

· 05 ·

信息安全的保证体系 和 评 估 方 法

安全保护等级

GB17859--999 标准规定了计算机系统安全保护能力的五个等级：

损害客体

安全保护等级	国家安全	社会秩序和公共利益	公民、法人和其他组织	保护对象/适用范围
第一级：用户自主保护级			损害	小微企业、乡镇单位一般的信息系统
第二级：系统审计保护级		损害	严重损害	中型企业、县市级单位一般的信息系统
第三级：安全标记保护级	损害	严重损害		地市级以上国家机关、企事业单位的重要信息系统
第四级：结构化保护级	严重损害	特别严重损害		国家重要领域、重要部门中的特别重要系统以及核心系统
第五级：访问验证保护级	特别严重损害			国家重要领域、重要部门的极端重要的系统

逐级增高



安全保护等级

- **第一级 用户自主保护级：**本级的计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。本级实施的是自主访问控制，即计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。
- **第二级 系统审计保护级：**本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。在自主访问控制的基础上控制访问权限扩散。
- **第三级 安全标记保护级：**本级的计算机信息系统可信计算基具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。本级的主要特征是计算机信息系统可信计算基对所有主体及其所控制的客体（例如：进程、文件、段、设备）实施强制访问控制。
- **第四级 结构化保护级：**本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。考虑隐蔽通道。对外部主体能够直接或间接访问的所有资源（例如：主体、存储客体和输入输出资源）实施强制访问控制。
- **第五级 访问验证保护级：**本级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。与第四级相比，自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。访问控制能够为每个命名客体指定命名用户和用户组，并规定他们对客体的访问模式。没有存取权的用户只允许由授权用户指定对客体的访问权。



安全风险管理的

◆ 在风险评估实施前，应该考虑：

- ① 确定风险评估的范围。
- ② 确定风险评估的目标。
- ③ 建立适当的组织结构。
- ④ 建立系统性的风险评估方法。
- ⑤ 获得最高管理者对风险评估策划的批准。

◆ 风险评估的基本要素为脆弱性、资产、威胁、风险和安全措施，与这些要素相关的属性分别为业务战略、资产价值、安全需求、安全事件和残余风险，这些也是风险评估要素的一部分。

◆ 风险计算模型包含信息资产、弱点/脆弱性、威胁等关键要素。每个要素有各自的属性，信息资产的属性是资产价值，弱点的属性是弱点被威胁利用后对资产带来的影响的严重程度，威胁的属性是威胁发生的可能性。风险计算的过程如下。

- ① 对信息资产进行识别，并对资产赋值。
- ② 对威胁进行分析，并对威胁发生的可能性赋值。
- ③ 识别信息资产的脆弱性，并对弱点的严重程度赋值。
- ④ 根据威胁和脆弱性计算安全事件发生的可能性。
- ⑤ 结合信息资产的重要性和发生安全事件的可能性，计算信息资产的风险值。