

Passing Standard: 700 out of 1000 (CAT adaptive)

Format & Timing: Computerized Adaptive Testing (English): 100-150 items, up to 3 hours. (Pearson VUE)

Testing Windows: On-demand, year-round

1. OFFICIAL 2026 BLUEPRINT DOMAINS & WEIGHTINGS**CISSP-1: Security and Risk Management****Weight: 16%**Confidentiality, Integrity, and Availability (CIA), Security Governance Principles, Alignment with Business Strategy, and Organizational Roles, Compliance, Legal, and Regulatory Issues (Cybercrime, Licensing, Intellectual Property, Transborder Data Flow, GDPR, HIPAA) and (ISC)² Code of Ethics, Business Continuity**CISSP-2: Asset Security****Weight: 10%**

Information and Asset Classification, Categorization, and Ownership (Data Owner, Asset Owner, Custodian, Steward, Processor, Controller), Privacy Protection, Data Lifecycle States (Data at Rest, Data in Transit, Data in Use), and Data Remanence, Asset Retention Policies, End-of-Life (EOL)/End-of-Support (EOS), and

CISSP-3: Security Architecture and Engineering**Weight: 13%**

Secure Design Principles (Least Privilege, Defense in Depth, Fail-Safe, Economy of Mechanism, Zero Trust, Privacy by Design) and Security Models (Bell-LaPadula, Biba, Clark-Wilson, Brewer-Nash), Security Capabilities of Information Systems: TPM, HSM, Trusted Computing Base (TCB), Reference Monitor,

CISSP-4: Communication and Network Security**Weight: 13%**

Secure Network Architecture: OSI and TCP/IP Models, IPv4/IPv6, Secure Protocols, DNSSEC, Micro-Segmentation (VLANs, VxLAN, SD-WAN, Zero Trust Network Access), Wireless, Cellular (4G/5G), and IoT Communication Security (WPA2/WPA3, 802.1X, EAP, Bluetooth, Zigbee, RFID), Secure Network

CISSP-5: Identity and Access Management (IAM)**Weight: 13%**

Physical and Logical Access Control to Assets, Authentication Factors (Something You Know/Have/Are, Biometrics FRR/FAR/CER), and Multifactor Authentication (MFA), Federated Identity Management (FIM), Single Sign-On (SSO), Kerberos, SAML, OAuth 2.0, OpenID Connect (OIDC), and Credential Management,

CISSP-6: Security Assessment and Testing**Weight: 12%**

Design and Validate Assessment, Test, and Audit Strategies (Internal, External, Third-Party; SOC 1/2/3 Reports under AT-C 320 / Trust Services Criteria), Security Control Testing: Vulnerability Assessments, Penetration Testing (Black/White/Gray Box, Phases), Breach and Attack Simulation (BAS), and Log Reviews, Software

CISSP-7: Security Operations**Weight: 13%**

Investigations and Digital Forensics: Evidence Collection, Order of Volatility, Chain of Custody, eDiscovery, and Criminal/Civil/Administrative Law, Logging, Monitoring, and Detection: SIEM, SOAR, UEBA, Intrusion Detection/Prevention (HIDS/NIDS), Threat Intelligence Feeds, and Continuous Monitoring,

CISSP-8: Software Development Security**Weight: 10%**

Security in the Software Development Lifecycle (SDLC): Agile, Waterfall, DevSecOps, Maturity Models (CMMI, SAMM, BSIMM), and CI/CD Pipeline Security, Security Controls in Development Environments: Source Code Repositories, Version Control, Application Security (OWASP Top 10, Buffer Overflows, SQLi, XSS,

2. PRIMARY STATUTORY & REGULATORY AUTHORITIES TESTED*** (ISC)² Common Body of Knowledge (CBK) - CISSP CBK (2024)**

The eight-domain examinable body of knowledge

*** ISO/IEC 27001 - ISO/IEC 27001:2022**

Information security management system standard

3. EXAMINER TRAPS & HIGH-YIELD PASS STRATEGY

Key Challenge: Enormous breadth across governance, engineering, and operations at a managerial judgment level.