**信息安全工程复习提纲**

**第一章 信息安全工程**

1、信息安全工程的概念？（2种）

2、信息安全工程与软件工程的区别？

3、信息安全的目标（纵向，4条）并简要阐述？

4、什么是信息安全保障？

5、什么是PDRR安全模型？

6、什么是信息系统安全保障模型？（保障要素、安全特征、生命周期，图）

7、信息系统安全保障要素主要包括？

8、什么是信息系统安全生命周期？（图）

**第二章 ISSE过程**

1、什么是ISSE？

2、ISSE的指导思想？

3、ISSE的过程？（5个阶段，图）

4、信息系统安全需求挖掘分为哪三部分？（图）

5、信息系统安全定义分为哪四部分？（图）

6、ISSE基本功能？（6个）

7、简述信息系统安全保障工程实施简要框架？（图）

**第三章 SSE-CMM过程**

1、什么是SSE-CMM？

2、SSE-CMM的重要用途？

3、SSE-CMM包含哪三类过程域？

4、项目过程域的2个目标？

5、组织过程域包括？

6、SSE-CMM将通用安全工程过程域分为哪三个基本单元？

7、安全工程的主要目标之一？安全风险包括了哪三点？

8、SSE-CMM为什么认为安全工程跟其他学科一样？

9、SSE-CMM中与工程相关的过程域？

10、什么是信任度？以什么形式交流？

11、SSE-CMM模型为确保分离出安全工程基本特征，设计有哪两个维数？

12、什么是域维？

13、什么是能力维？

14、有多少种过程域？

15、过程域与基本实践的关系？

16、公共特征与通用实践的关系？

17、SSE-CMM能力级别？与其对应的公共特征？

18、SSE-CMM模型作用？

19、SSE-CMM用于哪三种场合（应用）？

20、什么是过程改进推荐方法IDEAL？（图）

21、什么是能力评估？什么是SSAM？

22、SSAM能力评估方法过程？

23、ISSE与SSE-CMM的比较？（来源、思路、作用、过程结构、体系结构、缺陷）

24、ISSE功能过程与SSE-CMM过程域的对应关系？

25、什么是数据安全能力成熟度模型？（能力成熟度等级、数据生命周期、数据安全能力，图）

**第四章 信息安全等级保护**

1、什么是信息系统安全等级保护？

2、信息系统安全等级保护的核心观念？（8字版本、16字版本）

3、信息系统安全等级保护的目的？

4、信息系统安全等级保护原则？（4条）

5、信息系统安全等级保护等级的划分及内容？（5级）

6、信息系统安全等级对应保护手段？

7、信息系统安全等级两个关键定级要素？

8、受侵害的客体？（3个）

9、侵害的程度？（3个）

10、信息系统安全保护等级划分依据？（表格）

11、信息系统安全等级保护体系？（4个）

12、《信息系统安全等级保护基本要求》的组织方式？

13、《信息系统安全等级保护基本要求》分为哪两大类？

14、信息系统安全等级保护基本原理、方法、目标？（16字目标）

15、信息系统安全防护按哪4个层次进行防护措施设计？

16、什么是安全域？

17、安全域划分的考虑因素？（3条）

**第五章 信息安全管理**

1、什么是信息安全管理？

2、信息安全管理的内容有哪些？（4条）

3、信息安全管理的原则有哪些？（8条，归西综一、防风冻成狗）

4、信息安全管理的安全因素是？（图）

5、信息安全管理模型是？（图）

6、什么是信息安全管理体系ISMS？

7、什么是PDCA戴明环循环模型？

8、ISMS的特点是？（3条）

9、ISMS的建设过程是？（6条）

10、信息安全管理体系的建立分为哪6步？

11、什么是ISMS风险评估？

12、ISMS风险评估有哪2个过程？

13、ISMS风险评估中风险识别的范围是哪三个？

14、信息安全管理体系监视和评审过程是？

15、什么是ISMS内部审核？

16、信息安全管理体系评审的时机是？

17、发生何种情况时应适时进行管理评审？

**第六章 信息安全风险评估**

1、什么是信息安全风险评估？（对哪4方面进行分析）

2、信息安全风险评估的最终目的？

3、什么是信息安全管理体系的核心环节？

4、什么是信息安全保障体系建设过程中的重要评价方法和决策机制？

5、信息安全风险评估的原则？（6条，可可完整，最小时间成本，要保密哦！）

6、什么是信息安全风险评估的对象？

7、什么是信息安全风险评估的基本要素？（7点）

8、什么是资产？

9、资产安全特性的三个要素？

10、资产的存在形式？

11、什么是威胁？

12、威胁的来源是？（环境、人为）

13、什么是脆弱性？

14、脆弱性分为哪两方面？

15、什么是安全风险？

16、安全风险的基本要素和存在的基本条件？（3条）

17、安全风险的计算公式？

18、什么是影响？

19、什么是影响的后果的表现形式？（2种）

20、什么是安全控制措施？

21、什么是安全控制措施的实施领域？（4个）

22、什么是安全需求？

23、安全需求来源于哪三个方面？

24、风险要素之间的关系是？（图）

25、信息安全风险的评估过程是？（图）

26、风险的3种计算公式？

27、安全控制措施分为哪三种？

28、什么是安全控制措施的确认？

29、选择安全控制措施时因考虑的因素是？（4点）

30、什么是安全控制措施的最终结果？

31、控制风险有哪4种方法？

32、什么是OCTAVE法？

33、什么是层次分析法？

34、信息安全风险评估方法分为哪三点？

**第七章 信息安全策略**

1、什么是信息安全策略？

2、什么是PPDR模型？

3、信息安全策略提供了什么？（4点）

4、信息安全策略的分类（3点）

5、信息安全策略的内容？

6、信息安全策略的制定原则？（3点）

7、信息安全策略的制定流程？

8、信息安全策略管理方法？

9、信息安全策略规范？