性；

f) 确保审核结果报告提交相关管理者；

g) 保留审核方案和审核结果等相关文件化信息以作为证据。

9.3 管理评审

最高管理者应按策划的时间间隔评审组织的 ISMS，以确保其持续的适宜性，充分性和有效性。

管理评审应考虑：

a) 跟踪以往管理评审提出改进措施的实施状况；

b) 与 ISMS 相关的内外部环境的变化；

c) 信息安全绩效和趋势的反馈，包括：

1) 不符合与纠正措施；

2) 监视和测量的结果；

3) 以往审核的结果；

4) 信息安全目标的达成状况；

d) 相关方的反馈；

e) 风险评估的结果和风险处置计划的实施状况；

f) 持续改进的机会。

管理评审的输出应包括持续改进的机会和任何 ISMS 需要变更的相关决定。

组织应保留管理评审结果的文件化信息以作为证据。

10 改进

10.1 不符合及纠正措施

出现不符合时，组织应：

a)对不符合做出反应，如适用：

1) 采取行动控制和纠正；

2) 根据后果的处理；

b)评估采取措施的必要性，以消除不符合的原因，并通过以下方式使得不符合不再发生或不在其他地方发生，通过：

1) 对不符合进行评审；

2) 确定不符合的原因；

3) 确定是否存在类似的不符合和发生的可能；

c)实施所需的措施；

d)审查已采取纠正措施的有效性；

e)如果有必要的话，改进 ISMS。

纠正措施应对不符合产生适当的影响。

组织应保留以下文件化信息以作为证据：

f)不符合的性质和后续措施；

g)任何纠正措施的结果。

10.2 持续改进

组织应不断提高 ISMS 的适宜性，充分性和有效性。

附 录 A

（规范性附录）

参考的控制目标和控制措施

表 A.1 所列的控制目标和控制措施，直接与 ISO / IEC 27002:2013[1]的第 5 至 18 章所对应，并应在实施 6.1.3 节时所使用。

表 A.1 控制目标和控制措施

A.5 信息安全方针		
A.5.1 信息安全管理方向		
目标：依据业务要求和相关法律法规提供管理指导并支持信息安全。		
A.5.1.1	信息安全方针	控制措施 应制定一组信息安全方针，并由管理者批准、发布以及传达给所有员工和外部相关方。
A.5.1.2	信息安全方针的评审	控制措施 应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.6 信息安全组织		
A.6.1 内部组织		
目标：建立一个管理框架，以启动和控制组织内信息安全的实施和运行。		
A.6.1.1	信息安全的角色和职责	控制措施 所有信息安全职责应被定义及分配。
A.6.1.2	责任分割	控制措施 冲突的职责和权限应被分开，以减少对组织资产未经授权或无意的修改与误用。
A.6.1.3	与监管机构的联系	控制措施 应与监管机构保持适当的联系。
A.6.1.4	与特殊利益团体的联系	控制措施 与特定利益团队、其他专业安全论坛或行业协会应保持适当联系。
A.6.1.5	项目管理中的信息安全	控制措施 应处理项目管理中的信息安全，不论项目类型。
A.6.2 移动设备和远程办公		
目标：确保远程办公和使用移动设备的安全性。		
A.6.2.1	移动设备策略	控制措施 应使用配套策略和安全措施来防范因使用移动设备带来的风险。
A.6.2.2	远程办公	控制措施 应使用配套策略和安全措施来保护在远程对信息的访问、处理和存储。
A.7 人力资源安全		
A.7.1 任用之前		
目标：确保雇员和承包方人员理解其职责、考虑对其承担的角色是适合的。		

A.7.1.1	审查	控制措施 对所有任用的候选者的背景验证核查应按照相关法律、法规、道德规范和对应的业务要求、被访问信息的类别和觉察的风险来执行。
A.7.1.2	任用的条款及条件	控制措施 员工和承包方人员应同意并签署任用合同中关于表明他们和组织的信息安全职责条款和条件。
A.7.2 任用中		
目标：确保员工和承包方人员用户知悉并履行信息安全职责。		
A.7.2.1	管理职责	控制措施 管理者应要求员工和承包方人员按照组织已建立的方针策略和规程对安全尽心尽力。
A.7.2.2	信息安全意识，教育和培训	控制措施 组织的所有员工，适当时，包括承包方人员应受到与其工作职能相关的适当的意识培训和组织方针策略及程序的定期更新培训。
A.7.2.3	纪律处理过程	控制措施 对于安全违规的雇员，应有一个正式与可沟通的纪律处理过程。
A.7.3 任用的终止或变化		
目标：保证组织利益是雇佣终止和变更的一部分。		
A.7.3.1	任用终止或变化的责任	控制措施 应该界定任用终止或变更后依然有信息安全责任和义务的员工或承包方人员，并进行沟通和执行。
A.8 资产管理		
A.8.1 对资产负责		
目标：实现和保持对组织资产的适当保护。		
A.8.1.1	资产清单	控制措施 应识别与信息和信息处理设施相关的资产，并编制和维护资产清单。
A.8.1.2	资产责任人	控制措施 应为资产清单内的资产指定责任人。
A.8.1.3	资产的合理使用	控制措施 与信息处理设施有关的信息和资产合理使用规则应被确定、形成文件并加以实施。
A.8.1.4	资产的归还	控制措施 所有员工、外部方用户在合同终止或协议终止后应归还组织的资产。
A.8.2 信息分类		
目标：确保信息得到与其重要性程度相适应的保护。		
A.8.2.1	信息的分类	控制措施 信息应依照法律要求、对组织的价值，关键性和敏感性进行分类。
A.8.2.2	信息的标记	控制措施 应按照组织所采纳的分类机制建立和实施一组合适的信息标记和处理程序。
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，建立和实施一组合适的处理规程。
A.8.3 介质处理		

目标：为了防止存储在介质上的信息被未经授权的披露，修改，删除或破坏。		
A.8.3.1	可移动介质的管理	控制措施 根据组织采用的分类机制来执行可移动介质管理流程。
A.8.3.2	介质的处置	控制措施 不再需要的介质，应使用正式的规程可靠并安全地处置。
A.8.3.3	运输中的物理介质	控制措施 包含信息的介质在传输过程中，应加以保护，防止未经授权的访问，滥用或损坏。
A.9 访问控制		
A.9.1 访问控制的业务要求		
目标：控制对信息和信息处理设施的访问。		
A.9.1.1	访问控制策略	控制措施 应建立访问控制策略，形成文件，并基于业务和访问的安全要求进行评审。
A.9.1.2	访问网络和网络服务	控制措施 用户应仅能访问已获专门授权使用的网络和网络服务。
A.9.2 用户访问管理		
目标：确保授权用户访问系统和服务，并防止未授权的访问。		
A.9.2.1	用户注册和注销	控制措施 应有正式的用户注册和注销规程，来支撑访问权限的分配。
A.9.2.2	用户访问权限的提供	控制措施 应有正式的用户权限控制规程来授权或撤销对所有信息系统及服务的访问。
A.9.2.3	特殊权限管理	控制措施 应限制和控制特殊权限的分配及使用。
A.9.2.4	用户保密认证信息的管理	控制措施 应使用正式的管理规程来控制保密认证信息的分配。
A.9.2.5	用户访问权的复查	控制措施 资产所有者应当定期审查用户的访问权限。
A.9.2.6	移除或调整访问权限	控制措施 所有工作人员和外部人员用户，当合同或协议终止后，应删除或调整其信息和信息处理设施的访问权限。
A.9.3 用户职责		
目标：确保用户对身份认证信息的保护责任。		
A.9.3.1	保密认证信息的使用	控制措施 应要求用户按照组织规定来使用保密认证信息。
A.9.4 系统和应用程序的访问控制		
目标：防止对系统和应用的未授权使用。		
A.9.4.1	信息访问限制	控制措施 应依据访问控制策略来限制对信息和应用系统功能的访问。
A.9.4.2	安全登录规程	控制措施 如访问控制策略需要，应通过安全登录程序控制对系统和应用的访问。
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，并确保口令质量。

A.9.4.4	特权实用程序的使用	控制措施 对可能超越系统和应用程序控制措施的实用程序的使用应加以限制并严格控制。
A.9.4.5	程序源码的访问控制	控制措施 对程序源代码的访问应被限制。
A.10 密码学		
A.10.1 密码控制		
目标：使用密码适当有效的保护信息的保密性、真实性和/或完整性。		
A.10.1.1	密码使用控制策略	控制措施 应开发和实施信息保护密码控制策略。
A.10.1.2	密钥管理	控制措施 应开发和实施密钥的使用、保护的策略并贯穿其整个生命周期。
A.11 物理环境安全		
A.11.1 安全区域		
目标：防止对组织场所和信息的未授权物理访问、损坏和干扰。		
A.11.1.1	物理安全边界	控制措施 应设置安全边界来保护包含敏感信息、关键信息和信息处理设施的区域。
A.11.1.2	物理入口控制	控制措施 安全区域应由适合的入口控制所保护，以确保只有授权的人员才允许访问。
A.11.1.3	办公室、房间和设施的安全保护	控制措施 应为办公室、房间和设施设计并采取物理安全措施。
A.11.1.4	外部和环境威胁的安全防护	控制措施 应设计并采取物理安全措施来防范自然灾害、恶意攻击或意外事故。
A.11.1.5	在安全区域工作	控制措施 应设计和应用用于安全区域工作的规程。
A.11.1.6	交付和交接区	控制措施 类似于交付和交接区这样非授权可以进入的场所应加以控制，如果可能，应与信息处理设施隔离，以避免未授权访问。
A.11.2 设备		
目标：防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。		
A.11.2.1	设备安置和保护	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.11.2.2	支持性设施	控制措施 应保护设备使其免于支持性设施的失效而引起的电源故障和其他中断。
A.11.2.3	布缆安全	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，免遭拦截或破坏。
A.11.2.4	设备维护	控制措施 设备应予以正确地保护，以确保其持续的可用性和完整性。
A.11.2.5	资产的移动	控制措施 设备、信息或软件在获得授权之前不应带出组织场所。

A.11.2.6	场外设备和资产安全	控制措施 应对组织场所外的资产采取安全措施，要考虑工作在组织场所外的不同风险。
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核查，以确保在处置之前，任何敏感信息和注册软件已被删除或安全地写覆盖。
A.11.2.8	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得到适当的保护。
A.11.2.9	清除桌面和清屏策略	控制措施 应采取清空桌面上的文件、可移动存储介质的策略和清空信息处理设施屏幕的策略。
A.12 操作安全		
A.12.1 操作程序和职责		
目标：确保正确、安全的操作信息处理设施。		
A.12.1.1	文件化的操作程序	控制措施 操作规程应形成文件，并提供给所有需要的用户。
A.12.1.2	变更管理	控制措施 对影响信息的组织、业务流程、信息处理设施和系统的变更应加以控制。
A.12.1.3	容量管理	控制措施 资源的使用应加以监视、调整，并做出对于未来容量要求的预测，以确保拥有所需的系统性能。
A.12.1.4	开发，测试和运行环境的分离	控制措施 开发及测试环境应与运营环境分离，减少未授权访问和改变运行系统的风险。
A.12.2 恶意软件防护		
目标：确保信息和信息处理设施不受恶意软件侵害。		
A.12.2.1	控制恶意软件	控制措施 应实施恶意代码的监测、预防和恢复的控制措施，并与适当的提高用户安全意识相结合。
A.12.3 备份		
目标：防止数据丢失。		
A.12.3.1	信息备份	控制措施 应按照已设的备份策略，定期备份和测试信息、软件和系统镜像。
A.12.4 记录和监控		
目标：记录事况并生成证据。		
A.12.4.1	事况日志	控制措施 应产生记录用户活动、异常情况、故障和信息安全事况的日志，并定期评估。
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的活动应记入日志，对其保护，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设施的时钟应使用已设的单一参考时间源进行同步。

A.12.5 运行软件的控制		
目标：保证运行系统的完整性。		
A.12.5.1	运行系统软件的安装	控制措施 应实施控制在运行系统上安装软件的规程。
A.12.6 技术漏洞管理		
目标：防止利用技术脆弱性。		
A.12.6.1	技术漏洞的管理	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风险。
A.12.6.2	限制软件安装	控制措施 应建立和实施控制用户安装软件的规则。
A.12.7 信息系统审计考虑		
目标：将业务系统审计过程的影响最小化。		
A.12.7.1	信息系统审计控制	控制措施 涉及对运行系统核查的审计要求和活动，应谨慎地加以规划并取得批准，以便最小化造成业务过程中断的风险。
A.13 通信安全		
A.13.1 网络安全管理		
目标：确保网络中信息的安全性并保护支持性的信息处理设施。		
A.13.1.1	网络控制	控制措施 应管理和控制网络，以保护系统和应用程序中的信息。
A.13.1.2	网络服务安全	控制措施 所有网络服务的安全机制、服务级别和管理要求，应予以确定并包含在网络服务协议中，无论这些服务是否由公司内部提供还是外包。
A.13.1.3	网络隔离	控制措施 应在网络中隔离信息服务、用户及系统信息。
A.13.2 信息传输		
目标：维护组织与任何外部实体的信息传输安全。		
A.13.2.1	信息传输的策略和程序	控制措施 应建立正式的传输策略、规程和控制措施，以保证所有类型的通信设施间的信息传输安全。
A.13.2.2	信息传输协议	控制措施 应建立组织与外部方传输业务信息安全传输的协议。
A.13.2.3	电子消息	控制措施 涉及电子消息的信息应适当保护。
A.13.2.4	保密或不泄露协议	控制措施 应确定组织信息保护需要的保密性或不泄露协议的要求，定期评审并形成文档。
A.14 信息系统获取、开发和维护		
A.14.1 信息系统的安全要求		
目标：确保安全是信息系统生命周期中的组成部分。包括对通过公共网络提供服务的信息系统要求。		

A.14.1.1	安全需求分析和说明	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 在公共网络应用服务中传输的信息应被保护，以免遭受欺诈、合同纠纷，未经授权的披露和修改。
A.14.1.3	保护应用服务交易	控制措施 应用服务交易中所涉及到的信息应加以保护，以防止不完整的传输、路由错误、未经授权的消息改变、未授权的披露和未经授权的消息复制或重放。
A.14.2 开发和支持过程中的安全		
目标：确保在整个信息系统开发生命周期中设计与实施信息安全。		
A.14.2.1	安全开发策略	控制措施 应制定及应用关于软件和系统的开发规则。
A.14.2.2	系统变更控制程序	控制措施 应使用正式的变更控制程序来控制开发生命周期中对系统的变更。
A.14.2.3	运行平台变更后的技术评估	控制措施 当运行平台发生变更时，应对业务的关键应用进行评审和测试，以确保对组织的运行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，只限于必要的变更，且对所有的变更加以控制。
A.14.2.5	安全系统设计原则	控制措施 应建立、保持文件化的安全系统工程的设计原则，并应用到任何信息系统开发工作中。
A.14.2.6	安全的开发环境	控制措施 组织应建立并适当保护开发环境的安全，并涵盖整个系统开发周期。
A.14.2.7	外包软件开发	控制措施 组织应监管和监视外包的系统开发活动。
A.14.2.8	系统安全性测试	控制措施 在开发的过程中，必须测试安全功能。
A.14.2.9	系统验收测试	控制措施 在建立新系统、升级系统和更新版本时，必须建立验收测试程序和相关准则。
A.14.3 测试数据		
目标：确保测试数据的安全。		
A.14.3.1	测试数据的保护	控制措施 测试数据应被仔细筛选、保护和控制。
A.15 供应商关系		
A.15.1 供应商关系中的信息安全		
目标：确保供应商访问的组织资产的安全。		
A.15.1.1	供应商关系的信息安全策略	控制措施 对于减小供应商访问组织资产风险的信息安全要求应得到供应商的认可并形成文件。

A.15.1.2	供应商协议中的安全	控制措施 应建立与信息安全相关的要求并获得供应商的认可。包括可能处理、存储及交换组织信息，或提供 IT 基础设施部件的供应商。
A.15.1.3	信息和通信技术供应链	控制措施 与供应商的协议应包括解决信息、通信技术服务、产品供应链相关信息安全风险的要求。
A.15.2 供应商服务交付管理		
目标：维持与供应商协议中商定的信息安全要求和服务交付水平。		
A.15.2.1	监视和审查供应商服务	控制措施 组织应定期监视，评审和审计供应商提供的服务。
A.15.2.2	供应商服务变更管理	控制措施 应管理供应商提供服务的变更,包括维护、改进现有的信息安全策略、程序和控制措施，应考虑所涉及业务信息、系统、流程的关键性以及风险的重新评估。
A.16 信息安全事件管理		
A.16.1 信息安全事件和改进的管理		
目标：确保一致和有效的方法来管理信息安全事件，包括安全事件和弱点的报告。		
A.16.1.1	职责和程序	控制措施 应建立管理职责和程序，以确保快速、有效和有序地响应信息安全事件。
A.16.1.2	报告信息安全事态	控制措施 信息安全事态应尽可能快地通过适当的管理渠道进行报告。
A.16.1.3	报告信息安全弱点	控制措施 应要求信息系统和服务的所有员工、承包方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。
A.16.1.4	信息安全事况的评估和决策	控制措施 应对信息安全事况进行评估，以确定是否应归类为信息安全事件。
A.16.1.5	信息安全事件的响应	控制措施 信息安全事件应依照文件化的程序进行响应。
A.16.1.6	从信息安全事件中学习	控制措施 从分析和解决信息安全事件中获取知识，减少未来事件发生的可能性或影响。
A.16.1.7	证据的收集	控制措施 组织应制定并应用程序，以识别、收集、获取和保存可作为证据的信息。
A.17 信息安全方面的业务连续性管理		
A.17.1 信息安全连续性		
目标：信息安全的连续性应融入组织的业务连续性管理。		
A.17.1.1	规划信息安全连续性	控制措施 组织应确定其在不利情形时信息安全和信息安全管理的连续性要求，如危机或灾难时。
A.17.1.2	实施信息安全的连续性	控制措施 组织应建立、实施、保持文件化的过程、程序、控制措施，以保证在不利情形时所要求的信息安全连续性等级。

A.17.1.3	验证、评审和评估信息安全连续性	控制措施 组织应每隔一段时间核查其建立和实施的信息安全连续性控制措施，以确保他们在不利情形时是有效的。
A.17.2 冗余		
目标：确保信息处理设施的可用性。		
A.17.2.1	信息处理设施的可用性	控制措施 信息处理设施应当实现充分的冗余，以满足可用性要求。
A.18 符合性		
A.18.1 符合法律和合同的要求		
目标：避免违反相关信息安全的法律、法令、法规或信息安全相关的合同义务的任何安全要求。		
A.18.1.1	识别适用的法律和合同的要求	控制措施 对每一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取的方法，应得到清晰的识别，形成文件并保持更新。
A.18.1.2	知识产权	控制措施 应实施适当的规程，以确保在使用具有专利权软件产品时，符合法律、法规和合同要求。
A.18.1.3	记录的保护	控制措施 按照法律、法规、合同和业务需求保护文件化信息，以免遭受损失、破坏、篡改，未经授权的访问和擅自发布。
A.18.1.4	隐私和个人信息的保护	控制措施 应依照相关的法律、法规的要求，确保隐私和个人信息的保护。
A.18.1.5	密码控制措施的规则	控制措施 使用密码控制措施应遵从相关的协议、法律和法规。
A.18.2 信息安全评审		
目标：确保信息安全设施依照组织的策略和程序运行和实施。		
A.18.2.1	信息安全的独立评审	控制措施 组织管理信息安全的方法及其实施（例如信息安全的控制目标、控制措施、策略、过程和规程）应按照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，也应进行独立评审。
A.18.2.2	符合安全政策和标准	控制措施 管理者应定期评审其职责范围内的信息处理流程和规程被正确的执行，以确保符合安全策略、标准和其他安全要求。
A.18.2.3	技术符合性评审	控制措施 应定期评审信息系统是否符合组织信息安全策略和标准。

参考文献

[1] ISO/IEC 27002:2013 信息技术-安全技术-信息安全控制实用规则
[2] ISO/IEC 27003 信息技术-安全技术-信息安全管理体系-改进指南
[3] ISO/IEC 27004 信息技术-安全技术-信息安全管理-测量
[4] ISO/IEC 27005 信息技术-安全技术-信息安全风险管理
[5] ISO 31000:2009,风险管理-原则与指南
[6] ISO/IEC 导则 第 1 部分 针对 ISO 的补充程序, 2012