



ITIL Prince2
ITSM M_O_R 业务连续性
运维 CISA 工具
ITSS ISO27001 BCM
CISM 运维 Prince2 咨询 ITSS 运维
IS ISMS CHE 培训 BCM 培训 CISSP RISK IT
ZBBIX ISO27001 Nagios
CISP ISO22301
iTop

跟我学信息安全管理

ISO27001条文解析（附录A） 樊忠林

信息安全管理专家委员会发布
2016年5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

樊忠林

樊忠林老师在信息技术领域具有丰富的开发、运维经验，曾在众多项目的开发和实施过程中担任重要角色，并且拥有多年的授课经验。不但拥有知识理论的功底，又有实战与实践的经验，高度的责任感，积极进取，在教育培训中不断的与学员分享与实践，丰富的跨行工作经历练就了其独到的视野及敏锐的洞察力，其超前的观念与专业水平在教学中得到了众多从业人员及团队的好评。

典型项目经验：

卫材（中国）药业有限公司信息安全评估审计咨询项目

上海微创医疗器械（集团）有限公司ISO27001咨询项目

上海民航华东凯亚系统集成有限公司ISO27001咨询项目

中国电信股份有限公司云计算分公司ISO27001咨询项目

连连科技有限公司ISO27001咨询项目



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 樊忠林
- ☐ 附录A 2016年5月28日 师鑫



认证标准-要求附录条款



ISO27001信息安全管理层次



控制领域	控制目标	控制措施
A5	1	2
A6	2	7
A7	3	6
A8	3	10
A9	4	14
A10	1	2
A11	2	15
A12	7	14
A13	2	7
A14	3	13
A15	2	5
A16	1	7
A17	2	4
A18	2	8
14	35	114

某公司信息安全现状

- “我们已经投入了资金，购买了安全产品，在公司内部推行了防病毒软件，但是越做越没有方向感，安全问题仍然存在，公司内部病毒继续横行！”
- “我们已经制订了本部门的安全规定，但是公司没有方向性规定，我们在部门也不好强行推行。”
- “公司现有的安全规定太空泛、太多，没有参考的原则，没有明确的目标，员工日常行为无法落实。”
- “我们接触到公司的核心机密很多，但是不了解公司在这方面的具体要求和做的工作，也不知道该怎么做。”
- 安全策略就是指导一个组织如何安全运作的管理条例，它是对企业安全目标、理念、规范和责任的高度概括。安全策略应该随着时间持续改善，并且独立于特定的技术，同时应当用正式的规章制度保证既定策略的执行。所以，一个好的安全策略应当至少包含以下几点：
 - ✓ 信息安全的明确定义
 - ✓ 安全策略明确实现的目标
 - ✓ 明确信息安全所包含的各个方面的一般性和特殊性责任
 - ✓ 详细的安全策略应包括合法性需求；安全培训需求；病毒防范和检测策略；业务持续性计划等
 - ✓ 可疑的安全事件的通报流程

某公司信息安全现状（总结）

- 某公司有不完整的企业安全策略，基本由各部门根据自己业务性质制定（如法律部、IT部、人事），无明确的安全发展目标；
- 对于已有的安全策略，某公司无文档化的执行流程、实施步骤、监督和审计制度，无法在部门和普通员工间具体落实；
- 某公司没有年度计划性的安全资金预算，只有各部门根据业务需求分散的投入资金。

某集团公司信息安全现状

- “我的商务技术科长已经作出了限制，但是我们某公司的详细技术方案中午给运营商，下午就出现在竞争对手的讨论会上！这种事一而再，再而三得发生，究竟该谁负责？”
- “我们的技术人员和运营商交流时，不讲的详细些，怎么打动客户？我怎么知道有什么限制？”
- “某公司员工关于内部的核心详细技术分析报告，竟然出现在公开的媒体杂志上。该员工也不知道该报告是如何流出的。这种事我该向哪个部门反映？”
- “我的同学、朋友在竞争对手工作，他总是向我打听我们公司的内部消息，我到底哪些话可以讲，哪些话不可以讲？我该向哪个部门了解该方面公司的规定？”
- “我们的竞争对手对于员工泄密是抓一个杀一个，为什么我们的部门处理这么手软？”
- “业界评论，与同行业企业相比，某公司的商业机密比较容易获取。”
- 安全组织描述组织内的角色定义、应承担的责任和全面的信息安全通报结构。一个合理的管理架构应当在组织的信息安全执行中贯穿始终，包括在启动、监控以及强制执行等阶段。这个管理架构应当与公司的安全策略及其实践保持一致。

某集团公司信息安全现状（总结）

- 某公司没有专门的安全部门，法律部和IT部有部分安全职能，但这两个部门属于四级部门，其他部门认为只是服务性的部门，不是公司的核心部门。这两个部门没有足够的权利去部署、执行安全制度；
- 某公司无安全汇报机构，出现问题时多数人不知道该向哪个部门汇报。

A-5 安全方针

- ❖ A-5 安全方针

- A-5-1 信息安全管理方向

- ❖ A-5-1-1 信息安全方针

- 信息安全方针文件应由管理者批准、发布并传达给所有员工和外部相关方。

- ❖ A-5-1-2 信息安全方针评审

- 应按计划的时间间隔或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、充分性和有效性和全面性。

A-6 信息安全组织

❖ A-6 信息安全组织

- A-6-1 内部组织
- A-6-2 移动设备和远程办公

❖ A-6-1-1 信息安全的角色和职责

- 所有信息安全职责应被定义及分配。

❖ A-6-1-2 与监管机构的联系

- 应与监管机构保持适当的接触。

❖ A-6-1-3 与特殊利益团体的联系

- 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-6-1-4 项目管理中的信息安全

- 信息安全应融入项目管理中，与项目类型无关。

❖ A-6-1-5 职责分离

- 冲突的职责和权限应被分开，减少对资产未经授权或无意的修改与误用。

A-6 信息安全组织

- ❖ A-6 信息安全组织

- A-6-1 内部组织

- A-6-2 移动设备和远程办公

- ❖ A-6-2-1 移动设备策略

- 应使用配套策略和安全措施来防止移动设备带来的风险。

- ❖ A-6-2-2 远程办公

- 应使用配套策略和措施来保护信息访问，处理和远程储备。

某公司信息安全现状

- “在和运营商的交流、讲标中，会议后发现竞争对手利用酒店人员将录音设备安装在会议现场，造成技术机密和商业机密被对手掌握。员工事先没有意识检查会场。”
- “IT部门发现有人通过电子邮件将招投标和技术解决方案发给不明厂商。”
- “有员工发现同部门或其他部门出现安全事故的时候，靠感觉去决定处理流程。”
- “公司的临时工只有劳务协议，但是临时工同样可以接触到公司的部分核心机密。”

某公司信息安全现状（总结）

- 员工安全培训少，只有特定的职位有培训。员工没有普遍的安全意识，安全技能严重不足；
- 新员工需签保密协议。公司有职位和角色的定义，有违反规定处理。总的来说，公司有不完善的安全制度，但无细化到可执行的文件。没有处理流程，只根据突发事件处理；
- 职务说明书内没有明确岗位的安全职责，岗位的安全级别简单与行政级别挂钩。不利于员工的自觉遵守。

A-7 人力资源安全

❖ A-7 人力资源安全

- A-7-1 任用之前
- A-7-2 任用中
- A-7-3 任用的终止或变化

❖ A-7-1-1 筛选

- 根据相关法律、法规、道德规范，对员工、合同人员以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、访问信息的类别和已知风险。

❖ A-7-1-2 任用的条款和条件

- 作为合同义务的一部分，员工应同意并签订就业合同的条款和条件，应当载明其对组织信息安全的职责。

A-7 人力资源安全

❖ A-7 人力资源安全

- A-7-1 任用之前
- A-7-2 任用中
- A-7-3 任用的终止或变化

❖ A-7-2-1 管理职责

- 管理层应要求员工、合同方和第三方用户应用符合组织建立的安全策略和程序的安全。

❖ A-7-2-2 信息安全意识，教育和培训

- 组织内所有员工、相关合同人员以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和程序。

❖ A-7-2-3 纪律处理过程

- 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 人力资源安全

❖ A-7 人力资源安全

- A-7-1 任用之前
- A-7-2 任用中
- A-7-3 任用的终止或变化

❖ A-7-3-1 任用终止或变化的责任

- 任用终止或变更后依然有信息安全责任和义务的人，应该被界定和传达雇员或外部方执行。

某公司信息安全现状

- 某公司大部分员工对信息资产不甚了解，不知道何为信息资产；
- 某公司曾经要求部分信息分级，虽然分为绝密、保密、公司内部公开、公司外部公开，但标准不统一，致使分出来的级别不统一；
- 某公司纸面文档如合同、标书、研发文档、重大项目评审资料等有正式的保密标准，但中间文档及没有盖章的文档没有保密；
- 某公司电子文档访问授权分类太粗，但一旦授权，使用者对技术文件的处理几乎得不到控制，无法追踪；
- 某公司系统管理人员不需要授权、审批流程；
- 信息资产分类和控制说明信息资产的分类和控制应当包括信息所有权的确定、信息资产的分类，以及这些信息资产的安全控制。

某公司信息安全现状（总结）

- 某公司大多数员工不懂得什么是信息资产，公司也并没有标准的分级，员工无意泄露的信息就是公司的秘密资料，被竞争对手获得后会使公司流失机密技术资产、商务竞争中面临损失、竞争力下降。

A-8 资产管理

❖ A-8 资产管理

- A-8-1 对资产负责
- A-8-2 信息分类
- A-8-3 介质处理

❖ A-8-1-1 资产清单

- 应确定与信息 and 信息处理设施相关的资产，编制并维护资产清单。

❖ A-8-1-2 资产责任人

- 库存的资产应有人负责。

❖ A-8-1-3 资产的允许使用

- 与信息处理设施相关的信息和资产可接受使用规则应被确认、形成文件并加以实施。

❖ A-8-1-4 资产的归还

- 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 资产管理

❖ A-8 资产管理

- A-8-1 对资产负责
- A-8-2 信息分类
- A-8-3 介质处理

❖ A-8-2-1 信息的分类

- 信息应按照其对组织的价值，法律要求，敏感性和关键性分类。

❖ A-8-2-2 信息的标记

- 根据组织采用的信息分类方案，应制定并实施一套信息标记流程。

❖ A-8-2-3 资产的处理

- 根据组织采用的信息分类方法，应制定并实施一套资产处理流程。

A-8 资产管理

❖ A-8 资产管理

- A-8-1 对资产负责
- A-8-2 信息分类
- A-8-3 介质处理

❖ A-8-3-1 可移动介质的管理

- 根据组织采用的分类方法来执行可移动介质管理流程。

❖ A-8-3-2 介质的处理

- 不再需要的介质，应使用正式的规程可靠并安全的处置。

❖ A-8-3-3 物理介质传输

- 在传输过程中，包含信息的介质应加以保护，防止未经授权的访问，滥用或损坏。

某公司信息安全现状

- “公司IT系统有用户的注册登记、注销的流程。但不能及时掌握由于岗位变更等原因而造成的员工的权限没有更新，回收。缺少系统用户的定期审查的流程制度。”
- “公司各部门存在不按规定授权其他人访问系统的现象，高级权限使用者将密码告诉下属人员代办业务，下属人员看到公司内部其他机密的信息，如其他员工评议、奖金、薪资等。”
- “项目开发和产品设计的讨论组没有规范的访问控制，不相关的人可以随意进入，设计的思想概念时有流出。”
- “合同审批时，所有需要批准的人都可以接触到所有项目相关的文档。商业秘密很容易获得”。
- 计算机系统服务和数据的系统访问控制要基于业务系统的要求，正常的规则应该针对接入系统、网络服务、应用系统、系统数据等不同层次要求进行权限的分配，同时，为了检测未被授权用户和激活用户的活动，应该增加监控手段。

某公司信息安全现状（总结）

- 公司没有文档化的系统访问控制流程，造成系统访问控制较混乱。公司的经营、管理信息被泄漏到非授权的层面，并存在被竞争对手利用的风险。

A-9 访问控制

❖ A-9 访问控制

- A-9-1 访问控制的业务要求
- A-9-2 用户访问管理
- A-9-3 用户职责
- A-9-4 系统和应用程序的访问控制

❖ A-9-1-1 访问控制策略

- 应建立一个访问控制策略，并基于业务和访问的安全进行评审。

❖ A-9-1-2 网络服务的使用政策

- 应建立一个访问控制策略，并基于业务和访问的安全进行评审。

A-9 访问控制

❖ A-9 访问控制

- A-9-1 访问控制的业务要求
- A-9-2 用户访问管理
- A-9-3 用户职责
- A-9-4 系统和应用程序的访问控制

❖ A-9-2-1 用户注册和注销

- 应为所有系统和服务中所有用户类型的授权和撤销建立一套注册与注销的流程。

❖ A-9-2-2 用户访问权限开通

- 应有正式的用户访问开通程序，以分配和撤销对于所有信息系统及服务的访问。

❖ A-9-2-3 特权管理

- 应限制和控制特殊权限的分配以及使用

❖ A-9-2-4 用户秘密认证信息的管理

- 应使用正式的管理流程来控制秘密认证信息的分配。

❖ A-9-2-5 用户访问权的复查

- 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

- 当合同或协议终止后，应删除或调整所有工作人员和外部人员用户信息和信息处理设施的访问权限。

A-9 访问控制

❖ A-9 访问控制

- A-9-1 访问控制的业务要求
- A-9-2 用户访问管理
- **A-9-3 用户职责**
- A-9-4 系统和应用程序的访问控制

❖ A-9-3-1 秘密认证信息的使用

- 应要求用户按照组织安全实践来使用秘密认证信息。

A-9 访问控制

❖ A-9 访问控制

- A-9-1 访问控制的业务要求
- A-9-2 用户访问管理
- A-9-3 用户职责
- A-9-4 系统和应用程序的访问控制

❖ A-9-4-1 信息访问限制

- 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 安全登录程序

- 如果访问控制策略需要，应通过安全登录程序控制对操作系统的访问。

❖ A-9-4-3 口令管理系统

- 口令管理系统应采用交互式口令并确保口令质量。

❖ A-9-4-4 特权使用程序的使用

- 对可能超越系统和应用程序控制措施的实用工具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

- 对程序源代码的访问应被限制。

A-10 密码

- ❖ A-10 密码

- A-10-1-1 密码控制

- ❖ A-10-1-1 加密使用控制政策

- 应制定和实施信息保护密码控制策略。

- ❖ A-10-1-2 密钥管理

- 应制定和实施密钥的使用，保护，试用期策略并贯穿其整个生命周期。

某公司信息安全现状

- 全公司范围内没有物理安全的紧急安全事件流程并且对这些流程进行演练，仅在生产线上举行过消防疏散的演习，当在其他办公部门则不了解消防疏散流程，也没有进行过演习。尤其是公司高级管理层和重要职能部门所在的A座6楼，也没有应急演练；
- 公司没有总的部署物理环境的策略，只有部门根据自己的业务需求零散的部署。大楼B座生产部门只布置了4个监控系统，没有整合；大楼A座没有布置监控系统；
- 案例，发生安全事件，被盗窃了2部手提电脑，2块硬盘，和多个CPU，而且丢失的手提电脑和硬盘上有非常机密的数据，而且监视系统缺少了该段时间的监视录像；
- 公司的核心业务信息系统所在的主机房的安全问题尤为严重，从技术上来讲，主机房安全措施严重缺乏，如无监控手段、无专人监控，没有进出控制手段，机房环境恶劣，无架空地板、布线混乱、中央空调、防水、防火等完全不能满足服务器运行的基本要求。并且担当着全公司业务核心应用系统的服务器房没有隔离区，工程货物、备件等堆放在里面，给公司的安全运维造成隐患；
- 物理和环境安全措施用来禁止未授权访问、破坏和干扰IT服务。与关键和敏感的业务活动紧密联系的IT设施必须采取严密的安全措施，即采用适当的门禁控制手段和安全检查手段。设备应当物理保护起来以防止安全威胁和环境的破坏，信息及信息系统应当保护起来以防止未经授权的泄露、修改、偷盗。

某公司信息安全现状（总结）

- 公司没有对物理环境实行过系统的安全威胁评估；
- 公司的物理安全的检查流程存在问题；
- 规划时没有考虑到IT运行的特殊要求，只按照常规的办公区来规划。IT的投入不能满足某公司日益信息化的需求；
- 相比业界其他公司而言，公司运作的所面临的物理风险过高。

A-11 物理和环境安全

- ❖ A-11 物理和环境安全

- A-11-1 安全区域

- A-11-2 设备

- ❖ A-11-1-1 物理安全边界

- 应设置安全边界来保护包含敏感信息，危险信息和信息处理设施的安全。

- ❖ A-11-1-2 物理入口控制

- 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

- 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

- 应设计并采集物理安全措施来防范自然灾害，恶意攻击或事故。

- ❖ A-11-1-5 在安全区域工作

- 应设计和应用用于安全区域工作的物理保护措施和指南。

- ❖ A-11-1-6 交付和交界区

- 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 物理和环境安全

- ❖ A-11 物理和环境安全

- A-11-1 安全区域

- A-11-2 设备

- ❖ A-11-2-1 设备的安置和保护

- 应妥善安置以及保护设备，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 支持性设备

- 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

- 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-11-2-4 设备维护

- 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-11-2-5 资产的移动

- 设备、信息或软件在授权之前不应带出组织。

- ❖ A-11-2-6 场外设备和资产安全

- 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 物理和环境安全

- ❖ A-11 物理和环境安全

- A-11-1 安全区域

- A-11-2 设备

- ❖ A-11-2-7 设备的安全处置或再利用

- 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覆盖。

- ❖ A-11-2-8 无人值守的用户设备

- 用户应确保无人值守的用户设备有适当的保护。

- ❖ A-11-2-9 清楚桌面和清屏策略

- 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。

Thank you

信息安全管理先锋论坛

樊忠林

特别鸣谢



特别鸣谢

