《信息安全评估》知识点串讲

一、安全评估基础与标准

1、评估概念：广义和狭义的分类，狭义指信息安全风险评估。
2、评估意义：提高安全针对性，降低了成本，提供适度安全。
3、评估工具：包括系统、平台、分析等工具，但不包括经验工具和物理环境工具。
4、**TCSEC** 标准
（1）针对**计算机系统**安全进行评估。
（2）分成了 ABCD **四个级别**和 7 个小类（级别）。
（3）从 **B1 级**开始**强制保护**和使用**安全标签**。
5、**ITSEC** 标准
（1）针对所有的 **IT 产品**或**系统**进行评估。
（2）首次提出了**保密性、完整性、可用性**。
（3）提出了**安全功能**和**功能评估（保证）**两大部分。
（4）分为 10 类安全功能和 6 级的安全强度。
6、FC 标准：首次提出了 **PP** 的概念（标准化的需求）。
7、CC 标准
（1）CC 继承了 PP、功能和保证分离等优势。发展为 ISO/IEC **15408**，GB/T **18336** 等同采用了 ISO/IEC **15408**。
（2）CC 通用性：体系架构、使用者（研发、评估、用户）、全球通用、所有 IT 产品。
（3）CC 标准包括：**简介和一般模型**、安全**功能要求**、安全**保证要求**。
（4）CC 标准构成：类-子类-组件-元素所构成的。
（5）CC 标准概念：评估对象-**TOE**、保护轮廓-**PP**、安全目标-**ST**、**EAL（EAL1-EAL7）**

二、信息安全风险评估

1. 风险**要素**：
（1）**资产**：业务、安全、分类等有关。有形和无形、物理和逻辑、静态和动态、硬件和软件等分类。
（2）**威胁**：安全风险**外部**原因，因素包括来源、动机、方式、对象、频率和程度。
（3）**脆弱性**：安全风险**内部**原因，技术和管理脆弱性，主体、分布、程度。
（4）**安全措施**：防护、检测、纠正、威慑措施。
（5）补充：**残余风险**，需要进行持续跟踪和监视。
2. 风险评估方法
（1）途径：**基线**评估、**详细**评估和**组合**评估。
（2）方式：以**自评估**为主，**自评估**和**检查评估**相互结合和互为补充。
（3）分析：**知识**分析、**模型**分析、**定量**分析和**定性**分析。
3. 风险分析
（1）定量分析：**ALE=SLE*ARO=AV*EF*ARO**
（2）定性分析：知识、理论、经验的决定性因素。
4. 风险评估过程
（1）**准备**：团队、目标、范围、计划、方案、方法、工具、协议、授权书等。
（2）**要素**识别：资产、威胁、脆弱性、安全措施。
（3）**风险**分析：**定量**分析、**定性**分析，以及二者结合。
（4）**结果**判定：什么风险、影响、等级、**处理建议**。
（5）如上的四个阶段，每一个阶段产生的文档和记录。

三、信息系统审计

1. 作用：合规性（**安全性、真实性、效益性、合法性**的等方面）
2. 内容：总体审计、安全技术、安全管理、建设经济性、建设管理、效益评价。
3. 流程：**1-目标、2-范围、3-依据、4-组建团队、5-实施审**计、**6-审计报告、7-后续活动**。
4. 类型与报告：**SAS70** 和 **SOC** 的区别（范围不同、周期不同）。

（END）

温馨提示：为了减少学习的负担和聚焦核心，知识点总结写的是关键的精要的要点，并非是知识点的全文，请一定进一步结合官方的教材进行扩充补充、理解和掌握全面，以免产生以偏概全的问题。