国际标准　　ISO/IEC 27001

第二版

2013－10－19

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

参考号
ISO/IEC 27001:2013（E）

目录

1 范围.....5
2 规范性引用文件.....5
3 术语和定义.....5
4 组织环境.....5
4.1 理解组织及其环境.....5
4.2 理解相关方的需求和期望.....5
4.3 确定信息安全管理体系的范围.....5
4.4 信息安全管理体系.....6
5 领导.....6
5.1 领导和承诺.....6
5.2 方针.....6
5.3 组织角色、职责和权限.....7
6 规划.....7
6.1 应对风险和机会的措施.....7
6.1.1 总则.....7
6.1.2 信息安全风险评估.....7
6.1.3 信息安全风险处置.....8
6.2 信息安全目标和规划实现.....8
7 支持.....9
7.1 资源.....9
7.2 能力.....9
7.3 意识.....9
7.4 沟通.....10
7.5 文件记录信息.....10
7.5.1 总则.....10
7.5.2 创建和更新.....10
7.5.3 文件记录信息的控制.....10
8 运行.....11
8.1 运行的规划和控制.....11
8.2 信息安全风险评估.....11
8.3 信息安全风险处置.....11
9 绩效评价.....11
9.1 监视、测量、分析和评价.....11
9.2 内部审核.....12
9.3 管理评审.....12
10 改进.....13
10.1 不符合和纠正措施.....13
10.2 持续改进.....14
附 录 A（规范性附录）参考控制目标和控制措施.....15
参考文献.....23

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）是为国际标准化制定专门体制的国际组织。国家机构是 ISO或IEC的成员，他们通过各自的组织建立技术委员会参与国际标准的制定，来处理特定领域的技术活动。 ISO和IEC技术委员会在共同感兴趣的领域合作。其他国际组织、政府和非政府等机构，通过联络ISO和IEC参与这项工作。ISO和IEC已经在信息技术领域建立了一个联合技术委员会 ISO/IEC JTC1。

国际标准的制定遵循 ISO/IEC导则第2部分的规则。

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

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

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

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

引言

0.1总则

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

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

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

标准可被内部和外部相关方使用，评估组织的能力是否满足组织自身信息安全要求。本标准中要求的顺序并不能反映他们的重要性或意味着他们的实施顺序。列举的条目仅用于参考目的。ISO/IEC27000描述了信息安全管理体系的概述和词汇,参考了信息安全管理体系标准族(包括 ISO/IEC 27003、ISO/IEC 27004和 ISO/IEC 27005）以及相关的术语和定义。

0.2与其他管理体系的兼容性

本标准应用了 ISO/IEC导则第一部分 ISO补充部分附录 SL中定义的高层结构、相同的子章节标题、相同文本、通用术语和核心定义。因此保持了与其它采用附录 SL的管理体系标准的兼容性。附录 SL定义的通用方法对那些选择运作单一管理体系（可同时满足两个或多个管理体系标准要求）的组织来说是十分有益的。

信息技术 -安全技术 -信息安全管理体系 -要求

1 范围

本标准从组织环境的角度，为建立、实施、运行、保持和持续改进信息安全管理体系规定了要求。本标准还规定了为适应组织需要而定制的信息安全风险评估和处置的要求。本标准规定的要求是通用的，适用于各种类型、规模和特性的组织。组织声称符合本标准时，对于第 4章到第 10章的要求不能删减。

2 规范性引用文件

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

ISO/IEC 27000，信息技术 —安全技术 —信息安全管理体系 —概述和词汇

3 术语和定义

ISO/IEC 27000中的术语和定义适用于本标准。

4 组织环境

4.1 理解组织及其环境

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

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

4.2 理解相关方的需求和期望

组织应确定：

a) 与信息安全管理体系有关的相关方；

b) 这些相关方与信息安全有关的要求。

注：相关方的要求可能包括法律法规要求和合同义务。

4.3 确定信息安全管理体系的范围

组织应确定信息安全管理体系的边界和适用性，以建立其范围。当确定该范围时，组织应考虑：

a）在 4.1中提及的外部和内部问题；

b）在 4.2中提及的要求；

c）组织所执行的活动之间以及与其它组织的活动之间的接口和依赖性范围应文件化并保持可用性。

4.4 信息安全管理体系

组织应按照本标准的要求建立、实施、保持和持续改进信息安全管理体系。

5 领导

5.1 领导和承诺

高层管理者应通过下列方式展示其关于信息安全管理体系的领导力和承诺：

a）确保建立信息安全方针和信息安全目标，并与组织的战略方向保持一致；

b）确保将信息安全管理体系要求整合到组织的业务过程中；

c）确保信息安全管理体系所需资源可用；

d）传达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实现其预期结果；

f）指导并支持人员为信息安全管理体系的有效实施作出贡献；

g）促进持续改进；

h）支持其他相关管理角色在其职责范围内展示他们的领导力。

5.2 方针

高层管理者应建立信息安全方针，以：

a）与组织的宗旨相适用；

b）包含信息安全目标（见 6.2）或为信息安全目标提供框架；

c）包含满足适用的信息安全相关要求的承诺；

d）包含信息安全管理体系持续改进的承诺。

信息安全方针应：

e）文件化并保持可用性；

f）在组织内部进行传达；

g）适当时提供给相关方。

5.3 组织角色、职责和权限

高层管理者应确保分配并传达了信息安全相关角色的职责和权限。

高层管理者应分配下列职责和权限：

a）确保信息安全管理体系符合本标准的要求；

b）将信息安全管理体系的绩效报告给高层管理者。

注：高层管理者可能还要分配在组织内部报告信息安全管理体系绩效的职责和权限。

6 规划

6.1 应对风险和机会的措施

6.1.1 总则

当规划信息安全管理体系时，组织应考虑 4.1中提及的问题和 4.2中提及的要求，确定需要应对的风险和机会，以：

a）确保信息安全管理体系能实现其预期结果；

b）防止或减少意外的影响；

c）实现持续改进。

组织应规划：

d）应对这些风险和机会的措施；

e）如何

1） 整合和实施这些措施并将其纳入信息安全管理体系过程；

2） 评价这些措施的有效性。

6.1.2 信息安全风险评估

组织应定义并应用风险评估过程，以：

a）建立并保持信息安全风险准则，包括：

1） 风险接受准则；

2） 执行信息安全风险评估的准则；

b）确保重复性的信息安全风险评估可产生一致的、有效的和可比较的结果；

c）识别信息安全风险：

1） 应用信息安全风险评估过程来识别信息安全管理体系范围内的信息丧失保密性、完整性和可用性的相关风险；

2） 识别风险负责人；

d）分析信息安全风险：

1） 6.1.2 c）1）中所识别风险发生后将导致的潜在影响；

2） 6.1.2 c）1）中所识别风险发生的现实可能性；

3） 确定风险级别；

e）评价信息安全风险；

1） 将风险分析结果同 6.1.2 a）建立的风险准则进行比较；

2） 为实施风险处置确定已分析风险的优先级。

组织应保留信息安全风险评估过程的文件记录信息。

6.1.3 信息安全风险处置

组织应定义并应用信息安全风险处置过程，以：

a）在考虑风险评估结果的前提下，选择适当的信息安全风险处置选项；

b）为实施所选择的信息安全风险处置选项，确定所有必需的控制措施；

注：组织可按要求设计控制措施，或从其他来源识别控制措施。

c）将 6.1.3 b）所确定的控制措施与附录 A的控制措施进行比较，以核实没有遗漏必要的控制措施；

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

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

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

e）制定信息安全风险处置计划；

f）获得风险负责人对信息安全风险处置计划以及接受信息安全残余风险的批准。组织应保留信息安全风险处置过程的文件记录信息。

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

6.2 信息安全目标和规划实现

组织应在相关职能和层次上建立信息安全目标。信息安全目标应：

a）与信息安全方针一致；

b）可测量（如可行）；

c）考虑适用的信息安全要求以及风险评估和风险处置结果；

d）被传达；

e）适当时进行更新。

组织应保留关于信息安全目标的文件记录信息。

当规划如何实现其信息安全目标时，组织应确定：

f）要做什么；

g）需要什么资源；

h）由谁负责；

i）什么时候完成；

j）如何评价结果。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持和持续改进信息安全管理体系所需的资源。

7.2 能力

组织应：

a）确定从事影响信息安全执行工作的人员在组织的控制下从事其工作的必要能力；

b）确保人员在适当教育，培训和经验的基础上能够胜任工作；

c）适用时，采取措施来获得必要的能力，并评价所采取措施的有效性；

d）保留适当的文件记录信息作为能力方面的证据。

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

7.3 意识

人员在组织控制下从事其工作时应意识到：

a）信息安全方针；

b）他们对有效实施信息安全管理体系的贡献，包括信息安全绩效改进后的益处；

c）不符合信息安全管理体系要求可能的影响。

7.4 沟通

人员在组织的控制下从事其工作时应意识到：组织应确定有关信息安全管理体系在内部和外部进行沟通的需求，包括：

a）什么需要沟通；

b）什么时候沟通；

c）跟谁进行沟通；

d）由谁负责沟通；

e）影响沟通的过程。

7.5 文件记录信息

7.5.1 总则

组织的信息安全管理体系应包括：

a）本标准要求的文件记录信息；

b）组织为有效实施信息安全管理体系确定的必要的文件记录信息。

注：不同组织的信息安全管理体系文件记录信息的详略程度取决于：

1） 组织的规模及其活动、过程、产品和服务的类型；

2） 过程的复杂性及其相互作用；

3） 人员的能力。

7.5.2 创建和更新

创建和更新文件记录信息时，组织应确保适当的：

a）标识和描述（例如：标题、日期、作者或参考编号）；

b）格式（例如：语言，软件版本，图表）和介质（例如：纸质介质，电子介质）；

c）评审和批准其适用性和充分性。

7.5.3 文件记录信息的控制

信息安全管理体系和本标准所要求的文件记录信息应予以控制，以确保：

a）无论何时何地需要，它都是可用并适合使用的；

b）它被充分保护（例如避免丧失保密性、使用不当或丧失完整性）。

对于文件记录信息的控制，适用时，组织应处理下列问题：

c）分发、访问、检索和使用；

d）存储和保存，包括可读性的保持；

e）变更控制（例如版本控制）；

f）保留和和处置。

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

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

8 运行

8.1 运行的规划和控制

组织应规划、实施和控制满足信息安全要求所需的过程，并实施 6.1中确定的措施。组织还应实施

这些规划来实现 6.2中所确定的信息安全目标。

组织应保持文件记录信息达到必要的程度：有信心证明过程是按计划执行的。

组织应控制计划了的变更，评审非预期变更的后果，必要时采取措施减缓负面影响。

组织应确保外包的过程已确定，并处于可控状态。

8.2 信息安全风险评估

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

组织应保留信息安全风险评估结果的文件记录信息。

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记录信息。

9 绩效评价

9.1 监视、测量、分析和评价

组织应评价信息安全绩效和信息安全管理体系的有效性。

组织应确定：

a）什么需要监视和测量，包括信息安全过程和控制措施；

b）监视、测量、分析和评价的方法，适用时，确保结果有效；

注：选择的方法最好产生可比较和可再现的结果，这样才能被认为是有效的。

c）什么时候应执行监视和测量；

d）谁应实施监视和测量；

e）什么时候应对监视和测量的结果进行分析和评价；

f）谁应分析和评价这些结果。

组织应保留适当的文件记录信息作为监视和测量结果的证据。

9.2 内部审核

组织应按计划的时间间隔进行内部审核，以提供信息确定信息安全管理体系是否：

a）符合

1） 组织自身信息安全管理体系的要求；

2） 本标准的要求；

b）得到有效的实施和保持。

组织应：

c）规划、建立、实施和保持审核方案，包括频次、方法、职责、计划要求和报告。审核方案应考虑所关注过程的重要性以及以往审核的结果；

d）为每次审核定义审核准则和审核范围；

e）审核员的选择和审核的实施应确保审核过程的客观性和公正性；

f）确保审核结果报告给相关的管理者；

g）保留文件记录信息作为审核方案和审核结果的证据。

9.3 管理评审

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

管理评审应包括下列方面的考虑：

a）以往管理评审的措施的状态；

b）与信息安全管理体系相关的外部和内部问题的变更；

c）信息安全绩效的反馈，包括下列方面的趋势：

1） 不符合和纠正措施；

2） 监视和测量结果；

3） 审核结果；

4） 信息安全目标的实现；

d）相关方的反馈；

e）风险评估的结果和风险处置计划的状态；

f）持续改进的机会。

管理评审的输出应包括与持续改进机会有关的决定，以及变更信息安全管理体系的所有需求。

组织应保留文件记录信息作为管理评审结果的证据。

10 改进

10.1 不符合和纠正措施

当发生不符合时，组织应：

a）对不符合做出反应，适用时：

1） 采取措施控制并纠正不符合；

2） 处理后果；

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

1） 评审不符合；

2） 确定不符合的原因；

3） 确定是否存在或可能发生相似的不符合；

c）实施所需的措施；

d）评审所采取纠正措施的有效性；

e）必要时，对信息安全管理体系实施变更。纠正措施应与所遇不符合的影响相适应。组织应保留文件记录信息作为下列事项的证据：

f）不符合的性质以及所采取的所有后续措施；

g）所有纠正措施的结果。

10.2 持续改进

组织应持续改进信息安全管理体系的适宜性、充分性和有效性。

附 录 A

（规范性附录）

参考控制目标和控制措施

表 A.1所列的控制目标和控制措施是直接源自并与 ISO/IEC DIS 27002:2013[1]第 5到 18章一致，可用于 6.1.3节的情境。

表 A.1 控制目标和控制措施

A.5 信息安全策略		
A.5.1 信息安全的管理方向 目标：依据业务要求和相关法律法规提供管理方向并支持信息安全。		
A.5.1.1	信息安全策略	控制措施 信息安全策略集应由管理者定义、批准、发布并传达给员工和相关外部方。
A.5.1.2	信息安全策略的评审	控制措施 信息安全策略应按计划的时间间隔或当重大变化发生时进行评审，以确保其持续的适宜性、充分性和有效性。
A.6 信息安全组织		
A.6.1 内部组织 目标：建立管理框架，以启动和控制组织范围内的信息安全的实施和运行。		
A.6.1.1	信息安全角色和职责	控制措施 所有的信息安全职责应予以定义和分配。
A.6.1.1	信息安全角色和职责	控制措施 所有的信息安全职责应予以定义和分配。
A.6.1.2	职责分离	控制措施 分离相冲突的责任及职责范围，以降低未授权或无意识的修改或者不当使用组织资产的机会。
A.6.1.3	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.6.1.4	与特定利益集团的联系	控制措施 应保持与特定利益集团、其他安全论坛和专业协会的适当联系。
A.6.1.5	项目管理中的信息安全	控制措施 无论项目是什么类型，在项目管理中都应处理信息安全问题。
A.6.2 移动设备和远程工作 目标：确保远程工作和使用移动设备时的安全。		
A.6.2.1	移动设备策略	控制措施 应采用策略和支持性安全措施来管理由于使用移动设备带来的风险。
A.6.2.2	远程工作	控制措施 应实施策略和支持性安全措施来保护在远程工作场地访问、处理或存储的信息。
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、适于考虑让其承担的角色。		
A.7.1.1	审查	控制措施 关于所有任用候选者的背景验证核查应按照相关法律、法规、道德规范和对应的业务要求、被访问信息的类别和察觉的风险来执行。
A.7.1.2	任用条款和条件	控制措施 与雇员和承包方人员的合同协议应声明他们和组织的信息安全职责。
A.7.2 任用中		

目标：确保雇员和承包方人员知悉并履行其信息安全职责。		
A.7.2.1	管理职责	控制措施 管理者应要求所有雇员和承包方人员按照组织已建立的策略和规程对信息安全尽心尽力。
A.7.2.2	信息安全意识、教育和培训	控制措施 组织的所有雇员，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策略及规程的定期更新培训。
A.7.2.3	纪律处理过程	控制措施 应有一个正式的、已传达的纪律处理过程，来对信息安全违规的雇员采取措施。
A.7.3 任用的终止或变更目标：将保护组织利益作为变更或终止任用过程的一部分。		
A.7.3.1	任用终止或变更职责	控制措施 应定义信息安全职责和义务在任用终止或变更后保持有效的要求，并传达给雇员或承包方人员，予以执行。
A.8 资产管理		
A.8.1 对资产负责 目标：识别组织资产，并定义适当的保护职责。		
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的资产，编制并维护这些资产的清单。
A.8.1.2	资产所有权	控制措施 清单中所维护的资产应分配所有权。
A.8.1.3	资产的可接受使用	控制措施 信息及与信息和信息处理设施有关的资产的可接受使用规则应被确定、形成文件并加以实施。
A.8.1.4	资产的归还	控制措施 所有的雇员和外部方人员在终止任用、合同或协议时，应归还他们使用的所有组织资产。
A.8.2 信息分类 目标：确保信息按照其对组织的重要性受到适当级别的保护。		
A.8.2.1	信息的分类	控制措施 信息应按照法律要求、价值、关键性以及它对未授权泄露或修改的敏感性予以分类。
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规程。
A.8.2.3	信息的处理	控制措施 应按照组织所采纳的信息分类机制建立和实施处理资产的规程。
A.8.3 介质处置 目标：防止存储在介质上的信息遭受未授权泄露、修改、移动或销毁。		
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分类机制实施可移动介质的管理规程。
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	物理介质传输	控制措施 包含信息的介质在运送时，应防止未授权的访问、不当使用或毁坏。
A.9 访问控制		
A.9.1 安全区域 目标：限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 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。
A.9.1.2	网络和网络服务的访问	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	用户注册及注销	控制措施 应实施正式的用户注册及注销规程，使访问权限得以分配。
A.9.2.2	用户访问开通	控制措施 应实施正式的用户访问开通过程，以分配或撤销所有系统和服务所有用户类型的访问权限。
A.9.2.3	特殊访问权限管理	控制措施 应限制和控制特殊访问权限的分配及使用。
A.9.2.4	用户秘密鉴别信息管理	控制措施 应通过正式的管理过程控制秘密鉴别信息的分配。
A.9.2.5	用户访问权限的复查	控制措施 资产所有者应定期复查用户的访问权限。
A.9.2.6	撤销或调整访问权限	控制措施 所有雇员、外部方人员对信息和信息处理设施的访问权限应在任用、合同或协议终止时撤销，或在变化时调整。
A.9.3 用户职责目标：使用户承担保护认证信息安全的责任。		
A.9.3.1	使用秘密鉴别信息	控制措施 应要求用户在使用秘密鉴别信息时，遵循组织的实践。
A.9.4 系统和应用访问控制 目标：防止对系统和应用的未授权访问。		
A.9.4.1	信息访问控制	控制措施 应依照访问控制策略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 在访问控制策略要求下，访问操作系统和应用应通过安全登录规程加以控制。
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，并应确保优质的口令。
A.9.4.4	特殊权限使用工具软件的使用	控制措施 对于可能超越系统和应用程序控制措施的适用工具软件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.10 密码学		
A.10.1 密码控制 目标：恰当和有效的利用密码学保护信息的保密性、真实性或完整性。		
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 宜开发和实施贯穿整个密钥生命周期的关于密钥使用、保护和生存期的策略。
A.11 物理和环境安全		
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	物理安全周边	控制措施 应定义安全周边和所保护的区域，包括敏感或关键的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	外部环境威胁的安全防护	控制措施 为防止自然灾难、恶意攻击或事件，应设计和采取物理保护措施。
A.11.1.5	在安全区域工作	控制措施 应设计和应用工作在安全区域的规程。
A.11.1.6	交接区安全	控制措施 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，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 应安置或保护设备，以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会。
A.11.2.2	支持性设施	控制措施 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。
A.11.2.3	布缆安全	控制措施 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或损坏。
A.11.2.4	设备维护	控制措施 设备应予以正确地维护，以确保其持续的可用性和完整性。
A.11.2.5	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。
A.11.2.6	组织场外设备和资产的安全	控制措施 应对组织场所外的设备采取安全措施，要考虑工作在组织场所以外的不同风险。
A.11.2.7	设备的安全处置或在利用	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。
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。
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。
A.12 操作安全		
A.12.1 操作规程和职责 目标：确保正确、安全的操作信息处理设施。		
A.12.1.1	文件化的操作规程	控制措施 操作规程应形成文件并对所有需要的用户可用。
A.12.1.2	变更管理	控制措施 对影响信息安全的组织、业务过程、信息处理设施和系统等的变更应加以控制。
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。
A.12.1.4	开发、测试和运行环境分离	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环境的风险。
A.12.2 恶意软件防护 目标：确保对信息和信息处理设施进行恶意软件防护。		
A.12.1.1	控制恶意软件	控制措施 应实施恶意软件的检测、预防和恢复的控制措施，以及适当的提高用户安全意识。
A.12.3 备份 目标：为了防止数据丢失。		

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和软件。
A.12.4 日志和监视 目标：记录事态和生成证据。		
A.12.4.1	事态记录	控制措施 应产生记录用户活动、异常情况、故障和信息安全事态的事态日志，并保持定期评审。
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.12.5 运行软件的控制 目标：确保运行系统的完整性。		
A.12.5.1	在运行系统上安装软件	控制措施 应实施规程来控制在运行系统上安装软件。
A.12.6 技术脆弱性管理 目标：防止技术脆弱性被利用。		
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	限制软件安装	控制措施 应建立和实施软件安装的用户管理规则。
A.12.7 信息系统审计考虑 目标：将运行系统审计活动的影响最小化。		
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，以便使造成业务过程中断最小化。
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，以保护系统中信息和应用程序的安全。
A.13.1.2	网络服务安全	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.13.2 信息传递 目标：保持组织内以及与组织外信息传递的安全。		
A.13.2.1	信息传递策略和规程	控制措施 应有正式的传递策略、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传递。
A.13.2.2	信息传递协议	控制措施 协议应解决组织与外部方之间业务信息的安全传递。
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	保密性或不泄露协议	控制措施 应识别、定期评审并记录反映组织信息保护需要的保密性或不泄露协议的要求。
A.14 系统获取、开发和维护		
A.14.1 信息系统的安全需求 目标：确保信息安全是信息系统整个生命周期中的一个有机组成部分。这也包括提供公共网络服务的信息系统的要求。		
A.14.1.1	信息安全要求	控制措施

	分析和说明	信息安全相关要求应包括新的信息系统要求或增强已有信息系统的要求。
A.14.1.2	公共网络应用服务安全	控制措施 应保护公共网络中的应用服务信息，以防止欺骗行为、合同纠纷、未授权泄露和修改。
A.14.1.3	保护应用服务交易	控制措施 应保护涉及应用服务交易的信息，以防止不完整传送、错误路由、未授权消息变更、未授权泄露、未授权消息复制或重放。
A.14.2 开发和支持过程中的安全 目标：应确保进行信息安全设计，并确保其在信息系统开发生命周期中实施。		
A.14.2.1	安全开发策略	控制措施 应建立软件和系统开发规则，并应用于组织内的开发。
A.14.2.2	系统变更控制规程	控制措施 应通过使用正式变更控制程序控制开发生命周期中的系统变更。
A.14.2.3	运行平台变更后应用的技术评审	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严格控制。
A.14.2.5	安全系统工程原则	控制措施 应建立、记录和维护安全系统工程原则，并应用到任何信息系统实施工作。
A.14.2.6	安全开发环境	控制措施 组织应建立并适当保护系统开发和集成工作的安全开发环境，覆盖整个系统开发生命周期。
A.14.2.7	外包开发	控制措施 组织应管理和监视外包系统开发活动。
A.14.2.8	系统安全测试	控制措施 在开发过程中，应进行安全功能测试。
A.14.2.9	系统验收测试	控制措施 对于新建信息系统和新版本升级系统，应建立验收测试方案和相关准则。
A.14.3 测试数据 目标：确保保护测试数据。		
A.14.3.1	系统测试数据的保护	控制措施 测试数据应认真地加以选择、保护和控制。
A.15 供应商关系		
A.15.1 供应商关系的信息安全 目标：确保保护可被供应商访问的组织资产。		
A.15.1.1	供应商关系的信息安全策略	控制措施 为减缓供应商访问组织资产带来的风险，应与供应商协商并记录相关信息安全要求。
A.15.1.2	处理供应商协议的安全问题	控制措施 应与每个可能访问、处理、存储组织信息、与组织进行通信或为组织提供 IT 基础设施组件的供应商建立并协商所有相关的信息安全要求。
A.15.1.3	信息和通信技术供应链	控制措施 供应商协议应包括信息和通信技术服务以及产品供应链相关信息安全风险处理的要求。
A.15.2 供应商服务交付管理 目标：保持符合供应商交付协议的信息安全和服务交付的商定水准。		
A.15.2.1	供应商服务的	控制措施

	监视和评审	组织应定期监视、评审和审计供应商服务交付。
A.15.2.2	供应商服务的变更管理	控制措施 应管理供应商服务提供的变更，包括保持和改进现有的信息安全策略、规程和控制措施，并考虑到业务信息、系统和涉及过程的关键程度及风险的再评估。
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，包括安全事件和弱点的传达。		
A.16.1.1	职责和规程	控制措施 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。
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 应要求使用组织信息系统和服务的所有雇员和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	评估和确定信息安全事态	控制措施 信息安全事态应被评估，并且确定是否划分成信息安全事件。
A.16.1.5	信息安全事件响应	控制措施 应具有与信息安全事件响应相一致的文件化规程。
A.16.1.6	对信息安全事件的总结	控制措施 获取信息安全事件分析和解决的知识应被用户降低将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 组织应定义和应用识别、收集、获取和保存信息的程序，这些信息可以作为证据。
A.17 业务连续性管理的信息安全方面		
A.17.1 信息安全连续性 目标：组织的业务连续性管理体系中应体现信息安全连续性。		
A.17.1.1	信息安全连续性计划	控制措施 组织应确定不利情况下（例如，一个危机或危难时）信息安全的要求和信息安全管理连续性。
A.17.1.2	实施信息安全连续性计划	控制措施 组织应建立、文件化、实施和维护过程、规程和控制措施，确保在负面情况下要求的信息安全连续性级别。
A.17.1.3	验证、评审和评价信息安全连续性计划	控制措施 组织应定期验证已制定和实施信息安全业务连续性计划的控制措施，以确保在负面情况下控制措施的及时性和有效性。
A.17.2 冗余 目标：确保信息处理设施的有效性。		
A.17.2.1	信息处理设施的可用性	控制措施 信息处理设备应冗余部署，以满足高可用性需求。
A.18 符合性		
A.18.1 符合法律和合同要求 目标：避免违反任何法律、法令、法规或合同义务以及任何安全要求。		
A.18.1.1	可用法律及合同要求的识别	控制措施 对每一个信息系统和组织而言，所有相关的法律依据、法规和合同要求，以及为满足这些要求组织所采用的方法，应加以明确地定义、形成文件并保持更新。
A.18.1.2	知识产权（IPR）	控制措施 应实施适当的规程，以确保相关的知识产权和所有权的软件产品的使用，符合法律、法规和合同的要求。
A.18.1.3	保护记录	控制措施

		应防止记录的遗失、毁坏、伪造、非授权访问和非授权删除，以满足法令、法规、合同和业务的要求。
A.18.1.4	隐私和个人身份信息保护	控制措施 隐私和个人身份信息保护应确保符合相关法律、法规的要求。
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：确保信息安全实施及运行符合组织策略和程序。		
A.18.2.1	独立的信息安全评审	控制措施应定期或发生较大变更时对组织的信息安全处置和实施方法（即控制目标、控制、策略、过程和信息安全程序）进行评审。
A.18.2.2	符合安全策略和标准	控制措施 管理者应定期对所辖职责范围内的信息安全过程和规程评审，以确保符合相应的安全政策、标准及其他安全要求。
A.18.2.3	技术符合性评审	控制措施 信息系统应被定期评审是否符合组织的信息安全政策和标准。

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 27003:2010，信息技术 -安全技术 -信息安全管理体系实施指南。

[3] ISO/IEC 27004:2009，信息技术 -安全技术 -信息安全管理 -测量。

[4] ISO/IEC 27005:2011，信息技术 -安全技术 -信息安全风险管理。

[5] ISO 31000:2009，风险管理 -原则和指南。

[6] ISO/IEC 导则第一部分， ISO 补充部分 -ISO:2012 专用程序。