目录

前言 3
0 引言 4
0.1 总则 4
0.2 与其他管理系统标准的兼容性 4
1. 范围 5
2 规范性引用文件 5
3 术语和定义 5
4 组织景况 5
4.1 了解组织及其景况 5
4.2 了解相关利益方的需求和期望 5
4.3 确立信息安全管理体系的范围 6
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 组织的角色，职责和权限 7
6. 计划 7
6.1 应对风险和机遇的行为 7
6.2 信息安全目标及达成目标的计划 9
7 支持 9
7.1 资源 9
7.2 权限 9
7.3 意识 10
7.4 沟通 10
7.5 记录信息 10
8 操作 11
8.1 操作的计划和控制措施 11
8.2 信息安全风险评估 11
8.3 信息安全风险处置 11
9 性能评价 12
9.1 监测、测量、分析和评价 12
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)参考控制目标和控制措施 15
参考文献 28

前言

0 引言

0.1 总则

本标准提供建立、实施、保持和持续改进信息安全管理体系的要求。采用信息安全管理体系是组织的一项战略性决策。组织信息安全管理体系的建立和实施受组织的需要和目标、安全要求、所采用的过程、规模和结构的影响。所有这些影响因素可能随时间发生变化。

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，并给相关方建立风险得到充分管理的信心。

重要的是，信息安全管理体系是组织的过程和整体管理结构的一部分并集成在其中，并且在过程、信息系统和控制措施的设计中要考虑到信息安全。信息安全管理体系的实施要与组织的需要相符合。

本标准可被内部和外部各方用于评估组织的能力是否满足自身的信息安全要求。

本标准中表述要求的顺序不反映各要求的重要性或实施顺序。条款编号仅为方便引用。

ISO/IEC 27000 参考信息安全管理体系标准族（包括 ISO/IEC 27003[2]、ISO/IEC 27004[3]、ISO/IEC 27005[4]）及相关术语和定义，给出了信息安全管理体系的概述和词汇。

0.2 与其他管理体系标准的兼容性

本标准应用了 ISO/IEC 导则第一部分的 ISO 补充部分附录 SL 中定义的高层结构、同一子条款标题、同一文本、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 定义的通用方法有助于组织选择实施单一管理体系来满足两个或多个管理体系标准要求。

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（context）下建立、实施、运行、保持和持续改进信息安全管理体系的要求。本标准还包括了根据组织需求而进行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、规模或性质的组织。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

下列参考文件的部分或整体在本文档中属于标准化引用，对于本文件的应用必不可少。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 中界定的术语和定义适用于本文件。

4 组织环境（context）

4.1 理解组织及其环境（context）

组织应确定与其意图相关的，且影响其实现信息安全管理体系预期结果能力的外部和内部情况（issue）。

注：对这些情况的确定，参见 ISO31000：2009[5]，5.3 中建立外部和内部环境的内容。

4.2 理解相关方的需求和期望

组织应确定：

a) 信息安全管理体系相关方；

b) 这些相关方的信息安全要求。

注：相关方的要求可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范围

组织应确定信息安全管理体系的边界及其适用性以建立其范围。

在确定范围时，组织应考虑：

a) 4.1 中提到的外部和内部情况；

b) 4.2 中提到的要求；

c) 组织执行活动之间以及与其他组织执行活动之间的接口和依赖关系。

该范围应形成文件化信息并可用。

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 领导力

5.1 领导力和承诺

最高管理者应通过以下方式证明信息安全管理体系的领导力和承诺：

a) 确保信息安全方针和信息安全目标已建立，并与组织战略方向一致；

b) 确保将信息安全管理体系要求整合到组织过程中；

c) 确保信息安全管理体系所需资源可用；

d) 传达有效的信息安全管理及符合信息安全管理体系要求的重要性；

e) 确保信息安全管理体系达到预期结果；

f) 指导并支持相关人员为信息安全管理体系有效性做出贡献；

g) 促进持续改进；

h) 支持其他相关管理者角色，在其职责范围内展现领导力。

5.2 方针

最高管理者应建立信息安全方针，方针应：

a) 与组织意图相适宜；

b) 包括信息安全目标（见 6.2）或为信息安全目标的设定提供框架；

c) 包括对满足适用的信息安全要求的承诺；

d) 包括持续改进信息安全管理体系的承诺。

信息安全方针应：

e) 形成文件化信息并可用；

f) 在组织内得到沟通；

g) 适当时，对相关方可用。

5.3 组织的角色，职责和权限

最高管理者应确保与信息安全相关角色的职责和权限得到分配和沟通。

最高管理者应分配职责和权限，以：

a) 确保信息安全管理体系符合本标准的要求；

b) 向最高管理者报告信息安全管理体系绩效。

注：最高管理者也可为组织内报告信息安全管理体系绩效，分配职责和权限。

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 中提到的问题和 4.2 中提到的要求，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预期结果；

b) 预防或减少意外的影响；

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) 将这些措施整合到信息安全管理体系过程中，并予以实施；

2) 评价这些措施的有效性。

6.1.2 信息安全风险评估

组织应定义并应用信息安全风险评估过程，以：

a) 建立和维护信息安全风险准则，包括:

1) 风险接受准则；

2) 信息安全风险评估实施准则。

b) 确保重复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，以识别信息安全管理体系范围内与信息保密性、完整性和可用性损失有关的风险；

2) 识别风险责任人；

d) 分析信息安全风险：

1) 评估 6.1.2 c) 1)中所识别的风险发生后，可能导致的潜在后果；

2) 评估 6.1.2 c) 1)中所识别的风险实际发生的可能性；

3) 确定风险级别；

e) 评价信息安全风险：

1) 将风险分析结果与 6.1.2 a)中建立的风险准则进行比较；

2) 排列已分析风险的优先顺序，以便于风险处置。

组织应保留信息安全风险评估过程的文件化信息。

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基础上，选择适合的信息安全风险处置选项；

b) 确定实施已选的信息安全风险处置选项所必需的全部控制措施；

注：组织可根据需要设计控制措施，或从任何来源识别控制措施。

c) 将 6.1.3 b)确定的控制措施与附录 A 中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 包含了控制目标和控制措施的综合列表。本标准用户可使用附录 A，以确保没有忽略必要的控制措施。

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) 制定适用性声明，包含必要的控制措施（见 6.1.3 b）和 c））及其选择的合理性说明（无论该控制措施是否已实施），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) 获得风险责任人对信息安全风险处置计划的批准，及对信息安全残余风险的接受。

组织应保留信息安全风险处置过程的文件化信息。

注：本标准中的信息安全风险评估和处置过程与 ISO 31000[5]中给出的原则和通用指南

是一致的。

6.2 信息安全目标和实现规划

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的结果；

d) 得到沟通；

e) 在适当时更新。

组织应保留信息安全目标的文件化信息。

在规划如何实现信息安全目标时，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) 确定从事在组织控制下且会影响组织的信息安全绩效的工作的人员的必要能力；

b) 确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c) 适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；

d) 保留适当的文件化信息作为能力的证据。

注：适用的措施可包括，例如针对现有雇员提供培训、指导或重新分配；雇佣或签约有

能力的人员。

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) 其对信息安全管理体系有效性的贡献，包括改进信息安全绩效带来的益处；

c) 不符合信息安全管理体系要求带来的影响。

7.4 沟通

组织应确定与信息安全管理体系相关的内部和外部的沟通需求，包括：

a) 沟通内容；

b) 沟通时间；

c) 沟通对象；

d) 谁应负责沟通；

e) 影响沟通的过程。

7.5 文件化信息

7.5.1 总则

组织的信息安全管理体系应包括：

a) 本标准要求的文件化信息；

b) 组织为有效实施信息安全管理体系所确定的必要的文件化信息。

注：不同组织的信息安全管理体系文件化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

创建和更新文件化信息时，组织应确保适当的：

a) 标识和描述（例如标题、日期、作者或编号）；

b) 格式（例如语言、软件版本、图表）和介质（例如纸质、电子介质）；

c) 对适宜性和充分性的评审和批准。

7.5.3 文件化信息的控制

信息安全管理体系及本标准所要求的文件化信息应予以控制，以确保：

a) 在需要的地点和时间，是可用和适宜的；

b) 得到充分的保护（如避免保密性损失、不恰当使用、完整性损失等）。

为控制文件化信息，适用时，组织应开展以下活动：

c) 分发，访问，检索和使用；

d) 存储和保护，包括保持可读性；

e) 控制变更（例如版本控制）；

f) 保留和处置。

组织确定的为规划和运行信息安全管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

注：访问隐含着允许仅浏览文件化信息，或允许和授权浏览及更改文件化信息等决定。

8 运行

8.1 运行规划和控制

组织应对满足信息安全要求及实施 6.1 中确定的措施所需的过程予以规划、实施和控制。组织也应实施计划以实现 6.2 中确定的信息安全目标。

组织应保持文件化信息达到必要的程度，以确信过程按计划得到执行。

组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻负面影响。

组织应确保外包过程得到确定和控制。

8.2 信息安全风险评估

组织应考虑 6.1.2 a)建立的准则，按计划的时间间隔，或当重大变更提出或发生时，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) 需要被监视和测量的内容，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，适用时，以确保得到有效的结果。

注：所选的方法宜产生可比较和可再现的有效结果。

c) 何时应执行监视和测量；

d) 谁应监视和测量；

e) 何时应分析和评价监视和测量的结果；

f) 谁应分析和评价这些结果。

组织应保留适当的文件化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，提供信息以确定信息安全管理体系是否：

a) 符合

1) 组织自身对信息安全管理体系的要求；

2) 本标准的要求。

b) 得到有效实施和保持。

组织应：

c) 规划、建立、实施和保持审核方案（一个或多个），包括审核频次、方法、职责、规划要求和报告。审核方案应考虑相关过程的重要性和以往审核的结果；

d) 确定每次审核的审核准则和范围；

e) 选择审核员，实施审核，确保审核过程的客观性和公正性；

f) 确保将审核结果报告至相关管理者；

g) 保留文件化信息作为审核方案和审核结果的证据。

9.3 管理评审

最高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。

管理评审应考虑：

a) 以往管理评审要求采取措施的状态；

b) 与信息安全管理体系相关的外部和内部情况的变化；

c) 信息安全绩效有关的反馈，包括以下方面的趋势：

1) 不符合和纠正措施；

2) 监视和测量结果；

3) 审核结果；

4) 信息安全目标完成情况；

d) 相关方反馈；

e) 风险评估结果及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相关的决定以及变更信息安全管理体系的任何需求。

组织应保留文件化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) 通过以下方法，评价采取消除不符合原因的措施的需求，防止不符合再发生，或在其他地方发生：

1) 评审不符合；

2) 确定不符合的原因；

3) 确定类似的不符合是否存在，或可能发生；

c) 实施需要的措施；

d) 评审所采取的纠正措施的有效性；

e) 必要时，对信息安全管理体系进行变更。

纠正措施应与所遇到的不符合的影响程度相适应。

组织应保留文件化信息作为以下方面的证据：

f) 不符合的性质及所采取的后续措施；

g) 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[1]第 5 到 18 章一致，并在 6.1.3 环境中被使用。

表 A.1 控制目标和控制措施

A.5 信息安全方针和策略（POLICES）		
A.5.1 信息安全管理指导		
目标：依据业务要求和相关法律法规为信息安全提供管理指导和支持。		
A.5.1.1	信息安全方针和策略	*控制措施* 信息安全方针和策略应由管理者批准、发布并传达给所有员工和外部相关方。
A.5.1.2	信息安全方针和策略的评审	*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和策略评审，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	责任分割	*控制措施* 应分割冲突的责任和职责范围，以降低未授权或无意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	与特定相关方的联系	*控制措施* 应保持与特定相关方、其他专业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* 应解决项目管理中的信息安全问题，无论项目类

		型。
A.6.2 移动设备和远程工作		
目标：确保远程工作和移动设备使用的安全。		
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以管理使用移动设备时带来的风险。
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以保护在远程工作地点访问、处理或存储的信息。
A.7 人力资源安全		
A.7.1 任用前		
目标：确保员工和承包方理解其职责，并适合其角色。		
A.7.1.1	审查	*控制措施* 对所有任用候选者的背景验证核查应按照相关法律法规和道德规范进行，并与业务要求、访问信息的等级（8.2）和察觉的风险相适宜。
A.7.1.2	任用条款及条件	*控制措施* 应在员工和承包商的合同协议中声明他们和组织对信息安全的职责。
A.7.2 任用中		
目标：确保员工和承包方意识到并履行其信息安全职责。		
A.7.2.1	管理职责	*控制措施* 管理者应要求所有员工和承包商按照组织已建立的方针策略和规程应用信息安全。
A.7.2.2	信息安全意识、教育和培训	*控制措施* 组织所有员工，适当时包括承包商，应接受与其工作职能相关的适宜的意识教育和培训，及组织方针策略及规程的定期更新的信息。
A.7.2.3	纪律处理过程	*控制措施* 应建立正式的且被传达的纪律处理过程以对信息安全违规的员工采取措施。
A.7.3 任用的终止和变更		
目标：在任用变更或终止过程中保护组织的利益。（PART 未体现）		
A.7.3.1	任用职责的终止或变更	*控制措施*

		应确定任用终止或变更后仍有效的信息安全职责和责任，传达至员工或承包商并执行。
A.8 资产管理		
A.8.1 资产职责		
目标：识别组织资产并确定适当的保护职责。		
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相关的资产，并编制、维护这些资产的清单。
A.8.1.2	资产责任主体	*控制措施* 应确定资产清单中的资产责任主体。
A.8.1.3	资产的可接受使用	*控制措施* 应确定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，形成文件并加以实施。
A.8.1.4	资产归还	*控制措施* 所有员工和外部用户在任用、合同或协议终止时，应归还其占用的所有组织资产。
A.8.2 信息分级		
目标：确保信息按照其对组织的重要程度受到适当级别的保护。		
A.8.2.1	信息的分级	*控制措施* 信息应按照法律要求、价值、关键性及其对未授权泄露或修改的敏感性进行分级。
A.8.2.2	信息的标记	*控制措施* 应按照组织采用的信息分级方案，制定并实施一组适当的信息标记规程。
A.8.2.3	资产的处理	*控制措施* 应按照组织采用的信息分级方案，制定并实施资产处理规程。
A.8.3 介质处理		
目的：防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。		
A.8.3.1	移动介质的管理	*控制措施* 应按照组织采用的分级方案，实施移动介质管理规程。
A.8.3.2	介质的处置	*控制措施* 应使用正式的规程安全地处置不再需要的介质。

A.8.3.3	物理介质的转移	*控制措施* 包含信息的介质在运送中应受到保护，以防止未授权访问、不当使用或毁坏。
A.9 访问控制		
A.9.1 访问控制的业务要求		
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* 应基于业务和信息安全要求，建立访问控制策略，形成文件并进行评审。
A.9.1.2	网络和网络服务的访问	*访问控制* 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：确保授权用户对系统和服务的访问，并防止未授权的访问。		
A.9.2.1	用户注册和注销	*控制措施* 应实施正式的用户注册及注销过程来分配访问权限。
A.9.2.2	用户访问配置	*控制措施* 应对所有系统和服务的所有类型用户实施正式的用户访问配置过程以分配或撤销访问权限。
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和使用。
A.9.2.4	用户的秘密鉴别信息管理	*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* 资产责任主体应定期对用户的访问权限进行复查。
A.9.2.6	访问权限的移除或调整	*控制措施* 所有员工和外部用户对信息和信息处理设施的访问权限在任用、合同或协议终止时，应予以移除，或在变更时予以调整。
A.9.3 用户职责		

目标：使用户承担保护其鉴别信息的责任。		
A.9.3.1	秘密鉴别信息的使用	*控制措施* 应要求用户遵循组织在使用秘密鉴别信息时的惯例。
A.9.4 系统和应用访问控制		
目的：防止对系统和应用的未授权访问。		
A.9.4.1	信息访问限制	*控制措施* 应按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* 当访问控制策略要求时，应通过安全登录规程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，并应确保优质的口令。
A.9.4.4	特权实用程序的使用	*控制措施* 对于可能超越系统和应用控制措施的实用程序的使用应予以限制并严格控制。
A.9.4.5	程序源代码的访问控制	*控制措施* 应限制对程序源代码的访问。
A.10 密码		
A.10.1 密码控制		
目标： 确保适当和有效地使用密码技术以保护信息的保密性、真实性和（或）完整性。		
A.10.1.1	密码控制的使用策略	*控制措施* 应开发和实施用于保护信息的密码控制使用策略。
A.10.1.2	密钥管理	*控制措施* 应制定和实施贯穿其全生命周期的密钥使用、保护和生存期策略。
A.11 物理和环境安全		
A.11.1 安全区域		
目标：防止对组织信息和信息处理设施的未授权物理访问、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。
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	
A.11.1.5	在安全区域工作	*控制措施* 应设计和应用安全区域工作规程。
A.11.1.6	交接区	*控制措施* 访问点（例如交接区）和未授权人员可进入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、干扰或损坏
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	组织场所外的设备与资产安全	*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部分应进行核查，以确保在处置或再利用之前，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，并对所需用户可用。
A.12.1.2	变更管理	*控制措施* 应控制影响信息安全的变更，包括组织、业务过程、信息处理设施和系统变更。
A.12.1.3	容量管理	*控制措施* 应对资源的使用进行监视，调整和预测未来的容量需求，以确保所需的系统性能。
A.12.1.4	开发、测试和运行环境的分离	*控制措施* 应分离开发、测试和运行环境，以降低对运行环境未授权访问或变更的风险。
A.12.2 恶意代码防范		
目标：确保信息和信息处理设施防范恶意代码。		
A.12.2.1	恶意代码的控制	*控制措施* 应实施检测、预防和恢复控制措施以防范恶意代码，并结合适当的用户意识教育。
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* 应按照既定的备份策略，对信息、软件和系统镜像进行备份，并定期测试。

A.12.4 日志和监视		
目的：记录事态并生成证据。		
A.12.4.1	事态日志	*控制措施* 应产生、保持并定期评审记录用户活动、异常、错误和信息安全事态的事态日志。
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，并对日志进行保护和定期评审。
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与单一的参考源进行同步。
A.12.5 运行软件控制		
目标：确保运行系统的完整性。		
A.12.5.1	运行系统的软件安装	*控制措施* 应实施运行系统软件安装控制规程。
A.12.6 技术脆弱性管理		
目标：防止对技术脆弱性的利用。		
A.12.6.1	技术脆弱性的管理	*控制措施* 应及时获取在用的信息系统的技术脆弱性信息，评价组织对这些脆弱性的暴露状况并采取适当的措施来应对相关风险。
A.12.6.2	软件安装限制	*控制措施* 应建立并实施控制用户安装软件的规则。
A.12.7 信息系统审计的考虑		
目标：使审计活动对运行系统的影响最小化。		
A.12.7.1	信息系统审计的控制	*控制措施* 涉及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.13 通信安全		
A.13.1 网络安全管理		

目标：确保网络及其支持性信息处理设施中的信息得到保护。		
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中的信息。
A.13.1.2	网络服务的安全	*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括在网络服务协议中，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 信息传输		
目标： 保持在组织内及与外部实体间传输信息的安全。		
A.13.2.1	信息传输策略和规程	*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进行的信息传输。
A.13.2.2	信息传输协议	*控制措施* 协议应解决组织与外部方业务信息的安全传输。
A.13.2.3	电子消息发送	*控制措施* 应适当保护包含在电子消息发送中的信息。
A.13.2.4	保密或不泄露协议	*控制措施* 应识别、定期评审和文件化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 信息系统的安全要求		
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	信息安全要求分析和说明	*控制措施* 新建信息系统或增强现有信息系统的要求中应包括信息安全相关要求。
A.14.1.2	公共网络上应用服务的安全保护	*控制措施* 应保护在公共网络上的应用服务中的信息以防止欺诈行为、合同纠纷以及未经授权的泄露和修改。
A.14.1.3	应用服务交易的保护	*控制措施* 应保护应用服务交易中的信息，以防止不完整的传输、错误路由、未授权的消息变更、未授权的

		泄露、未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：确保信息安全在信息系统开发生命周期中得到设计和实施。		
A.14.2.1	安全的开发策略	*控制措施* 针对组织内的开发，应建立软件和系统开发规则并应用。
A.14.2.2	系统变更控制规程	*控制措施* 应使用正式的变更控制规程来控制开发生命周期内的系统变更。
A.14.2.3	运行平台变更后对应用的技术评审	*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* 应不鼓励对软件包进行修改，仅限于必要的变更，且对所有变更加以严格控制
A.14.2.5	安全的系统工程原则	*控制措施* 应建立、文件化和维护安全的系统工程原则，并应用到任何信息系统实施工作中
A.14.2.6	安全的开发环境	*控制措施* 组织应针对覆盖系统开发生命周期的系统开发和集成活动，建立安全开发环境，并予以适当保护。
A.14.2.7	外包开发	*控制措施* 组织应督导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* 应在开发过程中进行安全功能测试。
A.14.2.9	系统验收测试	*控制措施* 应建立对新的信息系统、升级及新版本的验收测试方案和相关准则。
A.14.3 测试数据		
目标：确保用于测试的数据得到保护。		
A.14.3.1	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 供应商关系中的信息安全		
目标：确保供应商可访问的组织资产受到保护。		
A.15.1.1	供应商关系的信息安全策略	*控制措施* 为降低供应商访问组织资产的相关风险，应与供应商就信息安全要求达成一致，并形成文件
A.15.1.2	在供应商协议中解决安全	*控制措施* 应与每个可能访问、处理、存储、传递组织信息或为组织信息提供 IT 基础设施组件的供应商建立所有相关的信息安全要求，并达成一致。
A.15.1.3	信息与通信技术供应链	*控制措施* 供应商协议应包括信息与通信技术服务以及产品供应链相关的信息安全风险处理要求。
A.15.2 供应商服务交付管理		
目标：保持与供应商协议一致的信息安全和服务交付的商定级别。		
A.15.2.1	供应商服务的监视和评审	*控制措施* 组织应定期监视、评审和审核供应商服务交付。
A.15.2.2	供应商服务的变更管理	*控制措施* 应管理供应商所提供服务的变更，包括保持和改进现有的信息安全策略、规程和控制措施，管理应考虑变更涉及到的业务信息、系统和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 信息安全事件的管理和改进		
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，包括对安全事态和弱点的沟通。		
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* 应通过适当的管理渠道尽快地报告信息安全事态。
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员工和承包商注意并报告任何观察到的或可疑的系统或服务中

		的信息安全弱点。
A.16.1.4	信息安全事态的评估和决策	*控制措施* 应评估信息安全事态并决定其是否属于信息安全事件。
A.16.1.5	信息安全事件的响应	*控制措施* 应按照文件化的规程响应信息安全事件。
A.16.1.6	从信息安全事件中学习	*控制措施* 应利用在分析和解决信息安全事件中得到的知识来减少未来事件发生的可能性和影响。
A.16.1.7	证据的收集	*控制措施* 组织应确定和应用规程来识别、收集、获取和保存可用作证据的信息。
A.17 业务连续性管理的信息安全方面”		
A.17.1 信息安全的连续性		
目标：应将信息安全连续性纳入组织业务连续性管理之中。		
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（如危机或灾难）下，对信息安全及信息安全管理连续性的要求。
A.17.1.2	实施信息安全连续性	*控制措施* 组织应建立、文件化、实施并维持过程、规程和控制措施，以确保在不利情况下信息安全连续性达到要求的级别。
A.17.1.3	验证、评审和评价信息安全连续性	*控制措施* 组织应定期验证已建立和实施的信息安全连续性控制措施，以确保这些措施在不利情况下是正当和有效的。
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* 信息处理设施应具有足够的冗余以满足可用性要求。
A.18 符合性		
A.18.1 符合法律和合同要求		
目标：避免违反与信息安全有关的法律、法规、规章或合同义务以及任何安全要求。		

A.18.1.1	可用的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，所有相关的法律、法规、规章和合同要求，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	*控制措施* 应实施适当的规程，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.18.1.3	记录的保护	*控制措施* 应根据法律、法规、规章、合同和业务要求，对记录进行保护以防其丢失、毁坏、伪造、未授权访问和未授权发布。
A.18.1.4	个人身份信息的隐私和保护	*控制措施* 应依照相关的法律、法规和合同条款的要求，确保个人身份信息的隐私和保护。
A.18.1.5	密码控制规则	*控制措施* 密码控制措施的使用应遵从所有相关的协议、法律和法规。
A.18.2 信息安全评审		
目标：确保依据组织方针策略、规程实施和运行信息安全。		
A.18.2.1	信息安全的独立评审	*控制措施* 应按计划的时间间隔或在重大变化发生时，对组织的信息安全管理方法及其实施（如信息安全的控制目标、控制措施、方针策略、过程和规程）进行独立评审。
A.18.2.2	符合安全策略和标准	*控制措施* 管理者应定期评审其职责范围内的信息处理、规程与适当的安全方针策略、标准和任何安全要求的符合性。
A.18.2.3	技术符合性评审	*控制措施* 应定期评审信息系统与组织的信息安全方针策略和标准的符合性。

参考文献

[1] ISO/IEC 27002:2013, 信息技术 — 安全技术 — 信息安全控制的实务守则.

[2] ISO/IEC 27002:2010, 信息技术 — 安全技术 — 信息安全管理系统实施指南.

[3] ISO/IEC 27002:2009, 信息技术 — 安全技术 — 信息安全管理 — 测量.

[4] ISO/IEC 27002:2011, 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 指示, 第一部分 综合 ISO 补充 — ISO:2012 具体规程.