访问控制实践

* 拒绝未定义的用户或匿名帐户访问系统。
* 限制和监控管理员和其他强大帐户的使用。
* 在登录尝试失败达到一定次数后暂停或延迟访问功能 在
* 用户离开公司后立即删除过时的用户
* 帐户 在 30 到 60 天后暂停非活动帐户。
* 执行严格的访问标准。
* 执行需要知道和最少特权的做法。 （最小特权：给予员工足够的权利和特权来执行他们应该做的事情，仅此而已）
* 禁用不需要的系统功能、服务和端口。
* 替换帐户的默认密码设置。
* 限制和监控全局访问规则。
* 从帐户和组成员资格中删除冗余资源规则。
* 从资源访问列表中删除多余的用户 ID、帐户和基于角色的帐户。
* 强制密码轮换。
* 执行密码要求（长度、内容、寿命、分发、存储和传输）。
* 审核系统和用户事件和操作，并定期审查报告。
* 保护审计日志。

安全控制

* 预防、检测、纠正或最小化安全风险的保障措施。
* 数据安全措施集

定义

安全控制是一组推荐的网络防御措施，它提供了具体且可行的方法来阻止当今最普遍和最危险的攻击。

优点

* 控制的一个主要优点是它们可以优先考虑并关注较少数量的具有高回报结果的行动。
* 这些控制措施之所以有效，是因为它们源自主要威胁报告中突出显示的最常见攻击模式，并在非常广泛的政府和行业从业者社区中进行了审查。

它是做什么用的？

* 它们的创建是 为了回答“我们需要做什么才能阻止已知攻击”这个问题。
* 持续价值的关键在于，控件会根据从 Verizon 到 Symantec 的组织识别和分析的新攻击进行更新，因此控件可以阻止或减轻这些攻击。

**安全控制有两种分类方式：**

1. 按控制性质分类

* Administrative Controls
* Logical Controls
* controls

按控制过程的不同阶段

* 2.
* Physical
* Technical
* Controls
* /

分类控制的

1. **行政控制**

这些包括政策、标准、程序和指南的制定和发布；风险管理;人员筛选；进行安全意识培训；实施变更控制程序。

定义

* 管理控制是指根据组织的安全目标定义人员或业务实践的政策、程序或指南。
* 行政控制是制定并确保遵守政策和程序的过程。
* 它们往往是员工可以做、必须始终做或不能做的事情。

行政控制类别：

* 政策
* 标准
* 程序
* 指南

示例：

* 政策（例如业务连续性计划、访问控制政策、灾难恢复计划）
* 程序
* 人员控制（定义：人员控制表明公司的优势和劣势。其目的是有效地利用所有员工在组织内实现最大利益的潜力。）
* 监督结构（定义：管理委员会，其中非管理人员是成员，对管理决策的某些方面具有监督权。）
* 测试（例如漏洞扫描，渗透测试、安全审计/审查、风险评估、安全扫描）

1. **技术控制（又名逻辑控制）**

这些包括实施和维护访问控制机制、密码和资源管理、识别和身份验证方法、安全设备以及基础设施的配置.

定义：

技术控制是硬件保护系统免受网络攻击的重新和软件组件。防火墙、入侵检测系统 (IDS)、加密以及识别和验证机制都是技术控制的示例。

可参考：

* 识别和认证方法
* 安全设备
* 基础设施配置

示例：

预防性

* 加密
* 智能卡
* 网络认证
* 访问控制列表 (ACL)
* 文件完整性审计 软件
* 修补
* IPS

侦探

* 安全日志
* NIDS
* HIDS

纠正/恢复

* IPS
* 从备份中恢复
* 修补

1. **物理控制**

视情况对组织的物理安全对策会有所不同。国防部等政府机构可能在大楼门口配备武装警卫。许多组织不处于破坏国家安全的位置，因此武装警卫不是必需的。在许多情况下，接待员会迎接任何新来访者，并为现场访问做出适当的安排。

定义：

这些包括控制个人进入设施和不同部门、锁定系统并移除不必要的软盘或 CD-ROM 驱动器、保护设施周边、监视入侵和环境控制。

示例：

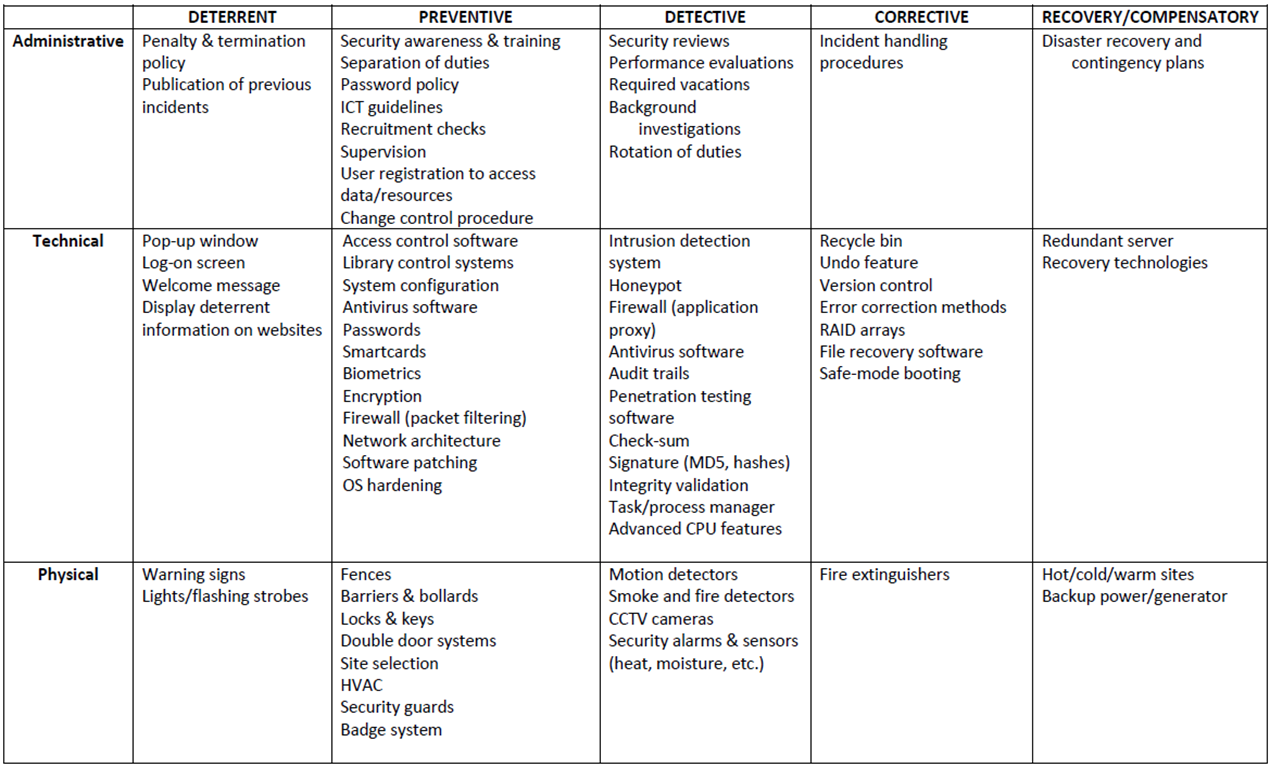
* 自动屏障和护柱
* 楼宇管理系统，如供暖、HVAC、升降机/电梯控制等
* CCTV- 闭路电视
* 电子物品监控 - EAS
* 火灾探测
* GIS 制图系统
* 对讲机和 IP 电话
* 照明控制系统
* 周界入侵检测系统
* 基于雷达的检测& 周边监控雷达
* 安全警报
* 视频墙
* 电力监控系统
* 笔记本电脑锁

根据控制过程的不同阶段进行分类

* 威慑：控制首先阻止攻击，阻止人们破坏安全，例如警告、横幅、登录消息、假闭路电视摄像头警告人们，网站上的安全措施告诉人们他们受到保护
* 预防性：使攻击难以成功的控制，例如防火墙（阻止不受欢迎的流量）、加密、锁门
* 侦探性：检测是否发生攻击的控制，例如校验和、入侵检测系统、职责轮换、安全审计、监视器和 se nsors，安装在建筑物中以检测入侵者的运动传感器，闭路电视摄像机，有时会告知系统何时受到攻击的防火墙，通过网络监视主机和计算机上的活动的入侵检测系统
* 纠正：安全的纠正方面，逆转损害的控制，例如版本控制，事件处理程序，灭火器，撤消，回收站，DOS 攻击（禁止 IP 地址以阻止服务器堵塞），灭火器（发生火灾时扑灭），事件处理程序（告诉员工发生事件时该怎么做）
* 恢复：在地震或海啸等重大灾难后使系统恢复正常的控制措施，例如灾难恢复计划、热/冷/暖站点、备用电源，

一般示例：

超速（有罚款和处罚，以及减速带、检测 – 安全摄像头等预防性控制）



根据控制过程的不同阶段进行分类

1. **阻止租金：** 首先阻止攻击的控制，阻止人们破坏安全，例如警告、横幅、登录消息、假闭路电视摄像机警告人们，网站上的安全措施告诉人们他们受到保护
2. **预防：** 控制使它变得困难使攻击成功，例如防火墙（阻止不受欢迎的流量）、加密、锁门
3. **侦探：** 检测是否发生攻击的控制，例如校验和、入侵检测系统、职责轮换、安全审计、监视器和传感器、安装在系统中的运动传感器检测入侵者的建筑物、闭路电视摄像机、有时会告知系统何时受到攻击的防火墙、监控网络上主机和计算机活动的入侵检测系统
4. **纠正：** 安全的纠正方面，逆转损害的控制，例如版本控制、事件处理程序、灭火器、撤消、回收站、DOS 攻击（禁止 IP 地址以阻止服务器堵塞s)、灭火器（发生火灾时将其扑灭）、事件处理程序（告诉员工发生事件时该怎么做）
5. **恢复：** 在地震或海啸等重大灾难后使系统恢复正常的控制措施，例如灾难恢复计划, 热/冷/暖站点, 备用电源

的

**,** 现实

**生活** *中* 例子或广告如何防止火灾发生， *预防性* - 确保没有无人看管的开放式炉灶，不使用时关闭电源插座， *侦探* - 烟雾探测器，家里的闭路电视， *纠正 -* 灭火器， *恢复 -* 保险和基金未雨绸缪

**常用的安全方法**

为了满足 AIC 三元组的关键要求，可以采用多种常用的安全方法：

* 最小特权
* 防御深度
* 最小化
* 保持简单
* 分区
* 使用阻塞点
* 安全地/安全地失败
* 利用不可预测
* 性 职责分离

**最小特权**

**规定：** 不要提供超过要求的特权。这适用于用户和应用程序。

* 示例：来宾帐户没有管理权限，身份不明的应用程序不应有权更改系统文件等。）
* 此原则不仅适用于计算机系统上的用户和应用程序的权限，还适用于其他非信息系统权限一个组织的工作人员。
* 最小特权原则是一种预防性控制，因为它减少了可能被滥用的特权数量，从而限制了潜在的损害。
* 应用此原则的一些示例包括：
* 如果用户需要共享文件，则只授予他们读取访问权限，并确保禁用写访问权限
* 不允许服务台人员创建或删除用户帐户（如果他们可能不得不这样做）要做的是重置密码
* 不允许软件开发人员将软件从开发服务器移动到生产服务器
* 特权：访问数据以运行进程和应用程序的能力
* 产品：通过向不可信的用户提供更少的特权来保持系统更稳定

**深度防御** （多种类型不同层次的安全控制）

* 纵深防御的原则是拥有不止一层或不止一层的防御。
* 这一原则背后的原因是任何一层或类型的防御都可能被攻破，无论你认为它多么强大和可靠，但两层或更多层更难攻破。
* 当您结合两种或多种不同类型的防御机制时，纵深防御最有效——
* 例如在 Internet 和您的 LAN 之间使用防火墙，加上 IP 安全架构 (IPSEC) 来加密 LAN 上的所有敏感流量。在这种情况下，即使您的防火墙受到威胁，攻击者仍然必须破坏 IP 安全才能获取您在 LAN 中流动的数据。

例如。

第一层 - 威慑控制（易于实施，用它来警告黑客不要攻击，违反政策可能不合法）

第二层 - 预防控制（防火墙安装在服务器上，监控所有流量 gg btw 互联网和内部网络并拦截任何可疑活动）

第 3 层 - 侦探层（网络监控工具，如入侵检测系统，会提醒人们注意系统上发生的任何攻击）

第 4 层 - 纠正层（安装的软件，如防病毒软件，可以清除计算机上的病毒被感染）

第五层——恢复层（数据备份，系统崩溃时恢复系统软件的另一个映像）

一般来说，不同类型的控制应该一起使用：

* 首先，预防控制应该到位，尝试和杜绝安全事故的发生；
* 其次，侦探控制是必要的，这样你就可以知道预防控制是有效还是失败；
* 第三，需要纠正控制来帮助您有效地应对安全事件并遏制损害。
* 然而，纵深防御原则并不意味着您应该不分青红皂白地应用所有您可以掌握的控制和安全措施： 必须在纵深防御方法提供的安全与财务、人力和组织方面的安全性之间找到平衡点您愿意为之花费的资源。 这种平衡通过 成本效益分析解决。

**最小化**

*声明：*  系统不应运行任何非严格要求完成其分配任务

* 的应用程序最小化原则是最小权限原则的近亲，主要适用于系统配置。
* 例如，一台其唯一功能是用作电子邮件服务器的计算机应该只安装和启用电子邮件服务器软件。应禁用或根本不安装所有其他服务和协议，以消除任何危害或滥用的可能性。
* 优点：坚持最小化原则不仅可以增加安全性，而且通常还可以提高性能，节省存储空间，通常是一种良好的系统管理实践。

**保持简单**

安全系统应该保持简单，因为引入的任何复杂性都会导致整个系统的不安全

* 性复杂性是安全性的最大敌人。复杂系统本质上更不安全，因为它们难以设计、实施、测试和保护。
* 系统越复杂，我们就越不能保证它会按预期运行。
* 尽管信息系统和流程的复杂性必然会随着我们对功能的期望越来越高而增加，但我们应该非常小心地在可避免的复杂性和不可避免的复杂性之间划清界线，不要为了花里胡哨的功能而牺牲安全性，以免事后后悔。
* 当您必须在功能多的复杂系统和功能少但足够的简单系统之间做出选择时，请选择简单的系统。