

CISSP考试大纲与100道高频试题解析

按 ISC2 当前 CISSP 考试大纲整理 | 中文复习资料 | 含答案与逐题解析

核查说明：考试大纲、领域名称、权重和考试形式依据 ISC2 官方 CISSP Certification Exam Outline 页面整理。试题为原创练习题，按 CISSP 八大领域分布，不引用真实考试题。

一、CISSP考试大纲核查版

官方考试信息：CISSP 属于高级网络安全认证，考试覆盖 8 个安全知识领域。英文 CAT 考试为 100-150 题、3 小时；中文等线性考试为 125 题、3 小时。通过分数为 700/1000。

领域	权重	本资料题量	核心考点
安全与风险管理	15%	15	CIA 三元组、治理与合规、职业道德、风险管理、隐私与法律、业务连续性
资产安全	10%	10	数据分类、数据所有权、保留与销毁、隐私保护、数据生命周期
安全架构与工程	13%	13	安全模型、密码学、可信计算、物理安全、嵌入式与工业系统
通信与网络安全	13%	13	网络分层、安全协议、分段与隔离、无线安全、远程访问
身份与访问管理	13%	13	认证授权、联合身份、访问控制模型、特权管理、生命周期管理
安全评估与测试	12%	12	审计策略、漏洞评估、渗透测试、日志与监控、测试报告
安全运营	13%	13	事件响应、取证、变更管理、灾难恢复、补丁与配置
软件开发安全	11%	11	安全 SDLC、威胁建模、代码安全、供应链、DevSecOps

安全与风险管理

- 理解并应用保密性、完整性、可用性、不可否认性、真实性、隐私与安全治理原则。
- 建立安全策略、标准、程序和指南，并把风险评估结果转化为可执行控制。
- 掌握法律法规、合同要求、职业道德、人员安全、业务连续性和供应链风险。

资产安全

- 识别信息和资产，明确数据所有者、保管者和用户职责。
- 按敏感度分类和标记数据，覆盖收集、使用、存储、传输、保留、归档和销毁。
- 选择适合的隐私保护、数据泄露防护和介质管理控制。

安全架构与工程

- 将安全原则嵌入系统、硬件、软件、云、物联网、工业控制和物理环境架构。
- 理解安全模型、评估准则、加密机制、密钥管理、可信平台和安全能力。
- 用纵深防御、最小权限、失效安全和安全默认配置降低系统性风险。

通信与网络安全

- 设计和保护网络架构、传输机制、边界控制、无线和远程访问。
- 理解 OSI/TCP-IP 分层、安全协议、VPN、NAC、微分段和零信任网络访问。
- 把可用性、弹性、加密、监控和访问控制纳入网络设计。

身份与访问管理

- 管理身份生命周期，覆盖注册、证明、配置、复核、撤销和特权控制。
- 区分识别、认证、授权、问责，并选择合适的 MFA、SSO、联邦和目录服务。
- 掌握 DAC、MAC、RBAC、ABAC、物理与逻辑访问控制。

安全评估与测试

- 设计安全测试、控制评估、漏洞评估、渗透测试和审计活动。
- 理解测试频率、范围、独立性、证据留存和报告要求。

- 通过日志、指标、代码审查和配置检查验证控制有效性。

安全运营

- 执行日志管理、监控、事件响应、取证、补丁管理、变更管理和灾难恢复。
- 理解检测、遏制、根除、恢复、经验总结等事件响应阶段。
- 把人员、流程、技术和法律证据链要求结合起来。

软件开发安全

- 把安全需求、威胁建模、代码审查、测试和发布控制嵌入 SDLC。
- 理解常见漏洞、API 安全、第三方组件、CI/CD、环境隔离和变更控制。
- 选择安全架构、编码规范和供应链控制以降低应用风险。

二、100道高频练习题与解析

使用建议：先独立答题，再看答案。CISSP

更关注管理判断、风险优先级、职责边界和控制选择，而不是单纯背工具名称。

安全与风险管理

1. 【安全与风险管理 - CIA 三元组】在 CIA 三元组

专项审查中，某组织希望把安全要求纳入经营决策。首先应建立什么？

- A. 最新安全设备
- B. 高级管理层批准的安全治理框架
- C. 仅由 IT 维护的技术标准
- D. 临时安全会议

答案：B

解析：安全必须由治理驱动，治理框架明确目标、责任、风险偏好和问责。本题归入 CISSP 的“安全与风险管理”领域，考点是 CIA 三元组。

2. 【安全与风险管理 - 治理与合规】在 治理与合规

专项审查中，风险评估发现高影响低概率风险。下一步最合理的是？

- A. 忽略低概率风险
- B. 按风险偏好选择规避、降低、转移或接受
- C. 立即关闭业务
- D. 只记录不处理

答案：B

解析：CISSP 强调以业务风险和风险偏好决定处置策略。本题归入 CISSP 的“安全与风险管理”领域，考点是治理与合规。

3. 【安全与风险管理 - 职业道德】在 职业道德 专项审查中，安全策略与标准的主要区别是什么？

- A. 策略更具体
- B. 标准给出强制性具体要求
- C. 标准只适用于供应商
- D. 策略不需管理层批准

答案：B

解析：策略表达管理意图，标准给出必须满足的具体要求。本题归入 CISSP 的“安全与风险管理”领域，考点是职业道德。

4. 【安全与风险管理 - 风险管理】在 风险管理 专项审查中，职业道德冲突中，CISSP 持证人应优先保护什么？

- A. 个人便利
- B. 公众、社会和基础设施安全
- C. 供应商利益
- D. 短期利润

答案：B

解析：ISC2 职业道德强调保护社会、公共利益和必要信任。本题归入 CISSP 的“安全与风险管理”领域，考点是风险管理。

5.【安全与风险管理 - 隐私与法律】在 隐私与法律 专项审查中，业务连续性分析中 BIA 的主要输出是什么？

- A. 漏洞编号
- B. 关键业务、影响和恢复目标
- C. 防火墙规则
- D. 代码缺陷清单

答案：B

解析：BIA 用来识别关键流程、影响、RTO/RPO 等恢复要求。本题归入 CISSP 的“安全与风险管理”领域，考点是隐私与法律。

6.【安全与风险管理 - 业务连续性】在 业务连续性 专项审查中，某组织希望把安全要求纳入经营决策。首先应建立什么？

- A. 最新安全设备
- B. 高级管理层批准的安全治理框架
- C. 仅由 IT 维护的技术标准
- D. 临时安全会议

答案：B

解析：安全必须由治理驱动，治理框架明确目标、责任、风险偏好和问责。本题归入 CISSP 的“安全与风险管理”领域，考点是 业务连续性。

7.【安全与风险管理 - CIA 三元组】在 CIA 三元组 专项审查中，风险评估发现高影响低概率风险。下一步最合理的是？

- A. 忽略低概率风险
- B. 按风险偏好选择规避、降低、转移或接受
- C. 立即关闭业务
- D. 只记录不处理

答案：B

解析：CISSP 强调以业务风险和风险偏好决定处置策略。本题归入 CISSP 的“安全与风险管理”领域，考点是 CIA 三元组。

8.【安全与风险管理 - 治理与合规】在 治理与合规 专项审查中，安全策略与标准的主要区别是什么？

- A. 策略更具体
- B. 标准给出强制性具体要求
- C. 标准只适用于供应商
- D. 策略不需管理层批准

答案：B

解析：策略表达管理意图，标准给出必须满足的具体要求。本题归入 CISSP 的“安全与风险管理”领域，考点是治理与合规。

9.【安全与风险管理 - 职业道德】在 职业道德 专项审查中，职业道德冲突中，CISSP 持证人应优先保护什么？

- A. 个人便利
- B. 公众、社会和基础设施安全
- C. 供应商利益
- D. 短期利润

答案：B

解析：ISC2 职业道德强调保护社会、公共利益和必要信任。本题归入 CISSP 的“安全与风险管理”领域，考点是职业道德。

10.【安全与风险管理 - 风险管理】在 风险管理 专项审查中，业务连续性分析中 BIA 的主要输出是什么？

- A. 漏洞编号
- B. 关键业务、影响和恢复目标
- C. 防火墙规则
- D. 代码缺陷清单

答案：B

解析：BIA 用来识别关键流程、影响、RTO/RPO 等恢复要求。本题归入 CISSP 的“安全与风险管理”领域，考点是风险管理。

11.【安全与风险管理 - 隐私与法律】在 隐私与法律 专项审查中，某组织希望把安全要求纳入经营决策。首先应建立什么？

- A. 最新安全设备
- B. 高级管理层批准的安全治理框架
- C. 仅由 IT 维护的技术标准
- D. 临时安全会议

答案：B

解析：安全必须由治理驱动，治理框架明确目标、责任、风险偏好和问责。本题归入 CISSP 的“安全与风险管理”领域，考点是 隐私与法律。

12.【安全与风险管理 - 业务连续性】在 业务连续性 专项审查中，风险评估发现高影响低概率风险。下一步最合理的是？

- A. 忽略低概率风险
- B. 按风险偏好选择规避、降低、转移或接受
- C. 立即关闭业务
- D. 只记录不处理

答案：B

解析：CISSP 强调以业务风险和风险偏好决定处置策略。本题归入 CISSP 的“安全与风险管理”领域，考点是业务连续性。

13.【安全与风险管理 - CIA 三元组】在 CIA 三元组 专项审查中，安全策略与标准的主要区别是什么？

- A. 策略更具体
- B. 标准给出强制性具体要求
- C. 标准只适用于供应商
- D. 策略不需管理层批准

答案：B

解析：策略表达管理意图，标准给出必须满足的具体要求。本题归入 CISSP 的“安全与风险管理”领域，考点是 CIA 三元组。

14.【安全与风险管理 - 治理与合规】在 治理与合规 专项审查中，职业道德冲突中，CISSP 持证人应优先保护什么？

- A. 个人便利
- B. 公众、社会和基础设施安全
- C. 供应商利益
- D. 短期利润

答案：B

解析：ISC2 职业道德强调保护社会、公共利益和必要信任。本题归入 CISSP 的“安全与风险管理”领域，考点是治理与合规。

15.【安全与风险管理 - 职业道德】在 职业道德 专项审查中，业务连续性分析中 BIA 的主要输出是什么？

- A. 漏洞编号
- B. 关键业务、影响和恢复目标
- C. 防火墙规则
- D. 代码缺陷清单

答案：B

解析：BIA 用来识别关键流程、影响、RTO/RPO 等恢复要求。本题归入 CISSP 的“安全与风险管理”领域，考点是 职业道德。

资产安全

16.【资产安全 - 数据分类】在 数据分类 专项审查中，谁通常负责决定数据分类和访问授权要求？

- A. 数据所有者
- B. 网络管理员
- C. 外部审计员
- D. 普通用户

答案：A

解析：数据所有者负责分类、授权要求和保护级别。本题归入 CISSP 的“资产安全”领域，考点是 数据分类。

17.【资产安全 - 数据所有权】在 数据所有权 专项审查中，敏感介质报废前应优先确保什么？

- A. 外观完好
- B. 按敏感度清除、消磁或销毁
- C. 继续入库
- D. 只删除文件名

答案：B

解析：介质处置要防止残留数据泄露，需匹配数据敏感度。本题归入 CISSP 的“资产安全”领域，考点是 数据所有权。

18.【资产安全 - 保留与销毁】在 保留与销毁 专项审查中，数据保留期限应主要依据什么确定？

- A. 存储价格
- B. 法律、监管和业务要求
- C. 管理员习惯
- D. 文件大小

答案：B

解析：保留策略必须满足法律、监管、合同和业务需求。本题归入 CISSP 的“资产安全”领域，考点是 保留与销毁。

19.【资产安全 - 隐私保护】在 隐私保护 专项审查中，对个人信息做最小化收集体现了什么原则？

- A. 隐私设计
- B. 端口镜像
- C. 热备份
- D. 链路聚合

答案：A

解析：数据最小化是隐私保护和隐私设计的重要原则。本题归入 CISSP 的“资产安全”领域，考点是 隐私保护。

20.【资产安全 - 数据生命周期】在 数据生命周期 专项审查中，标记数据的主要目的是什么？

- A. 提高压缩率
- B. 让处理者识别敏感度和保护要求
- C. 减少备份
- D. 替代访问控制

答案：B

解析：标记帮助用户和系统按分类应用处理与保护规则。本题归入 CISSP 的“资产安全”领域，考点是 数据生命周期。

21.【资产安全 - 数据分类】在 数据分类 专项审查中，谁通常负责决定数据分类和访问授权要求？

- A. 数据所有者
- B. 网络管理员
- C. 外部审计员
- D. 普通用户

答案：A

解析：数据所有者负责分类、授权要求和保护级别。本题归入 CISSP 的“资产安全”领域，考点是 数据分类。

22.【资产安全 - 数据所有权】在 数据所有权 专项审查中，敏感介质报废前应优先确保什么？

- A. 外观完好
- B. 按敏感度清除、消磁或销毁
- C. 继续入库
- D. 只删除文件名

答案：B

解析：介质处置要防止残留数据泄露，需匹配数据敏感度。本题归入 CISSP 的“资产安全”领域，考点是 数据所有权。

23.【资产安全 - 保留与销毁】在 保留与销毁 专项审查中，数据保留期限应主要依据什么确定？

- A. 存储价格
- B. 法律、监管和业务要求
- C. 管理员习惯
- D. 文件大小

答案：B

解析：保留策略必须满足法律、监管、合同和业务需求。本题归入 CISSP 的“资产安全”领域，考点是 保留与销毁。

24.【资产安全 - 隐私保护】在 隐私保护 专项审查中，对个人信息做最小化收集体现了什么原则？

- A. 隐私设计
- B. 端口镜像
- C. 热备份
- D. 链路聚合

答案：A

解析：数据最小化是隐私保护和隐私设计的重要原则。本题归入 CISSP 的“资产安全”领域，考点是 隐私保护。

25.【资产安全 - 数据生命周期】在 数据生命周期 专项审查中，标记数据的主要目的是什么？

- A. 提高压缩率
- B. 让处理者识别敏感度和保护要求
- C. 减少备份
- D. 替代访问控制

答案：B

解析：标记帮助用户和系统按分类应用处理与保护规则。本题归入 CISSP 的“资产安全”领域，考点是 数据生命周期。

安全架构与工程

26.【安全架构与工程 - 安全模型】在 安全模型 专项审查中，安全架构中失效安全原则要求系统故障时默认如何处理？

- A. 默认开放
- B. 默认拒绝或保持安全状态
- C. 删除日志
- D. 绕过认证

答案：B

解析：失效安全要求异常时不扩大访问或暴露资产。本题归入 CISSP 的“安全架构与工程”领域，考点是 安全模型。

27.【安全架构与工程 - 密码学】在 密码学 专项审查中，公钥基础设施中 CA 的核心作用是什么？

- A. 压缩数据
- B. 签发和管理数字证书
- C. 替代防火墙
- D. 运行备份

答案：B

解析：CA 负责证书签发、验证链和撤销支持。本题归入 CISSP 的“安全架构与工程”领域，考点是 密码学。

28.【安全架构与工程 - 可信计算】在 可信计算 专项审查中，Bell-LaPadula 模型主要关注什么？

- A. 完整性
- B. 保密性
- C. 可用性
- D. 负载均衡

答案：B

解析：Bell-LaPadula 通过读写规则保护机密性。本题归入 CISSP 的“安全架构与工程”领域，考点是 可信计算。

29.【安全架构与工程 - 物理安全】在 物理安全 专项审查中，Biba 模型主要关注什么？

- A. 完整性
- B. 无线漫游
- C. 隐私告知
- D. 网络地址转换

答案：A

解析：Biba 模型强调防止低完整性数据污染高完整性对象。本题归入 CISSP 的“安全架构与工程”领域，考点是 物理安全。

30.【安全架构与工程 - 嵌入式与工业系统】在 嵌入式与工业系统 专项审查中，物理安全中的 mantrap 主要用于什么？

- A. 防止尾随进入
- B. 提高制冷效率
- C. 扩展无线覆盖
- D. 加密磁盘

答案：A

解析：Mantrap 通过双门控制降低尾随和未经授权进入风险。本题归入 CISSP 的“安全架构与工程”领域，考点是 嵌入式与工业系统。

31.【安全架构与工程 - 安全模型】在 安全模型 专项审查中，安全架构中失效安全原则要求系统故障时默认如何处理？

- A. 默认开放
- B. 默认拒绝或保持安全状态
- C. 删除日志
- D. 绕过认证

答案：B

解析：失效安全要求异常时不扩大访问或暴露资产。本题归入 CISSP 的“安全架构与工程”领域，考点是 安全模型。

32.【安全架构与工程 - 密码学】在 密码学 专项审查中，公钥基础设施中 CA 的核心作用是什么？

- A. 压缩数据
- B. 签发和管理数字证书
- C. 替代防火墙
- D. 运行备份

答案：B

解析：CA 负责证书签发、验证链和撤销支持。本题归入 CISSP 的“安全架构与工程”领域，考点是 密码学。

33.【安全架构与工程 - 可信计算】在可信计算专项审查中，Bell-LaPadula 模型主要关注什么？

- A. 完整性
- B. 保密性
- C. 可用性
- D. 负载均衡

答案：B

解析：Bell-LaPadula 通过读写规则保护机密性。本题归入 CISSP 的“安全架构与工程”领域，考点是可信计算。

34.【安全架构与工程 - 物理安全】在物理安全专项审查中，Biba 模型主要关注什么？

- A. 完整性
- B. 无线漫游
- C. 隐私告知
- D. 网络地址转换

答案：A

解析：Biba 模型强调防止低完整性数据污染高完整性对象。本题归入 CISSP 的“安全架构与工程”领域，考点是物理安全。

35.【安全架构与工程 - 嵌入式与工业系统】在嵌入式与工业系统专项审查中，物理安全中的 mantrap 主要用于什么？

- A. 防止尾随进入
- B. 提高制冷效率
- C. 扩展无线覆盖
- D. 加密磁盘

答案：A

解析：Mantrap 通过双门控制降低尾随和未经授权进入风险。本题归入 CISSP 的“安全架构与工程”领域，考点是嵌入式与工业系统。

36.【安全架构与工程 - 安全模型】在安全模型专项审查中，安全架构中失效安全原则要求系统故障时默认如何处理？

- A. 默认开放
- B. 默认拒绝或保持安全状态
- C. 删除日志
- D. 绕过认证

答案：B

解析：失效安全要求异常时不扩大访问或暴露资产。本题归入 CISSP 的“安全架构与工程”领域，考点是安全模型。

37.【安全架构与工程 - 密码学】在密码学专项审查中，公钥基础设施中 CA 的核心作用是什么？

- A. 压缩数据
- B. 签发和管理数字证书
- C. 替代防火墙
- D. 运行备份

答案：B

解析：CA 负责证书签发、验证链和撤销支持。本题归入 CISSP 的“安全架构与工程”领域，考点是密码学。

38.【安全架构与工程 - 可信计算】在可信计算专项审查中，Bell-LaPadula 模型主要关注什么？

- A. 完整性
- B. 保密性
- C. 可用性
- D. 负载均衡

答案：B

解析：Bell-LaPadula 通过读写规则保护机密性。本题归入 CISSP 的“安全架构与工程”领域，考点是可信计算。

通信与网络安全

39.【通信与网络安全 - 网络分层】在 网络分层 专项审查中，企业要限制攻击者横向移动，最有效的网络设计是？

- A. 网络分段和最小必要通信
- B. 单一扁平 VLAN
- C. 提高带宽
- D. 关闭资产清单

答案：A

解析：分段、ACL 和微分段可限制横向移动路径。本题归入 CISSP 的“通信与网络安全”领域，考点是 网络分层。

40.【通信与网络安全 - 安全协议】在 安全协议 专项审查中，保护传输中敏感数据最合适的控制是？

- A. 隐藏菜单
- B. 强加密通道并验证证书
- C. 提高日志级别
- D. 改文件名

答案：B

解析：TLS/VPN 等通道加密配合证书验证可抵御窃听和中间人攻击。本题归入 CISSP 的“通信与网络安全”领域，考点是 安全协议。

41.【通信与网络安全 - 分段与隔离】在 分段与隔离 专项审查中，NAC 的主要用途是什么？

- A. 检查终端状态并控制接入
- B. 替代备份
- C. 签发员工合同
- D. 销毁介质

答案：A

解析：网络准入控制根据身份、设备状态和策略决定是否接入。本题归入 CISSP 的“通信与网络安全”领域，考点是 分段与隔离。

42.【通信与网络安全 - 无线安全】在 无线安全 专项审查中，无线企业网络优先选择哪种认证方式？

- A. 开放网络
- B. WPA3-Enterprise 或 802.1X
- C. 共享明文密码
- D. 隐藏 SSID

答案：B

解析：企业无线应采用强认证和动态密钥管理。本题归入 CISSP 的“通信与网络安全”领域，考点是 无线安全。

43.【通信与网络安全 - 远程访问】在 远程访问 专项审查中，边界防护中 DMZ 的主要目的是什么？

- A. 隔离对外服务与内网
- B. 提高屏幕亮度
- C. 减少数据分类
- D. 替代身份管理

答案：A

解析：DMZ 将公网可访问服务与内部可信网络隔离。本题归入 CISSP 的“通信与网络安全”领域，考点是 远程访问。

44.【通信与网络安全 - 网络分层】在 网络分层 专项审查中，企业要限制攻击者横向移动，最有效的网络设计是？

- A. 网络分段和最小必要通信
- B. 单一扁平 VLAN
- C. 提高带宽
- D. 关闭资产清单

答案：A

解析：分段、ACL 和微分段可限制横向移动路径。本题归入 CISSP 的“通信与网络安全”领域，考点是 网络分层。

45.【通信与网络安全 - 安全协议】在 安全协议 专项审查中，保护传输中敏感数据最合适的控制是？

- A. 隐藏菜单
- B. 强加密通道并验证证书
- C. 提高日志级别
- D. 改文件名

答案：B

解析：TLS/VPN 等通道加密配合证书验证可抵御窃听和中间人攻击。本题归入 CISSP 的“通信与网络安全”领域，考点是安全协议。

46.【通信与网络安全 - 分段与隔离】在 分段与隔离 专项审查中，NAC 的主要用途是什么？

- A. 检查终端状态并控制接入
- B. 替代备份
- C. 签发员工合同
- D. 销毁介质

答案：A

解析：网络准入控制根据身份、设备状态和策略决定是否接入。本题归入 CISSP 的“通信与网络安全”领域，考点是分段与隔离。

47.【通信与网络安全 - 无线安全】在 无线安全 专项审查中，无线企业网络优先选择哪种认证方式？

- A. 开放网络
- B. WPA3-Enterprise 或 802.1X
- C. 共享明文密码
- D. 隐藏 SSID

答案：B

解析：企业无线应采用强认证和动态密钥管理。本题归入 CISSP 的“通信与网络安全”领域，考点是无线安全。

48.【通信与网络安全 - 远程访问】在 远程访问 专项审查中，边界防护中 DMZ 的主要目的是什么？

- A. 隔离对外服务与内网
- B. 提高屏幕亮度
- C. 减少数据分类
- D. 替代身份管理

答案：A

解析：DMZ 将公网可访问服务与内部可信网络隔离。本题归入 CISSP 的“通信与网络安全”领域，考点是远程访问。

49.【通信与网络安全 - 网络分层】在 网络分层 专项审查中，企业要限制攻击者横向移动，最有效的网络设计是？

- A. 网络分段和最小必要通信
- B. 单一扁平 VLAN
- C. 提高带宽
- D. 关闭资产清单

答案：A

解析：分段、ACL 和微分段可限制横向移动路径。本题归入 CISSP 的“通信与网络安全”领域，考点是网络分层。

50.【通信与网络安全 - 安全协议】在 安全协议 专项审查中，保护传输中敏感数据最合适的控制是？

- A. 隐藏菜单
- B. 强加密通道并验证证书
- C. 提高日志级别
- D. 改文件名

答案：B

解析：TLS/VPN 等通道加密配合证书验证可抵御窃听和中间人攻击。本题归入 CISSP 的“通信与网络安全”领域，考点是安全协议。

51.【通信与网络安全 - 分段与隔离】在 分段与隔离 专项审查中，NAC 的主要用途是什么？

- A. 检查终端状态并控制接入
- B. 替代备份
- C. 签发员工合同
- D. 销毁介质

答案：A

解析：网络准入控制根据身份、设备状态和策略决定是否接入。本题归入 CISSP 的“通信与网络安全”领域，考点是分段与隔离。

身份与访问管理

52.【身份与访问管理 - 认证授权】在 认证授权 专项审查中，员工离职后仍能访问系统，最直接暴露什么不足？

- A. 身份生命周期管理
- B. 机房消防
- C. 压缩策略
- D. 带宽规划

答案：A

解析：离职撤权属于身份生命周期管理。本题归入 CISSP 的“身份与访问管理”领域，考点是 认证授权。

53.【身份与访问管理 - 联合身份】在 联合身份 专项审查中，RBAC 授权主要基于什么？

- A. 用户角色
- B. 数据包大小
- C. 硬盘型号
- D. 办公室温度

答案：A

解析：RBAC 根据岗位角色授予权限，便于集中管理。本题归入 CISSP 的“身份与访问管理”领域，考点是 联合身份。

54.【身份与访问管理 - 访问控制模型】在 访问控制模型 专项审查中，MFA 的价值是什么？

- A. 增加单一密码长度
- B. 组合多类认证因素降低凭证失窃风险
- C. 替代授权
- D. 删除日志

答案：B

解析：MFA 结合知道、拥有、固有等因素增强认证可信度。本题归入 CISSP 的“身份与访问管理”领域，考点是 访问控制模型。

55.【身份与访问管理 - 特权管理】在 特权管理 专项审查中，特权账户应采用哪项控制？

- A. 共享账号
- B. 审批、限时授权和会话记录
- C. 永久管理员权限
- D. 关闭审计

答案：B

解析：PAM 控制特权授予、使用和追溯。本题归入 CISSP 的“身份与访问管理”领域，考点是 特权管理。

56.【身份与访问管理 - 生命周期管理】在 生命周期管理 专项审查中，联邦身份的主要好处是什么？

- A. 跨组织信任和单点登录
- B. 免除风险评估
- C. 替代加密
- D. 删除目录服务

答案：A

解析：联邦身份通过信任关系支持跨域认证和访问。本题归入 CISSP 的“身份与访问管理”领域，考点是 生命周期管理。

57.【身份与访问管理 - 认证授权】在 认证授权 专项审查中，员工离职后仍能访问系统，最直接暴露什么不足？

- A. 身份生命周期管理
- B. 机房消防
- C. 压缩策略
- D. 带宽规划

答案：A

解析：离职撤权属于身份生命周期管理。本题归入 CISSP 的“身份与访问管理”领域，考点是 认证授权。

58.【身份与访问管理 - 联合身份】在 联合身份 专项审查中，RBAC 授权主要基于什么？

- A. 用户角色
- B. 数据包大小
- C. 硬盘型号
- D. 办公室温度

答案：A

解析：RBAC 根据岗位角色授予权限，便于集中管理。本题归入 CISSP 的“身份与访问管理”领域，考点是 联合身份。

59.【身份与访问管理 - 访问控制模型】在 访问控制模型 专项审查中，MFA 的价值是什么？

- A. 增加单一密码长度
- B. 组合多类认证因素降低凭证失窃风险
- C. 替代授权
- D. 删除日志

答案：B

解析：MFA 结合知道、拥有、固有等因素增强认证可信度。本题归入 CISSP 的“身份与访问管理”领域，考点是 访问控制模型。

60.【身份与访问管理 - 特权管理】在 特权管理 专项审查中，特权账户应采用哪项控制？

- A. 共享账号
- B. 审批、限时授权和会话记录
- C. 永久管理员权限
- D. 关闭审计

答案：B

解析：PAM 控制特权授予、使用和追溯。本题归入 CISSP 的“身份与访问管理”领域，考点是 特权管理。

61.【身份与访问管理 - 生命周期管理】在 生命周期管理 专项审查中，联邦身份的主要好处是什么？

- A. 跨组织信任和单点登录
- B. 免除风险评估
- C. 替代加密
- D. 删除目录服务

答案：A

解析：联邦身份通过信任关系支持跨域认证和访问。本题归入 CISSP 的“身份与访问管理”领域，考点是 生命周期管理。

62.【身份与访问管理 - 认证授权】在 认证授权 专项审查中，员工离职后仍能访问系统，最直接暴露什么不足？

- A. 身份生命周期管理
- B. 机房消防
- C. 压缩策略
- D. 带宽规划

答案：A

解析：离职撤权属于身份生命周期管理。本题归入 CISSP 的“身份与访问管理”领域，考点是 认证授权。

63.【身份与访问管理 - 联合身份】在 联合身份 专项审查中，RBAC 授权主要基于什么？

- A. 用户角色
- B. 数据包大小
- C. 硬盘型号
- D. 办公室温度

答案：A

解析：RBAC 根据岗位角色授予权限，便于集中管理。本题归入 CISSP 的“身份与访问管理”领域，考点是 联合身份。

64.【身份与访问管理 - 访问控制模型】在 访问控制模型 专项审查中，MFA 的价值是什么？

- A. 增加单一密码长度
- B. 组合多类认证因素降低凭证失窃风险
- C. 替代授权
- D. 删除日志

答案：B

解析：MFA 结合知道、拥有、固有等因素增强认证可信度。本题归入 CISSP 的“身份与访问管理”领域，考点是 访问控制模型。

安全评估与测试

65.【安全评估与测试 - 审计策略】在 审计策略 专项审查中，审计员要求证明控制持续有效。最佳证据是什么？

- A. 口头说明
- B. 控制运行记录和可追溯日志
- C. 宣传材料
- D. 未签字纪要

答案：B

解析：可追溯证据比口头说明更能证明控制运行。本题归入 CISSP 的“安全评估与测试”领域，考点是 审计策略。

66.【安全评估与测试 - 漏洞评估】在 漏洞评估 专项审查中，渗透测试前最重要的管理文件是什么？

- A. 授权范围和规则
- B. 广告文案
- C. 员工生日表
- D. 办公座位图

答案：A

解析：测试必须有书面授权、范围、方法和停止条件。本题归入 CISSP 的“安全评估与测试”领域，考点是 漏洞评估。

67.【安全评估与测试 - 渗透测试】在 渗透测试 专项审查中，漏洞扫描与渗透测试的主要区别是什么？

- A. 前者识别已知弱点，后者尝试验证可利用性
- B. 二者完全相同
- C. 扫描只用于物理安全
- D. 渗透测试不需授权

答案：A

解析：渗透测试更进一步验证攻击路径和影响。本题归入 CISSP 的“安全评估与测试”领域，考点是 渗透测试。

68.【安全评估与测试 - 日志与监控】在 日志与监控 专项审查中，代码审查在安全测试中的价值是什么？

- A. 发现实现层安全缺陷
- B. 替代业务连续性
- C. 销毁旧介质
- D. 增加无线信号

答案：A

解析：代码审查可发现输入校验、认证、授权等实现问题。本题归入 CISSP 的“安全评估与测试”领域，考点是 日志与监控。

69.【安全评估与测试 - 测试报告】在 测试报告 专项审查中，控制测试频率应依据什么确定？

- A. 风险和合规要求
- B. 管理员心情
- C. 打印机数量
- D. 机房颜色

答案：A

解析：高风险和强监管控制通常需要更频繁测试。本题归入 CISSP 的“安全评估与测试”领域，考点是 测试报告。

70.【安全评估与测试 - 审计策略】在 审计策略 专项审查中，审计员要求证明控制持续有效。最佳证据是什么？

- A. 口头说明
- B. 控制运行记录和可追溯日志
- C. 宣传材料
- D. 未签字纪要

答案：B

解析：可追溯证据比口头说明更能证明控制运行。本题归入 CISSP 的“安全评估与测试”领域，考点是 审计策略。

71.【安全评估与测试 - 漏洞评估】在 漏洞评估 专项审查中，渗透测试前最重要的管理文件是什么？

- A. 授权范围和规则
- B. 广告文案
- C. 员工生日表
- D. 办公座位图

答案：A

解析：测试必须有书面授权、范围、方法和停止条件。本题归入 CISSP 的“安全评估与测试”领域，考点是 漏洞评估。

72.【安全评估与测试 - 渗透测试】在 渗透测试 专项审查中，漏洞扫描与渗透测试的主要区别是什么？

- A. 前者识别已知弱点，后者尝试验证可利用性
- B. 二者完全相同
- C. 扫描只用于物理安全
- D. 渗透测试不需授权

答案：A

解析：渗透测试更进一步验证攻击路径和影响。本题归入 CISSP 的“安全评估与测试”领域，考点是 渗透测试。

73.【安全评估与测试 - 日志与监控】在 日志与监控 专项审查中，代码审查在安全测试中的价值是什么？

- A. 发现实现层安全缺陷
- B. 替代业务连续性
- C. 销毁旧介质
- D. 增加无线信号

答案：A

解析：代码审查可发现输入校验、认证、授权等实现问题。本题归入 CISSP 的“安全评估与测试”领域，考点是 日志与监控。

74.【安全评估与测试 - 测试报告】在 测试报告 专项审查中，控制测试频率应依据什么确定？

- A. 风险和合规要求
- B. 管理员心情
- C. 打印机数量
- D. 机房颜色

答案：A

解析：高风险和强监管控制通常需要更频繁测试。本题归入 CISSP 的“安全评估与测试”领域，考点是 测试报告。

75.【安全评估与测试 - 审计策略】在 审计策略 专项审查中，审计员要求证明控制持续有效。最佳证据是什么？

- A. 口头说明
- B. 控制运行记录和可追溯日志
- C. 宣传材料
- D. 未签字纪要

答案：B

解析：可追溯证据比口头说明更能证明控制运行。本题归入 CISSP 的“安全评估与测试”领域，考点是 审计策略。

76.【安全评估与测试 - 漏洞评估】在 漏洞评估 专项审查中，渗透测试前最重要的管理文件是什么？

- A. 授权范围和规则
- B. 广告文案
- C. 员工生日表
- D. 办公座位图

答案：A

解析：测试必须有书面授权、范围、方法和停止条件。本题归入 CISSP 的“安全评估与测试”领域，考点是 漏洞评估。

安全运营

77.【安全运营 - 事件响应】在 事件响应 专项审查中，发现入侵后，在根除前通常应先做什么？

- A. 遏制影响并保全证据
- B. 立即删除日志
- C. 公开细节
- D. 重装全部系统

答案：A

解析：事件响应通常先识别和遏制，同时保护证据。本题归入 CISSP 的“安全运营”领域，考点是 事件响应。

78.【安全运营 - 取证】在 取证 专项审查中，取证中的证据链主要证明什么？

- A. 证据从收集到提交未被不当篡改
- B. 网络更快
- C. 备份更便宜
- D. 用户更满意

答案：A

解析：证据链记录保管、转移和访问过程，维护证据可信度。本题归入 CISSP 的“安全运营”领域，考点是 取证。

79.【安全运营 - 变更管理】在 变更管理 专项审查中，补丁管理应首先处理哪些漏洞？

- A. 业务关键且可被利用的高风险漏洞
- B. 编号最小的漏洞
- C. 最容易宣传的漏洞
- D. 所有低风险漏洞

答案：A

解析：补丁优先级应结合资产关键性、可利用性和影响。本题归入 CISSP 的“安全运营”领域，考点是 变更管理。

80.【安全运营 - 灾难恢复】在 灾难恢复 专项审查中，灾难恢复演练的主要目标是什么？

- A. 验证恢复计划可执行
- B. 替代审计
- C. 删除旧账号
- D. 降低屏幕亮度

答案：A

解析：演练用于验证人员、流程、技术和恢复时间目标。本题归入 CISSP 的“安全运营”领域，考点是 灾难恢复。

81.【安全运营 - 补丁与配置】在 补丁与配置 专项审查中，变更管理最重要的安全价值是什么？

- A. 降低未授权或未经测试变更风险
- B. 取消审批
- C. 禁止所有变更
- D. 替代监控

答案：A

解析：正式变更流程降低服务中断和安全回退失败风险。本题归入 CISSP 的“安全运营”领域，考点是 补丁与配置。

82.【安全运营 - 事件响应】在 事件响应 专项审查中，发现入侵后，在根除前通常应先做什么？

- A. 遏制影响并保全证据
- B. 立即删除日志
- C. 公开细节
- D. 重装全部系统

答案：A

解析：事件响应通常先识别和遏制，同时保护证据。本题归入 CISSP 的“安全运营”领域，考点是 事件响应。

83.【安全运营 - 取证】在 取证 专项审查中，取证中的证据链主要证明什么？

- A. 证据从收集到提交未被不当篡改
- B. 网络更快
- C. 备份更便宜
- D. 用户更满意

答案：A

解析：证据链记录保管、转移和访问过程，维护证据可信度。本题归入 CISSP 的“安全运营”领域，考点是 取证。

84.【安全运营 - 变更管理】在 变更管理 专项审查中，补丁管理应首先处理哪些漏洞？

- A. 业务关键且可被利用的高风险漏洞
- B. 编号最小的漏洞
- C. 最容易宣传的漏洞
- D. 所有低风险漏洞

答案：A

解析：补丁优先级应结合资产关键性、可利用性和影响。本题归入 CISSP 的“安全运营”领域，考点是 变更管理。

85.【安全运营 - 灾难恢复】在 灾难恢复 专项审查中，灾难恢复演练的主要目标是什么？

- A. 验证恢复计划可执行
- B. 替代审计
- C. 删除旧账号
- D. 降低屏幕亮度

答案：A

解析：演练用于验证人员、流程、技术和恢复时间目标。本题归入 CISSP 的“安全运营”领域，考点是 灾难恢复。

86.【安全运营 - 补丁与配置】在 补丁与配置 专项审查中，变更管理最重要的安全价值是什么？

- A. 降低未授权或未经测试变更风险
- B. 取消审批
- C. 禁止所有变更
- D. 替代监控

答案：A

解析：正式变更流程降低服务中断和安全回退失败风险。本题归入 CISSP 的“安全运营”领域，考点是 补丁与配置。

87.【安全运营 - 事件响应】在 事件响应 专项审查中，发现入侵后，在根除前通常应先做什么？

- A. 遏制影响并保全证据
- B. 立即删除日志
- C. 公开细节
- D. 重装全部系统

答案：A

解析：事件响应通常先识别和遏制，同时保护证据。本题归入 CISSP 的“安全运营”领域，考点是 事件响应。

88.【安全运营 - 取证】在 取证 专项审查中，取证中的证据链主要证明什么？

- A. 证据从收集到提交未被不当篡改
- B. 网络更快
- C. 备份更便宜
- D. 用户更满意

答案：A

解析：证据链记录保管、转移和访问过程，维护证据可信度。本题归入 CISSP 的“安全运营”领域，考点是 取证。

89.【安全运营 - 变更管理】在 变更管理 专项审查中，补丁管理应首先处理哪些漏洞？

- A. 业务关键且可被利用的高风险漏洞
- B. 编号最小的漏洞
- C. 最容易宣传的漏洞
- D. 所有低风险漏洞

答案：A

解析：补丁优先级应结合资产关键性、可利用性和影响。本题归入 CISSP 的“安全运营”领域，考点是 变更管理。

软件开发安全

90.【软件开发安全 - 安全 SDLC】在 安全 SDLC 专项审查中，设计阶段识别攻击路径并提出缓解措施属于什么？

- A. 威胁建模
- B. 介质销毁
- C. 灾难恢复演练
- D. 门禁巡检

答案：A

解析：威胁建模识别资产、威胁、攻击面和缓解措施。本题归入 CISSP 的“软件开发安全”领域，考点是 安全 SDLC。

91.【软件开发安全 - 威胁建模】在 威胁建模 专项审查中，安全 SDLC 的正确做法是什么？

- A. 上线后再考虑安全
- B. 从需求到维护持续嵌入安全活动
- C. 只依赖防火墙
- D. 禁止测试

答案：B

解析：安全应覆盖需求、设计、实现、测试、发布和维护。本题归入 CISSP 的“软件开发安全”领域，考点是 威胁建模。

92.【软件开发安全 - 代码安全】在 代码安全 专项审查中，防止 SQL 注入最直接的编码控制是什么？

- A. 参数化查询
- B. 隐藏表名
- C. 增加带宽
- D. 关闭备份

答案：A

解析：参数化查询把代码与数据分离，可有效防止注入。本题归入 CISSP 的“软件开发安全”领域，考点是 代码安全。

93.【软件开发安全 - 供应链】在 供应链 专项审查中，第三方组件安全管理应重点关注什么？

- A. 组件清单、漏洞和来源可信度
- B. 界面颜色
- C. 员工座位
- D. 打印速度

答案：A

解析：SBOM、版本、来源和漏洞跟踪是供应链安全重点。 本题归入 CISSP 的“软件开发安全”领域，考点是 供应链。

94.【软件开发安全 - DevSecOps】在 DevSecOps 专项审查中，CI/CD 中引入安全扫描体现什么理念？

- A. DevSecOps
- B. 物理隔离
- C. 手工审计替代
- D. 数据销毁

答案：A

解析：DevSecOps 将安全检查自动化并嵌入交付流水线。 本题归入 CISSP 的“软件开发安全”领域，考点是 DevSecOps。

95.【软件开发安全 - 安全 SDLC】在 安全 SDLC 专项审查中，设计阶段识别攻击路径并提出缓解措施属于什么？

- A. 威胁建模
- B. 介质销毁
- C. 灾难恢复演练
- D. 门禁巡检

答案：A

解析：威胁建模识别资产、威胁、攻击面和缓解措施。 本题归入 CISSP 的“软件开发安全”领域，考点是 安全 SDLC。

96.【软件开发安全 - 威胁建模】在 威胁建模 专项审查中，安全 SDLC 的正确做法是什么？

- A. 上线后再考虑安全
- B. 从需求到维护持续嵌入安全活动
- C. 只依赖防火墙
- D. 禁止测试

答案：B

解析：安全应覆盖需求、设计、实现、测试、发布和维护。 本题归入 CISSP 的“软件开发安全”领域，考点是 威胁建模。

97.【软件开发安全 - 代码安全】在 代码安全 专项审查中，防止 SQL 注入最直接的编码控制是什么？

- A. 参数化查询
- B. 隐藏表名
- C. 增加带宽
- D. 关闭备份

答案：A

解析：参数化查询把代码与数据分离，可有效防止注入。 本题归入 CISSP 的“软件开发安全”领域，考点是 代码安全。

98.【软件开发安全 - 供应链】在 供应链 专项审查中，第三方组件安全管理应重点关注什么？

- A. 组件清单、漏洞和来源可信度
- B. 界面颜色
- C. 员工座位
- D. 打印速度

答案：A

解析：SBOM、版本、来源和漏洞跟踪是供应链安全重点。 本题归入 CISSP 的“软件开发安全”领域，考点是 供应链。

99. 【软件开发安全 - DevSecOps】在 DevSecOps 专项审查中，CI/CD 中引入安全扫描体现什么理念？

- A. DevSecOps
- B. 物理隔离
- C. 手工审计替代
- D. 数据销毁

答案：A

解析：DevSecOps 将安全检查自动化并嵌入交付流水线。本题归入 CISSP 的“软件开发安全”领域，考点是 DevSecOps。

100. 【软件开发安全 - 安全 SDLC】在 安全 SDLC 专项审查中，设计阶段识别攻击路径并提出缓解措施属于什么？

- A. 威胁建模
- B. 介质销毁
- C. 灾难恢复演练
- D. 门禁巡检

答案：A

解析：威胁建模识别资产、威胁、攻击面和缓解措施。本题归入 CISSP 的“软件开发安全”领域，考点是 安全 SDLC。

三、考前核查清单

- 能解释每个控制背后的风险，而不是只记住控制名称。
- 能区分数据所有者、数据保管者、系统所有者、用户和审计员职责。
- 能把事件响应、灾难恢复、业务连续性和取证流程分开。
- 能按最小权限、职责分离、纵深防御、失效安全、默认安全做选择。
- 能识别题干中的关键词：最高管理层、业务影响、法律证据、数据生命周期、访问撤销、独立审计。

参考来源

ISC2 官方 CISSP Certification Exam Outline 页面: <https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline>

ISC2 官方 CISSP 认证页面: <https://www.isc2.org/certifications/cissp>

声明：本资料用于备考复习，题目为原创练习题，不代表真实考试题库。