#第一章 通过原则和策略的安全治理

1.1 理解和应用机密性、完整性和可用性的

安全的主要目标，CIA三元组 机密性、完整性和可用性，每条原则的重要性主要取决于组织的安全目标以及安全性所受到的威胁程度

1.1.1 机密性

- 机密性：限制未授权主体不能访问数据、客体或资源提供了高级别保证
- 针对机密性的攻击：捕捉网络通信、窃取密码文件、社会工程学、端口扫描、肩窥、偷听、嗅探攻击，人为错误
- 有助于机密性的对策： 加密、网络流量填充、严格的访问控制、严格的认证程序、数据分类和广泛的人员培训
- 机密性和完整性相互依赖

1.1.2 完整性

- 完整性：客体必须保持自身的正确性，并且只能由被授权的主体进行有意修改
- 针对完整性的破坏： 病毒、逻辑炸弹、未授权访问、编码和应用程序的错误、恶意修改、有企图的替换以及系统后门，人为错误
- 保护完整性的措施：严格的访问控制、严密的身份认证、入侵检测系统、加密、散列总和认证、接口限制、输入/功能检测以及广泛的人员培训
- 完整性依赖机密性，缺乏机密性，完整性无法维护

1.1.3 可用性

- 可用性：经过授权的主体被及时准许和不间断的访问客体
- 针对可用性的威胁：设备故障、软件错误、环境问题、DOS攻击、客体损坏和通信中断
- 可用性依赖完整性和机密性，缺乏完整性和机密性无法维护可用性

1.1.4 其他安全概念

1. 身份标识
    - 主体表明身份，并开启可问责性
    - 身份认证：认证或测试所声明身份合法性的过程就是身份认证，身份认证要求主体的附加信息必须完全对应于被表明的身份
2. 授权
    - 确保请求的活动或客体访问，可以获得通过身份认证和指派的权利和特权，对授权的定力使用了访问控制模型中的概念，如DAC,MAC或RBAC

3. 审计
    - 审计是对系统中未授权的或异常的活动进行检测的过程，日志为重建事件、入侵和系统故障的历史提供了审计跟踪，通过审计为起诉提供证据、生成问题报告和分析报告
    - 审计通常为操作系统和大多数应用程序和服务的内在特性，因此配置系统功能来记录特定类型时间的相关信息非常简单
4. 可问责性
    - 只有支持可问责性，才能正确实施组织的安全策略
    - 为 了获得切实可行的可问责性，在法律上你必须能够支持自己的安全性
5. 不可否认性
    - 不可否认性确保活动或事件的主体无法否认所发生的事情
    - 身份标识、身份认证、授权、可问责性和审计使不可否认性称为可能，使用数字证书、会话标识符、事务日志以及其他很多传输和访问控制机制，建立不可否认性

1.1.5 保护机制

许多控制通过使用保护机制对机密性、完整性和可用性保护

- 分层
    - 简单的使用连续的多重控制，也被称为深度防御，连续分层使用串行分层法
    - 分层还包括网络由多个独立实体组成的概念，所有构成的单个安全防线的网络系统之间存在协同作用，共筑安全防线
- 抽象
    - 为提高效率而使用的，将相似的元素放入组、类别或角色中，在为客体分类或主体分配角色时，就使用到抽象的概念
    - 抽象能够为安类型或功能分类的客体组分配安全控制方法，并抽象简化安全措施
- 数据隐藏：
    - 将数据置于主体不可访问或无法看到的存储空间，从而防止主体发现或访问数据
    - 不让未授权的访问者访问数据库是隐藏，限制分类级别较低的主体访问级别较高的数据是隐藏，组织应用程序直接访问硬件还是数据隐藏

1.2 应用安全治理原则

- 安全治理是实践行为的集合，这些实践都支持、定义和指导组织的安全工作相关
- 安全治理的共同目标就是维护业务流程，同时努力实现增长和弹性
- 安全治理也有合规性上的需求，是实施安全的解决方案和管理方法，安全是整个组织同时进行管理和控制的，而不只是在IT部门

1.2.1 安全功能战略、目标、任务和愿景的一致

- 安全管理计划能确保安全策略的适当创建、实现和实施

- 安全策略编制的最好方法是自上而下，高层或管理部门负责启动和定义组织的安全策略，安全策略为组织中较低级别的人员指出防线，中层管理部门的职责是在安全策略的指导下制定标准、基准、指导方针和程序，操作管理者和安全专家负责实现安全管理文档中规定的配置要求，用户遵守组织制定的安全策略
- 安全管理计划编制包括：定义安全角色；规定如何管理安全性、谁负责安全性 以及如何测试安全性的效益；开发安全策略；执行风险风险；对员工进行安全教育 安全管理计划团队开发的三种计划
- 战略计划： 相当稳定的长期计划，定义组织的目标，长期的目标和愿景在战略计划中被讨论，还包括风险评估
- 战术计划：中期计划，用于提供实现战略计划所提出目标的详细细节，包括项目计划、采购计划、雇佣计划、预算计划、维护计划、支持计划以及系统开发计划
- 操作计划：基于战略计划和战术计划制定的非常周详的计划，清楚说明了如何完成组织机构的各种目标，包括：培训计划、系统部署计划和产品设计计划

1.2.2 组织流程

- 安全治理需要照顾到组织的方方面面，包括收购、剥离和治理委员会等组织流程 变更控制/变更管理
- 安全环境的改变可能引入导致心脆弱性出现的漏洞、重叠、客体丢失和疏漏，面对变更，维持安全性的唯一方法就是系统的管理变更
- 变更管理的目的就是确保任何变更都不能降低或危机安全性，还负责能够将任何变更都回滚到先前的安全状态
- 并行变更是变更管理过程的示例，旧系统和新系统并行运行，确保新系统支持老系统所支持和提供的所有必须的业务功能性 数据分类
- 分类的主要目的： 根据重要性和敏感性给数据分配标签，对数据安全保护过程进行规范化和层次化
- 政府/军方分类： 绝密、秘密、机密、敏感但非机密、非机密
- 商业/私营部门的分类： 机密、隐私、敏感、公开

1.2.3 安全角色和责任

- 高级管理者：最终负责组织机构安全维护和最关心保护资产的人，高层管理者对安全解决方案的总体成败负有责任，并且对组织机构建立安全性予以适度关注并尽职尽责
- 安全专家：职责是保护安全性，包括制定和实现安全策略，安全专家不是决策制定者，只是实现者，决策都必须又高层管理制定
- 数据所有者： 分配给再安全解决方案中为了防止和保护信息而负责对信息进行分类的人，
- 数据管理员：负责实施安全策略和上层管理者规定的保护任务的用户，这些措施包括：完成和测试数据备份，确认数据的完整性，部署安全解决方案以及根据分类管理数据存储
- 用户：分配给具有安全系统访问权限的任何人

- 审计人员：负责测试和认证安全策略是否被正确实现以及衍生出来的安全解决方案是否合适，完成遵守情况报告和有效性报告，高层管理者审查这些报告

1.2.4 控制架构

- 安全指定计划必须从规划计划开始，然后规划标准和合规，最后进行实际的计划开发和设计
- 信息及相关控制目标（COBIT），记录了一整套优秀的IT安全实践

1.2.5 应尽关注和应尽职责

- 应尽关注：通过合理的关注保护组织利益，开发规范化的安全结构
- 应尽职责：不断实践维护应尽关注成果的活动，将安全结构应用到机构的IT基础设施中
- 高管必须做到应尽关注和应尽职责才能在出现损失时减少他们的过过失和职责

1.3 开发和文档化安全策略、标准、指导方针和程序

维护安全性是业务发展的重要组成部分

1.3.1 安全策略

- 规范化的最高层次就是安全策略，许多组织都采用多种类型的安全策略来定义或概括他们整体的安全策略
- 规章式的策略：用于让人们遵守规章制度的安全措施
- 建议式策略：讨论可接受的行为和活动，并且定义违背安全性的后果，这种策略解释了高层管理部门对组织内部安全和遵守规定的期望
- 信息式的安全策略：设计用于提供特定主体的相关信息或知识

1.3.2 安全标准、基准及指南

- 标准为硬件、软件、技术和安全控制方法的统一使用定义了强制性要求，标准是战术文档，定义达到安全策略指定的目标和总体方向的步骤和方法