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模型处置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）

**信息系统安全管理的概念：信息系统安全管理指通过计划、组织、领导、控制等环节来协调人力、物力、财力等资源，从而保证组织内的信息系统以及信息处理的安全。**

**五个组成要素：**

**管理的主体：信息系统的安全由谁来管理；**

**管理的客体：管理的对象是谁（计算机系统、外部设备、软件、网络以及信息）；**

**管理目标：要达到的管理结果；**

**管理手段：管理流程、管理制度和管理方法；**

**管理环境：在什么情况下、什么环境和什么条件下对信息系统安全实施管理。**

2. 如何理解信息系统安全管理中的分权和授权原则

**分权和授权是对特定职能活责任领域的管理功能实施分离、独立审计等分权，避免权力过分集中所带来的隐患。**

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

**信息系统安全管理措施中阐述的物理安全管理有：**

**机房和设施安全管理：对放置信息系统的空间和设施进行仔细周密的计划，对信息系统进行物理上的严密保护，以避免可能存在的不安全因素。既不欠保护，也不过保护；**

**环境和人身安全管理：物理安全管理需要考虑到防火、防漏水和水灾、防自然灾害等物理安全威胁。一旦出现这些威胁，能够及时处理，保证人员安全；**

**电磁泄漏管理：通过技术控制的手段，防止电磁泄漏。其主要方法有：一是通过电子隐藏技术掩盖信息系统的工作状态和保护信息；二是通过屏蔽等物理抑制手段，抑制一切有用信息的电磁外泄。**

**物理安全包括设备物理安全、环境物理安全、系统物理安全。**

**物理安全管理是保证物理安全的前提。**