信息安全管理
先锋论坛

跟我学信息安全管理

02、ISO27001条文解析　宽恕

信息安全管理专家委员会发布
2016年4月

信息安全管理论坛（http://www.iso27001cn.com）成立于2014年9月，为国内目前最专业的信息安全管理学习和实践交流平台。是学习信息安全管理方法、分享实战经验、提升实践水平的好地方！

关于我们

我们提供

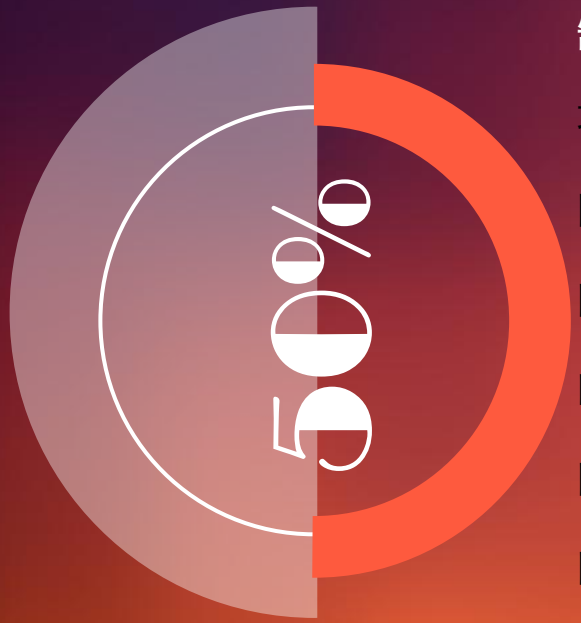
- 最全的信息安全管理资料
- 信安经理高薪工作机会推荐
- 每周专家讲堂（ 每周四晚上8点半YY频道89519382 ）
- 物美价廉的ISO27001课程团购

- 信息安全管理学习实践QQ群 207723402
- 微信 IT管理精英圈 itilxf_(记得有下划线)

欢迎关注

授课专家

宽恕



IT管理咨询顾问及讲师，十年IT行业工作经验，服务的客户领域涉及电信、金融、制造、能源等多个行业。

项目经验：

国有四大行之一的IT服务管理体系建设推广

国内某省级商业银行的IT服务管理体系与信息安全管理体系建设

四大国有资产管理公司配置管理审计项目

国内某石油化工企业安全体系建设评估项目

国内某通信公司数据安全差异评估项目

ISO27001-2013标准

条文解析

时间安排

- 正文　2016年4月28日　宽恕
- 附录A　2016年5月12日　师鑫
- 附录A　2016年5月28日　樊忠林

1 ISO27001的发展

2 ISO27001正文结构

3 ISO27001 2013版与2005版的差异

4 ISO27001的P-D-C-A

1

ISO27001发展

背景与发展

Background & Growth

TIPS

Author & copyright

- JTC1（Joint Technical Committee 1 联合技术分会1）
- SC27（Sub-committee 27分会）
- COPYRIGHT PROTECTED DOCUMENT

ISO copyright office Case postale 56 • CH-1211 Geneva 20

Tel. + 41 22 749 01 11

E-mail copyright@iso.org

Web www.iso.org

2

ISO27001正文结构

正文结构

Standard has been written in accordance with Annex SL

管理体系标准新结构和格式

- 国际标准化组织对管理体系标准在结构、格式、通用短语和定义方面进行了统一。这将确保今后编制或修订管理体系标准的持续性、整合性和简单化，这也将使标准更易读、易懂；
- 所有管理体系标准将遵循ISO Supplement Annex SL的要求，以便整合其他标准文件中的不同主题和要求，如：
  - 统一定义，如：组织、相关方、方针、目标、能力、符合性
  - 统一的表述，如：最高管理者应确保组织内的职责、权限得到规定和沟通

3

2013版与2005版差异

差异
Key Changes

- Standard has been written in accordance with Annex SL
- Does not emphasis PDCA cycle in same way as ISO/IEC27001:2005
- Definitions in 2005 version have been removed and relocated to ISO27000
- Requirements for management commitments have been revised and presented in the Leadership clause
- Term preventive action has been replaced with “actions to address, risks and opportunities” and features earlier in the standards
- The risk assessment requirements are more general
- SOA requirements are similar but with more clarity on the determination of controls by the risk treatment process
- Greater emphasis on setting the objectives ,monitoring performance and metrics
- The chapter on risk assessment and risk treatment has been relocated into section 6
- The controls are enhanced to reflect the changes of information security risks

4

ISO27001的P-D-C-A

PDCA

Continuity improvement

4.组织背景

Context of the organization

- 4.组织背景（或环境）
  - **4.1 理解组织及其背景**
  - 4.2 理解相关方的需求和期望
  - 4.3 确定ISMS的范围
  - 4.4 ISMS

- 4.1 理解组织及其背景
  - 组织应确定与其意图相关并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**。
- 内部环境
  - 治理、组织架构、角色与职责; 方针、目标、以及达成目标所采用的策略；
  - 组织拥有的**资源与能力**（如资产、时间、人力、流程、系统及技术）；
  - 与内部利益相关方的关系以及他们的**认识/价值观**；
  - 组织的**企业文化**；
  - 组织的**信息系统**、信息流、决策过程（正式与非正式）；
  - 组织采用的任何**标准、指南和模型**；
  - **契约关系**与安排的形式和程度。

4.组织背景

Context of the organization

- 4.组织背景（或环境）
  - **4.1 理解组织及其背景**
  - 4.2 理解相关方的需求和期望
  - 4.3 确定ISMS的范围
  - 4.4 ISMS

- 4.1 理解组织及其背景
  - 组织应确定与其意图相关并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。
- 外部环境
  - 组织以外的能够影响组织目标的，与组织的风险轮廓及风险管理相关的任何因素。
    - ✓ 社会和文化、政治、法律法规、金融、技术、经济以及竞争因素 (国际、国内或地区性)；
    - ✓ 影响组织目标达成的关键外部驱动力和趋势；
    - ✓ 利益相关方的认识及价值观；

4.组织背景

Context of the organization

- 4.组织背景（或环境）
  - **4.1 理解组织及其背景**
  - 4.2 理解相关方的需求和期望
  - 4.3 确定ISMS的范围
  - 4.4 ISMS

- 4.2 理解相关方的需求和期望
  - a) 组织应确定ISMS有关的相关方；
  - b) 组织应确定这些相关方与信息安全有关的要求。
- 相关方
  - 业务经理
  - 资产所有人
  - 项目经理
  - 消费者及客户
  - 商业伙伴
  - 监管机构
  - ……

4.组织背景

Context of the organization

- 4.组织背景（或环境）
  - **4.1 理解组织及其背景**
  - 4.2 理解相关方的需求和期望
  - 4.3 确定ISMS的范围
  - 4.4 ISMS

- 4.2 理解相关方的需求和期望
  - a) 组织应确定ISMS有关的相关方；
  - b) 组织应确定这些相关方与信息安全有关的要求。
- 应考虑相关方：
  - 组织为支持其运营、业务应用及服务，就信息处理、加工、存储、通讯及存档而制定的**原则、目标及业务要求**。
  - 组织及其商业伙伴、承包商、服务提供商应遵守的**任何法律、法规要求**或**合同责任**，以及上述各方的社会文化背景。
  - 信息安全风险管理流程--- 评估及处理组织面临的风险，考虑组织的整体业务目标及策略。

4.组织背景

Context of the organization

- 4.组织背景（或环境）
  - **4.1 理解组织及其背景**
  - 4.2 理解相关方的需求和期望
  - 4.3 确定ISMS的范围
  - 4.4 ISMS

- 4.2 理解相关方的需求和期望
  - a) 组织应确定ISMS有关的相关方；
  - b) 组织应确定这些相关方与信息安全有关的要求。

- 确定相关方有关信息安全的要求：
  - 移动设备及远程办公 (clause 6.2)
  - 信息分类 (clause 8.1)
  - 访问控制的业务要求 (clause 9.1)
  - 访问控制的系统及应用 (clause 9.2)
  - 物理及环境安全 (clause 11)
  - 备份 (clause 12.3)
  - 网络安全管理 (clause 13.1)
  - 信息传递 (clause 13.2)
  - 保密及不泄露协议 (clause 13.2.4)
  - 供应商链的信息安全 (clause 15.1)
  - 业务连续性管理的信息安全方面 (clause 17.1)
  - 遵守法律及合同要求 (clause 18.1)

4.组织背景

Context of the organization

- 4.组织背景（或环境）
  - **4.1 理解组织及其背景**
  - 4.2 理解相关方的需求和期望
  - 4.3 确定ISMS的范围
  - 4.4 ISMS

- 4.3 确定ISMS的范围
  - 组织应确定ISMS的边界和适用性，以确定其**范围**。
  - 在确定此范围时，组织应考虑：
  - a) 4.1 提及的外部和内部的情况；
  - b) 4.2 提及的要求；
  - c) 组织执行的和其它组织执行的活动之间的**接口和依赖关系**。
  - 范围应形成可用的文档化信息。

4.组织背景

Context of the organization

- 4.组织背景（或环境）
  - **4.1 理解组织及其背景**
  - 4.2 理解相关方的需求和期望
  - 4.3 确定ISMS的范围
  - 4.4 ISMS

- 4.4 ISMS
  - 组织应按照本国际标准的要求建立、实施、保持和持续改进**ISMS**。

5.领导力
Leadership

- 5.领导力
  - **5.1 领导力和承诺**
  - 5.2 方针
  - 5.3 组织的角色、职责和权限

- 5.1 领导力和承诺
  - 最高管理者应展示关于ISMS的领导力和承诺：
  - a) 确保信息安全**方针**和信息安全**目标**被建立，并与组织战略方向保持一致;
  - b) 确保信息安全管理体系的要求**集成**到组织的过程中;
  - c) 确保信息安全管理体系所需要的**资源**是可用的;
  - d) **传达**有效的信息安全管理和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其**预期的效果**;
  - f) **指导和支持**员工，有助于信息安全管理体系的效率;
  - g) 推进**持续改进**；
  - h) **支持其他相关管理角色**展示他们的领导力，同样适用于他们的职责范围。

5.领导力
Leadership

- 5.领导力
  - **5.1 领导力和承诺**
  - 5.2 方针
  - 5.3 组织的角色、职责和权限

- 5.2 方针
  - 最高管理者应建立信息安全方针：
  - a) 与组织的意图相适应;
  - 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) 包括满足有关信息安全适当要求的承诺;
  - d) 包括ISMS持续改进的承诺。
  - 信息安全方针应：
  - e) 形成可用的文件化信息;
  - f) 在组织内部得到沟通；
  - g) 适当时，对相关方可用。

5.领导力
Leadership

- 5.领导力
  - **5.1 领导力和承诺**
  - 5.2 方针
  - 5.3 组织的角色、职责和权限

- 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被**分配和传达**。
  - 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) 将ISMS绩效报告给最高管理者。
  - 注：最高管理者也可以分配组织内ISMS绩效报告的职责和权限。

5.领导力
Leadership

- 5.领导力
  - **5.1 领导力和承诺**
  - 5.2 方针
  - 5.3 组织的角色、职责和权限

- 5.3 组织的角色、职责和权限
  - 在用户/员工被授权访问敏感、关键的信息或个人身份识别信息前，须适当**告知其信息安全角色与职责**。
  - 须为用户/员工**提供指南**，定义组织内部对于他们角色的信息安全期望。
  - 须**激励**用户/员工履行组织的信息安全方针。
  - 用户/员工须拥有一定程度的，与其在组织内的角色与职责相关的**信息安全意识**。
  - 用户/员工须遵守**劳动合同中的条款**，包括组织的信息安全方针、实践、程序以及适当的工作方法。

6.策划
Planning

- 6.规划
  - 6.1 处理风险和机遇的行动
  - 6.1.1 总则
  - 6.1.2 信息安全风险评估
  - 6.1.3 信息安全风险处置
  - 6.2 可实现的信息安全目标和计划

- 6.1.1 总则
  - 当规划ISMS时，组织应考虑4.1提到的问题和4.2提到的要求，并确定需要处理的风险和机遇：
  - a) 确保ISMS实现预期的效果；
  - b) 防止或减少意外的影响；
  - c) 实现持续改进。
  - 组织应策划：
  - d) 处理这些风险和机遇的行动
  - 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) 评估这些行动的有效性。

6.策划
Planning

- 6.规划
  - 6.1 处理风险和机遇的行动
  - **6.1.1 总则**
  - 6.1.2 信息安全风险评估
  - 6.1.3 信息安全风险处置
  - 6.2 可实现的信息安全目标和计划

- 6.1. 2 信息安全风险评估
  - 组织应定义并应用一个信息安全风险评估过程：
  - a) 建立和维护信息安全风险准则，包括：
    - 1) 风险接受准则;
    - 2) 执行信息安全风险评估准则;
  - b) 确保重复的信息安全风险评估产生一致的、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，识别与ISMS范围内信息的保密性、完整性和可用性丢失相关的风险；和
    - 2) 识别风险所有人。

6.策划
Planning

- 6.规划
  - 6.1 处理风险和机遇的行动
  - **6.1.1 总则**
  - 6.1.2 信息安全风险评估
  - 6.1.3 信息安全风险处置
  - 6.2 可实现的信息安全目标和计划

- 6.1. 2 信息安全风险评估
  - 组织应定义并应用一个信息安全风险评估过程：
  - d) 分析信息安全风险：
    - 1) 确定在6.1.2c ）1 ）中识别的风险发生后会产生的潜在的后果；
    - 2) 确定在6.1.2c ）1 ）中识别的风险发生的现实的可能性；和
    - 3) 确定风险等级。
  - e) 评价信息安全风险：
    - 1) 风险分析的结果与6.1.2a ）建立的风险准则进行比较；和
    - 2) 对分析后的风险确定风险处理的优先级。
  - 组织应保留信息安全风险评估过程中的文档化信息。

6.策划
Planning

- 6.规划
  - 6.1 处理风险和机遇的行动
  - **6.1.1 总则**
  - 6.1.2 信息安全风险评估
  - 6.1.3 信息安全风险处置
  - 6.2 可实现的信息安全目标和计划

- 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理过程：
  - a) 选择适当的信息安全风险处置方案，考虑风险评估结果;
  - b) 确定所有控制措施对实施信息安全风险处置方案选择是必要的;
  - 注：组织可以设计所要求的控制措施，或从任何来源中识别它们。
  - c) 6.1.3 b)中确定的控制措施与附件A中的控制措施进行比较，并确认不是应的控制措施已被忽略;
  - 注 1：附件 A 中包含了控制目标和控制措施的完整列表。本国际标准的用户应以附录A为指导，确保非必要的控制措施被忽略。
  - 注 2：控制目标被隐含包括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详尽，可能还需要额外的控制目标和控制措施

6.策划
Planning

- 6.规划
  - 6.1 处理风险和机遇的行动
  - **6.1.1 总则**
  - 6.1.2 信息安全风险评估
  - 6.1.3 信息安全风险处置
  - 6.2 可实现的信息安全目标和计划

- 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理过程：
  - d) 编制一个包含应的控制措施（见 6.1.3b）和c）和选择理由的适用性声明，无论实施与否，并包含删减附件A中控制措施的理由;
  - e) 制定信息安全风险处置计划;和
  - f) 信息安全风险处理计划和残余信息安全风险接受获得风险所有人的批准。
  - 组织应保留信息安全风险的处置过程中的文档化信息。
  - 注意：本标准的信息安全风险评估和处置过程与ISO 31000 规定的原则和通用准则相一致。

6.策划
Planning

- 6.规划
  - 6.1 处理风险和机遇的行动
  - **6.1.1 总则**
  - 6.1.2 信息安全风险评估
  - 6.1.3 信息安全风险处置
  - 6.2 可实现的信息安全目标和计划

- 6.2 可实现的信息安全目标和计划
  - 组织应在相关职能和级别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) 是可测量的（如果可行）;
  - c) 考虑到适用的信息安全要求，以及风险评估和风险处置的结果;
  - d) 已被传达;和
  - e) 适当的更新。
  - 组织应保留信息安全目标的文档化信息。

6.策划
Planning

- 6.规划
  - 6.1 处理风险和机遇的行动
  - **6.1.1 总则**
  - 6.1.2 信息安全风险评估
  - 6.1.3 信息安全风险处置
  - 6.2 可实现的信息安全目标和计划

- 6.2 可实现的信息安全目标和计划
  - 组织应在相关职能和级别上建立信息安全目标。
  - 信息安全目标应：
  - 当计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) 谁负责;
  - i) 何时完成;和
  - j) 如何评估结果。

7.支持
Support

- 7.支持
  - **7.1 资源**
  - 7.2 能力
  - 7.3 意识
  - 7.4 沟通
  - 7.5 文档化的信息
  - 7.5.1 总则
  - 7.5.2 建立和更新
  - 7.5.3 文档化信息的控制

- 7.1 资源
  - 组织应确定并提供ISMS建立、实施、维护和持续改进所需的资源。

- 这意味着组织要确定需要哪些资源：
  - 预算
  - 人力资源
  - 流程
  - 技术
  - 培训及意识方案

7.支持
Support

- 7.支持
  - **7.1 资源**
  - 7.2 能力
  - 7.3 意识
  - 7.4 沟通
  - 7.5 文档化的信息
  - 7.5.1 总则
  - 7.5.2 建立和更新
  - 7.5.3 文档化信息的控制

- 7.2 能力
  - 组织应：
  - a) 确定员工工作的必备能力，这会影响到其控制下的信息安全绩效;
  - b) 确保这些人在适当的教育、培训或取得经验的基础上是能胜任的;
  - 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;和
  - d) 保留适当的文档化信息作为能力的证据。
  - 注：适用的行动可能包括，如：提供培训、指导、或重新分配现有雇员、或有能力人员的聘用或承包。

7.支持
Support

- 7.支持
  - **7.1 资源**
  - 7.2 能力
  - 7.3 意识
  - 7.4 沟通
  - 7.5 文档化的信息
  - 7.5.1 总则
  - 7.5.2 建立和更新
  - 7.5.3 文档化信息的控制

- 7.3 意识
  - 组织控制措施下工作的人员应意识到：
  - 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;和
  - c) 不符合ISMS要求所带来的影响。

7.支持
Support

- 7.支持
  - **7.1 资源**
  - 7.2 能力
  - 7.3 意识
  - 7.4 沟通
  - 7.5 文档化的信息
  - 7.5.1 总则
  - 7.5.2 建立和更新
  - 7.5.3 文档化信息的控制

- 7.4 沟通
  - 组织应确定有关ISMS内部和外部沟通的需求：
    - ✓ a) 沟通什么;
    - ✓ b) 何时沟通;
    - ✓ c) 和谁沟通;
    - ✓ d) 谁应参加沟通;
    - ✓ e) 怎样的沟通过程是有效的。

7.支持
Support

- 7.支持
  - **7.1 资源**
  - 7.2 能力
  - 7.3 意识
  - 7.4 沟通
  - 7.5 文档化的信息
  - 7.5.1 总则
  - 7.5.2 建立和更新
  - 7.5.3 文档化信息的控制

- 7.4 沟通
  - ISO/IEC 27001 里有许多其它要求，其中高级管理层需要与ISMS 相关的不同人员进行沟通。关于:
    - ✓ 与ISMS相关的内外部问题 (clause 4.1)
    - ✓ 理解ISMS所有利益相关方的需求与期望 (clause 4.2)
    - ✓ 确定 ISMS的范围 (clause 4.3)
    - ✓ 确保建立信息安全方针及目标，并应符合组织战略使命。 (clause 5.1)
    - ✓ 与员工和其它人员沟通信息安全管理的重要性 (clause 5.1)

7.支持
Support

- 7.支持
  - **7.1 资源**
  - 7.2 能力
  - 7.3 意识
  - 7.4 沟通
  - 7.5 文档化的信息
  - 7.5.1 总则
  - 7.5.2 建立和更新
  - 7.5.3 文档化信息的控制

- 7.5.1 总则
  - 组织的ISMS应包括：
  - a) 本国际标准所需要的文档化信息;和
  - b) 由组织确定的ISMS有效性必要的文档化信息。
  - 注：不同组织的ISMS文档化信息的多少与详略程度取决于：
    - 1) 组织的规模和活动的类型、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.支持
Support

- 7.支持
  - **7.1 资源**
  - 7.2 能力
  - 7.3 意识
  - 7.4 沟通
  - 7.5 文档化的信息
  - 7.5.1 总则
  - 7.5.2 建立和更新
  - 7.5.3 文档化信息的控制

- 7.5.2 建立和更新
  - 当建立和更新文档化信息时，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）；
  - b) 格式（如语言、软件版本、图形）和介质（如纸张，电子）；
  - c) 适当和足够的评审和批准。

7.支持
Support

- 7.支持
  - **7.1 资源**
  - 7.2 能力
  - 7.3 意识
  - 7.4 沟通
  - 7.5 文档化的信息
  - 7.5.1 总则
  - 7.5.2 建立和更新
  - 7.5.3 文档化信息的控制

- 7.5.3 文档化信息的控制
  - ISMS和本国际标准要求的文档化信息应被控制，以确保：
  - a) 当文档化信息被需要时是可用且适用的;
  - b) 得到充分的保护（例如保密性丧失、不正确的使用、完整性丧失）。

7.支持
Support

- 7.支持
  - **7.1 资源**
  - 7.2 能力
  - 7.3 意识
  - 7.4 沟通
  - 7.5 文档化的信息
  - 7.5.1 总则
  - 7.5.2 建立和更新
  - 7.5.3 文档化信息的控制

- 7.5.3 文档化信息的控制
  - ISMS和本国际标准要求的文档化信息应被控制，以确保：
  - 对于文档化信息的控制，组织应处理下列活动，适当时：
  - c) 分配、访问、检索和使用;
  - d) 存储和保存，包括易读性的保存;
  - e) 变更管理（例如版本控制）;
  - f) 保留和处置。
  - 由组织确定的ISMS计划和运行必要的外来文档化信息，应被恰当的识别和控制。
  - 注：访问意味着只允许查看文档化信息的决定，或允许和授权查看和变更文档化信息等。

8.运行
Operation

- 8.运行
  - **8.1 运行计划及控制**
  - 8.2 信息安全风险评估
  - 8.3 信息安全风险处置

- 8.1 运行计划及控制
  - 组织应策划、实施和控制用来满足信息安全要求过程，并实施在 6.1 中确定的行动。组织还应实施计划，以实现在 6.2 中确定的信息安全目标。
  - 组织应保存相关的文档化信息，以保证过程已按照计划完成。
  - 组织应控制计划内的变更并评审非计划变更的结果，必要时，采取措施以减轻任何不良影响。
  - 组织应确保外包过程被确定和受控。

8.运行
Operation

- 8.运行
  - **8.1 运行计划及控制**
  - 8.2 信息安全风险评估
  - 8.3 信息安全风险处置

- 8.2 信息安全风险评估
  - 组织应按计划的时间间隔或重大变更被提出或发生时执行信息安全风险评估，考虑6.1.2a) 中建立的准则。
  - 组织应保留信息安全风险评估结果的相关文档化信息。

8.运行
Operation

- 8.运行
  - 8.1 运行计划及控制
  - 8.2 信息安全风险评估
  - 8.3 信息安全风险处置

- 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档化信息。

6.1.3 C

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。本标准用户可使用附录A，以确保没有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。

9.绩效评价

Performance evaluation

- 9.绩效评价
  - **9.1 监视、测量、分析和评价**
  - 9.2 内部审计
  - 9.3 管理评审

- 9.1 监视、测量、分析和评价
  - 组织应评价信息安全绩效和ISMS的有效性。
  - 组织应确定：
  - a) 需要进行监视和测量的对象，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，当适用时，以**确保有效的结果**;
  - 注：选择的方法应产生可比较的和可再现的结果，该方法被考虑是有效的。
  - c) 监视和测量**什么时候**应被执行;
  - d) **谁**应**监视和测量**;
  - e) 监视和测量的结果**什么时候**应进行**分析和评价**;
  - f) **谁**应**分析和评价**这些结果。
  - 组织应**保留**适当的监视和测量**结果**的文档化信息作为证据。

9.绩效评价
Performance evaluation

- 9.绩效评价
  - **9.1 监视、测量、分析和评价**
  - 9.2 内部审计
  - 9.3 管理评审

- 9.2 内部审核
  - 组织应按计划的时间间隔进行内部审计来提供ISMS处于信息哪一种：
  - a) 符合
    - 1) 组织自身ISMS的要求;
    - 2) 本国际标准的要求;
  - b) 有效地实施和保持。
  - 组织应：
  - c) 计划、建立、实施和维护审计程序，包括频率、方法、职责、计划要求和报告。审计程序应考虑相关过程和以往审计结果的重要性;
  - d) 定义每次审核的准则和范围;
  - e) 选择审核员和审核组长以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层;
  - g) 保留审核程序和审核结果相关的文档化信息作为证据。

9.绩效评价
Performance evaluation

- 9.绩效评价
  - **9.1 监视、测量、分析和评价**
  - 9.2 内部审计
  - 9.3 管理评审

- 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) 以往管理评审行动的状态;
  - b) 与ISMS相关的内外部问题的变化;
  - c) 反馈信息安全绩效和趋势，包括：
    - 1) 不符合与纠正措施;
    - 2) 监视和测量结果;
    - 3) 审核结果;
    - 4) 信息安全目标的完成;

9.绩效评价
Performance evaluation

- 9.绩效评价
  - **9.1 监视、测量、分析和评价**
  - 9.2 内部审计
  - 9.3 管理评审

- 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：
  - 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档化信息作为证据。

10.改进
Improvement

- 10.改进
  - **10.1 不符合及纠正措施**
  - 10.2 持续改进

- 10.1 不符合及纠正措施
  - 出现不符合时，组织应：
  - a) 对不符合作出反应，如适用：
    - 1) 采取行动控制和纠正不符合;
    - 2) 处理结果;
  - b) 评价消除不符合原因采取行动的需要，为了不在发生或不在其他地方发生，通过：
    - 1) 评审不符合;
    - 2) 确定不符合的原因;
    - 3) 确定是否存在类似的不符合或发生的可能性;

10.改进
Improvement

- 10.改进
  - **10.1 不符合及纠正措施**
  - 10.2 持续改进

- 10.1 不符合及纠正措施
  - 出现不符合时，组织应：
  - c) 实施所需的任何行动;
  - d) 评审已采取纠正措施的有效性;
  - e) 如果有必要的话，改变ISMS。
  - 纠正措施应对不符合产生适当的影响。
  - 组织应保留以下文档化信息作为证据：
  - f) 不符合的性质和后续措施;
  - g) 任何纠正措施的结果。

10.改进
Improvement

- 10.改进
  - **10.1 不符合及纠正措施**
  - 10.2 持续改进

- 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。

Thank you

宽恕

信息安全管理先锋论坛

特别鸣谢

北宙咨询 North Universe

Trendsetting Consulting

艾拓咨询 AituoXianfeng Consulting

特别鸣谢

ITIL 先锋论坛