信息安全管理

题型

判断题	2’ * 10
选择题	2’ * 15
问答题（+画图）	10’ * 5
附加题	10’

简答重点

信息安全管理体系

概念：

信息安全管理体系，ISMS，是组织在 整体或特定范围 内，建立的信息安全 方针和目标，以及完成这些目标所使用的 方法和手段，所构成的 体系

建立 ISMS 的步骤：

1. 信息安全管理体系的 策划与准备
2. 信息安全管理体系的 文件编制
3. 建立 信息安全 管理框架
4. 信息安全管理体系的 运行
5. 信息安全管理体系的 审核与评审

信息系统安全等级保护

等级保护工作包括五个阶段：

定级、备案、安全 建设和整改、信息安全等级 测评、信息安全 检查

目的：

体现 国家管理意志；构建 国家信息安全 保障体系；保障 信息化发展 和维护 国家安全；

关键所在：

是基于信息系统所承载应用的重要性以及该应用损毁后带来的影响程度，来判断风险是否控制在可接受的范围内

定级：

定级 是首要环节、重要环节、开始环节，但 不是核心环节

定级原则：自主定级、自主保护、监督指导

定级要素：

- 受侵害的客体：
  国家安全；社会秩序和公共利益；公民、法人和其他组织的合法权益；
- 对客体的侵害程度：
  造成 一般损害 / 严重损害 / 特别严重损害

安全等级：

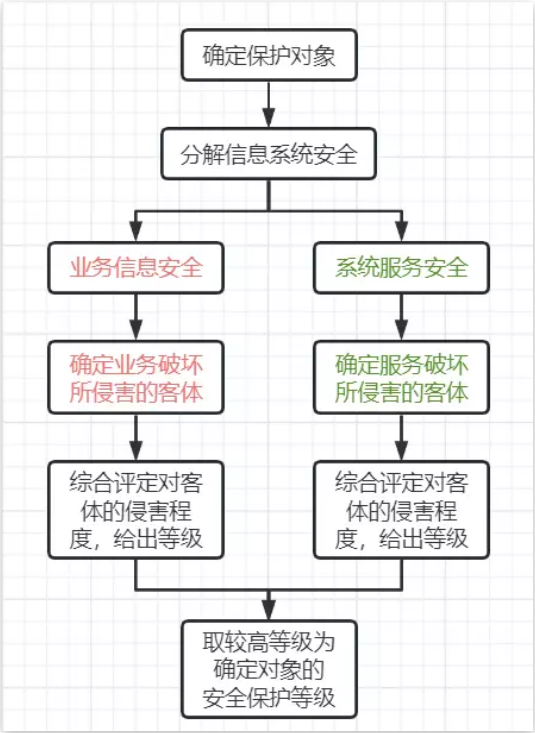
信息系统的安全保护等级分为五级，分别为：

1. 会对 公民、法人和其他组织的合法权益 造成损害
2. 会对 公民、法人和其他组织的合法权益 产生严重损害，或者对 社会秩序和公共利益 造成损害
3. 会对 社会秩序和公共利益 产生严重损害，或者对 国家安全 造成损害
4. 会对 社会秩序和公共利益 造成特别严重损害，或者对 国家安全 造成严重损害
5. 会对 国家安全 造成特别严重损害

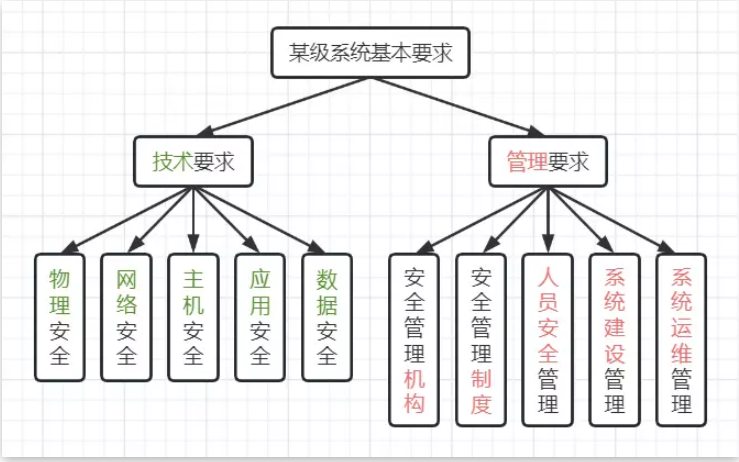
安全等级矩阵表：

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序和公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

定级流程图：



等保定级系统的达标要求：



技术 要求：

物理 安全、网络 安全、主机 安全、应用 安全、数据 安全

管理 要求：

安全管理 机构、安全管理 制度、人员安全 管理、系统建设 管理、系统运维 管理

等保测评的目的：

验证 信息系统 是否满足 相应安全保护等级

等保测评：

包括 安全控制测试 和 系统整体测试 两个方面

信息系统生命周期

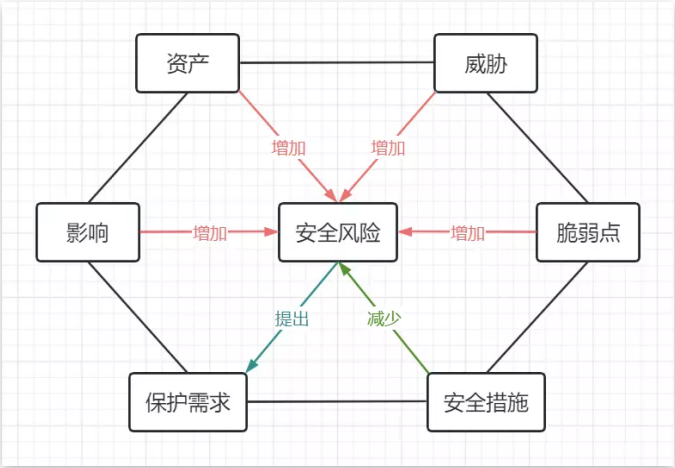
信息系统生命周期一般包括信息系统的 规划、设计、实施、运维 和 废弃 五个阶段，风险评估活动应贯穿于信息系统生命周期的各个阶段

信息安全风险管理

七大要素：

资产、威胁、脆弱点、安全措施、安全风险、保护需求、影响

七大要素的关系图：



七大要素的详细关系：

- 威胁 利用 脆弱点 导致安全风险的产生；
- 资产 具有价值，并对组织业务有一定影响，资产价值及 影响 越大，则其面临的安全风险越大；
- 安全措施 能抵御威胁、减少脆弱点，因而能减少安全风险；
- 风险的存在及对风险的认识导出 保护需求，保护需求通过安全措施来满足或实现；

风险评估

概念：

评估 信息安全漏洞 对 信息资产 带来的 威胁和影响，及其 发生的可能性

基线风险评估：

根据实际情况，对信息系统进行 基线安全检查，得出 基本的安全需求，通过选择并实施标准的安全措施来管理风险

详细风险评估：

根据实际情况，对信息系统进行 详细安全检查，得出 详细的安全需求，通过选择并实施标准的安全措施来管理风险

流程：

风险评估准备；资产识别与评估；威胁识别与评估；脆弱点识别与评估；已有安全措施的确认；风险分析；安全措施的选取；风险评估文件和记录

综合风险评估：

基线风险评估 耗费资源少、简单而便捷，但不够准确，适合一般环境的评估；

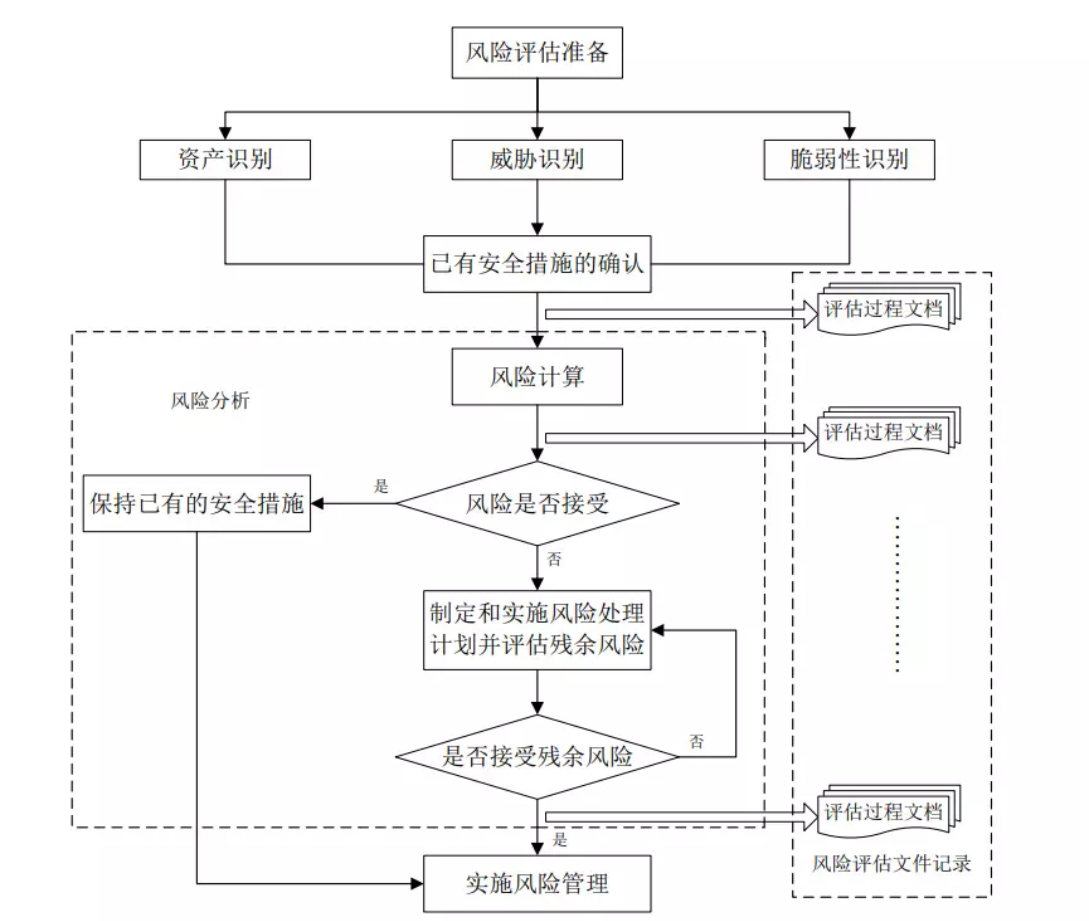
详细风险评估 耗费资源多、细致而准确，适合严格限定边界的较小范围内的评估；

因而实践当中多是采用二者结合的 综合风险评估 方式；

流程：

高层风险分析；依据 基线 或 详细 风险分析结果选取相应安全措施；IT 系统安全策略；IT 安全计划；

详细风险评估流程图：



选择重点

风险评估、应急响应、ISO 27001 所关注的 11 大领域

1. 安全策略：
指定信息安全方针，为信息安全提供管理指引和支持，并定期评审

2. 信息安全的组织：
建立信息安全管理组织体系，在内部开展和控制信息安全的实施。

3. 资产管理：
核查所有信息资产，做好信息分类，确保信息资产受到适当程度的保护。

4. 人力资源安全：
确保所有员工、合同方和第三方了解信息安全威胁和相关事宜以及各自的责任、义务，以减少人为差错，盗窃，欺诈或误用设施的风险

5. 物理和环境安全：
定义安全区域，防止对办公场所和信息的未授权访问、破坏和干扰；
保护设备的安全，防止信息资产的丢失、损坏或被盗，以及对企业业务的干扰；

6. 通信和操作管理：
制定操作规程和职责，确保信息处理设施的正确和安全操作；建立系统规划和验收准则，将系统失效的风险降到最低；防范恶意代码和移动代码，保护软件和信息的完整性；做好信息备份和网络安全管理，确保信息在网络中的安全，确保其支持性基础设施得到保护；建立媒体处置和安全的规程，防止资产损坏和业务活动的中断；防止信息和软件在组织之间交换时丢失，修改或误用。

7. 访问控制：
制定访问控制策略，避免信息系统的非授权访问，并让用户了解其职责和义务，包括网络访问控制，操作系统访问控制，应用系统和信息访问控制，监视系统访问和使用，定期检测未授权的活动；当使用移动办公和远程控制时，也要确保信息安全

8. 系统采集、开发和维护：
标示系统的安全要求，确保安全成为信息系统的内置部分，控制应用系统的安全，防止应用系统中用户数据的丢失，被修改或误用；
通过加密手段保护信息的保密性，真实性和完整性；
控制对系统文件的访问，确保系统文档，源程序代码的安全；严格控制开发和支持过程，维护应用系统软件和信息安全；

9. 信息安全事故管理：
报告信息安全事件和弱点，及时采取纠正措施，确保使用持续有效的方法管理信息安全事故，并确保及时修复。

10. 业务连续性管理：
目的是为了减少业务活动的中断，使关键业务过程免受主要故障或天灾的影响，并确保及时恢复

11. 符合性：
信息系统的设计、操作、使用和管理要符合法律法规的要求，符合组织安全方针和标准，还要控制系统审计，使信息审核过程的效力最大化，干扰最小化

信息安全的 符合性检查 包括：
法律法规 符合性；技术标准 符合性；安全策略 符合性；

业务连续性管理 BCM 的原则是预防为先，恢复为后
预防的目的 是 减少灾难发生的可能性
预防的策略 包括：制止控制（减少威胁的可能性）和预防控制（保护企业的弱点区域，以防御危险的发生并降低其影响）

访问控制 包括三个要素：主体、客体 和 控制策略

主要的访问控制类型有 3 种模式：自主访问控制（DAC）、强制访问控制（MAC）和 基于角色访问控制（RBAC）
DAC：
每个客体有一个所有者，可按照各自意愿将客体访问控制权限授予其他主体；
用户有权对自身所创建的文件、数据表等访问对象进行访问，并可将其访问权授予其他用户或收回其访问权限；
MAC：
由系统对用户所创建的对象，按照规定的规则控制用户权限及操作对象的访问；
每个用户及文件都被赋予一定的安全级别，只有 系统管理员 才可确定用户和组的访问权限；

信息安全的发展阶段
三个阶段：通讯保密阶段、信息安全阶段、安全保障阶段
四个阶段：通讯保密阶段、计算机安全阶段、IT 安全阶段、安全保障阶段

2017 年 6 月 1 日起，《网络安全法》开始施行
2021 年 9 月 1 日起，《数据安全法》开始施行
2021 年 11 月 1 日起，《个人信息保护法》开始施行

信息安全管理体系：
特点：
以预防控制为主；强调合规性；强调全过程和动态控制；关注关键性信息资产
作用：
强化信息安全意识，规范信息安全行为，贯彻信息安全保障体系；
确保业务持续开展并将损失降到最低程度；
通过体系认证，可以提高组织的知名度与信任度；

在 建立信息安全管理体系 时，首先 应该做的事情是 建立信息安全方针和目标

信息安全管理体系是 PDCA 模型 动态持续改进 的一个循环体

PDCA 循环是能使任何一项活动有效进行的工作程序

PDCA 模型：
Plan ： 计划，确定信息安全管理体系的范围、方针和目标，形成文件
Do ： 实施，完成这些目标，做文件已经规定的事情
Check ： 检查，对安全措施的实施情况进行符合性检查
Action ： 处理，根据检查的结果，采取纠正和预防措施，实现 ISMS 的持续改进

PDCA 循环是螺旋式上升和发展的，推动 PDCA 循环的 关键 是 处理 阶段

风险评估可分为四个阶段：
风险评估准备、风险识别、风险评价、风险处理

风险评估 过程中的 预防性控制措施 是 入侵监测方法

常见的风险评估方法：
基线 风险评估方法；详细 风险评估方法；综合 风险评估方法

安全基线：类比于木桶理论，是安全木桶的最短板或者是信息系统的最低安全要求

风险管理：降低、避免、转移、接受 风险

资产评估：
对资产的 价值 或 重要程度 进行评估，多数情况下只能以 定性 的形式

威胁评估：
威胁可分为五大类：不可抗力、组织缺陷、人员错误、技术错误、故意行为
威胁评估的结果一般都是 定性 的

脆弱点的特点：
弱点是资产本身存在的；单纯的弱点本身不会对资产造成损害；威胁总是要利用资产的弱点才可能造成危害；资产脆弱点具有隐蔽性；同一资产可能有多个脆弱点；

脆弱点可分为 技术脆弱点 和 管理脆弱点
技术 脆弱性识别：物理环境、服务器、网络结构、数据库、应用系统
管理 脆弱性识别：技术管理，组织管理

信息安全策略制定 的三个基本原则 确定性、 完整性 和 有效性

IS0 17799 的 内容结构 按照 管理域、控制目标、控制措施 进行组织

ISO 17799/ISO 27001 最初是由 英国 提出的国家标准

所有 与信息系统 有关人员 对于信息安全管理负有责任

在 PDR 安全模型中最核心的组件是 策略

在完成了大部分策略的编制工作后，需要对其进行总结和提炼，产生的成果文档被称为 可接受使用策略 AUP

安全审计跟踪 是 安全审计系统 检测并追踪 安全事件 的过程

判断重点

信息 是通过 在数据上施加某些约定 而 赋予这些数据的 特殊含义

信息安全不等同于网络安全

GB 17859 与目前等级保护所规定的安全等级的含义不同，GB 17859 中的等级划分为现在的等级保护奠定了基础

> 《计算机信息系统安全保护等级划分准则》（GB 17859–1999）将计算机系统的安全保护划分为 5 个等级，分别是：
> 1 用户自主保护级；2 系统审计保护级；3 安全标记保护级；4 结构化保护级；5 访问验证保护级；
> 《信息安全等级保护管理办法》将信息系统的安全保护划分为 5 个等级，分别是：
> 1 自主保护级；2 指导保护级；3 监督保护级；4 强制保护级；5 专控保护级；

《信息系统安全等级保护测评准则》将测评分为 安全控制测评 和 系统整体测评 两个方面

信息安全领域内 最关键和最薄弱 的环节是 人

在信息安全事件管理中，报告 安全方面的 漏洞或弱点 和 发现并报告 安全事件 是员工应该完成的活动

在信息安全管理中进行 责任追查和惩处，可以 有效解决 人员 安全意识薄弱 问题

我国刑法中有关计算机犯罪的规定，定义了 2 种新的犯罪类型

> 刑法有关计算机犯罪的规定，总体上可以分为两大类：
> 一类是 纯粹的计算机犯罪，即刑法第 285 条、第 286 条单列的两种计算机犯罪独立罪名；另一类 不是纯粹的计算机犯罪，而是隐含于其他犯罪罪名中的计算机犯罪形式。例如，刑法第 287 条规定：“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。”
> 之所以要区分这两种类别，是因为第二类犯罪与传统犯罪之间并无本质区别，只是在犯罪工具使用上有所不同而已，因此不需要为其单列罪名，而第一类犯罪不仅在具体手段和侵犯客体方面与传统犯罪存在差别，而且有其特殊性，传统犯罪各罪名已无法包括这些犯罪形式，因此为其单列罪名。

一旦发现计算机违法犯罪案件，信息系统所有者应当在 24 小时内 迅速向当地公安机关报案，并配合公安机关的取证和调查

按照 BS 7799 标准，信息安全管理应当是一个 持续改进的周期性过程

信息安全发展历经了三个主要阶段：

1. 通讯保密 阶段：在这个阶段中，关注的是通信内容的保密性属性，保密等同于信息安全
2. 信息安全 阶段：人们发现，在原来所关注的 保密性 属性之外，还有其他方面的属性也应当是信息安全所关注的，这其中最主要的是 完整性 和 可用性 属性，由此构成了支撑信息安全体系的三要素
3. 安全保障 阶段：安全保障，就是在统一安全策略（安全策略 P）的 指导 下（安全策略只是指导作用，非核心），安全事件的事先预防（保护 P），事发处理（检测 D 和 响应 R），事后恢复（恢复 R ）四个主要环节相互配合，构成一个完整的保障体系

一个完整的 信息安全保障体系，应当包括 安全策略（Policy）、保护（Protection）、检测（Detection）、响应（Reaction）、恢复（Restoration）五个主要环节

风险评估过程包括对已有安全措施的确认，这里的 安全措施 可分为 预防性安全措施 和 保护性安全措施
预防性 安全措施：降低 威胁利用脆弱点导致 安全事件发生的可能性
保护性 安全措施：减少 因安全事件 发生对信息系统造成的影响

我国在 2006 年提出的《2006~2020年国家信息化发展战略》将“建设国家信息安全保障体系”作为 9 大战略发展方向之一

2003 年 7 月国家信息化领导小组第三次会议发布的 27 号文件，是指导我国信息安全保障工作和加快推进信息化的纲领性文献

安全管理的合规性，主要是指 在有章可循的基础上，确保 信息安全工作符合 国家法律、法规、行业标准、机构内部的 方针和规定

信息安全的 层次化特点 决定了 应用系统 的安全 不仅取决于 应用层安全机制，同样依赖于 底层的物理、网络和系统等层面的安全状况

实现信息安全 的途径要借助两方面的控制措施：技术措施 和 管理措施，从这里就能看出 技术和管理并重 的基本思想

虽然在安全评估过程中采取 定量评估 能获得 准确 的分析结果，但是由于 参数确定较为困难，往往 实际 评估 多采取定性评估，或者 定性和定量评估相结合 的方法

定性 安全风险评估结果中，级别较高的 安全风险应当 优先采取 控制措施予以应对

系统备份 与普通数据备份的不同在于，它不仅备份系统中的数据，还备份系统中安装的应用程序、数据库系统、用户设置、系统参数等信息，以便迅速 恢复整个系统

信息技术基础设施库（ITIL），是由 英国 发布的关于 IT 服务管理最佳实践的建议和指导方针，旨在解决 IT 服务质量不佳的情况

美国 国家标准技术协会 NIST 发布的《SP800-30》中详细阐述了 IT 系统风险管理内容

通常在风险评估的实践中，综合 利用 基线风险评估 和 详细风险评估 的优点，将二者结合起来

为防止业务中断，保护 关键业务 过程免受信息系统失误或灾难的影响，应定义恢复的 优先顺序 和 时间指标，并 针对业务中断 进行 风险评估

信息系统安全等级定级 由 业务信息安全 和 系统服务安全 组成

如果信息系统只承载一项业务，可以直接为该信息系统确定等级，不必划分业务子系统


完全准备好考试的我
第一题