**2017年信息安全工程师考试下午试题加答案（二）**

新开的**信息安全工程师考试**分属该考试“信息系统”专业，位处中级资格。大家在找试题做练习的时候是否苦恼没有资源？希赛软考学院为大家整理了一些下午试题的练习，供大家参考，希望能有所帮助。

阅读下列说明，回答问题1至问题4，将解答填入答题纸的对应栏内。

【说明】

设计源于需求，需求源于目标。要弄清安全的需求，就要首先明确安全的管理目标。一般而言，针对安全的管理目标包括政策需求和业务需求。获取和分析安全需求通常是从国家法律、组织政策、业务策略和责任追究等方西出发，而这些都是系统管理层需要考虑的内容。安全信息系统构建的最终目标，就是要求通过多层次手段最终所实现的信息系统完全满足管理层的要求。

在初始盼段和设计阶段，为了确保信息系统的安全属性真正达到设计时确定的安全目标，安全设计可以参照以下几个设计原则：

需要对应用系统进行风险分析；

确认安全风险并将安全需求具体化；

通过在应用中实现安全机制来满足安全需求；

安全机制被正确地设计。

在实施阶段至最终处理阶段，安全设计可以参照以下几个设计原则：

需要正确地实施安全机制；需要正确地配置安全属性；

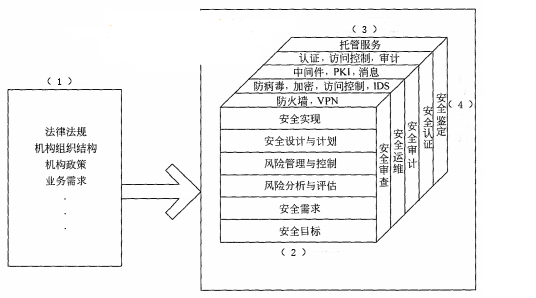
需要正确地使用和管理安全属性；

针对信息系统的安全管理有清晰的安全目标；

安全管理包括对安全需求的管理，例如，要对风险和成本进行平衡，以确保满足管理目标。

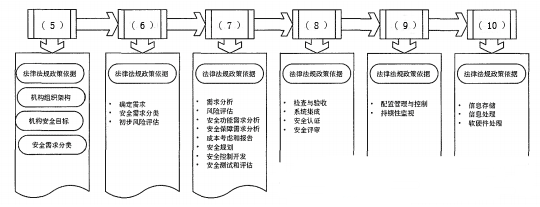
在安全信息系统构建过程中，需要遵循这些原则采取具体的机制和措施，以求达到安全目标和安全需求。

信息系统安全体系（ISSA)，其基本框架如下图所示。



      信息系统安全体系框架

国外广泛采用的是NIST SP800-64标准《信息安全开发生命周期中的安全考虑指南》。该《指南》介绍了把安全纳入信息系统开发生命周期的所有阶段（从初始阶段到最终处理阶段）的框架。引用NIST SP800-64的《指南》作为参考，SDLC基本上可分为6个主要阶段，各阶段的安全措施与步骤如下图所示。



      SDLC的6个主要阶段

【问题1】（4分）

根据信息系统安全体系（ISSA）的基本内容将信息系统安全体系框架图中的（1）—（4）空补充完整。

【问题2】（3分）

根据信息系统开发生命周期的6个阶段将信息系统开发生命周期（SDLC）图中的（5）—（10）空补充完整。

【问题3】（5分）

在构建信息系统模型时，要解决开放式环境带来的复杂、多变的安全威胁应该怎样设计信息系统？（2分）该如何实现？（3分）

【问题4】（3分）

要实现系统的安全，也不能仅从技术角度考虑，也需要从哪些方面来寻找一个平衡点？

**参考答案**

【问题1】

（1）法律法规与政策

（2）安全管理体系

（3）安全技术体系

（4）标准规范体系

【问题2】

（5）安全依据

（6）初始阶段

（7）设计阶段

（8）实施阶段

（9）运维阶段

（10）最终处理阶段

【问题3】

1.风险分析

2.安全策略

3.安全架构

【问题4】

从技术、管理、风险控制、策略来寻找平衡点