

CISP-CISO

考试大纲及高频考试试题

注册信息安全管理人員
精选100题 - 含答案解析与难度说明

十大知识域覆盖 | 考试大纲 | 详细解析

本资料仅供学习参考，不构成考试承诺
请勿用于非法用途

CISP-CISO 考试大纲

一、考试说明

- 认证名称：CISP-CISO（注册信息安全管理人員）
- 认证机构：中国信息安全测评中心（CNITSEC）
- 考试题型：全部为单项选择题（客观题）
- 题量与分值：共100道题，每题1分，满分100分
- 合格标准：70分及以上
- 考试时长：120分钟
- 考试形式：线下笔试或机考（全国33个考点）
- 方向定位：偏重信息安全管理、治理、合规与风险评估

二、十大知识域及CISO考试权重

1. 信息安全保障	10%	信息安全发展阶段、CIA三要素、安全保障框架（PDR/IATF/WDPRC）、纵深防御
2. 网络安全监管	10%	网络安全法、数据安全法、个人信息保护法、等保2.0、关键信息基础设施保护
3. 信息安全管理	16%	ISMS建设、ISO 27001标准、PDCA循环、风险评估、风险处置策略、安全策略
4. 业务连续性	10%	BCM/BCP/DRP、BIA业务影响分析、RTO/RPO、应急响应PDCERF模型、灾难备份
5. 安全工程与运营	12%	SSE-CMM、SDL安全开发、SOC安全运营、社会工程学防范、内容安全、零信任
6. 安全评估	12%	TCSEC/CC评估标准、风险评估方法论、渗透测试、等保测评、代码审计SAST/DAST
7. 信息安全支撑技术	8%	密码学（对称/非对称/哈希）、PKI、Kerberos、访问控制（DAC/MAC/RBAC）、国密算法
8. 物理与网络通信安全	8%	物理环境安全、TEMPEST、OSI/TCP-IP协议安全、防火墙/IDS/IPS、VPN、DMZ
9. 计算环境安全	8%	操作系统安全加固、恶意代码防护、Web安全（SQL注入/XSS）、DLP、数据库安全
10. 软件安全开发	6%	SDL安全开发生命周期、OWASP 10、STRIDE威胁建模、SCA组件分析、DevSecOps

Top

三、CISO与CISE方向对比

- CISE（注册信息安全工程师）：偏重技术实践，适合安全厂商、安全服务供应商的技术岗位
- CISO（注册信息安全管理人員）：偏重管理策略，适合甲方信息中心、IT管理和安全管理部门
- 两者共享相同的十大知识域教材，区别在于各知识域的出题权重不同
- CISO在“信息安全管理”(16%)、“安全评估”(12%)、“安全工程与运营”(12%)占比更高
- CISE在“物理与网络通信安全”(12%)、“计算环境安全”(12%)、“安全支撑技术”(10%)占比更高

四、CISO高频考点提示

ISMS建设：PDCA循环各阶段内容、ISO 27001标准核心控制域、ISMS文件体系层次

风险管理：风险评估流程、风险处置四种策略、残余风险概念、定性vs定量分析

法律法规：网络安全法/数据安全法/个人信息保护法核心条款、等保2.0五个等级与流程

业务连续性：BCP与DRP区别、RTO/RPO含义与计算、PDCERF应急响应模型、灾难备份类型

安全评估：TCSEC/CC评估等级、CVSS评分体系、渗透测试流程、等保测评结论

支撑技术：对称/非对称加密区别、数字签名功能、PKI组件、RBAC/DAC/MAC对比

目 录

- 第一章 信息安全保障（共10题）
- 第二章 网络安全监管（共10题）
- 第三章 信息安全管理（共17题）
- 第四章 业务连续性（共10题）
- 第五章 安全工程与运营（共12题）
- 第六章 安全评估（共12题）
- 第七章 信息安全支撑技术（共8题）
- 第八章 物理与网络通信安全（共8题）
- 第九章 计算环境安全（共8题）
- 第十章 软件安全开发（共6题）

合计：101题

第一章 信息安全保障（共10题）

1. 信息安全发展的第三个阶段是？

- A. 通信安全阶段
- B. 计算机安全阶段
- C. 信息安全保障阶段
- D. 网络安全阶段

答案：C 难度：易

解析：

信息安全发展经历了三个主要阶段：第一阶段是通信安全阶段（二战至20世纪70年代），主要关注通信保密；第二阶段是计算机安全阶段（20世纪70-90年代），以《可信计算机系统评估准则》（TCSEC）为代表；第三阶段是信息安全保障阶段（20世纪90年代至今），强调通过技术、管理和工程的综合手段保障信息的CIA三要素（保密性、完整性、可用性），代表框架包括IATF信息保障技术框架。

2. 下列哪一项不属于信息安全的CIA三要素？

- A. 保密性（Confidentiality）
- B. 完整性（Integrity）
- C. 可用性（Availability）
- D. 可审计性（Auditability）

答案：D 难度：易

解析：

CIA三要素是信息安全的核心属性：保密性确保信息不被未经授权访问；完整性确保信息不被篡改或破坏；可用性确保授权用户能及时访问信息。可审计性是支撑CIA目标实现的手段和属性，不属于三要素本身。其他扩展属性包括真实性、抗抵赖性等。

3. PDR模型中的三个要素是？

- A. 保护、检测、响应
- B. 策略、检测、恢复
- C. 防御、攻击、响应
- D. 保护、防御、恢复

答案：A 难度：易

解析：

PDR模型是最早的动态安全模型之一，由Protection（保护）、Detection（检测）、Response（响应）三个要素组成。该模型强调安全是一个动态过程，通过保护措施降低风险，通过检测及时发现威胁，通过响应快速处置安全事件。后来发展为P²DR（加入Policy策略）和WPDRRC（加入Warning预警和Recovery恢复）。

4. IATF（信息保障技术框架）将信息系统划分为几个领域？

- A. 两个
- B. 三个
- C. 四个

D. 五个

答案：C 难度：中

解析：
IATF由美国国家安全局（NSA）制定，将信息保障技术框架分为四个领域：1）本地计算环境（服务器、工作站、操作系统和应用的安全）；2）区域边界（局域网边界的访问控制和入侵检测）；3）网络和基础设施（传输安全、路由安全）；4）支撑性基础设施（PKI体系和KMI密钥管理）。IATF强调深度防御（Defense-in-Depth）策略和人员、技术、运维三要素。

5. 下列关于纵深防御（Defense-in-Depth）的描述，错误的是？

- A. 通过多层安全防护措施降低单点失败的风险
- B. 纵深防御仅依赖技术手段
- C. 纵深防御涵盖人员、技术和运维三个维度
- D. 纵深防御要求攻击者需突破多层防线才能成功

答案：B 难度：易

解析：
纵深防御是IATF框架的核心思想，强调通过人员（培训、意识教育）、技术（防火墙、IDS、加密等）和运维（流程、制度、审计）三个维度的多层防护来保障安全。纵深防御不单纯依赖技术手段，管理和技术相结合才能构建有效的防御体系。

6. 信息安全保障的最终目标是？

- A. 保护信息系统的安全
- B. 保障业务的连续性和安全运行
- C. 部署安全产品
- D. 通过安全认证

答案：B 难度：易

解析：
信息安全保障的核心目标是保障组织业务的连续性和安全运行，而不是单纯的技术防护或产品部署。安全是服务于业务的，信息安全工作的出发点是识别业务风险，通过技术和管理手段将风险降低到可接受水平，确保业务在安全的环境下持续运转。

7. 下列哪个安全模型强调“安全是一个持续改进的过程”？

- A. TCSEC
- B. PDCA
- C. ITSEC
- D. CC

答案：B 难度：易

解析：
PDCA（Plan-Do-Check-Act）模型强调安全管理是一个持续改进的循环过程：Plan（计划）制定安全策略和方案；Do（实施）执行安全措施；Check（检查）评估安全效果；Act（改进）持续优化。PDCA被广泛应用于ISMS（信息安全管理体系）的建设和运行中，体现了安全管理的动态性和持续改进特征。TCSEC、ITSEC、CC是安全评估标准而非管理模型。

8. WPDRRC模型在PDR基础上增加了哪两个环节？

- A. 预警和恢复
- B. 策略和恢复
- C. 预防和审计
- D. 计划和改进

答案：A 难度：中

解析：

WPDRRC模型在PDR（保护-检测-响应）基础上增加了Warning（预警）和Recovery（恢复）两个环节，形成了Warning-Protection-Detection-Response-Recovery-Counterattack（预警-保护-检测-响应-恢复-反击）的完整安全循环。该模型强调了事前预警和事后恢复的重要性，体现了安全防护的全生命周期管理。

9. 下列关于信息安全保障框架的描述，正确的是？

- A. IATF仅适用于政府机构
- B. 等级保护是中国特有的信息安全保障制度
- C. ISO27001是技术评估标准
- D. TCSEC仍然是目前最新的安全评估标准

答案：B 难度：中

解析：

等级保护（等保2.0）是中国特有的信息安全保障制度，依据《网络安全法》和GB/T 22239-2019标准实施，要求网络运营者按定级、备案、建设整改、等级测评、监督检查五个步骤落实安全保护义务。IATF适用于各类组织；ISO27001是信息安全管理标准而非技术评估标准；TCSEC已被CC（通用准则）取代，不再是最新标准。

10. 在信息安全的属性中，抗抵赖性（Non-repudiation）主要解决什么问题？

- A. 信息被篡改的问题
- B. 信息泄露的问题
- C. 行为发送方否认其行为的问题
- D. 系统不可用的问题

答案：C 难度：易

解析：

抗抵赖性（不可否认性）确保信息的行为发送方不能否认其发送行为，行为接收方不能否认其接收行为。通常通过数字签名、时间戳、审计日志等技术手段实现。抗抵赖性不同于保密性（防止信息泄露）、完整性（防止信息被篡改）和可用性（确保系统可用），它解决的是事后追溯和责任认定问题。

第二章 网络安全监管（共10题）

11. 《网络安全法》正式施行的时间是？

- A. 2016年11月7日
- B. 2017年6月1日
- C. 2018年1月1日
- D. 2017年1月1日

答案：B 难度：易

解析：

《中华人民共和国网络安全法》于2016年11月7日由全国人大常委会通过，自2017年6月1日起正式施行。这是中国网络安全领域的基础性法律，明确了网络运营者的安全保护义务、关键信息基础设施保护要求、个人信息保护规则以及网络安全事件应急响应机制。

12. 根据《网络安全法》，网络运营者应当履行的安全保护义务不包括？

- A. 制定内部安全管理制度和操作规程
- B. 采取技术措施防范计算机病毒和网络攻击
- C. 自行决定安全保护等级不需备案
- D. 留存网络日志不少于六个月

答案：C 难度：中

解析：

《网络安全法》第二十一条规定网络运营者应履行五项安全保护义务：1）制定内部安全管理制度和操作规程；2）采取防范计算机病毒和网络攻击的技术措施；3）采取监测、记录网络安全状态的技术措施，日志留存不少于六个月；4）采取数据分类、备份和加密措施；5）按规定留存网络日志。安全保护等级需按等保制度定级并到公安机关备案，不能自行决定不备案。

13. 网络安全等级保护2.0的核心标准是？

- A. GB/T 22239-2008
- B. GB/T 22239-2019
- C. GB/T 22240-2008
- D. GB/T 25058-2019

答案：B 难度：易

解析：

等保2.0的核心标准是GB/T

22239-2019《信息安全技术

网络安全等级保护基本要求》，于2019年12月1日实施，替代了等保1.0的GB/T

22239-2008。等保2.0扩展了保护对象（增加云计算、移动互联、物联网、工业控制系统和大数据），强化了通信传输安全和个人信息保护要求，采用“一个中心，三重防护”的架构理念。

14. 《数据安全法》对数据实行什么分类制度？

- A. 二级分类
- B. 三级分类

- C. 四级分类
- D. 五级分类

答案：B 难度：中

解析：

《数据安全法》第二十一条规定国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度以及被篡改、破坏、泄露或非法获取、非法利用后对国家安全、公共利益或个人、组织合法权益的危害程度，对数据实行分类分级保护。具体分为一般数据、重要数据和核心数据三个级别，不同级别适用不同的保护要求。

15. 根据《个人信息保护法》，处理个人信息应当遵循的首要原则是？

- A. 最小必要原则
- B. 公开透明原则
- C. 合法、正当、必要和诚信原则
- D. 目的限制原则

答案：C 难度：中

解析：

《个人信息保护法》第五条明确规定，处理个人信息应当遵循合法、正当、必要和诚信原则，这是首要的、总括性的原则。在此基础上延伸出最小必要原则（第六条——收集个人信息应限于实现处理目的的最小范围）、公开透明原则（第七条——应公开个人信息处理规则）、目的限制原则、质量原则和责任原则等。

16. 关键信息基础设施（CII）的认定由哪个部门负责？

- A. 公安部
- B. 国家网信部门
- C. 工业和信息化部
- D. 国家安全部

答案：B 难度：中

解析：

《网络安全法》第三十一条规定，关键信息基础设施的具体范围和安全保护办法由国务院制定。国务院授权国家网信部门统筹协调有关部门对关键信息基础设施的安全保护工作。国家网信部门负责CII的认定和统筹协调，公安机关负责安全保卫和等级保护工作，行业主管监管部门负责本行业本领域的CII认定指导。

17. 网络安全等级保护的工作流程中，“定级备案”之后紧接着的环节是？

- A. 等级测评
- B. 建设整改
- C. 监督检查
- D. 系统备案

答案：B 难度：易

解析：

等保2.0的工作流程包括五个步骤：1）定级（确定系统安全保护等级）；2）备案（到公安机关网安部门备案）；3）建设整改（依据等级要求进行安全建设和整改）；4）等级测评（由第三方测评机构进行测评）；5）监督检查（公安机关定期监督检查）。定级备案之后是建设整改环节，依据等保基本要求和安全设计要求进行差距分析和整改。

18. 根据《网络安全法》，网络运营者收集个人信息时应遵守的原则不包括？

- A. 明确收集目的
- B. 获得信息主体的同意
- C. 收集所有可能的数据以备后用
- D. 公开收集和使用规则

答案：C 难度：易

解析：

《网络安全法》第四十一条规定网络运营者收集个人信息必须遵循合法、正当、必要的原则，明示收集和使用信息的目的、方式和范围，并经被收集者同意。不得收集与其提供的服务无关的个人信息，不得违反法律、法规规定收集和使用个人信息。“收集所有可能的数据以备后用”违反了必要原则和目的限制原则。

19. 等保2.0将安全保护等级分为几级？

- A. 三级
- B. 四级
- C. 五级
- D. 六级

答案：C 难度：易

解析：

等保2.0将信息系统安全保护等级分为五级：第一级（自主保护级，受到破坏会对公民法人合法权益造成损害）；第二级（指导保护级，损害社会秩序和公共利益）；第三级（监督保护级，严重损害社会秩序和公共利益或国家安全）；第四级（强制保护级，特别严重损害社会秩序和公共利益或国家安全）；第五级（专控保护级，特别严重损害国家安全）。

20. 违反《网络安全法》的规定，未经用户同意收集个人信息的，最高可处罚款多少？

- A. 一万元
- B. 五万元
- C. 十万元
- D. 一百万元

答案：D 难度：中

解析：

《网络安全法》第六十四条规定，违反第四十一条规定收集使用个人信息的，由有关主管部门责令改正，可以根据情节单处或并处警告、没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得的处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。情节严重的可责令停业整顿、关闭网站、吊销许可证。

第三章 信息安全管理（共17题）

21. 信息安全管理（ISMS）的核心标准是？

- A. ISO/IEC 27001
- B. ISO/IEC 27002
- C. ISO/IEC 27005
- D. ISO/IEC 27006

答案：A 难度：易

解析：

ISO/IEC

27001是信息安全管理（ISMS）的要求标准，定义了建立、实施、运行、监视、评审、保持和改进ISMS的规范要求，是ISMS认证审核的依据。ISO/IEC

27002是信息安全控制措施的实践指南（原133个控制措施，2013版缩减为114个，2022版重组为93个）；ISO/IEC

27005是信息安全风险管理指南；ISO/IEC 27006是认证机构要求。

22. PDCA循环中“Check”（检查）阶段的主要工作是？

- A. 制定信息安全策略和目标
- B. 实施安全控制措施
- C. 评估安全措施的有效性和符合性
- D. 采取纠正措施持续改进

答案：C 难度：易

解析：

PDCA循环四个阶段：Plan（计划）——制定信息安全策略、目标和风险管理方案；Do（实施）——执行安全控制措施和流程；Check（检查）——通过内部审核、管理评审、绩效测量等手段评估安全措施的有效性和符合性；Act（改进）——根据检查结果采取纠正和预防措施，持续改进ISMS。Check阶段的核心是验证实施效果是否达到预期目标。

23. ISO 27001标准中ISMS的PDCA循环中，“Do”阶段不包含以下哪项？

- A. 风险评估
- B. 风险处置
- C. 内部审核
- D. 实施风险处置计划

答案：C 难度：中

解析：

在ISO

27001的PDCA框架中：Plan阶段包括建立ISMS范围、信息安全策略、风险评估方法等；Do阶段包括实施风险处置计划、实施选定的控制措施、开展培训和教育等；Check阶段包括管理评审、内部审核、ISMS有效性测量等；Act阶段包括纠正措施、预防措施和持续改进。内部审核属于Check阶段而非Do阶段。

24. 构成信息安全风险的三个关键要素是？

- A. 人员、流程、技术

- B. 资产、威胁、脆弱性
- C. 攻击、防御、恢复
- D. 硬件、软件、数据

答案：B 难度：易

解析：

信息安全风险评估的基本要素是资产、威胁和脆弱性（漏洞/弱点）。资产是组织需要保护的信息及其支撑设施；威胁是可能对资产造成损害的潜在原因；脆弱性是资产或其防护措施中可被威胁利用的弱点。风险值=威胁发生的可能性 x 脆弱性被利用的可能性 x 资产价值。风险处置策略包括风险规避、风险降低、风险转移和风险接受。

25. 风险处置的四种策略是？

- A. 规避、降低、转移、接受
- B. 消除、控制、转移、忽略
- C. 预防、检测、响应、恢复
- D. 避免、减轻、保险、忽略

答案：A 难度：易

解析：

风险处置的四种基本策略：1）风险规避（Risk Avoidance）——通过消除风险源或停止产生风险的活动来消除风险，如关闭不必要的服务；2）风险降低（Risk Mitigation/Reduction）——通过安全控制措施降低风险到可接受水平，如部署防火墙和IDS；3）风险转移（Risk Transfer）——将风险的后果转移给第三方，如购买网络安全保险或外包安全运维；4）风险接受（Risk Acceptance）——在评估后决定不采取额外措施，接受残余风险。

26. 在信息安全风险评估中，以下哪个不属于应识别的信息资产？

- A. 网络设备
- B. 客户资料
- C. 办公桌椅
- D. 系统管理员

答案：C 难度：易

解析：

信息资产识别应关注与业务和信息系统相关的资产，包括：硬件资产（服务器、网络设备、存储设备）、软件资产（操作系统、应用软件、数据库）、数据资产（客户资料、财务数据、业务文档）、人员资产（系统管理员、关键技术人员）、服务资产（网络服务、数据处理服务）。办公桌椅不属于信息资产，属于普通固定资产。

27. 信息安全策略的制定者应当是？

- A. IT部门负责人
- B. 组织的高级管理层
- C. 安全工程师
- D. 外部咨询机构

答案：B 难度：易

解析：

信息安全策略（方针）应由组织的高级管理层正式制定和发布，体现管理层对信息安全目标和方向承诺。信息安全策略是ISMS的顶层文件，明确了组织的信息安全总体目标、原则和方向，为后续制定具体的标准、流程和程序提供框架。虽然具体起草可能由安全部门执行，但审批和发布必须由高层管理者进行，确保权威性和有效性。

28. 信息安全文件的层次结构中，处于最顶层的是？

- A. 具体操作规程

- B. 信息安全策略
- C. 各项管理制度
- D. 记录和表单

答案：B 难度：易

解析：

ISMS文件体系通常分为四个层次（四层文件体系）：第一层——信息安全策略（方针），是顶层文件，阐述总体方向和原则；第二层——各项管理制度和标准，规定具体管理要求；第三层——操作规程和指南，指导具体操作实施；第四层——记录和表单，作为执行证据。策略在最顶层，为整个体系提供指导框架。

29. 企业在建立ISMS时，以下哪个不是关键成功因素？

- A. 来自高级管理层的明确支持和承诺
- B. 全体员工的参与
- C. 仅依赖IT部门的技术人员
- D. 员工安全意识培训和教育

答案：C 难度：易

解析：

ISMS建设的关键成功因素包括：1）高级管理层的明确支持和承诺（最高管理层推动）；2）全体员工参与（不仅是IT部门，而是所有部门所有人员）；3）对企业员工提供安全意识和技能培训教育；4）所有管理者、员工及合作伙伴理解并遵照执行安全策略。仅依赖IT部门是常见误区，信息安全管理是全员参与的工作。

30. 以下关于风险管理中“残余风险”的描述，正确的是？

- A. 残余风险是实施安全措施后仍然存在的风险
- B. 残余风险可以被完全消除
- C. 残余风险不需要关注
- D. 残余风险仅来自外部威胁

答案：A 难度：中

解析：

残余风险（Residual

Risk）是指在实施风险处置措施后仍然存在的风险。残余风险=原始风险-安全措施降低的风险。残余风险不可完全消除，因为安全措施无法覆盖所有威胁和脆弱性，且存在实施成本与效益的平衡。残余风险应由管理层进行评审和接受（风险接受决策），并定期重新评估。

31. ISMS内部审核的目的是？

- A. 发现系统技术漏洞
- B. 验证ISMS是否符合ISO 27001标准要求和组织自身要求
- C. 测试网络安全设备的性能
- D. 进行渗透测试

答案：B 难度：中

解析：

ISMS内部审核（内审）是Check阶段的核心活动，目的是验证ISMS是否符合ISO/IEC

27001标准的要求、符合组织自身的信息安全策略和程序要求、安全控制措施得到有效实施和维护。内审由组织内部经过培训的审核员执行（应独立于被审核区域），通常每年至少进行一次。内审关注的是管理体系的有效性和符合性，而非技术漏洞扫描或渗透测试。

32. ISO 27001中管理评审的输入不包括以下哪项？

- A. 内审和管理评审结果

- B. 风险评估和风险处置状态
- C. 员工个人绩效考核
- D. 纠正措施的状态

答案：C 难度：中

解析：

ISO

27001管理评审的输入包括：1）以往管理评审的跟踪措施；2）ISMS方针、目标和过程的变更；3）信息安全状况反馈（事件、不符合等）；4）风险评估和风险处置状态；5）威胁和脆弱性信息；6）改进建议；7）相关方反馈；8）纠正措施的状态；9）内审和合规性审核结果。员工个人绩效考核不是管理评审的直接输入，虽然安全绩效考核可以作为整体反馈的一部分。

33. 以下哪种风险评估方法属于定量分析方法？

- A. 风险矩阵法
- B. 年度预期损失（ALE）法
- C. 德尔菲法
- D. 头脑风暴法

答案：B 难度：中

解析：

定量风险评估使用数值化数据进行计算，如年度预期损失（ALE）法： $ALE = SLE \times ARO$ （单次损失期望） $\times$ ARO（年度发生频率），通过量化资产价值、威胁频率和损失程度计算风险值。定性分析包括风险矩阵法（将风险按高/中/低等级划分）、德尔菲法（专家意见法）、头脑风暴法等，侧重于描述风险特征而非精确计算。定量方法需要详细数据支持但结果更客观。

34. 信息安全管理体​​系建设中，“范围界定”的主要目的是？

- A. 确定安全预算
- B. 明确ISMS覆盖的组织、系统、流程和物理边界
- C. 确定认证机构
- D. 确定风险评估方法

答案：B 难度：中

解析：

范围界定（Scope

Definition）是ISMS建设的第一步，目的是明确ISMS覆盖的边界，包括：组织边界（哪些部门纳入ISMS范围）、物理边界（哪些办公场所和设施纳入范围）、系统边界（哪些信息系统和网络纳入范围）、流程边界（哪些业务流程纳入范围）。范围界定直接影响后续风险评估、控制措施选择和认证审核的范围。范围过大会增加成本，过小会遗漏关键资产。

35. 信息安全管理中的“最小权限原则”是指？

- A. 每个用户只能访问一个系统
- B. 用户仅获得完成工作任务所需的最小权限
- C. 系统只安装最少数量的软件
- D. 密码长度最短

答案：B 难度：易

解析：

最小权限原则（Principle of Least Privilege）要求每个用户、进程或系统仅获得完成其合法任务所需的最小权限集合，不多给任何多余权限。该原则是访问控制的核心原则之一，可有效降低权限滥用和内部威胁风险。实施方式包括：基于角色的访问控制（RBAC）、权限定期审查、临时权限到期回收、特权账户管理等。

36. 信息安全事件管理的标准流程顺序是？

- A. 准备→检测→遏制→根除→恢复→总结
- B. 检测→准备→恢复→遏制→根除→总结
- C. 准备→恢复→检测→遏制→根除→总结
- D. 检测→遏制→准备→根除→恢复→总结

答案：A 难度：易

解析：

信息安全事件管理遵循PDCERF模型，六个阶段依次为：1) Preparation（准备）——建立应急响应团队、预案和工具；2) Detection（检测）——发现和确认安全事件；3) Containment（遏制）——限制事件影响范围；4) Eradication（根除）——消除事件根因；5) Recovery（恢复）——恢复系统正常运行；6) Follow-up（总结）——总结经验教训，改进防护措施。

37. 根据ISO 27001，以下哪个角色负责ISMS的整体实施和运行？

- A. 内部审核员
- B. 信息安全管理者代表（CISO/安全负责人）
- C. 外部认证机构
- D. IT运维人员

答案：B 难度：中

解析：

ISO

27001要求组织指定管理层成员（通常为CISO或信息安全负责人/管理者代表）负责ISMS的整体建立、实施、运行、监视、评审和改进。该角色负责向最高管理层报告ISMS绩效、协调风险评估和风险处置、推动安全意识培训、管理内部审核和管理评审。内部审核员负责执行审核但不负责ISMS整体运行；外部认证机构负责认证审核不参与日常运行。

第四章 业务连续性（共10题）

38. RTO（恢复时间目标）的含义是？

- A. 系统故障后数据丢失的最大容忍量
- B. 系统中断后恢复业务运行所需的最长时间
- C. 数据备份的频率
- D. 灾难恢复的预算

答案：B 难度：易

解析：

RTO（Recovery Time Objective，恢复时间目标）是指系统或业务中断后，必须恢复服务运行的最长可容忍时间。RTO关注的是“多快能恢复”——从系统中断到服务恢复的时间窗口。RTO越短意味着需要更快的恢复方案（如热备站），成本也越高。例如RTO=4小时意味着系统必须在故障后4小时内恢复运行。

39. RPO（恢复点目标）的含义是？

- A. 系统恢复运行所需的时间
- B. 允许丢失的最大数据量（以时间衡量）
- C. 数据恢复的物理位置
- D. 备份策略的名称

答案：B 难度：易

解析：

RPO（Recovery Point Objective，恢复点目标）是指在系统或业务中断时允许丢失的最大数据量，以时间单位衡量。RPO关注的是“能容忍丢失多少数据”——从最后一次备份到故障发生之间的时间。RPO=0意味着不能丢失任何数据（需要实时同步）；RPO=24小时意味着最多容忍丢失最近24小时的数据，需要每天备份。

40. BCP（业务连续性计划）与DRP（灾难恢复计划）的主要区别是？

- A. BCP关注技术恢复，DRP关注管理流程
- B. BCP关注业务层面的连续性，DRP关注IT系统的灾难恢复
- C. 两者完全相同
- D. BCP仅适用于自然灾害

答案：B 难度：中

解析：

BCP（Business Continuity Plan）从业务层面出发，确保在灾难或重大中断期间关键业务流程能够持续或快速恢复，涵盖人员、设施、供应商等非IT要素。DRP（Disaster Recovery Plan）是BCP的子集，聚焦IT基础设施和系统的灾难恢复，包括数据备份、备用数据中心、系统切换等技术方案。简言之：BCP关注“业务怎么继续”，DRP关注“系统怎么恢复”。

41. 灾难恢复中，热站（Hot Site）的特点是？

- A. 仅提供场地，无设备和数据
- B. 有设备和网络但不实时同步数据
- C. 设备齐全且数据实时同步，可立即接管
- D. 不需要任何设备

答案：C 难度：中

解析：

灾难恢复站点分为三类：1) 热站 (Hot Site) —— 配备完整的硬件设备、网络连接和软件环境，数据实时同步，灾难发生时可在最短时间内 (分钟级到小时级) 接管业务运行，成本最高；2) 温站 (Warm Site) —— 有设备和网络但数据非实时同步，恢复时间中等 (小时级到天级)，成本适中；3) 冷站 (Cold Site) —— 仅提供场地和基本设施，无设备和数据，恢复时间最长 (天级到周级)，成本最低。

42. 业务影响分析 (BIA) 的主要目的是？

- A. 评估员工满意度
- B. 识别关键业务流程，分析中断影响，确定RTO和RPO
- C. 进行渗透测试
- D. 评估网络安全设备性能

答案：B 难度：中

解析：

BIA (Business Impact Analysis, 业务影响分析) 是BCP的核心步骤，主要目的包括：1) 识别组织的关键业务流程和支持性资源；2) 分析业务中断对组织的财务、运营、法律和声誉影响；3) 确定每个关键业务流程的RTO (恢复时间目标) 和RPO (恢复点目标)；4) 确定业务恢复的优先级顺序。BIA结果为后续制定BCP和DRP提供基础数据，帮助组织合理分配恢复资源。

43. 应急响应PDCERF模型中，“根除” (Eradication) 阶段的主要工作是？

- A. 建立应急响应团队和预案
- B. 发现和确认安全事件
- C. 限制事件影响范围
- D. 彻底消除安全事件的根本原因

答案：D 难度：易

解析：

PDCERF模型六个阶段：Preparation (准备) 建立团队能力；Detection (检测) 发现确认事件；Containment (遏制) 限制影响范围 (如隔离受感染主机)；Eradication (根除) 彻底消除事件根本原因 (如清除恶意代码、修补漏洞、关闭后门)；Recovery (恢复) 恢复系统正常运行 (如从备份恢复数据、验证系统完整性)；Follow-up (总结) 编写事件报告、总结经验教训。根除阶段的关键是消除威胁源头防止复发。

44. 以下哪种备份策略在恢复时需要的时间最短？

- A. 全量备份
- B. 增量备份
- C. 差异备份
- D. 完全备份+增量备份组合

答案：A 难度：中

解析：

备份策略对比：1) 全量备份 —— 每次备份所有数据，恢复时只需一份备份即可，恢复时间最短，但备份耗时长且占用空间大；2) 增量备份 —— 仅备份上次备份后变化的数据，备份速度快、空间小，但恢复时需全量+所有增量备份依次恢复，恢复时间最长；3) 差异备份 —— 备份上次全量备份后所有变化的数据，恢复需全量+最近一次差异备份，恢复时间居中。

从恢复速度看：全量最快，差异次之，增量最慢。

45. 以下关于计算机取证原则的描述，错误的是？

- A. 取证过程中应保持证据链的完整性
- B. 取证应在不改变原始证据的前提下进行
- C. 取证人员可以随意修改证据以便分析
- D. 取证过程应有详细记录和文档

答案：C 难度：中

解析：

计算机取证的基本原则：1）证据完整性——确保证据在收集、传输、存储过程中不被篡改，使用哈希值验证证据完整性；2）最小改动原则——在不改变原始证据的前提下进行分析，对原始存储介质做比特级镜像后再分析；3）证据链（监管链）——记录证据从收集到呈堂的完整流转过程，确保每个环节可追溯；4）文档化——全程详细记录操作步骤、时间、人员和工具。随意修改证据会破坏证据的合法性和可信度。

46. 在灾难恢复中，“同城双活”模式的优势是？

- A. 成本最低
- B. 两个数据中心同时提供服务，数据零丢失，故障自动切换
- C. 仅适用于小型企业
- D. 恢复时间长

答案：B 难度：中

解析：

同城双活是指两个数据中心在同一城市同时运行业务，数据实时同步。优势：RPO≈0（数据零丢失）、RTO≈0（业务无感知切换）、两个中心都承载业务不浪费资源。劣势是建设成本高、要求两个数据中心距离适中（通常相距30-100公里以兼顾延迟和灾难隔离）。相比之下，主备模式（Active-Standby）成本较低但存在资源闲置；两地三中心模式在异地增加灾备中心可应对大范围灾难。

47. BCM（业务连续性管理）体系的基础是？

- A. 灾难恢复技术
- B. 业务连续性策略和BCM项目启动
- C. 数据备份方案
- D. 安全设备部署

答案：B 难度：中

解析：

BCM体系的建设遵循PDCA循环，其基础阶段包括：1）BCM策略制定——明确BCM的目标、范围和原则，获得管理层授权和承诺；2）项目启动和管理——建立BCM组织架构、分配角色和职责、制定项目计划。在此基础上进行BIA（业务影响分析）和风险评估，然后制定BCP和DRP，最后通过演练和测试验证有效性。技术和设备是支撑手段，策略和管理是BCM体系的基础。

第五章 安全工程与运营（共12题）

48. SSE-CMM（系统安全工程能力成熟度模型）将能力分为几个等级？

- A. 3个
- B. 4个
- C. 5个
- D. 6个

答案：C 难度：中

解析：

SSE-CMM将安全工程能力成熟度分为5个等级：1级——非正式执行级（不能重复过程）；2级——计划和跟踪级（可规划但不可预测）；3级——充分定义级（过程已标准化并可重复）；4级——量化控制级（过程可测量和量化管理）；5级——持续改进级（基于数据持续优化过程）。SSE-CMM还定义了11个安全工程过程域（如评估威胁、评估脆弱性、评估风险等）和11个项目/组织过程域。

49. 安全运营中心（SOC）的核心功能不包括？

- A. 安全事件监控和告警
- B. 安全日志集中收集和分析
- C. 直接修改业务系统代码
- D. 安全事件响应和处置协调

答案：C 难度：易

解析：

SOC（Security Operations Center）的核心功能包括：1）安全事件监控——7x24小时监控安全告警和异常行为；2）日志集中收集和分析——聚合防火墙、IDS/IPS、EDR、WAF等设备日志进行关联分析；3）威胁情报集成——结合威胁情报识别攻击行为；4）事件响应协调——对接安全事件进行分级、分诊和处置协调；5）安全态势感知——可视化展示整体安全态势。SOC不直接修改业务系统代码，这是开发团队和安全代码审计团队的职责。

50. SDL（安全开发生命周期）中，威胁建模应在哪个阶段进行？

- A. 需求分析阶段
- B. 设计阶段
- C. 编码阶段
- D. 测试阶段

答案：B 难度：中

解析：

在SDL（Security Development Lifecycle）中，威胁建模（Threat Modeling）在设计阶段进行。威胁建模基于架构和设计文档，使用STRIDE等方法分析系统面临的威胁（Spoofing身份欺骗、Tampering数据篡改、Repudiation否认、Information Disclosure信息泄露、Denial of Service拒绝服务、Elevation of Privilege权限提升），在设计阶段识别威胁并制定防护方案，避免在编码或测试阶段才发现架构级安全问题，降低修复成本。

51. 社会工程学攻击的核心特点是？

- A. 利用技术漏洞
- B. 利用人性弱点而非技术手段
- C. 仅通过邮件发起
- D. 需要高级编程技能

答案：B 难度：易

解析：

社会工程学（Social

Engineering）攻击的核心是利用人性弱点（信任、好奇心、恐惧、贪婪、权威服从等）而非技术手段获取信息或访问权限。常见手法包括钓鱼邮件（Phishing）、鱼叉式钓鱼（Spear

Phishing）、电话诈骗（Vishing）、物理尾随、诱饵攻击（USB投放）等。防御手段主要是安全意识培训和教育，技术防护（邮件过滤、MFA）是辅助手段。

52. 安全运营中的“事件分级”通常依据什么进行？

- A. 事件发生时间
- B. 事件对业务的影响程度和紧急程度
- C. 报告人的级别
- D. 受影响系统的品牌

答案：B 难度：易

解析：

安全事件分级主要依据事件对业务的影响程度（如数据泄露量、系统停机时长、受影响用户数）和紧急程度（是否正在发生、是否持续扩散）进行。常见分级方式：P1/紧急——严重影响核心业务，需立即响应；P2/高——影响重要业务，需快速响应；P3/中——影响有限，需及时处理；P4/低——影响轻微，可计划处理。分级决定了响应资源的调配和升级机制。

53. 以下关于内容安全的描述，错误的是？

- A. 内容安全包括数字版权管理
- B. 内容安全涉及网络舆情监控
- C. 内容安全仅关注文本内容
- D. 内容安全包括信息保护和过滤

答案：C 难度：中

解析：

内容安全涵盖多个维度：1）数字版权管理（DRM）——保护数字内容的版权，防止未经授权复制和分发；2）信息保护——对敏感信息进行分类、标记和保护，防止泄露；3）网络舆情监控——监测网络舆论动态，识别负面舆情和有害信息传播；4）内容过滤——对网络内容进行审查和过滤，阻断违法有害信息。内容安全不仅关注文本，还包括图片、视频、音频等多媒体内容的安全管理。

54. STRIDE威胁建模框架中，“T”代表什么？

- A. Trust（信任）
- B. Tampering（篡改）
- C. Threat（威胁）
- D. Testing（测试）

答案：B 难度：中

解析：

STRIDE是微软提出的威胁建模框架，六个字母分别代表六类威胁：S——Spoofing（身份欺骗/伪装）；T——Tampering（数据篡改）；R——Repudiation（否认/抵赖）；I——Information Disclosure（信息泄露）；D——Denial of Service（拒绝服务）；E——Elevation of

Privilege（权限提升）。STRIDE框架帮助在设计阶段系统性识别系统面临的各类威胁，并对应到CIA等安全属性进行防护设计。

55. 在安全运营中，SIEM系统的主要作用是？

- A. 部署防火墙规则
- B. 收集、关联和分析安全日志，提供告警和报告
- C. 进行渗透测试
- D. 管理员工密码

答案：B 难度：中

解析：

SIEM（Security Information and Event Management，安全信息和事件管理）系统的核心作用：1）日志收集——从防火墙、IDS/IPS、服务器、应用等多源收集安全日志；2）关联分析——通过预定义规则和关联引擎发现跨设备的攻击行为模式；3）实时告警——检测到可疑行为时发出告警；4）合规报告——生成合规审计所需的报表；5）威胁狩猎——支持安全分析师主动搜索威胁。SIEM不直接部署防火墙规则或执行渗透测试，而是提供安全态势感知和分析能力。

56. 安全意识培训的对象应当是？

- A. 仅IT部门员工
- B. 仅安全团队
- C. 全体员工
- D. 仅新入职员工

答案：C 难度：易

解析：

安全意识培训的对象是组织全体员工，因为人是安全防线中最薄弱的环节。社会工程学攻击、钓鱼邮件、弱密码等威胁可影响任何员工，不限IT部门。培训内容应分层定制：普通员工——基础安全意识（密码安全、钓鱼识别、数据保护）；IT人员——安全开发和运维规范；管理层——安全治理和合规要求。培训应定期进行（至少每年一次），配合模拟钓鱼测试验证效果。

57. DevSecOps的核心理念是？

- A. 安全应在开发完成后统一处理
- B. 将安全实践集成到开发流程中，实现安全左移
- C. 仅由安全团队负责安全
- D. 安全会拖慢开发效率，应尽量减少

答案：B 难度：中

解析：

DevSecOps的核心是“安全左移”（Shift Left Security），将安全实践集成到DevOps开发流程的每个阶段：需求和设计阶段进行威胁建模；编码阶段使用安全编码规范和IDE插件；CI阶段进行SAST（静态代码分析）和SCA（组件分析）；CD阶段进行DAST（动态测试）；运行时部署RASP和EDR。核心理念是“安全是每个人的责任”（Security is everyone's responsibility），通过自动化工具集成实现安全不阻塞开发流程。

58. 零信任安全架构的核心原则是？

- A. 信任内网，不信任外网
- B. 从不信任，始终验证
- C. 一次认证，永久信任
- D. 仅使用防火墙进行隔离

答案：B 难度：中

解析：

零信任（Zero Trust）的核心原则是“从不信任，始终验证”（Never Trust, Always Verify）。传统边界安全模型信任内网内部流量，零信任认为内网和外部网络一样不可信，所有访问请求无论来源都需进行身份验证和授权。零信任架构要素：1）身份作为访问控制基础（IdP认证）；2）设备健康检查；3）最小权限；4）微隔离（基于身份而非IP的细粒度访问控制）；5）持续监控和动态信任评估。

59. SOC的运行模式中，Tier 1分析师的主要职责是？

- A. 进行深度事件调查和取证
- B. 对告警进行初步分诊和过滤
- C. 制定安全策略
- D. 管理安全设备采购

答案：B 难度：中

解析：

SOC通常采用分层运行模式：Tier

1（一线分析师）——对安全告警进行初步分诊（Triage），过滤误报，对确认事件进行分级和路由；Tier

2（二线分析师）——对复杂事件进行深入调查、取证分析和威胁狩猎；Tier

3（三线分析师/高级分析师）——处理重大安全事件、进行高级威胁分析、改进检测规则和流程。Tier

1是SOC的“第一道防线”，快速筛选大量告警，将真正需要关注的事件升级给Tier 2。

第六章 安全评估（共12题）

60. TCSEC（可信计算机系统评估准则）将系统安全分为几个等级？

- A. 3个
- B. 4个
- C. 5个
- D. 7个

答案：B 难度：中

解析：

TCSEC（橙皮书）将系统安全分为4个等级7个子级：D（最小保护）、C1（自主安全保护）、C2（受控访问保护）、B1（标识安全保护）、B2（结构化保护）、B3（安全域）、A1（验证设计）。D级最低无安全要求，A1最高要求形式化验证。TCS EC由美国国防部于1985年发布，是第一个计算机安全评估标准，已被国际通用准则CC取代。

61. CC（通用准则）评估中，PP（保护轮廓）的作用是？

- A. 描述具体产品的安全功能
- B. 对一类TOE的安全需求进行与技术实现无关的描述
- C. 评估结论报告
- D. 评估方法说明

答案：B 难度：中

解析：

CC（Common Criteria, ISO/IEC 15408）中的核心概念：PP（Protection Profile, 保护轮廓）是对某一类评估对象（TOE）的安全需求描述，与技术实现无关，是用户需求层面的文档，定义了该类产品应满足的安全功能要求（SFR）和安全保证要求（SAR）。ST（Security Target, 安全目标）描述具体产品的安全需求，是PP的实现。TOE（Target of Evaluation）是被评估的产品或系统。EAL（评估保证级）是保证要求的等级。

62. 信息安全风险评估中，风险值的基本计算公式是？

- A. 风险 = 资产价值 x 威胁频率
- B. 风险 = 威胁可能性 x 脆弱性严重程度 x 资产价值
- C. 风险 = 资产数量 x 威胁数量
- D. 风险 = 漏洞数量 x 攻击次数

答案：B 难度：中

解析：

风险评估的基本公式：风险值 = 威胁发生的可能性 x 脆弱性被利用的可能性（严重程度） x 资产价值。三个要素缺一不可：仅有威胁无脆弱性不构成风险（无漏洞可利用），仅有脆弱性无威胁也不构成风险（无人利用），资产价值决定了风险的影响程度。定性评估时通常使用风险矩阵（高/中/低等级组合），定量评估时使用具体数值计算。

63. 渗透测试与漏洞扫描的主要区别是？

- A. 渗透测试使用工具，漏洞扫描不使用

- B. 渗透测试深度验证漏洞并评估实际影响，漏洞扫描批量发现已知漏洞
- C. 两者完全相同
- D. 漏洞扫描比渗透测试更深入

答案：B 难度：易

解析：

漏洞扫描是自动化过程，使用扫描工具按特征库批量检测已知漏洞，覆盖面广但误报率高，无法发现逻辑漏洞和未知漏洞。渗透测试是人工驱动的过程，在漏洞扫描基础上进行深度验证和利用，能发现业务逻辑漏洞、权限绕过等复杂问题，并评估漏洞的实际影响和利用链。简言之：漏洞扫描告诉你“有什么漏洞”，渗透测试告诉你“漏洞能造成什么危害”。

64. 等级保护测评的结论分为几种？

- A. 2种
- B. 3种
- C. 4种
- D. 5种

答案：C 难度：中

解析：

等保测评结论分为四种：1）优——不存在安全问题或仅存在低风险问题，所有高风险和中风险问题均已整改；2）良——存在少量中风险问题但无高风险问题，整体安全状况良好；3）中——存在中风险问题但无高风险问题，需限期整改；4）差——存在高风险安全问题，需立即整改。测评结论由具有资质的第三方测评机构出具，测评报告是等保合规的重要证明文件。

65. 在信息安全审计中，审计证据的充分性主要取决于？

- A. 审计人员的数量
- B. 审计证据的数量和质量
- C. 审计时间长短
- D. 审计预算多少

答案：B 难度：中

解析：

审计证据的充分性取决于审计证据的数量和质量。数量方面——收集足够多的证据样本以确保覆盖面；质量方面——证据应具有相关性（与审计目标相关）、可靠性（来源可信、未经篡改）和时效性（反映当前状态）。审计人员需要在充分性和成本之间取得平衡，采用风险导向审计方法，对高风险领域收集更多证据。审计证据类型包括文档审查、访谈记录、系统日志、配置检查记录等。

66. IT审计中，“合规性审计”的主要目标是？

- A. 发现系统技术漏洞
- B. 验证IT系统是否符合法律法规、标准和内部策略的要求
- C. 测试系统性能
- D. 评估员工技能水平

答案：B 难度：中

解析：

合规性审计的主要目标是验证组织的IT系统和管理实践是否符合适用的法律法规（如《网络安全法》《数据安全法》）、行业标准（如PCI-DSS、ISO

27001）和内部安全策略的要求。合规性审计关注“是否按规定执行”，而非技术漏洞发现。审计内容包括安全策略执行情况、访问控制合规性、日志留存合规性、数据保护措施落实情况等。技术漏洞扫描属于安全评估而非合规性审计范畴。

67. 以下哪个不属于信息安全风险评估的途径？

- A. 基于资产的风险评估
- B. 基于攻击模拟的风险评估
- C. 基于员工绩效考核的风险评估
- D. 基于场景的风险评估

答案：C 难度：中

解析：

风险评估的主要途径包括：1) 基于资产的风险评估——以资产为切入点分析资产面临的威胁和脆弱性；2) 基于攻击模拟的风险评估——通过模拟攻击者行为路径分析风险；3) 基于场景的风险评估——构建典型风险场景分析影响。基于员工绩效考核不是风险评估途径，虽然人员安全意识和能力是风险因素之一，但绩效考核本身不是风险评估方法。

68. 渗透测试报告中，执行摘要（Executive Summary）的读者主要是？

- A. 技术工程师
- B. 管理层和高管
- C. 开发人员
- D. 安全分析师

答案：B 难度：易

解析：

渗透测试报告中的执行摘要面向管理层和高管的概述，使用非技术语言总结测试范围、主要发现、高风险漏洞汇总和总体安全评价。执行摘要帮助管理层快速了解安全态势、做出修复优先级决策和资源分配。报告的技术详情部分才是面向技术团队的，包含漏洞技术描述、复现步骤、PoC证据和具体修复方案。

69. CVSS（通用漏洞评分系统）3.1版中，最高分（严重）的范围是？

- A. 7.0-8.9
- B. 8.0-9.9
- C. 9.0-10.0
- D. 8.0-10.0

答案：C 难度：中

解析：

CVSS

3.1版将漏洞严重程度分为四个等级：低（Low, 0.1-3.9）、中（Medium, 4.0-6.9）、高（High, 7.0-8.9）、严重（Critical, 9.0-10.0）。CVSS基础评分通过攻击向量、攻击复杂度、所需权限、用户交互、影响范围以及CIA三性影响等维度计算。CVSS还包含时间评分（考虑补丁可用性、利用成熟度等时间因素）和环境评分（根据组织特定环境调整）。

70. 代码审计中，SAST（静态应用安全测试）的主要特点是？

- A. 需要运行程序才能检测漏洞
- B. 在不运行程序的情况下分析源代码或字节码
- C. 仅能发现运行时漏洞
- D. 必须在生产环境中执行

答案：B 难度：中

解析：

SAST (Static Application Security Testing) 在不运行程序的情况下，通过分析源代码、字节码或二进制文件检测安全漏洞。特点：1) 可在开发早期阶段使用（编码阶段即可检测）；2) 覆盖率高能发现已知的代码模式漏洞（如SQL注入、XSS、硬编码密码）；3) 误报率较高需要人工确认；4) 无法发现运行时漏洞和配置问题。DAST（动态应用安全测试）在程序运行时检测，能发现运行时漏洞但覆盖率有限。两者互补使用效果最佳。

71. 在等保2.0中，“一个中心三重防护”的三重防护是指？

- A. 防火墙、IDS、VPN
- B. 安全通信网络、安全区域边界、安全计算环境
- C. 物理安全、网络安全、应用安全
- D. 边界防护、内部防护、终端防护

答案：B 难度：中

解析：

等保2.0的“一个中心三重防护”安全架构：一个中心——安全管理中心（集中管控安全策略、统一管理安全设备和审计日志）；三重防护——1）安全通信网络（网络架构安全、通信传输安全、可信接入）；2）安全区域边界（边界防护、访问控制、入侵防范、恶意代码防范）；3）安全计算环境（身份鉴别、访问控制、安全审计、入侵防范、数据完整性和保密性保护）。该架构体现了纵深防御理念。

第七章 信息安全支撑技术（共8题）

72. 以下哪种加密算法属于对称加密算法？

- A. RSA
- B. AES
- C. ECC
- D. DSA

答案：B 难度：易

解析：

对称加密算法使用同一密钥进行加密和解密，特点是速度快、适合大量数据加密。常见对称算法：AES（高级加密标准，密钥长度128/192/256位）、DES（数据加密标准，已不安全）、3DES（三重DES）、SM4（国密对称算法）。非对称加密使用公钥/私钥对，特点是安全性高但速度慢，常见：RSA、ECC（椭圆曲线）、DSA、SM2（国密非对称算法）。

73. 数字签名的主要作用不包括以下哪项？

- A. 保证信息完整性
- B. 提供不可否认性
- C. 验证发送者身份
- D. 保证信息保密性

答案：D 难度：易

解析：

数字签名使用发送方的私钥对消息摘要进行加密，主要功能：1）身份认证——验证消息确实来自声称的发送者；2）完整性——通过摘要验证消息未被篡改；3）不可否认性（抗抵赖）——发送方不能否认其签名行为。数字签名不能保证信息保密性，保密性需要通过加密实现。在实际应用中，通常先签名再加密（或同时使用）以同时实现保密性和不可否认性。

74. PKI（公钥基础设施）的核心组件不包括？

- A. CA（证书颁发机构）
- B. RA（注册机构）
- C. CRL（证书吊销列表）
- D. IDS（入侵检测系统）

答案：D 难度：中

解析：

PKI的核心组件包括：1）CA（Certificate Authority，证书颁发机构）——签发和管理数字证书；2）RA（Registration Authority，注册机构）——受理证书申请和身份验证；3）CRL/OCSP——证书吊销列表或在线证书状态协议，用于验证证书是否有效；4）证书库——存储和发布数字证书；5）密钥管理——密钥生成、备份和恢复。IDS（入侵检测系统）是网络安全设备，不属于PKI组件。

75. 以下关于Kerberos认证协议的描述，正确的是？

- A. Kerberos使用对称加密进行认证
- B. Kerberos使用非对称加密进行认证
- C. Kerberos不需要密钥分发中心

D. Kerberos仅适用于单机环境

答案：A 难度：中

解析：

Kerberos是MIT开发的网络认证协议，使用对称加密（而非非对称加密）进行认证。核心组件：1）KDC（密钥分发中心）——包括AS（认证服务器）和TGS（票据授予服务器）；2）认证流程：客户端向AS请求TGT（票据授予票据），再持TGT向TGS请求服务票据（TGS Ticket），最后用服务票据访问目标服务。Kerberos通过票据机制实现单点登录（SSO），票据有时间限制可防止重放攻击。Kerberos v5使用AES加密。

76. 基于角色的访问控制（RBAC）中，权限分配的基本流程是？

- A. 用户→权限
- B. 用户→角色→权限
- C. 用户→资源
- D. 角色→用户

答案：B 难度：中

解析：

RBAC（Role-Based Access Control）通过角色作为中间层连接用户和权限：1）管理员定义角色并分配权限给角色（角色→权限映射）；2）将用户分配到角色中（用户→角色映射）；3）用户通过角色间接获得权限。RBAC的优势：简化权限管理（只需管理角色而非每个用户）、支持职责分离（SoD约束）、便于组织结构变动时的权限调整。RBAC模型包括基本RBAC、层次RBAC（支持角色继承）、约束RBAC（支持职责分离约束）。

77. 自主访问控制（DAC）的特点是？

- A. 由系统强制执行安全标签
- B. 资源所有者可以自主决定其他用户的访问权限
- C. 所有人具有相同权限
- D. 仅管理员可以分配权限

答案：B 难度：中

解析：

DAC（Discretionary Access Control，自主访问控制）的核心特点是资源的所有者（创建者）可以自主决定将资源的访问权限授予其他用户。DAC基于用户身份和访问控制列表（ACL）实现，灵活性高但安全性相对较低——用户可能不当授权导致信息泄露。MAC（强制访问控制）由系统强制执行安全标签（如机密/秘密/公开），用户不能自行更改权限，安全性更高但灵活性低。RBAC（基于角色的访问控制）介于两者之间。

78. 国密算法SM2属于哪种类型的加密算法？

- A. 对称加密
- B. 非对称加密（公钥加密）
- C. 哈希算法
- D. 流密码

答案：B 难度：中

解析：

国密算法体系：1）SM2——非对称加密算法（椭圆曲线公钥密码算法），用于数字签名、密钥交换和公钥加密，对标RSA/ECC；2）SM3——密码杂凑算法（哈希函数），输出256位摘要，对标SHA-256；3）SM4——分组对称加密算法，密钥长度128位，对标AES；4）SM9——标识密码算法（基于标识的非对称密码算法）。国密算法已在金融、政务等领域广泛推广，等保2.0要求关键信息基础设施优先使用国密算法。

79. AAA认证框架中的三个A分别代表？

- A. 认证、授权、审计
- B. 认证、访问、审计
- C. 验证、授权、计费
- D. 认证、授权、计费

答案：D 难度：易

解析：

AAA框架：Authentication（认证）——验证用户身份是否合法（“你是谁”）；Authorization（授权）——确定已认证用户可以访问哪些资源和执行哪些操作（“你能做什么”）；Accounting（计费/审计）——记录用户的行为和资源使用情况（“你做了什么”）。常见AAA协议：RADIUS（远程认证拨号用户服务）、TACACS+（终端访问控制器访问控制系统+）。AAA框架广泛应用于网络接入控制、VPN认证和运维审计场景。

第八章 物理与网络通信安全（共8题）

80. 物理安全中，TEMPEST技术主要防范什么？

- A. 物理入侵
- B. 电磁泄漏
- C. 火灾
- D. 水灾

答案：B 难度：中

解析：

TEMPEST (Transient Electromagnetic Pulse Emanation Standard) 技术主要防范电磁泄漏辐射 (EMSEC, 发射安全)。计算机等电子设备在运行过程中会产生电磁辐射, 这些辐射可能被截获并重建显示内容, 导致信息泄露。TEMPEST防护措施包括: 使用低辐射设备、电磁屏蔽 (屏蔽室、屏蔽机箱)、滤波 (电源线和信号线滤波器)、距离防护 (安全隔离距离)、红黑隔离 (处理敏感信息的红网与不处理的黑网物理隔离)。

81. 防火墙的工作模式中, 透明模式的特点是?

- A. 防火墙对网络是可见的, 需要配置IP地址
- B. 防火墙对网络是透明的 (不可见), 工作在二层 (链路层)
- C. 透明模式不需要任何配置
- D. 透明模式仅支持HTTP流量

答案：B 难度：中

解析：

防火墙工作模式: 1) 透明模式 (Transparent/桥接模式) ——防火墙工作在数据链路层 (二层), 无需配置IP地址, 对网络拓扑透明 (即插即用), 适合已建网络中快速部署防火墙而不改变网络结构; 2) 路由模式 ——防火墙工作在网络层 (三层), 配置IP地址并参与路由, 支持NAT, 适合新建网络; 3) 混合模式 ——同时支持透明和路由模式。透明模式的局限是不支持NAT和路由功能。

82. OSI参考模型共有几层?

- A. 5层
- B. 6层
- C. 7层
- D. 8层

答案：C 难度：易

解析：

OSI (开放系统互连) 参考模型由ISO制定, 分为7层 (从下到上): 1) 物理层 ——传输比特流; 2) 数据链路层 ——帧传输和MAC地址寻址; 3) 网络层 ——IP寻址和路由; 4) 传输层 ——端到端连接 (TCP/UDP); 5) 会话层 ——会话管理; 6) 表示层 ——数据格式转换和加密; 7) 应用层 ——网络服务接口。TCP/IP模型简化为4层: 网络接口层、网络层、传输层、应用层。

83. IPSec VPN中, ESP协议提供的功能不包括?

- A. 数据加密
- B. 数据完整性验证
- C. 数据源认证
- D. 反向路由追踪

答案：D 难度：中

解析：

IPSec (Internet Protocol Security) 包含两个主要协议：1) ESP (Encapsulating Security Payload, 封装安全载荷)——提供数据加密、数据完整性验证、数据源认证和防重放攻击服务；2) AH (Authentication Header, 认证头)——提供数据完整性验证、数据源认证和防重放攻击，但不提供加密。IPSec还使用IKE (Internet Key Exchange) 进行密钥交换。反向路由追踪不是IPSec的功能，而是网络诊断技术。

84. IDS与IPS的主要区别是？

- A. IDS检测并阻断，IPS仅检测告警
- B. IDS仅检测告警，IPS检测并阻断
- C. 两者完全相同
- D. IDS是硬件，IPS是软件

答案：B 难度：易

解析：

IDS (Intrusion Detection System, 入侵检测系统)——以旁路 (镜像) 方式部署，仅检测和告警安全威胁，不主动阻断攻击，优点是不影响网络流量；IPS (Intrusion Prevention System, 入侵防御系统)——以串行方式部署，检测到威胁后不仅告警还能主动阻断 (丢弃数据包、重置连接)，优点是实时防护但可能影响正常流量。IPS可视为IDS的增强版，现代NGFW通常集成IPS功能。

85. 以下关于VPN的描述，错误的是？

- A. VPN通过隧道协议在公网上建立安全通信通道
- B. VPN使用加密技术保护数据传输
- C. VPN可以隐藏内部网络的真实IP地址
- D. VPN完全替代了防火墙的功能

答案：D 难度：易

解析：

VPN (Virtual Private Network, 虚拟专用网络) 通过隧道协议 (如IPSec、SSL/TLS、PPTP、L2TP) 在公共网络上建立加密的通信隧道，提供数据保密性、完整性和身份认证。VPN可以隐藏内部网络的真实IP地址 (NAT/隧道封装)。但VPN不替代防火墙的功能——VPN负责安全传输，防火墙负责访问控制和边界防护，两者是互补关系。现代网络安全通常将VPN和防火墙集成部署 (如NGFW内置VPN功能)。

86. WPA3相比WPA2在安全性方面的主要改进是？

- A. 使用更长的加密密钥
- B. 使用SAE协议替代PSK，防止离线字典攻击
- C. 支持更多设备连接
- D. 提高了传输速度

答案：B 难度：中

解析：

WPA3相比WPA2的主要安全改进：1) 使用SAE (Simultaneous Authentication of Equals, 对等同步认证) 协议替代WPA2的PSK (预共享密钥) 四步握手，SAE抵抗离线字典攻击——攻击者无法在离线状态

下暴力破解密码；2）前向保密（Forward Secrecy）——即使密码泄露，之前捕获的加密流量也无法解密；3）WPA3-Personal要求密码长度至少8位（WPA2无强制要求）；4）WPA3-Enterprise提供192位加密套件（政府级安全）。

87. DMZ（非军事区）在网络架构中的主要作用是？

- A. 放置内部机密数据
- B. 放置对外提供服务的服务器，隔离内外网络
- C. 存储备份数据
- D. 作为管理员远程访问入口

答案：B 难度：易

解析：

DMZ（Demilitarized

Zone，非军事区/隔离区）是位于内外网络之间的缓冲区域，用于放置需要对外提供服务的服务器（如Web服务器、邮件服务器、DNS服务器）。DMZ的作用：1）隔离内部网络——外部用户只能访问DMZ中的服务，不能直接访问内部网络；2）降低风险——即使DMZ中服务器被入侵，攻击者仍需突破内部防火墙才能到达内网。DMZ通常通过两道防火墙实现（外部防火墙→DMZ→内部防火墙→内网）或通过防火墙的三网卡实现。

第九章 计算环境安全（共8题）

88. 在Windows系统中，以SYSTEM权限运行的服务存在安全风险是因为？

- A. SYSTEM权限是最低权限
- B. SYSTEM权限是最高权限，服务被入侵后攻击者获得最高控制权
- C. SYSTEM权限无法访问网络
- D. SYSTEM权限无法执行任何操作

答案：B 难度：易

解析：

Windows系统中SYSTEM（LocalSystem）是最高权限账户，比Administrator权限更高。以SYSTEM权限运行的服务一旦被利用（如通过漏洞或权限提升），攻击者将获得系统最高控制权，可以执行任意操作包括安装后门、窃取凭据、禁用安全软件。安全建议：服务应以最小权限账户运行（如Network Service或专用服务账户），避免使用SYSTEM权限，减少被入侵后的影响范围。

89. 以下哪种技术可以有效防止SQL注入攻击？

- A. 使用参数化查询（预编译语句）
- B. 仅在前端进行输入验证
- C. 使用更复杂的SQL语句
- D. 增加数据库密码长度

答案：A 难度：易

解析：

参数化查询（预编译语句）是最有效的SQL注入防护手段。原理：预编译时数据库先解析SQL语句结构（模板），再绑定参数值，参数值仅作为数据处理不会被解析为SQL语法。即使用户输入包含' OR 1=1--等恶意内容，数据库也将其视为普通字符串而非SQL指令。仅在前端验证不可靠（可被绕过）；增加密码复杂度与SQL注入防护无关。其他防护措施还包括：最小权限原则、输入白名单过滤、关闭错误回显、部署WAF等。

90. 跨站脚本攻击（XSS）中，危害最大的类型是？

- A. 反射型XSS
- B. 存储型XSS
- C. DOM型XSS
- D. 基于Cookie的XSS

答案：B 难度：易

解析：

XSS三种类型：1）反射型XSS——恶意脚本来自用户请求参数，服务器反射到响应页面，需用户点击恶意链接触发，一次性的；2）存储型XSS——恶意脚本被永久存储在服务器端（如数据库中的留言/评论），其他用户访问时自动触发，持久化且无需用户点击特定链接，危害最大；3）DOM型XSS——纯客户端JavaScript漏洞，不经过服务器。存储型XSS影响范围广、持续时间长，是危害最大的类型。

91. 恶意代码（Malware）中，蠕虫与病毒的主要区别是？

- A. 蠕虫需要宿主文件，病毒不需要

- B. 蠕虫能自我传播不需要用户干预，病毒需要宿主文件和用户触发
- C. 蠕虫只感染Windows系统
- D. 病毒比蠕虫危害更大

答案：B 难度：中

解析：

病毒（Virus）需要附着在宿主文件（如可执行文件、文档宏）上，需要用户执行受感染的文件才能触发和传播。蠕虫（Worm）是独立程序，不需要宿主文件，能利用网络漏洞或系统弱点自动自我传播，无需用户干预即可大规模扩散（如永恒之蓝蠕虫利用MS17-010漏洞传播）。蠕虫的传播速度通常远快于病毒，因为不需要等待用户行为。木马（Trojan）伪装成合法程序，不自我复制但提供后门。

92. 数据防泄露（DLP）的核心功能是？

- A. 加密所有存储数据
- B. 识别、监控和保护敏感数据，防止其通过未经授权的渠道泄露
- C. 定期备份数据
- D. 防止病毒感染

答案：B 难度：中

解析：

DLP（Data Loss

Prevention，数据防泄露）的核心功能：1）数据发现和分类——识别网络和终端中的敏感数据（如身份证号、信用卡号、商业机密）；2）数据监控——监控敏感数据的使用和传输行为（邮件、USB拷贝、云上传、即时通讯）；3）数据保护——通过阻断、加密、告警等方式防止敏感数据通过未经授权的渠道泄露。DLP分为网络DLP（监控网络传输）、终端DLP（监控终端操作）和存储DLP（扫描存储中的敏感数据）。DLP不替代加密或备份功能。

93. 在Linux系统中，设置文件SUID位的命令是？

- A. chmod u+s filename
- B. chown root filename
- C. chgrp root filename
- D. chmod 644 filename

答案：A 难度：中

解析：

SUID（Set User ID）位使普通用户执行该文件时以文件所有者（通常是root）的权限运行。设置SUID位的命令：chmod u+s filename 或 chmod 4755 filename（4表示SUID）。常见SUID程序如passwd（普通用户执行时以root权限修改/etc/shadow）。SUID是Linux安全审计的重点——如果SUID程序存在命令执行功能（如find -exec、vim的:!command），可能被利用进行权限提升。安全建议：定期审计SUID文件，移除不必要的SUID位。

94. 数据库安全中，视图（View）的主要安全作用是？

- A. 提高查询速度
- B. 实现行/列级访问控制，限制用户只能看到授权的数据
- C. 备份数据
- D. 加密数据

答案：B 难度：中

解析：

数据库视图是一个虚拟表（基于查询结果定义），在安全方面的主要作用是实现行级和列级访问控制：1）列级控制——通过视图只暴露授权列（如隐藏薪水列，只暴露姓名和部门）；2）行级控制——通过WHERE条件限制用户只能看到授权行的数据（如各部门经理只能看到本部门数据）；3）简化权限管理——对用户授权视图的查询权限而非基表权限。视图不

直接提供加密或备份功能，而是作为访问控制的安全机制。

95. Web应用防火墙（WAF）与传统防火墙的主要区别是？

- A. WAF工作在物理层，传统防火墙工作在网络层
- B. WAF深入解析HTTP协议内容，检测和防护Web应用层攻击
- C. WAF比传统防火墙速度更快
- D. 传统防火墙能防御SQL注入

答案：B 难度：中

解析：

传统防火墙工作在网络层和传输层（三层/四层），基于IP地址、端口和协议进行访问控制，无法理解HTTP协议内容，不能防御应用层攻击（如SQL注入、XSS）。WAF工作在应用层（七层），深入解析HTTP请求和响应内容，能检测和防护Web应用安全攻击（SQL注入、XSS、CSRF、文件上传等）。现代NGFW（下一代防火墙）集成了部分WAF功能，但专业WAF在Web应用防护深度上更强。

第十章 软件安全开发（共6题）

96. 安全开发生命周期（SDL）中，安全需求分析应在哪个阶段进行？

- A. 编码阶段
- B. 测试阶段
- C. 需求分析阶段
- D. 部署阶段

答案：C 难度：易

解析：

在SDL中，安全需求分析应在需求分析阶段（项目早期）进行，与功能需求同步识别安全需求。安全需求来源包括：法律法规合规要求（如等保、个人信息保护）、业务安全需求（如用户认证、权限控制）、风险评估结果和历史教训。在需求分析阶段识别安全需求成本最低，到测试或部署阶段才发现安全问题修复成本呈指数级增长（“安全左移”理念的核心依据）。

97. OWASP Top 10中，2021版排名第一的安全风险是？

- A. 注入
- B. 失效访问控制
- C. 敏感数据泄露
- D. 安全配置错误

答案：B 难度：中

解析：

OWASP 2021版Top 10将“失效访问控制”（Broken Access Control）列为第一风险，从2017版的第五位上升。失效访问控制包括越权访问（IDOR、水平/垂直越权）、绕过权限检查等。2017版排名第一的“注入”下降到第三位。2021版的新增风险包括：不安全设计（第4位）、软件和数据完整性缺陷（第8位）、SSRF（第10位）。OWASP Top 10是Web应用安全开发的重要参考。

98. 软件成分分析（SCA）主要解决什么安全问题？

- A. 代码质量问题
- B. 第三方开源组件中的已知漏洞和许可证风险
- C. 开发人员技能评估
- D. 代码风格规范检查

答案：B 难度：中

解析：

SCA（Software Composition Analysis，软件成分分析）通过扫描项目依赖的第三方开源组件（库、框架），识别以下风险：1）已知漏洞——检测组件是否包含已公开的CVE漏洞（如Log4j2的CVE-2021-44228）；2）许可证合规——检查开源许可证类型是否符合组织策略（如GPL许可证可能影响商业产品）；3）组件版本管理——识别过时或废弃的组件版本。SCA工具如Snyk、OWASP Dependency-Check、Trivy等，是DevSecOps流水线的重要环节。

99. 以下哪个不属于安全编码的基本原则？

- A. 不信任外部输入，始终进行验证和净化
- B. 使用参数化查询防止SQL注入
- C. 将所有逻辑放在前端实现以提高性能
- D. 实施最小权限原则

答案：C 难度：中

解析：

安全编码基本原则：1）不信任外部输入——所有外部输入都需进行验证、净化和编码（输入验证白名单优于黑名单）；2）参数化查询——防止SQL注入；3）最小权限——应用程序和数据库连接使用最小权限账户；4）输出编码——根据输出上下文（HTML/JS/URL/CSS）进行实体编码防止XSS；5）安全默认值——默认配置应为最安全配置；6）纵深防御——多层防护而非单一防护。“将所有逻辑放在前端”违反安全原则——前端代码可被篡改，核心业务逻辑和安全校验必须在服务端实现。

100. 在DevSecOps CI/CD流水线中，DAST应在哪个阶段执行？

- A. 编码阶段
- B. 代码提交阶段
- C. CD部署后的测试环境阶段
- D. 需求分析阶段

答案：C 难度：中

解析：

DAST (Dynamic Application Security Testing, 动态应用安全测试) 需要应用在运行状态下进行测试，因此在CI/CD流水线中应在CD阶段——应用部署到测试环境或预生产环境后执行。DAST通过模拟攻击者的方式向运行中的应用发送恶意请求，检测运行时漏洞（如SQL注入、XSS、认证绕过等）。相比之下：SAST在CI阶段（编码后提交前）执行；SCA在构建阶段执行；DAST在CD阶段执行。这种分层测试确保在各个阶段都能发现不同类型的安全问题。

101. 供应链安全攻击的典型方式是？

- A. 直接入侵目标服务器
- B. 通过感染第三方组件或更新渠道间接入侵目标
- C. 发送钓鱼邮件
- D. 物理入侵数据中心

答案：B 难度：中

解析：

软件供应链安全攻击通过攻击第三方组件、开源依赖、软件更新渠道或开发工具链，间接入侵使用该组件/更新的目标组织。典型案例：1）SolarWinds事件——攻击者在Orion软件更新包中植入后门，影响18,000+客户包括美国政府机构；2）Log4j2漏洞——开源日志库漏洞影响全球数百万应用；3）npm/PyPI恶意包——在开源仓库发布恶意包诱导开发者安装。防御措施：SCA扫描、组件签名验证、镜像仓库安全、构建管道安全、零信任架构。