# CISSP 完整考试大纲与重点知识

说明：本文件基于 (ISC)² 2024 年 4 月更新的 CISSP 考试大纲，按 8 个域（Domains）结构化整理，包含每个域的核心知识点、记忆要点、考题套路、典型练习题（含详解）、备考计划与资源推荐，便于系统化复习与冲刺。使用时建议结合官方考试大纲与实操练习进行针对性训练。

## 目录

1. 快速概览（考试形式、题量、通过线、经验要求）
2. 备考建议与学习策略
3. 八大域（每域详解）
   * 域 1：Security & Risk Management（安全与风险管理）
   * 域 2：Asset Security（资产安全）
   * 域 3：Security Architecture & Engineering（安全体系结构与工程）
   * 域 4：Communication & Network Security（通信与网络安全）
   * 域 5：Identity & Access Management（身份与访问管理）
   * 域 6：Security Assessment & Testing（安全评估与测试）
   * 域 7：Security Operations（安全运营）
   * 域 8：Software Development Security（软件开发安全）
4. 典型练习题（含答案与详解）
5. 12 周备考计划（可调整）
6. 考试日与心理策略
7. 常见误区与答题技巧
8. 推荐资料与工具（书单、网站、练题平台）
9. 词汇表与速查表
10. 附录：考后步骤、持续专业教育（CPE）说明

## 1. 快速概览

* **证书名称**：CISSP（Certified Information Systems Security Professional）
* **颁发机构**：(ISC)²
* **考试形式（2024 刷新后）**：Computerized Adaptive Testing（CAT，自适应计算机考试）。
* **题量与时长**：100–150 题，考试时长为 **3 小时**。
* **题型**：多项选择题 & 先进题型（情景题、拖拽/排序等）。
* **及格标准**：按分数 700/1000 计分制（官方发布的通过线）。
* **工作经验要求**：一般需 5 年相关信息安全工作经验（或通过学历/相关认证折抵部分年限），通过考试后需完成 (ISC)² 背书流程以正式获得证书。

使用提示：以上为概要信息。参加考试前请务必以 (ISC)² 官方最新公告与考试大纲为准。

## 2. 备考建议与学习策略

### 核心原则

* **理解优先于死记**：CISSP 更多考察你在真实环境中如何权衡（治理、风险、合规与可操作性），不是简单背定义。
* **情境题导向训练**：多做情景题，训练跨域思维（题干常同时涉及风险、访问控制与运营场景）。
* **知识框架化**：把 8 个域做成思维导图或一页速查表，考试前用该图复盘。
* **错题本**：记录每次模拟中的错误与纠错思路，尤其是“看起来都对但只有一个最优答案”的题型。

### 学习工具与方法

* 按域分模块学习：每学完一域做 40–80 道题巩固；
* 做至少 3–5 套全真模拟（含计时练习）；
* 阅读官方大纲并把每个子主题映射到现实案例；
* 参与讨论组或学习伙伴，互换题目与解析，避免认知死角。

## 3. 八大域（每域详解）

### 域 1：Security & Risk Management（安全与风险管理）— **权重约 16%**

**核心目标**：掌握安全治理、法律合规、风险评估与管理、隐私与合规、企业安全策略与职业伦理。

**重点内容**： - CIA 三元组（保密性 Confidentiality、完整性 Integrity、可用性 Availability）的业务含义与案例应用； - 安全治理框架：公司治理如何与安全战略对齐；安全政策、标准、基线、程序与指南的区分与编写要点； - 风险管理流程：识别、评估（定性 / 定量）、应对（接受、转移、规避、减轻）、监控；风险登记册的要素； - 合规与法律：GDPR/隐私保护原则、数据主权、电子证据处理、合规性检查（审计）要求； - 业务连续性与灾难恢复（BCP / DRP）：关键业务识别、RTO（恢复时间目标）/ RPO（恢复点目标）、演练； - 供应链与第三方风险管理：供应商评估、合同条款（SLA、安全责任）、持续监控； - 职业道德与(ISC)² 行为准则：考生需知晓并承诺遵守。

**记忆技巧与答题要点**： - 风险应对策略四选一（接受/转移/规避/减轻）常出场，结合成本/业务影响判断最优方案； - 面对合规冲突时优先遵守适用法律/法规，再谈企业政策； - BCP/DRP 注重目标（RTO/RPO）和演练频率； - 题干中若涉及“最优治理层面”的决策，应选择策略性、长期且能兼顾合规的答案。

### 域 2：Asset Security（资产安全）— **权重约 10%**

**核心目标**：资产分类、数据生命周期管理、数据保护策略与对应控制。

**重点内容**： - 资产分类与分级（Public/Internal/Confidential/Restricted），以及与访问控制策略的映射； - 数据生命周期：创建、存储、使用、共享、归档与销毁；每一阶段的安全控制要点； - 数据标注与元数据管理：数据所有者（Owner）、数据监护人（Steward）、数据使用者角色与职责； - 数据隐私与敏感信息保护：PII、PHI 等的处理原则；最小暴露原则；数据脱敏/匿名化/伪匿名化技术； - 数据加密治理：静态数据（at-rest）、传输中数据（in-transit）、使用中数据（in-use）保护措施；密钥管理生命周期。

**记忆技巧与答题要点**： - 针对“如何保护数据”类题目，优先判断数据状态（静态/传输/使用）并选择合适控制（加密、访问控制、监控）； - 资产所有权与责任经常出题，明确谁来承担分类、权限审批与审计。

### 域 3：Security Architecture & Engineering（安全体系结构与工程）— **权重约 13%**

**核心目标**：掌握安全设计原则、常见安全模型、加密基础与系统硬件/软件安全性考量。

**重点内容**： - 安全设计原则：最小特权、默认拒绝、分层防御（Defense in Depth）、开闭原则、先验安全（Fail-Safe）、经济可行性； - 安全模型：Bell–LaPadula（机密性为主）、Biba（完整性为主）、Clark-Wilson（商业完整性）、非旁路授权模型等； - 加密学基础：对称/非对称加密、哈希函数、数字签名、公钥基础设施（PKI）、证书生命周期与撤销（CRL/OCSP）； - 密钥管理：生成、分发、存储、轮换、销毁；硬件安全模块（HSM）的角色； - 系统安全：可信计算、硬件根信任、固件安全、输入验证、防止缓冲区溢出与常见漏洞防护； - 安全架构框架（SABSA、TOGAF 与零信任架构（Zero Trust）思想）。

**记忆技巧与答题要点**： - 面对“加密技术/密钥管理”题目，注重密钥生命周期与信任链条； - 遇到“安全模型”类题，识别题干的目标（保护数据机密性还是完整性），快速映射模型（Bell-LaPadula vs Biba）；

### 域 4：Communication & Network Security（通信与网络安全）— **权重约 13%**

**核心目标**：网络体系结构安全、协议与传输安全、网络设备与安全边界设计。

**重点内容**： - 网络协议与模型（OSI / TCP-IP）与各层常见威胁（如链路层嗅探、传输层中间人、应用层注入）； - 边界防护：防火墙（包过滤、状态检测、下一代防火墙 NGFW）、入侵检测/防御（IDS/IPS）、代理、隔离（DMZ）； - 加密传输：TLS/SSL、IPsec、VPN 类型与使用场景（Site-to-Site vs Remote Access）； - 网络分段与微分段、子网划分、VLAN、SDN 与虚拟网络安全要点； - 无线安全（WPA2/WPA3、认证与加密、热点威胁、配置最佳实践）； - 常见网络攻击与防御（DDoS、ARP 欺骗、DNS 投毒、中间人攻击、重放攻击等）。

**记忆技巧与答题要点**： - 题目若涉及“远程安全访问”优先考虑 VPN 的类型与认证要求； - 在网络分段题目中，寻找能最小化攻击面并保持业务连续性的方案。

### 域 5：Identity & Access Management（身份与访问管理）— **权重约 13%**

**核心目标**：身份生命周期、认证与授权机制、访问控制模型及特权管理。

**重点内容**： - 身份识别、验证、授权与审计（IAM 的四大流程）； - 访问控制模型：自主访问控制（DAC）、强制访问控制（MAC）、角色基于访问控制（RBAC）、属性基于访问控制（ABAC）； - 认证方式：单因素/多因素认证（MFA）、生物识别、基于证书的认证（PKI）、SAML/OAuth/OpenID Connect 的基础与区别； - 身份联邦、单点登录（SSO）、身份即服务（IdaaS）与联合身份（Federation）； - 特权账号管理（PAM）、最小权限、分权审批流程； - 访问复核、访问日志与审计机制。

**记忆技巧与答题要点**： - 识别题干要点：是“认证”问题还是“授权”问题？ - 对于“SSO 与联合身份”类题，注意安全边界、注销与会话管理。

### 域 6：Security Assessment & Testing（安全评估与测试）— **权重约 12%**

**核心目标**：掌握安全评估方法、渗透测试、漏洞扫描、合规性审核与测评流程。

**重点内容**： - 安全评估计划与策略：测试范围、目标、规则、同意书（授权书）的重要性； - 自动化与手动测试：漏洞扫描、SAST（静态应用安全测试）、DAST（动态测试）、软件组成分析（SCA）； - 渗透测试与红队/蓝队演练、对抗演练（Purple Team）的作用； - 控制测试：技术控制与行政控制的测试方法； - 报告撰写：发现、风险等级、复现步骤、修复建议与优先级； - 持续合规监测与安全指标（KPI/ KRI）。

**记忆技巧与答题要点**： - 渗透测试强调范围与授权，未授权即为非法； - 报告中优先级排序应结合 CVSS、业务影响与可行性提出修复建议。

### 域 7：Security Operations（安全运营）— **权重约 13%**

**核心目标**：安全事件响应、取证、日志与监控、配置管理与日常运维控制。

**重点内容**： - 事件响应生命周期：准备、检测与分析、遏制、根除、恢复、事后总结； - 取证与链条保存（evidence handling）、法医级别日志要求； - 日志管理与 SIEM：日志收集、聚合、关联分析与告警管理； - 配置/变更管理、漏洞与补丁管理流程； - 物理/环境安全（设施与设备保护、访问控制）与人员安全（背景调查、离职流程）； - 威胁情报（TI）应用于运营的方式、自动化响应（SOAR）简介。

**记忆技巧与答题要点**： - 事件响应题目通常考察步骤顺序，注意“遏制 vs 根除”的区别； - 取证题中关注证据完整性（链条）与合法性（授权）；

### 域 8：Software Development Security（软件开发安全）— **权重约 10%**

**核心目标**：在软件开发生命周期（SDLC）中整体集成安全实践，防护常见软件缺陷。

**重点内容**： - 安全 SDLC：安全需求、威胁建模、静态/动态分析、代码审计、发布前的安全测试； - 常见 Web/应用漏洞：SQL 注入、跨站脚本（XSS）、跨站请求伪造（CSRF）、不安全的直接对象引用（IDOR）等，以及防御措施； - 第三方依赖与开源组件管理（SCA）、补丁策略与漏洞响应； - 安全默认配置、敏感信息处理（密钥/凭证管理）、日志与隐私保护在代码层面的实践； - 安全性度量与质量门槛（如安全缺陷密度、测试覆盖率）

**记忆技巧与答题要点**： - 面试/考试中涉及代码安全，优先考虑输入验证、输出编码与上下文相关的保护方法； - 第三方组件管理常被问到，强调版本管理、依赖扫描与紧急补丁策略。

## 4. 典型练习题（含答案与详解）

下面给出 10 道典型练习题，覆盖 8 个域的关键考点。均为模拟题型，含答案与解析，便于理解命题思路。

### 题 1（域 1 — 风险管理）

**题干**：公司准备上线一个处理敏感用户数据的新应用。安全团队评估发现某一流程存在较高的实现成本才能完全消除风险，但风险发生的概率较低，业务影响为中等。最优的风险处理策略应为下列哪项？

A. 风险接受

B. 风险规避

C. 风险转移（如保险）

D. 风险减轻（投入技术控制）

**答案**：C（风险转移）或 A（视组织风险承受能力）——**解析**：当完全消除风险成本过高且概率低时，常见做法是风险转移（如保险或合同条款）或在组织允许下接受风险。若题目强调在不影响合规/法律义务的前提下，则首选风险转移；若强调组织愿意承担，则选风险接受。考试题通常会通过细节区分最优项。

### 题 2（域 2 — 资产安全）

**题干**：哪项最能确保处于“传输中”状态的敏感数据的保密性？

A. 在源端与目标端对运行中的进程进行白名单控制

B. 使用基于角色的访问控制（RBAC）

C. 在传输链路中采用 TLS 或 IPsec 加密

D. 对数据进行日志记录与监控

**答案**：C。

**解析**：传输中数据的保密性主要通过加密传输层（如 TLS、IPsec）提供；其他选项有助于整体安全但不直接保证传输链路的保密性。

### 题 3（域 3 — 加密学）

**题干**：下列哪项最能验证数据在传输过程中未被篡改？

A. 对称密钥加密

B. 数字签名或消息认证码（MAC）

C. 数据脱敏

D. 访问控制列表

**答案**：B。

**解析**：数字签名或 MAC 用于验证完整性与来源，能检测篡改。

### 题 4（域 4 — 网络安全）

**题干**：为了保护企业边界免受外部网络攻击，应优先部署哪类设备？

A. 主机入侵检测系统（HIDS）

B. 网络防火墙与入侵防御（IDS/IPS）

C. 应用层 WAF（Web Application Firewall）

D. 安全信息与事件管理（SIEM）系统

**答案**：B。

**解析**：边界防护首要是网络防火墙与 IDS/IPS；WAF 更针对应用层；SIEM 则是监控与分析工具。

### 题 5（域 5 — IAM）

**题干**：机构希望减少长期口令泄露导致的风险，下列哪项为最佳措施？

A. 强制复杂口令并 90 天更换一次

B. 使用多因素认证（MFA）并限制密码重用

C. 增加密码长度并取消密码锁定策略

D. 关闭远程访问以防止口令被截取

**答案**：B。

**解析**：MFA 在减少凭证被滥用方面最有效，同时结合密码策略与限制重用效果更佳。

### 题 6（域 6 — 测试）

**题干**：渗透测试团队在未取得明确授权的情况下对客户环境进行测试，产生了系统中断。哪项描述最准确？

A. 因为是渗透测试属于安全工作，不构成问题。

B. 若无书面授权，行为可能构成非法入侵，渗透测试团队需对影响负责。

C. 只要测试有发现漏洞就能免责。

D. 渗透测试永远不应在生产环境执行。

**答案**：B。

**解析**：渗透测试必须在明确授权范围与协议下执行，未经授权可能违法或承担法律责任。

### 题 7（域 7 — 事件响应）

**题干**：在检测到勒索软件事件后，首要的响应行动应是什么？

A. 立即格式化受影响主机

B. 断开受影响主机的网络连接以阻止传播

C. 公开通知所有用户并发布细节

D. 立刻支付赎金以恢复业务

**答案**：B。

**解析**：初期遏制（如隔离/断网）是防止进一步传播与损害扩大的关键步骤；格式化或支付赎金并不是首选。

### 题 8（域 8 — 软件安全）

**题干**：在 Web 应用中防止 SQL 注入的有效措施是：

A. 在客户端使用 JavaScript 验证输入

B. 使用参数化查询（预编译语句）并进行输入验证

C. 将数据库放入 DMZ 区域

D. 仅允许内部 IP 访问数据库服务器

**答案**：B。

**解析**：参数化查询能够避免将输入直接拼接到 SQL 中，是防止 SQL 注入的主流做法；客户端验证不可靠。

### 题 9（综合题）

**题干**：公司 A 与外包方 B 签署开发合同，约定外包方负责某核心模块的开发并接触部分敏感数据。作为安全负责人，你最应该采取的步骤是？

A. 将所有敏感数据直接提供给外包方以便开发测试

B. 在合同中写明安全与保密条款、对外包方进行背景与安全能力评估，并把生产数据进行脱敏后提供

C. 取消外包，内部开发以更好保护数据

D. 仅在项目结束后对外包方进行安全评估

**答案**：B。

**解析**：涉及第三方与敏感数据时，应在合同中明确安全责任、进行安全评估，并尽量提供最小化/脱敏的数据用于测试与开发。

### 题 10（实践题）

**题干**：你管理的网络中发现异常流量指向外部未知 IP，SIEM 告警显示多个主机同时上传大量数据。作为第一步，你应该：

A. 关闭全部服务器以防止数据泄露

B. 立刻断开与外部网络连接并保留证据，同时通知 Incident Response 团队

C. 删除可疑文件并继续监控

D. 直接向客户公开说明数据泄露情况

**答案**：B。

**解析**：在保留证据的前提下尽快遏制（断网/隔离）并启动事件响应与通报流程是正确顺序。

## 5. 12 周备考计划（示例）

此计划以每天学习 1–2 小时为基础，依据工作/学习时间可适当压缩或拉长。

* **第 1–2 周**：通读官方考试大纲、熟悉 8 个域的总体结构；搭建思维导图；配置学习工具（题库、笔记、错题本）。
* **第 3–5 周**：深入域 1、域 2、域 3（每域至少完成 200 道练习题并整理错题）。
* **第 6–7 周**：深入域 4、域 5（网络与 IAM）；结合实验环境进行实操（搭建小型 VPN、测试 TLS 配置、实践 SSO）。
* **第 8 周**：域 6（测试方法）与域 7（运营/事件响应），实践演练写事件响应流程与取证思路。
* **第 9 周**：域 8（软件安全），结合 OWASP Top 10 做漏洞验证与防护练习。
* **第 10 周**：综合复习，做两套完整模拟题并计时；分析错题与薄弱点。
* **第 11 周**：按弱项补强，重做错题本，准备速查表与记忆卡片。
* **第 12 周**：冲刺（每日一套全真题），并做好考前准备（考点复盘、心理调节、考场流程熟悉）。

## 6. 考试日与心理策略

* 考前准备：熟悉 Pearson VUE 考场规则、证件要求；考前一晚保证充足睡眠；准备好必备证件与水、轻食；提前到达考场。
* 答题策略：先稳后快，遇到犹豫题做标记先跳过，答完易题后回头处理难题；注意题干关键词（NOT/EXCEPT/LEAST/BEST）；
* 心理调节：考试时遇到长题不要慌，分段阅读题干，找出业务目标与限制条件；三小时内合理安排短暂休息（若允许）。

## 7. 常见误区与答题技巧

* 误区：认为只要背书就能通过。解析题目时应以“实用性与可执行性”为衡量标准；
* 技巧：遇到多个看似正确答案，优先选择：合法合规 + 最小影响 + 可操作性；
* 注意题干是否限定成本/时间/法规等约束，这些往往决定“最优”选项；
* 对于“如何最快恢复业务”的题目，关注 RTO/RPO 与临时缓解措施（workaround）。

## 8. 推荐资料与工具

### 官方资源

* (ISC)² 官方 CISSP 考试大纲（Exam Outline）与 FAQ（长期以官方文档为准）。

### 书籍（经典）

* *CISSP Official (ISC)2 Practice Tests* — (ISC)² 官方题库练习（推荐做至少 2-3 遍）
* *CISSP Official Study Guide* — 体系化覆盖 8 个域的经典教材
* *Applied Cryptography*（加密学进阶）—— 对需深入理解加密原理的考生有帮助

### 在线平台与题库

* CCCure、Boson、Infosec、Cybrary、SANS（部分课程）等；
* OWASP（Web 安全实践）与 NIST 文档（框架、指南）。

### 实操工具（用于练习）

* 虚拟化环境：VMware/VirtualBox 构建实验环境；
* 网络实验：GNS3、EVE-NG；
* 渗透测试实践：Kali Linux、Metasploit、Burp Suite（社区版）

## 9. 词汇表与速查表（摘录常见术语）

* CIA：Confidentiality / Integrity / Availability
* RTO / RPO：恢复时间目标 / 恢复点目标
* MFA：Multi-Factor Authentication
* PKI：Public Key Infrastructure
* SAST / DAST / SCA：静态/动态/成分分析
* SIEM / SOAR：安全信息事件管理 / 安全编排自动化响应

## 10. 附录：考后步骤与持续专业教育（CPE）

* **背书（Endorsement）**：通过考试后，需由一名已认证的 (ISC)² 成员在规定时间内背书确认你的工作经验；若无法背书，可申请为 Associate of (ISC)² 并在 6 年内补齐经验。
* **CPE 要求**：持证人需每年维持一定数量的 CPE 学时与年费以保持证书有效性（具体以官方最新政策为准）。

## 附：使用许可与声明

本文件为学习参考资料，内容力求准确并基于 2024 年 4 月的考试大纲改版整理，但不替代 (ISC)² 官方考试大纲与政策。考试细则、题型或权重若有变更，请以 (ISC)² 官方公告为准。

*文档生成：CISSP 完整考试大纲与重点知识（中文） — 结束*