第 11 章 安全风险评估和等级保护作业

一、填空题

1、信息系统安全风险分析涉及 资产、威胁 、脆弱性 等三个基本要素。

2、评价资产的三个安全属性是 保密性、完整性 、可用性 。

3、信息系统安全等级保护实施应遵循 自主保护原则、 重点保护原则、 同步建设原则和 动态调整原则。

二、选择题

1、下列哪种情况不适宜进行安全风险评估（ D）

A. 设计规划或升级信息系统时 B.安全事件发生后

C. 组织发生结构性变动 D.信息系统运行维护阶段

2、资产的脆弱性具有（C ）特点，这是脆弱性识别中最为困难的部分。

A.不确定性 B.特殊性 C.隐蔽性 D.复杂性

3、以下哪种情况会出现欠保护（B）

A. 在资产价值级别大于威胁级别的情况下，以威胁级别作为信息系统（安全域）

的安全保护等级；

B. 在资产价值级别小于威胁级别的情况下，以资产价值级别作为信息系统（安

全域）的安全保护等级；

C. 在资产价值级别与威胁级别相同的情况下，该级别则为信息系统（安全域）

的安全保护等级；

D. 根据信息系统安全等级不同，采用不同的安全措施。

4、以下说法正确的是（AB ）

A. 根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性；

B. 根据威胁出现的频率和脆弱性的严重程度判断安全事件发生的可能性；

C. 根据资产的价值和脆弱性的严重程度判断安全事件发生的可能性；

D. 根据威胁出现的频率和资产的价值判断安全事件发生的可能性

5、以下说法正确的是（ABDE ）

A. 脆弱性识别需要具体到每个资产或组件上；

B. 安全措施的确认不需要具体到每个资产或组件上；

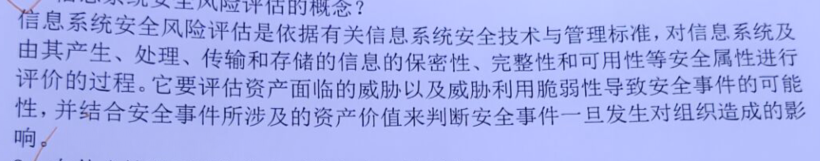
C. 保护性安全措施可以降低安全事件发生的可能性；

D. 保护性安全措施可以减少安全事件发生后对组织或系统造成的影响；

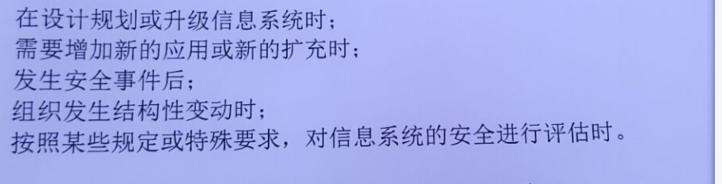
E. 安全措施的实施是以减少脆弱性或降低安全事件发生的概率为目标的。

三、简答题

1、信息系统安全风险评估的概念？



1. 在什么情况下进行信息系统安全风险评估？



1. 从风险评估的基本素出发解释风险分析的原理

