## 简答题

1、如何理解信息安全管理的内涵？

信息安全管理是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法。它是直接管理活动的结果，表示成方针、原则、目标、方法、过程、核查表等要素的集合。

信息安全管理是组织机构单位按照信息安全管理体系相关标准的要求，制定信息安全管理方针和策略，采用风险管理的方法进行信息安全管理计划、实施、评审检查、改进的信息安全管理执行的工作体系。体系一旦建立组织应按体系规定的要求进行运作，保持体系运作的有效性，信息安全管理体系应形成一定的文件，即组织应建立并保持一个文件化的信息安全管理体系，其中应阐述被保护的资产、组织风险管理的方法、控制目标及控制方式和需要的保证程度。

2、各信息安全风险因素之间的关系是怎样的？

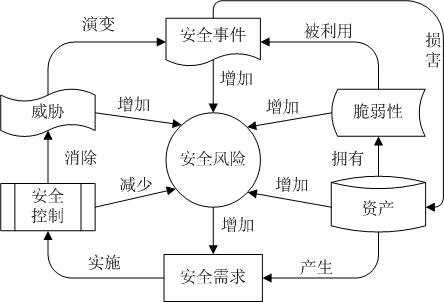
信息安全风险因素主要包括威胁、脆弱性、资产、安全控制等。

资产（Assets）是指对组织具有价值的信息资源，是安全策略保护的对象。

威胁（Threat）主要指可能导致资产或组织受到损害的安全事件的潜在因素。

脆弱性（Vulnerability）一般指资产中存在的可能被潜在威胁所利用的缺陷或薄弱点，如操作系统漏洞等。

安全控制（Security Control）是指用于消除或减低安全风险所采取的某种安全行为，包括措施、程序及机制等。



3、风险评估的主要任务有哪些？

识别组织面临的各种风险，了解总体的安全状况；

分析计算风险概率，预估可能带来的负面影响；

评价组织承受风险的能力，确定各项安全建设的优先等级；

推荐风险控制策略，为安全需求提供依据。

4、实施风险控制主要包括那些步骤？

第一步 对实施控制措施的优先级进行排序，分配资源时，对标有不可接受的高等级的风险项应该给予较高的优先级；

第二步 评估所建议的安全选项，风险评估结论中建议的控制措施对于具体的单位及其信息系统可能不是最适合或最可行的，因此要对所建议的控制措施的可行性和有效性进行分析，选择出最适当的控制措施；

第三步 进行成本效益分析，为决策管理层提供风险控制措施的成本效益分析报告；

第四步 在成本效益分析的基础上，确定即将实施的成本有效性最好的安全措施；

第五步 遴选出那些拥有合适的专长和技能，可实现所选控制措施的人员（内部人员或外部合同商），并赋以相应责任；

第六步 制定控制措施的实现计划，计划内容主要包括风险评估报告给出的风险、风险级别以及所建议的安全措施，实施控制的优先级队列、预期安全控制列表、实现预期安全控制时所需的资源、负责人员清单、开始日期、完成日期以及维护要求等；

第七步 分析计算出残余风险，风险控制可以降低风险级别，但不会根除风险，因此安全措施实施后仍然存在的残余风险。

5、CC标准与BS 7799标准有什么区别？

CC标准提倡安全工程的思想，通过信息安全产品的开发、评价、使用全过程的各个环节的综合考虑来确保产品的安全性。

BS 7799-1《信息安全管理实施细则》从11个方面定义了133项控制措施。

CC侧重于对系统和产品的技术指标，旨在支持产品（最终是指已经在系统中安装了的产品，虽然目前指的是一般产品）中IT安全特征的技术性评估。CC标准还有一个重要作用，即它可以用于描述用户对安全性的技术需求。BS7799则偏重于安全管理方面的要求。它不是一篇技术标准，而是管理标准。它处理的是对IT系统中非技术内容的检查。这些内容与人员、流程、物理安全以及一般意义上的安全管理有关。BS7799的目的是"为信息安全管理提供建议，供那些在其机构中负有安全责任的人使用。它旨在为一个机构提供用来制定安全标准、实施有效的安全管理时的通用要素，并得以使跨机构的交易得到互信"。

6、我国有关信息安全的法律法规有什么特点？

（1）信息安全法律法规体系初步形成

（2）与信息安全相关的司法和行政管理体系迅速完善

（3）目前法律规定中法律少而规章等偏多，缺乏信息安全的基本法。

（4）目前法律规定中法律少而规章等偏多，缺乏信息安全的基本法。

（5）与信息安全相关的其他法律有待完善

## 辨析题

1. 有人说“信息安全风险评估就是对信息系统的安全性进行检查”，你认为正确与否，为什么？

我认为不正确。

风险评估（Risk Assessment）是指对信息资产所面临的威胁、存在的弱点、可能导致的安全事件以及三者综合作用所带来的风险进行评估。作为风险管理的基础，风险评估是组织确定信息安全需求的一个重要手段。

风险评估的主要任务有：识别组织面临的各种风险，了解总体的安全状况；分析计算风险概率，预估可能带来的负面影响；评价组织承受风险的能力，确定各项安全建设的优先等级；推荐风险控制策略，为安全需求提供依据。

所以说信息安全风险评估不仅仅是对信息系统的安全性进行检查。

1. 有人说“保守国家秘密是那些涉密人员的事情，与我无关”，你认为正确与否，为什么？

我认为不正确。

一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务。国家秘密受法律保护。任何危害国家秘密安全的行为，都必须受到法律追究。作为中华人民共和国公民我们人人都应该学会保守国家秘密，维护国家安全。

## 名词解释

1、PDCA

PDCA（Plan、Do、Check、Act）是从管理学惯用的过程模型，是信息安全管理体系ISMS的演化基础。

2、风险评估

风险评估（Risk Assessment）是指对信息资产所面临的威胁、存在的弱点、可能导致的安全事件以及三者综合作用所带来的风险进行评估。

风险评估主要包括风险分析和风险评价

风险分析是指全面地识别风险来源及类型；

风险评价是指依据风险标准估算风险水平，确定风险的严重性。

3、风险控制

风险控制：是信息安全风险管理在风险评估完成之后的另一项重要工作

其任务是对风险评估结论及建议中的各项安全措施进行分析评估，确定优先级以及具体实施的步骤。

4、CVE

CVE（Common Vulnerabilities & Exposures），即通用漏洞及暴露，是IDnA（Intrusion Detection and Assessment）的行业标准。

5、CC标准

CC标准是“The Common Criteria for Information Technology security Evaluation”的缩写，《信息技术安全性通用评估标准》，在美国和欧洲等推出的测评准则上发展起来的。

6、BS7799

BS7799是英国标准协会（British Standards Institute，BSI）针对信息安全管理而制定的一个标准，共分为两个部分。

第一部分BS7799-1是《信息安全管理实施细则》，也就是国际标准化组织的ISO/IEC 17799标准的部分，主要提供给负责信息安全系统开发的人员参考使用，其中分11个标题，定义了133项安全控制（最佳惯例）。

第二部分BS7799-2是《信息安全管理体系规范》（即ISO/IEC 27001），其中详细说明了建立、实施和维护信息安全管理体系的要求，可用来指导相关人员去应用ISO/IEC 17799，其最终目的是建立适合企业所需的信息安全管理体系。

7、信息犯罪

信息犯罪是以信息技术为犯罪手段，故意实施的有社会危害性的，依据法律规定，应当予以刑罚处罚的行为。目前多数的信息犯罪均属于计算机及网络犯罪。

公安部 “所谓计算机犯罪，就是在信息活动领域中，以计算机信息系统或计算机信息知识作为手段，或者针对计算机信息系统，对国家、团体或个人造成危害，依据法律规定，应当予以刑罚处罚的行为”。

网络犯罪就是行为主体以计算机或计算机网络为犯罪工具或攻击对象，故意实施的危害计算机网络安全的，触犯有关法律规范的行为。