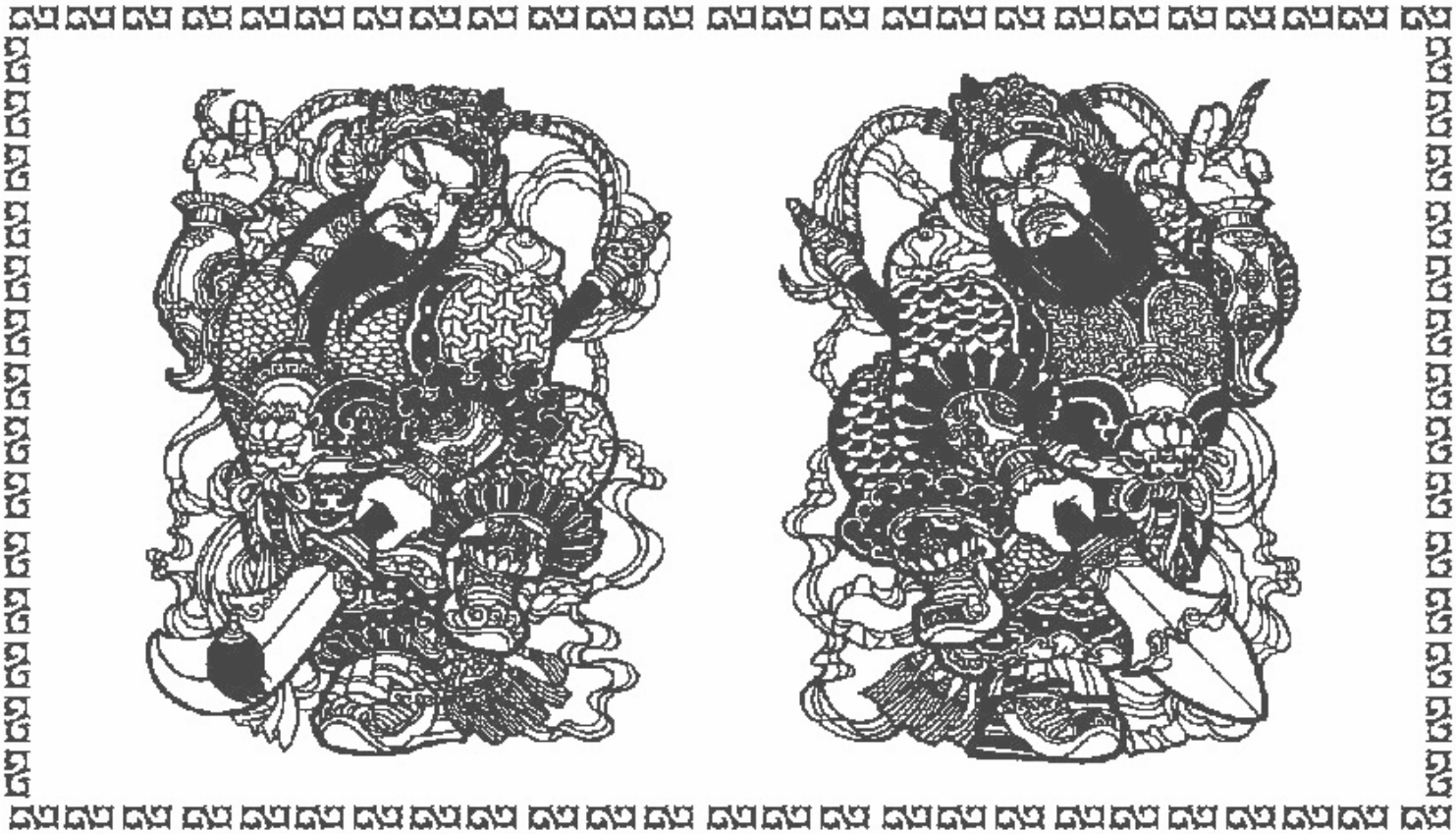


Chinadoors

ISO 27002:2007

深度解析之五

物理环境安全管理

提纲

- 第一部分 标准要求分析
- 第二部分 理解心得
- 第三部分 响应设计思路

第一部分 标准要求分析

安全控制目标和控制措施

- 27002在“物理和环境安全”管理类中，提供了**2个**控制目标和**13项**控制措施
  - → **安全区域**（目标1）
  - → **设备安全**（目标2）

9.1 安全区域

Secure Areas

9.1控制目标及措施——安全区域

Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference.

The protection provided should be commensurate with the identified risks.

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。

关键或敏感的信息处理设施要放置在安全区域内，并受到确定的安全边界的保护，包括适当的安全屏障和入口控制。这些设施要在物理上避免未授权访问、损坏和干扰。

所提供的保护要与所识别的风险相匹配。

9.1控制目标及措施——安全区域

控制目标	安全区域 防止对组织场所和信息的未授权物理访问、损坏和干扰
控制措施	物理安全边界 应使用安全边界（诸如墙、卡控制的入口或有人管理的接待台等屏障）来保护包含信息和信息处理设施的区域
	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
	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
	外部和环境威胁的安全防护 为防止火灾、洪水、地震、爆炸、社会动荡和其他形式的自然或人为灾难引起的破坏，应设计和采取物理保护措施
	在安全区域工作 应设计和运用用于安全区域工作的物理保护和指南
	公共访问、交接区安全 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，要与信息处理设施隔离，以避免未授权访问

控制措施分析

- 9.1.1 – –9.1.4说的是一些物理环境的控制要求，感觉没什么可说的，在制定响应的制度是参考即可
- 9.1.5要求对在安全区内活动和工作提供规范指南
- 9.1.6提出了关于“交接区”的设定和管理

9.2 设备安全

Equipment Security

9.2控制目标及措施——设备安全

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

Equipment should be protected from physical and environmental threats.

Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

目标：确保正确、安全的操作信息处理设施。

应建立所有信息处理设施的管理和操作职责和程序。这包括制定合适的操作程序。

当合适时，应实施责任分割，以减少疏忽或故意误用系统的风险。

9.2控制目标及措施——设备安全

控制目标	**设备安全** 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
控制措施	**设备安置和保护** 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
	支持性设施 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
	布缆安全 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
	设备维护 设备应予以正确地维护，以确保其持续的可用性和完整性
	组织场所外的设备安全 应对组织场所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
	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检查，以确保在销毁之前，任何敏感信息和注册软件已被删除或安全重写
	资产的移动 设备、信息或软件在授权之前不应带出组织场所

控制措施分析

- 9.2.1 “设备安置和保护”
  - → 建立设备安置标准，约束具体的活动

控制措施分析

- 9.2.2“支持性设施”
  - → 支持性设施包括了供电、供水、供热/通风/空调、通信等类型
  - → 部分支持性设施故障，直接会导致服务中断（如供电或通信中断），另外一部分支持性设施故障，则可能影响其它控制机制的有效性（如断水会导致消防设施受损）
  - → 应当建立相关的策略和设计实施标准，约束实施建设活动
  - → 建立规范和指南，指导检查和维护活动
  - → 保留管理过程证据

控制措施分析

- 9.2.3 “布缆安全”
  - → 线缆包括供电线缆和通信线缆
  - → 应当建立相关的策略和设计实施标准，约束规范具体的实施活动
  - → 要求保留遵循标准进行实施的过程证据

控制措施分析

- 9.2.4 “设备维护”
  - → 应当建立设备维护的管理制度
  - → 为约束和规范维护管理活动，可要求设备厂商提供维护指南或手册，从而实现操作层面的落实（信息处理设施的规模和复杂度不同，这部分具体的内容将有很大的差异）
  - → 产生和保留维护过程记录

控制措施分析

- 9.2.5 “组织场所外的设备安全”
  - → 这部分是关于设备在组织场所外使用的安全要求
  - → 可建立相关的使用规范和指南

控制措施分析

- 9.2.6“设备安全处置与重用”
  - → 这部分是跟介质管理相关的内容，要求建立介质处置的制度和规程，防止处置不当造成信息泄密
  - → 与处置相关的活动，也应当保留过程记录，以保证对于管理活动的可追溯性

控制措施分析

- 9.2.7“资产的移动”
  - → 要求对资产移动建立授权和记录机制，使得包含敏感信息的信息资产被带出的活动得到控制和记录
  - → 其实这部分与“资产管理”是相关联的，可以在资产管理制度中阐明相关要求
  - → 需要保留相关活动的申请、批准、带出、返还、检查等过程记录

第二部分 理解心得

物理安全的范畴

- 物理安全是一个技术出身的人通常不会太关注的范畴，认为这跟通常理解的信息安全技术之类的有较大的区别
- 按照一种思路，就能比较好理解物理安全的重要性
  - → 信息安全其核心是信息的安全
  - → 信息的安全，很大一部分要依赖于信息处理设施的安全
  - → 信息处理设施，有其物理环境，因此要依赖于物理安全控制
- CISSP AIO 对物理安全有专门的章节进行内容阐述，当时死记硬背各种火灾类型和灭火剂类型依然记忆犹新，说句实话还从来没有接触过
- 物理安全重点关注3部分，1环境、2设备、3介质，在27002中的“物理环境和设备安全”类中，没有涉及介质安全的讨论，而是把环境安全和设备安全列为重点

物理安全实践与2700x标准

- 去过不少银行的数据中心机房，直观感觉管理水平差异很大，有建设和运维都非常规范的，也有感觉就是一团乱的
- 看2700x的要求，认为如果顺着这样一个思路来理解和借鉴标准的内容，会比较容易一些
  - → 首先要设身处地从某个安全管理方向的场景出发，设想如果是自己要负责这方面管理工作，应该考虑到哪些方面，然后是顺着什么次序来逐步实践
  - → 然后，再借鉴2700x的要求，将其作为一个参考武器，来指导管理实践活动
  - → 切忌认为2700x这个标准就是一个安全管理的百科全书了，其实它只是一个武器，也切忌仅仅完全参照27002去安排实践，因为这个标准只是罗列，没有思路指导，27001提供了一些粗线条的实施思路指导，但不够细致

准确理解物理安全管理

- 物理安全管理，我说它本质上是一种人类智力的实践活动，因此它必须是一个管理的过程
- 但是，这个管理过程中，不可能仅仅依靠管理措施就能够达到管理目标，这跟“安全方针”、“人力资源安全”等管理类不太一样，那些管理过程主要依赖于管理措施（策略、标准、规范、流程）就能基本实现，而“物理安全管理”除了管理措施之外，还必须借助一些落实的技术措施进行辅助，例如：
  - → 环境安全中要求防火，就要有检测探头，就要有灭火系统
  - → 环境安全中要求物理访问控制，就要有门禁系统
- 因此，物理安全管理，在实际实践中，其内容范畴必然比27002里面提供的这些措施要更多，27002提供的是一些管理措施，但是不包括技术措施的内容

物理安全管理的实践思路

- 首先一个非常基本的原则是，**有多大风险提供多大保障**，控制措施的强度和投入成本，必须与信息的重要性相对应。按照这个原则，那么应当对信息和信息处理设施的分布情况进行调查，重点区域重点保护，体现出保障控制的级别差异来
- 接下来要分析一下风险，物理安全管理面对的主要风险是人为风险和环境风险，例如暴力闯入破坏、非授权访问、或者火灾、断电等事件
- 27002的中提供的第1个管理目标提出了很重要的一个原则：“**关键或敏感的信息处理设施要放置在安全区域内，并受到确定的安全边界的保护**”，比较理想情况是一个集中的数据中心机房，另外若干分布式受控的安全区域也是可以的，一种比较典型的情况是公司大办公环境和数据中心机房两级区域结构

物理安全管理的实践思路

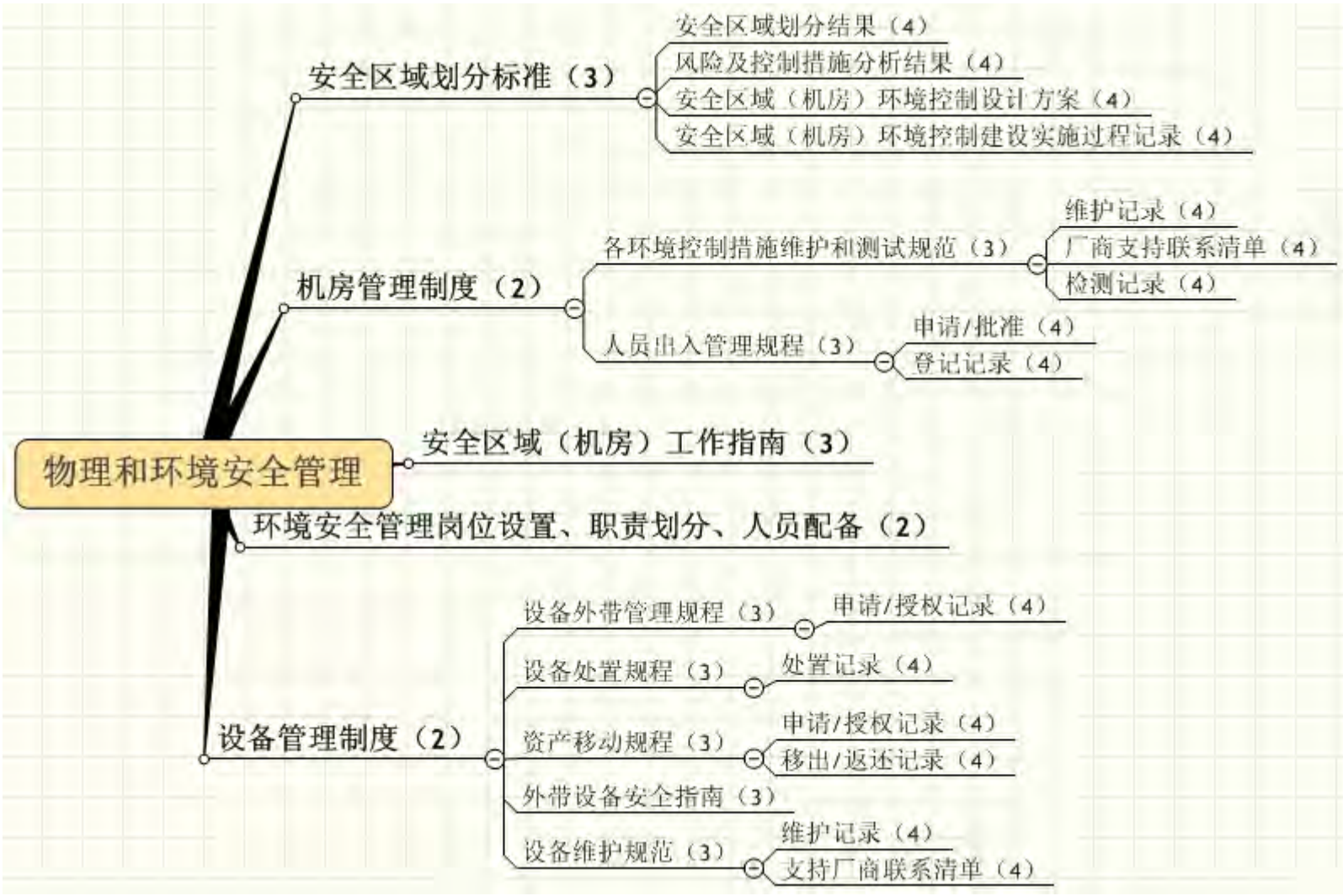
- 各个安全区域的边界需要明确，不能有明显的缺口，这方面不难理解，27002的章节9.1.1就是针对这部分内容阐述的
- 各区域的入口，要设置相应的访问控制手段，例如门禁系统，或者有专人值守，27002的章节9.1.2阐述相关内容，其提供的参考内容，可以在物理安全策略，或机房管理制度中有所体现
- 安全区域的环境控制，27002提供了参考内容，要全面考虑的话，可以参考等级保护的物理安全（技术）内容，那里有更多具体的要求，例如防火、防水、防雷击、防静电、防尘、温湿度控制等
- 参照建设标准，进行环境安全建设

物理安全管理的实践思路

- 建立环境安全措施的维护规范，并保留维护过程记录
- 在安全区域内部活动和工作，需要有管理上的指南，规定能做什么，不能做什么，以约束合法授权人员的行为
- 建立与设备安全管理相关的制度、规范、规程，并要求保留过程记录
- 明确物理安全管理维护的职责，定义岗位职责和人员配备，并形成文件
- 对相关岗位人员提供培训

第三部分 响应设计思路

响应设计


物理和环境安全管理
安全区域划分标准（3）
安全区域划分结果（4）
风险及控制措施分析结果（4）
安全区域（机房）环境控制设计方案（4）
安全区域（机房）环境控制建设实施过程记录（4）
机房管理制度（2）
各环境控制措施维护和测试规范（3）
维护记录（4）
厂商支持联系清单（4）
检测记录（4）
人员出入管理规程（3）
申请/批准（4）
登记记录（4）
安全区域（机房）工作指南（3）
环境安全管理岗位设置、职责划分、人员配备（2）
设备管理制度（2）
设备外带管理规程（3）
申请/授权记录（4）
设备处置规程（3）
处置记录（4）
资产移动规程（3）
申请/授权记录（4）
移出/返还记录（4）
外带设备安全指南（3）
设备维护规范（3）
维护记录（4）
支持厂商联系清单（4）

THE END

THANKS

Chinadoors