第 10 章 信息系统安全管理作业

一、填空题

1、ISO/IEC 27001 标准，采用“ 计划、实施、检查、处置 ”（PDCA）模型去架构所有信息系统管理体系的流程。

2、信息系统安全管理措施包括 物理安全管理、 系统安全管理、 运行安全管理、 数据安全管理、 人员管理和 技术文档安全管理。

3、信息系统安全等级保护是从与信息系统安全相关的 物理层面、 网络层面、 系统层面、 应用层面和 管理层面对信息和信息系统实施分等级保护。

二、选择题

1、信息系统安全管理措施中的运行安全管理不包括（C ）

A．故障管理 B.性能管理 C.配置管理 D.变更管理

2、不属于信息系统安全管理措施主要类型的是（ B）

A.管理控制 B.访问控制 C.技术控制 D.物理控制

3、属于信息系统安全管理措施中的人员安全管理原则之一是（A ）

A．最小特权原则 B.全员参与原则C. 主要领导负责原则 D.分权与授权原则

4、启动 PDCA 循环的启动器是指（ACDE ）

A．提供必需的资源 B.确定管理范围 C.选择风险管理方法D.确定评审方法 E.文件化实践

5、PDCA 模型实施阶段可能持续进行以下哪些操作（ABCD ）

A．测量信息系统安全管理体系满足安全方针和目标方面的业绩；

B．识别信息系统安全管理体系的改进，并有效实施；

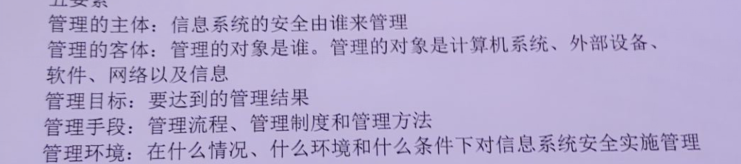
C．采取适当的纠正和预防措施；

D．针对结果，进行及时沟通，并与所有相关方磋商；

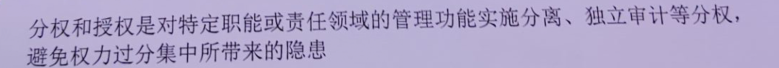
E．记录报告影响安全管理体系有效性的活动和事件。

三、简答题

1、信息系统安全管理的概念和五个组成要素（要素需简答说明）



1. 如何理解信息系统安全管理中的分权和授权原则



3、在信息系统安全管理措施中阐述的物理安全管理，与第 3 章的物理安全之间

是什么关系？分析说明

