examundo

CISSP 中文模拟考试

50 题，附答案。指南和译文由软件制作并核对，目前还没有人工审阅。

更新日期：2026 年 11 月 25 日 · examundo.tech/zh/cissp/

安全架构与工程

1. 哪个密码学概念可以确保发送方无法否认自己发送过某条消息？

Which cryptographic concept ensures that a sender cannot deny having sent a message?

A. 保密性
B. 完整性
C. 不可否认性
D. 身份验证

2. 一名安全架构师正在设计保护政府涉密数据的系统。应采用哪种安全模型，来防止信息从高密级流向低密级？

A security architect is designing a system to protect classified government data. Which security model should be implemented to prevent information from flowing from higher classification levels to lower classification levels?

A. Bell-LaPadula 模型
B. Clark-Wilson 模型
C. Brewer-Nash 模型
D. Biba 完整性模型

3. 一个电子商务应用需要与客户的浏览器安全地交换对称加密密钥。应使用哪种协议？

An e-commerce application needs to securely exchange symmetric encryption keys with customers' browsers. Which protocol should be used?

A. 使用 Diffie-Hellman 密钥交换的 TLS
B. 使用预共享密钥的传输模式 IPsec
C. 使用票据授予票据（TGT）的 Kerberos
D. 使用基于证书加密的 S/MIME

4. 一处安全设施要求进入服务器机房时必须做到双人完整性（two-person integrity）。哪种物理访问控制可以实现这个要求？

A secure facility requires two-person integrity for access to the server room. What type of physical access control implements this requirement?

A. 每季度更换密码的密码锁
B. 带视频监控记录所有进出的刷卡器
C. 带 PIN 键盘的生物识别读取器，用于多因素认证
D. 需要两名授权人员的双重认证捕人陷阱

5. 下列哪项安全原则最恰当地描述了纵深防御（defense in depth）？

Defense in depth is BEST described as which of the following security principles?

A. 部署多层安全控制来保护资产
B. 设计系统在出错时进入安全状态
C. 只授予用户完成工作所需的最小访问权限
D. 通过删除不必要的服务和功能来加固系统

6. 捕人陷阱（mantrap）属于哪一类物理安全控制?

A mantrap is classified as which type of physical security control?

A. 预防性控制
B. 补偿性控制
C. 检测性控制
D. 纠正性控制

---

7. 一个金融系统必须防止未授权用户修改交易记录，同时允许审计人员读取。哪种安全模型最能满足这个要求?

A financial system must prevent unauthorized users from modifying transaction records while allowing read access for auditing. Which security model BEST supports this requirement?

A. Bell-LaPadula 保密性模型
B. Brewer-Nash（中国墙）模型
C. Biba 完整性模型
D. Graham-Denning 访问控制模型

---

8. 一个组织要在云环境中实施新的加密系统来保护静态数据（data at rest）。该系统必须满足监管合规对密钥托管（key escrow）的要求，同时保持对云服务商的运营独立性。哪种做法最能同时满足这两个要求?

An organization is implementing a new cryptographic system to protect data at rest in a cloud environment. The system must support regulatory compliance requirements for key escrow while maintaining operational independence from the cloud provider. Which approach BEST satisfies both requirements?

A. 实施客户端加密，密钥由本地 HSM 管理，并把托管副本交给第三方密钥托管服务
B. 部署信封加密（envelope encryption），客户管理的密钥存放在云服务商的密钥管理服务中
C. 在数据库层实施透明数据加密，密钥存放在应用配置中
D. 使用云服务商的原生加密服务，启用自动密钥轮换，并备份到另一个云区域

---

9. 一名安全架构师要为处理多个密级文件的军事情报系统选择正式的安全模型。首要要求是防止信息流向较低密级。哪种模型最合适?

A security architect must select a formal security model for a military intelligence system handling documents at multiple classification levels. The PRIMARY requirement is preventing information from flowing to lower classification levels. Which model is MOST appropriate?

A. Biba 完整性模型
B. Clark-Wilson 完整性模型
C. Bell-LaPadula 模型
D. Brewer-Nash（中国墙）模型

---

10. 数据中心服务器机房上方的水管爆裂。哪种环境控制最能防止关键设备受到水损?

A data center experiences a water pipe burst above the server room. Which environmental control would have BEST prevented water damage to critical equipment?

A. 防止潮气渗入的正压系统
B. 带自动关断阀的水浸传感器
C. 把设备抬高到地面以上的架空地板
D. 带湿度监测和报警的 HVAC 系统

安全运营

11. 哪种配置管理做法最能发现生产服务器配置被未经授权地更改?

Which configuration management practice BEST detects unauthorized changes to production server configurations?

A. 定期把实际配置与已批准的基线对比
B. 自动批准特权管理员做出的变更
C. 只审查硬件采购记录，不检查服务器设置
D. 每次扫描后都用当前配置替换已批准的基线

---

12. 事件响应团队中，哪个角色负责最初发现并遏制事件?

Which role in an incident response team is responsible for initially identifying and containing the incident?

A. 事件协调员
B. 取证分析员
C. 第一响应人
D. 沟通负责人

---

13. 一起只对非关键系统造成轻微中断、且没有数据丢失的事件，通常应归为哪个严重等级?

An incident that causes minor disruption to non-critical systems with no data loss would typically be classified as what severity level?

A. 严重
B. 高
C. 低
D. 紧急

---

14. 事后复盘时，团队发现攻击者在被发现之前已潜伏了 87 天。哪项安全运营改进最能有效缩短今后的驻留时间（dwell time）?

During a post-incident review, the team identifies that the attacker maintained persistence for 87 days before detection. Which security operations improvement would MOST effectively reduce future dwell time?

A. 要求所有员工每季度参加安全意识培训
B. 在网络分段边界部署更多防火墙
C. 把漏洞扫描频率从每月一次提高到每周一次
D. 实施持续安全监控，配合行为分析和威胁狩猎

---

15. 物理安全的纵深防御通常包含多个层次。下列哪项是从最外层到最内层的正确顺序?

Defense in depth for physical security typically includes multiple layers. Which of the following represents the CORRECT order from outermost to innermost layer?

A. 周界围栏、建筑物门禁、房间门禁、设备锁
B. 设备锁、房间门禁、建筑物门禁、周界围栏
C. 房间门禁、设备锁、周界围栏、建筑物门禁
D. 建筑物门禁、周界围栏、设备锁、房间门禁

---

16. 哪种证据是原始证据的副本或复制品?

Which type of evidence consists of copies or reproductions of original evidence?

A. 次要证据（secondary evidence）
B. 最佳证据（best evidence）
C. 传闻证据（hearsay evidence）
D. 佐证证据（corroborative evidence）

---

17. 一个组织正在制定灾难恢复目标。业务要求关键系统必须在灾难发生后 4 小时内恢复。这个要求定义的是哪个恢复指标?

An organization is defining its disaster recovery objectives. The business requires that critical systems must be restored within 4 hours of a disaster. This requirement defines which recovery metric?

A. 平均修复时间（MTTR）
B. 最大可容忍停机时间（MTD）
C. 恢复时间目标（RTO）
D. 恢复点目标（RPO）

---

18. 一个组织的灾难恢复计划要求客户数据库的恢复时间目标（RTO）为 4 小时，恢复点目标（RPO）为 1 小时。哪种备份策略最能满足这些要求?

An organization's disaster recovery plan requires a recovery time objective (RTO) of 4 hours and a recovery point objective (RPO) of 1 hour for its customer database. Which backup strategy BEST meets these requirements?

A. 每 4 小时做一次差异备份，存放在本地
B. 每 6 小时做一次增量备份，磁带异地存放
C. 每周全量备份，每天增量备份
D. 每晚全量备份，并持续把数据库复制到温站

---

19. 一名第一响应人来到一台已被入侵的生产服务器前，它仍在运行并处理交易。按照 RFC 3227 的指导，实时取证时应该最先收集哪个数据源？

A first responder arrives at a compromised production server that is still powered on and actively processing transactions. Per RFC 3227 guidelines, which data source should be collected FIRST during live evidence acquisition?

A. CPU 寄存器和缓存
B. 系统 RAM（主内存）内容
C. ARP 缓存和路由表条目
D. 临时文件系统和交换空间数据

---

20. 一个 IT 部门遵循正式的变更管理流程。在对生产系统实施变更之前，应先完成哪个授权步骤？

An IT department follows a formal change management process. Which authorization step should occur BEFORE implementing a change to production systems?

A. 在非生产环境中测试变更
B. 获得变更咨询委员会（CAB）的批准
C. 在配置管理数据库中记录变更
D. 通知所有受影响的利益相关者

通信与网络安全

21. 一个组织为网络访问控制部署了 802.1X。哪个组件充当请求者（supplicant）和认证服务器之间的中间方？

An organization implements 802.1X for network access control. Which component acts as the intermediary between the supplicant and the authentication server?

A. 证书颁发机构
B. 网络控制器
C. 认证者
D. RADIUS 代理

---

22. 一个组织为无线安全部署了 WPA3-Enterprise。WPA3-Enterprise 使用哪种认证框架？

An organization implements WPA3-Enterprise for wireless security. What authentication framework does WPA3-Enterprise use?

A. 802.1X 与 EAP
B. MAC 地址过滤
C. 预共享密钥（PSK）
D. LEAP

---

23. 一个组织需要为在世界各地出差、网络连接不稳定的外勤人员提供安全的远程访问。该方案必须同时支持 TCP 和 UDP 流量，并且能穿过大多数防火墙。哪种 VPN 协议最合适？

An organization needs to provide secure remote access for field personnel who connect from various international locations with unreliable internet connectivity. The solution must support both TCP and UDP traffic and work through most firewalls. Which VPN protocol is MOST appropriate?

A. PPTP
B. SSL/TLS VPN
C. L2TP/IPSec
D. 隧道模式的 IPSec

---

24. 一家公司的 Web 应用遇到来自多个来源的流量激增，服务器已无法响应。最可能发生的是哪种攻击？

A company's web application experiences a surge in traffic from multiple sources, overwhelming the server's ability to respond. Which attack is MOST likely occurring?

A. 中间人攻击（MitM）
B. 跨站请求伪造（CSRF）
C. 会话劫持
D. 分布式拒绝服务（DDoS）

---

25. OSI 模型的哪一层负责通信主机之间端到端的可靠数据传输、流量控制和错误恢复?

Which OSI model layer is responsible for end-to-end reliable data delivery, flow control, and error recovery between communicating hosts?

A. 第 2 层，数据链路层
B. 第 4 层，传输层
C. 第 3 层，网络层
D. 第 5 层，会话层

---

26. 一个组织的 Web 服务器正遭受 SYN 洪水攻击。哪种防御技术最有效?

An organization is experiencing SYN flood attacks against its web server. Which defensive technique would be MOST effective?

A. 禁用 TCP 时间戳
B. 实施 MAC 地址过滤
C. 对 ICMP 数据包限速
D. SYN cookies

---

27. 为 Web 应用部署 TLS 时，新部署的最低可接受版本应是哪个?

When implementing TLS for a web application, which version should be considered the MINIMUM acceptable standard for new deployments?

A. TLS 1.0
B. SSL 3.0
C. TLS 1.2
D. TLS 1.1

---

28. 一家金融机构要求客户端和服务器之间进行双向认证（mutual authentication）。哪种 TLS 功能可以提供这种能力?

A financial institution requires mutual authentication between clients and servers. Which TLS feature provides this capability?

A. 会话恢复
B. 客户端证书认证
C. 完美前向保密（PFS）
D. 服务器名称指示（SNI）

---

29. 入侵检测系统（IDS）对正常的流量模式产生了大量告警。这属于哪种错误?

An intrusion detection system (IDS) is generating numerous alerts for normal traffic patterns. What type of error is occurring?

A. 误报（false positive）
B. 漏报（false negative）
C. 真阴性（true negative）
D. 真阳性（true positive）

---

30. 一家跨国公司遇到互联网路由中断。调查发现，一家外国 ISP 通过 BGP 宣告了该公司的 IP 地址空间。最可能发生的是哪种攻击？它与路由毒化（route poisoning）的主要区别是什么?

A multinational corporation experiences Internet routing disruptions. Investigation reveals that a foreign ISP is advertising the company's IP address space via BGP. Which attack is MOST likely occurring, and what is the PRIMARY difference from route poisoning?

A. BGP 劫持；它针对的是前缀所有权，而不是路由度量值
B. 路由毒化；它影响外部路由，而不是内部距离矢量协议
C. 路由抖动；它造成间歇性中断，而不是持续的流量重定向
D. AS 路径前置；它通过操纵自治系统编号来影响路由决策

资产安全

31. 一家金融服务公司的基线安全标准要求所有客户数据使用 AES-256 加密。风险评估发现，某些旧系统不支持 AES-256。安全架构师应采用什么流程来处理这个限制?

A financial services firm's baseline security standard requires AES-256 encryption for all customer data. A risk assessment reveals that certain legacy systems cannot support AES-256. What process should the security architect apply to address this constraint?

A. 裁剪（tailoring）
B. 补偿性控制
C. 范围界定（scoping）
D. 风险接受

---

32. 根据美国政府的密级政策，哪个标识适用于一旦未经授权披露，可以合理预期会对国家安全造成“严重损害”的信息?

Under U.S. government classification policy, which label applies to information whose unauthorized disclosure could reasonably be expected to cause 'serious damage' to national security?

A. 机密（Secret）
B. 受控非密信息（CUI）
C. 秘密（Confidential）
D. 绝密（Top Secret）

---

33. 在一个组织中，最终由谁负责确定数据的分类级别?

Who is ultimately responsible for determining the classification level of data within an organization?

A. 数据保管员（data custodian）
B. 数据所有者（data owner）
C. 安全管理员
D. 首席信息安全官（CISO）

---

34. 根据 HIPAA，一个组织必须把某些 HIPAA 合规文档至少保留 6 年，而根据适用的州法律则至少要保留 10 年。安全经理应建议这些文档的保留期限是多久?

An organization must retain certain HIPAA compliance documentation for a minimum of 6 years under HIPAA and a minimum of 10 years under an applicable state law. What retention period should the security manager recommend for that documentation?

A. 8 年，作为两项要求之间的折中
B. 10 年，以满足最严格的要求
C. 无限期保留，以避免合规风险
D. 6 年，以符合联邦 HIPAA 的要求

---

35. 一家跨国公司把欧盟客户的数据存放在云数据中心。法国客户担心他们的数据会被非欧盟实体依法强制调取。哪个原则最能解决这个担忧?

A multinational corporation stores EU customer data in cloud data centers. French customers are concerned about their data being legally compelled from non-EU entities. Which principle BEST addresses this concern?

A. 数据主权（data sovereignty）
B. 数据本地化（data localization）
C. 地理冗余
D. 数据驻留（data residency）

---

36. 一个组织的数据保留政策要求客户交易记录保存七年。期满后，处置流程的第一步是什么?

An organization's data retention policy requires keeping customer transaction records for seven years. At the end of this period, what is the FIRST step in the disposal process?

A. 确认不适用法律保留要求
B. 使用符合 DoD 5220.22-M 的工具覆写数据
C. 物理销毁所有存有这些数据的存储介质
D. 删除异地存储中的所有备份副本

---

37. 哪个角色主要负责确定组织数据资产的分类级别?

Which role is PRIMARILY responsible for determining the classification level assigned to an organizational data asset?

A. 数据管家（data steward）
B. 数据所有者（data owner）
C. 数据保管员（data custodian）
D. 数据处理者（data processor）

---

38. 一家医疗机构正在报废一批笔记本电脑，上面存有未加密的患者健康记录。哪种介质净化（sanitization）方法能提供最高程度的数据不可恢复保证?

A healthcare organization is decommissioning laptops that stored unencrypted patient health records. Which sanitization method provides the HIGHEST assurance of data irrecoverability?

A. 通过粉碎或焚烧进行物理销毁
B. 对加密密钥执行加密擦除（cryptographic erasure）
C. 使用随机数据七遍覆写
D. 使用 Type I 或 Type II 消磁机消磁

---

39. 一个组织要给一个新数据库分类，其中包含员工绩效评估、薪资信息和个人身份信息（PII）。未经授权披露可能造成竞争劣势和潜在的法律责任。最合适的分类级别是哪个?

An organization is classifying a new database containing employee performance reviews, salary information, and personally identifiable information (PII). The unauthorized disclosure could result in competitive disadvantage and potential legal liability. What classification level is MOST appropriate?

A. 机密（Secret）
B. 保密（Confidential）
C. 仅限内部使用（Internal Use Only）
D. 公开（Public）

---

40. 一家医疗机构要确定谁负责确保患者健康记录被正确分类、按监管要求保留，并且只有授权人员才能访问。谁对这些决定负主要责任?

A healthcare organization must determine accountability for ensuring patient health records are properly classified, retained according to regulatory requirements, and accessible only to authorized personnel. Who has PRIMARY responsibility for these decisions?

A. 数据处理者（Data Processor）
B. 首席信息安全官（CISO）
C. 数据所有者（Data Owner）
D. 数据保管员（Data Custodian）

安全与风险管理

41. 一名安全分析师发现，一名员工一直在没有业务理由的情况下访问机密的人力资源文件。该员工的岗位并不需要访问人力资源数据。最可能违反了哪项安全原则?

A security analyst discovers an employee has been accessing confidential HR files without business justification. The employee's role does not require access to HR data. Which security principle was MOST likely violated?

A. 知其所需
B. 纵深防御
C. 职责分离
D. 最小权限

---

42. 一个组织的 CISO 希望让安全计划与业务目标保持一致。哪个框架最适合这个目的?

An organization's CISO wants to align the security program with business objectives. Which framework is BEST suited for this purpose?

A. ISO 27002
B. COBIT
C. CIS Controls
D. NIST SP 800-53

---

43. 一家医疗机构遭到勒索软件攻击，患者记录被加密。CISO 向董事会报告了这起事件。CISO 体现的是哪个概念?

A healthcare organization suffers a ransomware attack that encrypts patient records. The CISO reports the incident to the board. Which concept is the CISO demonstrating?

A. 尽职调查（due diligence）
B. 职责分离
C. 谨慎人原则（prudent man rule）
D. 应尽关注（due care）

---

44. 一名 CISO 正在向董事会解释业务连续性计划（BCP）和灾难恢复计划（DRP）的关系。哪项说法最准确?

A CISO is explaining the relationship between Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) to the executive board. Which statement is MOST accurate?

A. BCP 只涉及 IT 系统和数据，而 DRP 涵盖所有业务运营
B. BCP 和 DRP 可以互换，描述的是同一个规划流程
C. DRP 是范围更广的战略计划，BCP 是其中的组成部分
D. BCP 是范围更广的战略计划，DRP 是侧重 IT 恢复的战术子集

---

45. 在灾难恢复演练中，发现备份磁带无法读取。BCP/DRP 生命周期的哪个阶段最可能被忽视了?

During a disaster recovery exercise, the backup tapes are found to be unreadable. Which phase of the BCP/DRP lifecycle was MOST likely neglected?

A. 风险评估
B. 业务影响分析（BIA）
C. 计划制定
D. 测试和演练

---

46. 一名风险分析师判断，某台文件服务器每年有 20% 的概率被勒索软件攻破，每次事件的预计损失为 50,000 美元。年度预期损失（ALE）是多少?

A risk analyst determines that a file server has a 20% annual probability of being compromised by ransomware, with an estimated loss of $50,000 per incident. What is the Annualized Loss Expectancy (ALE)?

A. $10,000
B. $50,000
C. $40,000
D. $250,000

---

47. 一个组织的安全团队正在制定新的访问控制政策。哪种文档类型应该限制最严格，并规定具体的强制性行动?

An organization's security team is developing a new access control policy. Which document type should be MOST restrictive and provide specific mandatory actions?

A. 程序（procedure）
B. 标准（standard）
C. 指南（guideline）
D. 政策（policy）

---

48. 一家公司正在为新的客户数据平台实施隐私设计（Privacy by Design）原则。哪种做法最能体现这个原则?

A company is implementing Privacy by Design principles for a new customer data platform. Which approach BEST demonstrates this principle?

A. 在投入生产之前，增加加密和访问控制来保护客户数据
B. 从最初设计起就把隐私控制内置到系统架构中，包括数据最小化和默认隐私设置
C. 对开发人员进行隐私要求培训，并开展隐私合规的代码审查
D. 在系统开发完成后进行隐私影响评估，以发现并整改隐私风险

---

49. 一家公司想转移与数据泄露相关的财务风险。它采用的是哪种策略?

A company wants to transfer financial risk associated with a data breach. Which strategy is being employed?

A. 风险缓解

B. 风险转移

C. 风险接受

D. 风险规避

---

50. 在一起涉及未经授权访问金融系统的安全事件中，哪个角色主要负责决定是否通知执法部门?

During a security incident involving unauthorized access to financial systems, which role is PRIMARILY responsible for determining whether law enforcement should be notified?

A. 事件响应团队负责人，因为他们掌握事件的最新信息

B. 首席信息安全官（CISO），因为他们负责所有安全事务

C. 高级管理层或法律顾问，因为这是涉及监管影响的业务和法律决定

D. 执法联络员，因为他们与外部机构保持联系

正确答案

1. C 不可否认性（non-repudiation）是指当事人不能否认自己做过某个操作，通常靠数字签名实现。发送方用私钥生成签名，别人可以用公钥验证，从而证明消息来源。身份验证只能确认身份，不一定能提供无法抵赖的证据，比如共享密码就分不清是谁操作的。保密性靠加密防止泄露，完整性通常靠哈希或 MAC 发现数据是否被改动，本身不能证明是谁发的。

2. A Bell-LaPadula 模型通过简单安全属性（不能向上读）和 *-属性（不能向下写）来保护保密性，防止信息从高密级流向低密级，是涉密环境中多级安全（multilevel security）的基础模型。Biba 和 Clark-Wilson 关注的是完整性，不是保密性。Brewer-Nash（中国墙，Chinese Wall）用于商业环境中防止利益冲突，不是按密级控制访问。

3. A TLS 配合 Diffie-Hellman，可以让双方在不安全的信道上建立共享密钥，是 HTTPS 的常规做法。使用临时 Diffie-Hellman（DHE/ECDHE）还能提供完美前向保密（perfect forward secrecy）。IPsec 多用于 VPN，需要预先配置，不适合面向任意客户端的网页流量。S/MIME 用于电子邮件加密。Kerberos 用于需要 KDC 和预先建立信任的企业环境，不适合公共电商场景。

4. D 双人完整性要求两名授权人员同时在场才能进入，防止单人擅自行动。双重认证的捕人陷阱（mantrap）（双门互锁通道）要求两人都通过认证才放行，核电设施和金融金库常用这种方式。生物识别加 PIN 只是单人的多因素认证。视频监控属于检测性控制，不能阻止一个人单独进入。密码锁让知道密码的人都能独自进入，密码共享还会削弱责任追溯。

5. A 纵深防御（也叫分层安全）是指部署多个相互独立的安全控制层，一层失效时，其他层仍能继续保护，例如防火墙、IDS/IPS、访问控制、加密和物理屏障配合使用。加固系统是减少攻击面，授予最小必要权限是最小权限原则（least privilege），出错时保持安全是故障安全（fail-safe/fail-secure）设计。

6. A 捕人陷阱（也叫 access control vestibule，即双门互锁通道）是预防性控制（preventive control），因为它要求在两道门前依次认证，且同一时间只开一道门，能在尾随（tailgating）和捎带进入（piggybacking）发生之前就阻止它们。检测性控制是在事件发生后发现问题，例如监控摄像头、运动传感器和审计日志。纠正性控制是在事件后修复损失，例如恢复备份和安装补丁。补偿性控制是在主要控制不可用时提供替代保护。

7. C Biba 通过“不能向上写”（防止低完整性主体破坏高完整性对象）和“不能向下读”（防止高完整性主体读取低完整性数据）来保护完整性，因此能防止交易记录被未授权修改。Bell-LaPadula 关注的是保密性。中国墙用于防止利益冲突。Graham-Denning 定义的是主体和对象的操作，不是以完整性为重点的模型。题目强调防止未授权修改，这是完整性问题，所以选 Biba。

8. A 客户端加密加本地 HSM 密钥管理，让加密操作不受云服务商控制，因此保持了对云服务商的独立性，同时可以通过第三方做受控的密钥托管，满足合规要求。使用云服务商的原生服务会形成供应商锁定，不满足独立性。云端管理密钥的信封加密仍然让密钥访问依赖服务商。数据库层 TDE 把密钥放在应用中，密钥保护不足，也没有解决托管要求。

9. C Bell-LaPadula 针对保密性实施强制访问控制（mandatory access control），有两条核心规则：简单安全属性（不能向上读）和 *-属性（不能向下写），防止信息从高密级流向低密级，正好符合题目要求。Biba 关注完整性，防止不可信主体的污染向上传播。Clark-Wilson 通过良构事务和职责分离保障商业完整性，没有密级格（lattice）的概念。Brewer-Nash 是动态限制访问，防止竞争组织之间的利益冲突。

10. B 带自动关断阀的水浸传感器能发现漏水，触发报警，并自动切断水源，尽量减少损失。传感器属于检测性控制，自动关断阀通过限制继续出水起到纠正作用。架空地板只能应对地面积水，防不了头顶的水管爆裂。正压系统防止外部污染物进入，管不了内部水管故障。HVAC 湿度监测只能发现环境潮湿，不能阻止爆管流出的水。

11. A 定期把实际配置与已批准的基线（baseline）对比，可以发现配置漂移（configuration drift），并为调查未经授权的变更提供依据。自动批准特权管理员的变更，等于绕过了变更授权。每次扫描后用当前配置替换基线，会把未授权的变更变成“正常”。只看硬件采购记录，发现不了服务器配置的变化。

12. C 第一响应人（first responder）是最先接触事件的人，负责识别事件，并立即采取遏制措施防止损失扩大。事件协调员管理整个响应流程并协调团队。取证分析员收集和分析证据，其中包括可能需要在遏制之前或期间保存的易失性证据。沟通负责人负责事件相关的内外部沟通。

13. C 低等级事件只是对非关键系统造成轻微中断，没有数据丢失，也没有重大业务影响。严重事件指影响核心业务的重大系统故障或数据泄露。高等级事件影响重要但非关键任务的系统，或造成有限的数据暴露。紧急事件指对生命、安全或关键基础设施的直接威胁。正确分级有助于合理分配资源并确定响应优先级。

14. D 驻留时间（攻击者在网络内停留的时长）要靠主动检测来缩短，只靠预防性控制不行。行为分析和威胁狩猎（threat hunting）能主动发现表明已被入侵的异常活动。漏洞扫描只能发现弱点，发现不了正在进行的威胁。安全培训降低的是最初被入侵的风险，不能检测入侵后的活动。更多防火墙属于预防性控制，解决不了检测缺口。持续监控和 UEBA 能把平均检测时间（MTTD）从几个月缩短到几天甚至几小时。

15. A 物理安全的纵深防御是由外向内分层的：先是周界控制（围栏、大门、保安），然后是建筑物入口控制（刷卡器、前台），再是内部房间控制（如服务器机房门禁），最后是资产层面的控制（上锁机柜、缆线锁）。这样攻击者必须突破多重屏障。其他选项的层次顺序都不对。分层思路在 CISSP 中既适用于物理安全，也适用于逻辑安全架构。

16. A 次要证据包括原始证据的副本、照片或复制品，在法庭上通常不如最佳证据（即原件）优先。最佳证据指原始文件或原物。佐证证据用来支持或印证其他证据，不一定是副本。传闻证据是转述别人说过的话，通常不被采纳。了解证据层级，对安全运营中的数字取证很重要。

17. C 恢复时间目标（RTO）规定了系统或流程中断后要在多长时间内恢复，“4 小时内恢复”是典型的 RTO。RPO 是可接受的数据丢失量，以时间衡量，例如最多丢失 2 小时的交易。MTD 是业务在影响变得不可接受之前能容忍的最长中断时间，RTO 必须在 MTD 之内留出业务恢复的时间。MTTR 是平均维修时间的运营指标，不是业务要求。

18. D RTO 4 小时是可接受的停机时间，RPO 1 小时是可接受的数据丢失量。在所列选项中，每晚全量备份加持续复制到温站（warm site）最合适：持续复制能满足 1 小时 RPO，配置得当并经过测试的温站能支持 4 小时内恢复。每 6 小时增量备份和每 4 小时差异备份都超过 1 小时 RPO，本地存放还有单点故障风险。每周或每天备份可能丢失长达 24 小时的数据。仍需通过恢复测试，验证启用温站和恢复数据库能在 4 小时内完成。

19. A RFC 3227 给出的易失性顺序示例是从寄存器和缓存开始，接着是一组同级的数据，包括路由表、ARP 缓存、进程表、内核统计信息和内存。再往后是临时文件系统，然后是磁盘、远程日志和监控数据、物理配置和网络拓扑，最后是归档介质。所以在这些选项中，应最先收集 CPU 寄存器和缓存。系统 RAM 与 ARP 缓存、路由表属于同一级，RFC 3227 并没有规定要先收集 RAM。

20. B 在所述的正式流程中，必须在实施前取得变更咨询委员会（Change Advisory Board，CAB）的批准，这样才能确保变更经过风险评估并符合业务需要，这是变更控制中的正式关卡。在非生产环境测试和通知利益相关者通常也要在实施前完成，但它们不是授权。配置管理数据库中的记录则是在变更实施后更新为新状态。CISSP 强调治理控制与技术准备并重。

21. C 在 802.1X 架构中，认证者（authenticator）（通常是交换机或无线接入点）充当中间方，把请求者（客户端设备）的认证请求转发给认证服务器，通常使用 RADIUS。认证者根据服务器的决定执行访问控制。RADIUS 代理可能出现在路径中，但它不是 802.1X 术语中定义的中间方。证书颁发机构负责签发证书，不参与实时认证流程。网络控制器不是标准的 802.1X 组件。

22. A WPA3-Enterprise 使用 802.1X 和可扩展认证协议（EAP），通过 RADIUS 服务器对每个用户单独认证，每人有各自的凭据，安全性达到企业级。这与使用对等同时认证（SAE）的 WPA3-Personal 不同。预共享密钥用于个人模式，不是企业模式。MAC 过滤安全性弱，因为地址很容易伪造。LEAP 是思科的专有协议，已被弃用且有已知漏洞，不属于 WPA3。

23. B SSL/TLS VPN 是最佳选择，因为它可以运行在 TCP 443 端口上，这个端口通常能穿过防火墙和 NAT 设备。基于隧道的 SSL/TLS VPN 可以承载 TCP 和 UDP 的应用流量，许多实现还提供基于 UDP 的数据通道以提高性能，并保留 TCP 作为备选。隧道模式 IPSec 支持 NAT 穿越，但可能被严格的防火墙拦截。L2TP/IPSec 同样依赖防火墙放行 IPsec 流量。PPTP 因常见认证配置存在已知漏洞，不适合安全通信。

24. D DDoS 攻击利用多个分散的来源向目标发送大量流量，耗尽服务器资源，使合法用户无法使用服务。关键线索是来自多个来源的流量激增和资源耗尽。中间人攻击是截获双方之间的通信，不靠流量洪泛。会话劫持是接管已认证的会话，不会造成流量激增。CSRF 利用已认证的会话执行未授权操作，也不涉及压垮服务器的大流量。

25. B 传输层（第 4 层）为源和目的进程提供端到端的通信服务。该层的 TCP 通过序号、确认、重传丢失的报文段以及滑动窗口流量控制来保证可靠性。UDP 也在这一层，提供无连接的尽力而为传输，适合速度比可靠性更重要的场合。数据链路层（第 2 层）用 MAC 地址在同一网段内逐节点传送。网络层（第 3 层）用逻辑 IP 地址在不同网络间路由数据包。会话层（第 5 层）管理应用间的对话控制和同步，不负责错误恢复。

26. D SYN cookies 让服务器在连接得到验证之前不为 TCP 握手分配资源，消除了状态耗尽的弱点，从而防御 SYN 洪水。服务器把连接信息编码进序列号，不再保存半开连接的状态。对 ICMP 限速针对的是另一种攻击途径，对 SYN 洪水无效。MAC 过滤是第 2 层控制，挡不住来自互联网的第 4 层攻击。禁用 TCP 时间戳只是去掉一个功能，无法防御 SYN 洪水造成的资源耗尽。

27. C 根据 NIST 和 PCI DSS 等行业标准，新部署的最低可接受版本是 TLS 1.2。它提供强密码套件，强制支持 SHA-256，并能防御已知攻击。TLS 1.0 和 1.1 因存在漏洞和弱密码支持而被弃用。SSL 3.0 有严重漏洞（POODLE 攻击），绝不应再使用。虽然 TLS 1.3 有更多改进，但 TLS 1.2 仍是合规和安全的最低基线。

28. B 客户端证书认证要求客户端在 TLS 握手时出示 X.509 证书，使双方互相验证对方身份，实现双向认证。标准 TLS 只认证服务器。SNI 让一个 IP 可以托管多个 TLS 站点，不影响认证方向。会话恢复加快重新连接，不改变认证要求。PFS 保证长期密钥泄露时会话密钥不受影响，但不提供双向认证。

29. A 误报是指 IDS 把合法流量错误地判定为恶意并发出告警。这会造成告警疲劳，浪费分析人员的时间。漏报是恶意流量未被发现，问题正好相反。真阳性是正确识别出真正的攻击。真阴性是正确识别出合法流量且不告警。误报属于调优问题，需要调整特征码、阈值或白名单。

30. A BGP 劫持是指某个自治系统（AS）未经授权宣告自己并不拥有的前缀，使其他 AS 把流量发往攻击者。路由毒化是 RIP 等距离矢量协议中合法的收敛技术，通过宣告无穷大的度量值来移除故障路由，不是针对前缀所有权的恶意行为。AS 路径前置是合法的流量工程手段，用来降低路由的优先级。路由抖动是路由宣告不稳定、状态反复变化，并不是有意重定向。劫持的本质是在域间路由中伪造前缀的来源权限。

31. A 裁剪（tailoring）是根据组织的具体限制、系统特点和运行环境调整基线安全控制，正适用于基线控制无法按规定实施的情况。范围界定是确定基线适用于哪些系统（即某项控制是否相关），不是调整相关但技术上做不到的控制。补偿性控制可以作为裁剪的一部分，在指定控制无法实施时提供适当保护。风险接受需要对剩余风险做出授权，它不是自动的最后一步，也不能代替满足适用的要求。

32. A 第 13526 号行政命令把涉密的国家安全信息分为三级。“机密”（Secret）适用于未经授权披露后可合理预期会对国家安全造成“严重损害”的信息。“绝密”（Top Secret）用于披露后可合理预期会造成“极其严重的损害”的信息。“秘密”（Confidential）是指可合理预期会造成“损害”的信息，没有“严重”这个限定。受控非密信息（CUI）不是密级，而是由 NARA 管理的另一类敏感但非涉密的联邦信息，有自己的处理要求。密级从低到高是 Confidential、Secret、Top Secret。

33. B 数据所有者（通常是业务部门经理或高管）最终负责确定分类级别，因为他们了解数据的业务价值和敏感性，并承担相应的风险。数据保管员负责实施技术控制，不决定分类级别。安全管理员执行别人制定的政策。CISO 制定总体的分类框架和政策，但不给每项数据资产分类，那是数据所有者的业务决策。区分制定框架（CISO）和资产分类（所有者）是 CISSP 的基础概念。

34. B 保留 10 年，以满足最严格的要求，这样同时满足两项适用的最低保留期限。州的 10 年要求并不取代联邦的义务，保留 10 年就同时满足了两者。保留 6 年会违反州法律。折中的 8 年达不到州法律的要求。无限期保留没有必要，成本高，还因保留数据超过所需时间而带来隐私风险。这种做法既满足两项法律义务，又不必无限期保留。

35. A 数据主权是指数据受其所在国家的法律和司法管辖，包括哪些政府可以强制调取。这正对应非欧盟政府对欧盟客户数据发出法律要求的担忧（例如美国的 CLOUD Act）。数据驻留只说明数据的物理存放地点，没有解决谁有权访问的管辖问题，数据可以存放在法国，却仍归美国母公司所有并可被其依法调取。数据本地化是要求数据留在境内的政策手段，是实现主权的工具，不是原则本身。地理冗余属于可用性概念，与法律调取无关。

36. A 处置任何数据之前，必须先确认没有法律保留（legal hold）、正在进行的诉讼、监管审计或其他义务要求继续保留。销毁受法律保留约束的数据，可能招致严重处罚，包括证据毁灭制裁和妨碍司法的指控。确认没有保全要求之后，才能进行技术销毁。物理销毁、覆写和删除备份都是有效的后续步骤，但在法律核实之前执行，会让组织面临法律责任。这是一道“像管理者一样思考”的题：合规和法律风险优先于技术执行。

37. B 数据所有者（通常是高级经理或业务部门高管）负责给数据资产指定分类级别，并定期复审。数据保管员（常是 IT 或系统管理员）实施所有者指定的安全控制，例如备份、访问控制列表和加密，但不做分类决定。数据管家关注数据质量、血缘和治理流程，不负责敏感性标签。数据处理者代表控制者或所有者处理数据，对分类政策没有决定权。CISSP 的说法是：所有者决定，保管员执行。

38. A 物理销毁的保证程度最高，因为它使介质彻底无法使用，任何方法都无法恢复。加密擦除只有在数据原本已加密时才有效，本题明确说数据未加密，所以不适用。七遍覆写有效，但理论上仍可能通过固件区域、坏扇区和预留空间恢复，在现代 SSD 上也不够可靠。消磁适用于磁性介质，对 SSD 无效，因为 SSD 用的是 NAND 闪存，不是磁存储。数据未加密且设备要报废时，物理销毁是黄金标准。

39. B “保密”（Confidential）是商业环境中合适的分类，适用于未经授权披露会对组织造成严重损害的数据，包括竞争损害和法律责任。PII、薪资数据和绩效评估合在一起，明显达到了这个门槛。“仅限内部使用”对有法律责任风险的数据来说太弱。“机密”（Secret）是政府的密级，商业环境通常不用。“公开”显然不适合敏感的员工数据。Confidential 级数据需要严格的访问控制，披露会造成严重危害，与本题的风险情况相符。

40. C 数据所有者（通常是业务经理或高管）对确定分类、保留要求和访问授权负主要责任，并对数据的业务价值和保护负责。数据保管员实施所有者指定的技术控制，不做政策决定。数据处理者代表控制者处理数据，没有分类决定权。CISO 提供安全指导和治理，但不拥有具体数据资产，那是业务职能。区分战略决策权（所有者）和战术实施（保管员），是 CISSP 资产安全域的基础。

41. A 知其所需（need-to-know）是指只有特定工作职能确实需要时才授予访问，即使用户有相应的许可级别也一样。该员工可能有权限访问这些文件（系统允许），但没有业务需要。最小权限与此密切相关，但它关注的是最小的权限级别，不是访问是否有业务需要的正当理由。职责分离是把任务分给多人以防止欺诈，与本题无关。纵深防御是分层的安全策略，不是访问原则。关键线索是“没有业务理由”，直接指向知其所需。

42. B COBIT（Control Objectives for Information and Related Technologies）专门用来让 IT 治理与业务目标保持一致，并提供管理框架。ISO 27002 是信息安全控制的实践准则，偏技术和运营，不侧重治理。NIST SP 800-53 为联邦系统提供安全和隐私控制，非常详细，但不是为了对齐业务目标。CIS Controls 是优先级排序的网络安全行动，偏战术，不是战略治理。当题目强调让安全与业务目标一致时，首选 COBIT。先想治理，再想控制。

43. D 应尽关注（due care）是指在正确的时间做正确的事，像合理谨慎的人那样行动。向董事会（以及在需要时向监管机构）报告泄露事件，就是应尽关注的例子。尽职调查（due diligence）是调查风险，并持续核实相应的保障措施和流程仍然有效，不只是部署前的研究和规划。谨慎人原则是说高管负有谨慎保护资产的受托责任，但本题问的是报告这个行为体现的是什么，答案是应尽关注。职责分离是分配任务以防欺诈，与本题无关。

44. D BCP 是一个全面的战略框架，涉及中断期间和之后所有关键业务职能的连续性，包括人员、流程、设施、供应链、通信和技术。DRP 范围更窄，是战术性文件，规定灾难事件后恢复 IT 系统、数据和基础设施的步骤。DRP 是 BCP 的组成部分，不是反过来。BCP 并不只关注 IT，那是 DRP 的范围。两者互补、相互依存，但不能互换。在 CISSP 考试中要“像管理者一样思考”：BCP 是业务战略层面，DRP 是技术恢复手册。

45. D 定期测试和演练可以验证恢复流程是否有效，包括备份的完整性。如果演练时磁带读不出来，说明之前的测试不够或根本没有做。业务影响分析（business impact analysis）找出关键系统和 RTO，不验证备份介质。风险评估识别威胁和漏洞，不测试控制措施。计划制定只是写出文档化的流程，没有测试就不知道它们是否可行。这是典型的考试情景：只有计划不够，还必须测试。

46. A ALE = SLE × ARO。SLE（单次预期损失）是一次事件的预计损失金额，即 $50,000。ARO（年度发生率）是预期每年发生的频率，即 0.20（20%）。ALE = $50,000 × 0.20 = $10,000。$50,000 只是 SLE，没有考虑年度发生频率。$250,000 是错误地把 $50,000 乘以 5（把概率倒过来当作频率）。$40,000 与题中数值没有数学关系。ALE 是定量风险分析的基石：如果防护措施的成本高于它能防止的 ALE，那么这项措施在经济上可能不划算。

47. B 标准（standard）规定了具体的配置、设置或要求（例如“所有密码必须至少 12 个字符”）。标准偏战术层面，可强制执行。政策是管理层意图的高层陈述，没有那么具体。程序描述落实政策和标准的分步工作流程，也可能是强制性的。指南是建议，不是强制要求。标准是最佳答案，因为它规定了可强制执行的要求，而程序规定的是执行这些要求的步骤。

48. B 隐私设计要求从一开始就把隐私嵌入系统架构，包括数据最小化（只收集必要的数据）和默认隐私（默认采用最有保护力的设置）等原则。开发之后再做隐私影响评估是被动的，不是主动的设计。部署前增加加密和访问控制解决的是安全问题，没有体现最小化收集和全程嵌入隐私的完整做法。开发人员培训有助于隐私，但不能保证隐私从最初设计就内置于架构。隐私设计是主动的预防性方法，不是开发后的补丁。

49. B 风险转移（risk transference）是把财务影响转给另一方，通常通过保险（网络责任险）或合同（带违约赔偿的云服务商 SLA）。该组织不是在规避风险（那意味着消除产生风险的活动），不是在缓解风险（实施控制措施以降低可能性或影响），也不是在接受风险（承认并记录，但不采取行动）。转移并不消除风险，只是转移了财务负担。这是 CISSP 考试中重点考查的基础风险管理概念。可以联想：保险、保修、带责任条款的外包。

50. C 是否让执法部门介入，是需要高级管理层或法律顾问批准的业务和法律决定，因为涉及可能的监管义务、诉讼风险、公开披露的影响和业务冲击。事件响应团队提供技术细节，但不做这种战略决定。CISO 虽然就安全事务提供建议，但通知执法部门涉及法律风险、合规（如数据泄露通知法）和企业声誉，需要高管层的权限。执法联络员负责促成联系，不决定是否发起。这体现了 CISSP 所要求的管理者视角：技术团队上报，管理层决定。

英文关键词

due care	应尽关注	像合理的人那样采取应有的保护行动
due diligence	尽职调查	调查风险并持续核实保护措施仍然有效
risk acceptance	风险接受	知道剩余风险并经授权承担它
risk transference	风险转移	把财务影响转给保险公司或第三方
risk avoidance	风险规避	停止会带来风险的活动
risk mitigation	风险缓解	用控制措施降低可能性或影响
residual risk	剩余风险	采取控制措施后仍然存在的风险
single loss expectancy (SLE)	单次预期损失	风险发生一次预计损失的金额
annualized rate of occurrence (ARO)	年度发生率	风险预计每年发生的次数
annualized loss expectancy (ALE)	年度预期损失	每年预计损失，等于 SLE 乘以 ARO
business continuity planning (BCP)	业务连续性计划	灾难期间和之后维持关键业务的战略计划
disaster recovery planning (DRP)	灾难恢复计划	灾难后恢复 IT 系统和数据的战术计划
business impact analysis (BIA)	业务影响分析	找出关键系统和所需恢复时间的分析
recovery time objective (RTO)	恢复时间目标	中断后恢复系统的目标时间

recovery point objective (RPO)	恢复点目标	可接受的数据丢失量，用时间表示
maximum tolerable downtime (MTD)	最大可容忍停机时间	业务能承受的最长中断时间
least privilege	最小权限	只给完成工作所需的最低权限
need-to-know	知其所需	因工作确实需要，才可接触某些信息
separation of duties	职责分离	把任务分给多人，防止舞弊
defense in depth	纵深防御	部署多层独立控制来保护资产
data owner	数据所有者	决定数据分类、保留和访问权的业务负责人
data custodian	数据保管员	按所有者的要求落实技术控制的人
data sovereignty	数据主权	数据受所在国家的法律管辖
legal hold	法律保留	因诉讼或调查而必须保留数据的要求
tailoring	裁剪	按实际限制调整基线安全控制
scoping	范围界定	判断基线控制适用于哪些系统
sanitization	介质净化	让介质上的数据无法恢复的处理
degaussing	消磁	清除磁性介质上的数据，对 SSD 无效
non-repudiation	不可否认性	做过某件事的一方事后不能否认
digital signature	数字签名	用私钥生成、用公钥验证的来源证明
key escrow	密钥托管	把密钥副本交给第三方保存
perfect forward secrecy (PFS)	完美前向保密	长期密钥泄露也不会暴露会话密钥
mantrap	捕人陷阱（双门互锁通道）	一次只开一扇门，防止尾随进入
preventive control	预防性控制	在事件发生前加以阻止的控制
detective control	检测性控制	发现已发生事件的控制，如监控录像
corrective control	纠正性控制	事件后修复损害的控制，如恢复备份
compensating control	补偿性控制	主要控制无法使用时的替代保护
false positive	误报	把正常流量判断为攻击
order of volatility	易失性顺序	取证时先收集最容易消失的数据
Change Advisory Board (CAB)	变更咨询委员会	评估并批准变更的小组

Examundo 是独立网站，与主办这些考试的机构没有隶属关系，也未获其认可。题目均为原创，不是考试真题。 examundo.tech/zh/cissp/