 INFOSECTRAIN

# CISSP

Certified Information  
System Security Professional

**2024**

Exam Preparation Training



[www.infosectrain.com](http://www.infosectrain.com)

## CISSP Program Overview

The CISSP® certification is one of the most renowned achievements within the realm of information security. Our training course is meticulously crafted to endow participants with the technical skills and managerial prowess necessary to effectively design, build, and oversee an organization's security framework, aligning with globally recognized information security norms.

(ISC)<sup>2</sup> is a globally recognized nonprofit organization dedicated to advancing the information security field. The CISSP® was the first credential in information security to meet the stringent requirements of ISO/IEC Standard 17024. It is looked upon as an objective measure of excellence and a highly reputed standard of achievement.



### Learn by Practice

Experience Immersive Learning with highly interactive sessions and hands-on labs



### Take Regular Assessments

Bridge knowledge-gaps with our free mock exams and high intensity skill assessments



### Earn CPEs

Complete your CPE target by getting CPEs and accessing our library of most trending courses

## Why CISSP® Training Course with InfosecTrain?

---

InfosecTrain is a leading IT security training and consulting organization offering best-in-class yet cost-effective, customized training programs to enterprises and individuals across the globe. We offer role-specific certification training programs and prepare professionals for the future. Our CISSP® certification training course provides participants with the technical and managerial skills that are in demand for designing, architecting, and managing an organization's security posture by using globally recognized information security standards.

Here's what you get when you choose InfosecTrain as your learning partner:

- **Flexible Schedule:** Training sessions to match your schedule and accommodate your needs.
- **Extended Post Training Support:** Ongoing assistance and support until the learners achieve their certification goals.
- **Recorded Sessions:** Access to LMS or recorded sessions for post-training reference.
- **Customized Training:** A training program that caters to your specific learning needs.
- **Knowledge Sharing Community:** Collaborative group discussions to facilitate knowledge sharing and learning.
- **Certificate:** Each candidate receives a certificate of participation as a testament to their accomplishment.
- **Expert Career Guidance:** Free career guidance and support from industry experts.

## Target Audience

---

- Chief Information Security Officer
- Chief Information Officer
- Director of Security
- IT Director/Manager
- Security Systems Engineer
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- Security Consultant
- Network Architect

## Pre-Requisites

To apply for the CISSP® certification, you need to:

- Have a minimum 5 years of cumulative paid full-time work experience in two or more of the 8 domains of the (ISC)<sup>2</sup> CISSP® Common Body of Knowledge (CBK).
- A one-year experience waiver can be earned with a 4-year college degree, regional equivalent, or additional credential from the (ISC)<sup>2</sup> approved list.

## About the **CISSP** Exam

Exam Name	CISSP CAT 2021	CISSP CAT 2024
Launch Date	Effective May 1, 2021	Effective April 15, 2024
Exam Duration	4 hours	<b>3 hours</b>
Number of Items	125-175	<b>100-150</b>
Exam Format	Multiple-choice and advanced innovative items	Multiple-choice and advanced innovative items
Passing Score	700 out of 1000 points	700 out of 1000 points
Language	English	English
Testing Center	(ISC) <sup>2</sup> Authorized PPC and PVTTC Select Pearson VUE Testing Centers	(ISC) <sup>2</sup> Authorized PPC and PVTTC Select Pearson VUE Testing Centers

**Note:** CISSP® is a registered mark of The International Information Systems Security Certification Consortium ((ISC)<sup>2</sup>). We are not an authorized training partner of (ISC)<sup>2</sup>.

## Course Objectives


---

You will be able to:


- Master core concepts of risk management, security governance, and compliance.
- Understand the ethical and legal requirements impacting information security.
- Learn to classify information and assets, ensuring appropriate protection.
- Understand data security controls and asset retention.
- Gain insights into secure design principles, engineering processes, and security models.
- Apply cryptography and secure architecture solutions effectively.
- Develop skills in designing and protecting network security.
- Manage secure network architecture and components.
- Implement comprehensive IAM solutions, including access control, identity management, and authentication mechanisms.
- Integrate third-party identity services and manage identities across different platforms.
- Conduct assessments and testing of security systems to identify vulnerabilities.
- Analyze and interpret test data to enhance security measures.
- Understand operational security controls, incident management, and disaster recovery.
- Support forensic investigations and understand the foundations of operational security.
- Enforce security controls in software development environments.
- Integrate security throughout the Software Development Life Cycle (SDLC).

## CISSP Course Highlights


---



**48-Hour LIVE**  
Instructor-led Training



Full **8-Domain**  
Exam Practice



Accredited  
**Instructors**



Learn from  
**Industry Experts**



### **100% Satisfaction Guarantee**

Not satisfied with your training on Day 1?  
You can get a refund or enroll in a different course.



### **Access Recorded Sessions**






Revisit your lectures, revise your concepts, and retain  
your knowledge From anywhere, whenever you want



### **Extended Post Training Support**

Get extended support even after you finish your training.  
We're here for you until you reach your certification  
goals.

## Who Should **Attend**

- 
 Chief Information Security Officers
- 
 Security Systems Administrators
- 
 Information Assurance Analysts
- 
 IT Security Engineers
- 
 Senior IT Security Consultants
- 
 Senior Information Security Risk Officers

## **CISSP** Examination Weights

Domain	% on 2021 CBK®	% on 2024 CBK®
Security and Risk Management	15%	16%
Security Architecture and Engineering	10%	10%
Asset Security	13%	13%
Communication and Network Security	13%	13%
Identity and Access Management (IAM)	13%	13%
Security Assessment and Testing	12%	12%
Security Operations	13%	13%
Software Development Security	11%	10%



## Our Expert **Instructors**

---

### **PRABH NAIR**

18+ Years Of Experience

CISSP-ISSAP | CGRC | CCSP | CSSLP | CCISO | CISM | CISA | CRISC | CGEIT | CIPM  
CIPPE | CDPSE

18+ years of IT industry experience, specializing in Information Security. Expertise spans Vulnerability Assessment & Penetration Testing, Application Security, IT Governance, Risk & Compliance, and Security Solutions. Led global Information Security operations for a US-based IT Service Provider with a presence in the US, Canada, India, and Sri Lanka. Delivered services to 250+ organizations across 25+ countries through diverse assignments.

### **PRASHANT**

14+ Years Of Experience

CISSP-ISSAP | CCSP | C|EH | CPISI

14+ years of experience as a seasoned Information Security professional with hands-on experience in auditing application's controls, identifying breaches in policies/controls, communicating gaps and risks associated with the business and providing solutions to the stakeholders.

Prashant's core strength is to help build a robust and effective security strategy and provide the most appropriate security solution for an organization. He is an acclaimed trainer, coach & mentor for more than 300 aspirants and has delivered tailor-made workshops to corporate learners from all over the world. He uses his hands-on experience and his firm hold on the ISMS knowledge to assist students understand the concepts and apply them in real time scenarios. He is very enthusiastic about helping students achieve their certification goals and makes sure that complete support is provided from his side for students' success.



**KK SINGH****18+ Years Of Experience****C|CISO | CISSP | CCSP | CISM | CRISC | CISA | CCSK | CCAK | CDPSE | CEH | RHCSA  
GRCA | GRCP | CPP | PSP | PCI | AZ-900 | GDPR**

With 18+ years of experience, KK is a seasoned Cyber Security Professional with a stellar record in developing and executing cybersecurity strategies for global organizations. He is an expert dedicated to safeguarding sensitive data and ensuring the integrity and availability of critical systems. He has extensive experience in the evolving cybersecurity landscape, excelling in areas such as risk management, incident response, security architecture, and both network and cloud security. His expertise also covers identity and access management, digital transformation security, DevSecOps, and compliance with standards like GDPR and ISO 27001. Equipped with advanced knowledge in blockchain, AI/ML security, and frameworks like Archer GRC, he is committed to staying ahead of emerging threats and delivering comprehensive protection for today's complex digital environment. Holding certifications such as C|CISO, CISSP, CCSP, CISM, CRISC, CISA, CCSK, CCAK, CDPSE, CEH, RHCSA, GRCA, GRCP, CPP, PSP, and PCI, KK is a recognized Cloud & Cybersecurity Strategist and a prominent CyberSec Leader, Speaker, and Mentor. He is committed to staying ahead of emerging threats and ensuring robust protection in today's complex digital world.


**SUJAY****15+ Years Of Experience****CSOA | CCSP | CISSP | ISO 27001 Lead Auditor | ITIL v3**

Nearly 15+ years of experience as a seasoned, technically inclined and highly empowered IT professional with strong emphasis on understanding business vision, requirements, effective communication and team building to deliver robust IT solutions and services. Sujay delivers power-packed training sessions on certification courses like CISSP, CCSP, AWS Architect, Cloud Architecture, Information Security Awareness. His sessions are highly interactive, maintaining a very high success rate throughout his courses.

# Happy Learners Across the World

**ARUP KUMAR BASAK** • 2nd  
CISM | CCSA | CC | CCNP | ITIL | CPISI  
1w • Edited • 🗨️

All praises for Almighty. Happy to share that i've passed CISSP today.Thanks to [Luke Ahmed](#) 🙏[Md Showkat Ali](#) vaiya [Thor Pedersen - Lead trainer at ThorTeaches](#) [Infosec Train](#) for all the guidance during this long journey ! [#isc2](#) [#cissp](#) [#informationsecurity](#) [#itgovernance](#) [#itsecurity](#) [#itoperations](#)


**ISC2** Your future. Secured.

**Aneesh Vidyasagar** • 2nd  
Network and Security engineer | Network Design&Implementation | CISS...  
1mo • 🗨️

I'm delighted to announce that I have achieved another milestone , CISSP !! After two years of planning, like things unfold when the time is right , meeting [Infosec Train](#) , and especially [Prabh Nair](#) was the turning point. In today's business-driven market, [Prabh Nair](#) stands out as an immensely passionate educator, dedicated to nurturing quality cyber security 'gladiators' as he fondly calls, for the industry.

**Vinitha Ravindran (CISM, CISSP, CCSP)** • 2nd  
Information Security Program Manager  
2w • Edited • 🗨️

I am very glad and humbled to have achieved this feat. 🙏

[ISC2](#) [#CISSP](#)

It was not easy (toughest exam ever taken in my professional life). Here is my journey of preparation -

These practice questions and tests helped to understand how the questions could be and how to think while answering them.

Materials that I used -

- Took 40 hours of training session from [Infosec Train](#), to understand the concepts.
- ISC2 CISSP Official Study Guide - Ninth Edition
- ISC2 CISSP Official Practice Tests - Third Edition [used LearnZ app for easy access to these questions]
- Materials from [#InfosecTrain](#) (training materials and question practice sets)
- Boson question practice
- LinkedIn Learning - Mike Chapple's CISSP videos (24 hours)
- YouTube and LinkedIn - [Prabh Nair](#) CISSP videos and other relevant materials

**Sumit Kumar, CISSP** • 2nd  
Cybersecurity Consultant | CISSP | CC | CyberArk CDE | IAM ...  
1w • 🗨️ [+ Follow](#) • ••

Excited to share that I've earned the CISSP certification on my first attempt! 🙏 Grateful for the support from mentors and colleagues who guided me through this journey. Ready to apply my enhanced skills in ensuring robust cybersecurity. I would like to specially thanks to

[Mike Chapple](#) for ISC2 official guide  
[Prabh Nair](#) from [Infosec Train](#) for CISSP training  
[Thor Pedersen - Lead trainer at ThorTeaches](#) - for fantastic course and tests on Udemy  
[Destination Certification Inc.](#) - Must review Mind map videos for all domains before attempting for exam

[#CISSP](#) [#Cybersecurity](#) [#cybersecurity](#) [#AchievementUnlocked](#)

**Jafar Hasan, CISSP** • 2nd  
CISSP | CC | ISO 27001:2022 Lead Auditor | CRTP | CEH | (IS...  
2mo • Edited • 🗨️ [+ Follow](#) • ••

🌟 Exciting Announcement! 🌟

I begin with gratitude to ALLAH – Alhamdulillah for guiding me and granting me the strength to persevere. ShukrAllah🙏

Thrilled to share that I've successfully Cleared the [ISC2](#) [#CISSP](#) Certification Exam, marking a significant milestone in My Cybersecurity journey! 🚀

First and foremost, huge appreciation to my mentor, [Prabh Nair](#) – God of CISSP & [Infosec Train](#), Who support and guide me in every situation, Your guidance and expertise have been the driving force behind this achievement.

**Naveen BJ** • 2nd  
Application Security Program Manager at Dell Technologies. Passionatel...  
2d • Edited • 🗨️ •••

Hello Everyone !!!

I am thrilled to share this with you all. 🙏

I provisionally passed the CISSP exam !!!

Thank you [Prashant Mohan, CISSP-ISSAP, CCSP](#) [Luke Ahmed](#) 🙏[Mike Chapple](#), [Prabh Nair](#), [Adam Gordon](#), [Sujit Christy](#), [ISC2 Central New Mexico Chapter](#), [Eric Conrad](#), [David R. Miller](#), [Destination Certification Inc.](#) 🙏[Damian Lager](#), [CCISO](#), [CISSP-ISSAP](#), [CRISC](#), [CISM](#), [CCSP](#) 🙏[Mohamed Afaf Peto Zenger](#) 🙏[Kelly Handelman](#) [Babun Gurusamy](#) 🙏[#cissp](#) [#cissptraining](#) [Guenevere \(Gwen\) Bettwy \('bet 'we\)](#) [Infosec Train](#) [ISC2 Colombo Chapter](#), [Sri Lanka](#), [Thor Pedersen](#) - Lead trainer at [ThorTeaches](#), [Srikanthan Kumarasingh](#), [Lakshan Srikanthan](#), [Rob Wischer](#), [SANS Institute](#)

## CISSP Domains

---



Domain 1: Security and Risk Management **(16%)**



Domain 2: Asset Security **(10%)**



Domain 3: Security Architecture and Engineering **(13%)**



Domain 4: Communication and Network Security **(13%)**



Domain 5: Identity and Access Management (IAM) **(13%)**



Domain 6: Security Assessment and Testing **(12%)**



Domain 7: Security Operations **(13%)**



Domain 8: Software Development Security **(10%)**



## Domain 1

# Security and Risk Management (16%)

---

### 1.1 Understand, adhere to, and promote professional ethics (2-4 items)

- » ISC2 Code of Professional Ethics
- » Organizational code of ethics

### 1.2 Understand and apply security concepts

- » Confidentiality, integrity, availability, authenticity, and nonrepudiation (5 Pillars of Information Security)

### 1.3 Evaluate, apply, and sustain security governance principles

- » Alignment of the security function to business strategy, goals, mission, and objectives
- » Organizational processes (e.g., acquisitions, divestitures, governance committees)
- » Organizational roles and responsibilities
- » Security control frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI), Federal Risk and Authorization Management Program (FedRAMP))

### 1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context

- » Cybercrimes and data breaches
- » Licensing and Intellectual Property requirements
- » Import/export controls
- » Transborder data flow
- » Issues related to privacy (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act)
- » Contractual, legal, industry standards, and regulatory requirements

**1.5 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, and industry standards)**

**1.6 Develop, document, and implement security policy, standards, procedures, and guidelines**

**1.7 Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements**

- » Business impact analysis (BIA)
- » External dependencies

**1.8 Contribute to and enforce personnel security policies and procedures**

- » Candidate screening and hiring
- » Employment Agreements and policy-driven requirements
- » Onboarding, transfers, and termination processes
- » Vendor, consultant, and contractor agreements and controls

**1.9 Understand and apply risk management concepts**

- » Threat and vulnerability identification
- » Risk analysis, assessment, and scope
- » Risk response and treatment (e.g., cybersecurity insurance)
- » Applicable types of controls (e.g., preventive, detection, corrective)
- » Control assessments (e.g., security and privacy)
- » Continuous monitoring and measurement
- » Reporting (e.g., internal, external)
- » Continuous improvement (e.g., risk maturity modeling)
- » Risk frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI))

**1.10 Understand and apply threat modeling concepts and methodologies**

### **1.11 Apply supply chain risk management (SCRM) concepts**

- » Risks associated with the acquisition of products and services from suppliers and providers (e.g., product tampering, counterfeits, implants)
- » Risk mitigations (e.g., third-party assessment and monitoring, minimum security requirements, service level requirements, silicon root of trust, physically unclonable function, software bill of materials)

### **1.12 Establish and maintain a security awareness, education, and training program**

- » Methods and techniques to increase awareness and training (e.g., social engineering, phishing, security champions, gamification)
- » Periodic content reviews to include emerging technologies and trends (e.g., cryptocurrency, artificial intelligence (AI), blockchain)
- » Program effectiveness evaluation



## Domain 2

# Asset Security (10%)

---

### 2.1 Identify and classify information and assets

- » Data classification
- » Asset Classification

### 2.2 Establish information and asset handling requirements

### 2.3 Provision information and assets securely

- » Information and asset ownership
- » Asset inventory (e.g., tangible, intangible)
- » Asset management

### 2.4 Manage data lifecycle

- » Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
- » Data collection
- » Data location
- » Data maintenance
- » Data retention
- » Data remanence
- » Data destruction

### 2.5 Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

### 2.6 Determine data security controls and compliance requirements

- » Data states (e.g., in use, in transit, at rest)
- » Scoping and tailoring
- » Standards selection
- » Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP) Cloud Access Security Broker (CASB))





## Domain 3

# Security Architecture and Engineering (13%)

---

### 3.1 Research, implement and manage engineering processes using secure design principles

- » Threat modeling
- » Least privilege
- » Defense in depth
- » Secure defaults
- » Fail securely
- » Separation of Duties (SoD)
- » Keep it simple and small
- » Zero Trust or trust but verify
- » Privacy by design
- » Shared responsibility
- » Secure access service edge

### 3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

### 3.3 Select controls based upon systems security requirements

### 3.4 Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

### 3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- » Client-based systems
- » Server-based systems
- » Database systems
- » Cryptographic systems
- » Industrial Control Systems (ICS)
- » Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- » Distributed systems
- » Internet of Things (IoT)
- » Microservices (e.g., application programming interface (API))
- » Containerization
- » Serverless
- » Embedded systems
- » High-Performance Computing (HPC) systems
- » Edge computing systems
- » Virtualized systems

### 3.6 Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)

- » Cryptographic life cycle (e.g., keys, algorithm selection)
- » Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
- » Public Key Infrastructure (PKI) (e.g., quantum key distribution)
- » Key management practices (e.g., rotation)
- » Digital signatures and digital certificates (e.g., non-repudiation, integrity)

### 3.7 Understand methods of cryptanalytic attacks

- » Brute force
- » Ciphertext only
- » Known plaintext
- » Frequency analysis
- » Chosen ciphertext

- » Implementation attacks
- » Side-channel
- » Fault injection
- » Timing
- » Man-in-the-Middle (MITM)
- » Pass the hash
- » Kerberos exploitation
- » Ransomware

### **3.8 Apply security principles to site and facility design**

#### **3.9 Design site and facility security controls**

- » Wiring closets/intermediate distribution facilities
- » Server rooms/data centers
- » Media storage facilities
- » Evidence storage
- » Restricted and work area security
- » Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
- » Environmental issues (e.g., natural disasters, man-made)
- » Fire prevention, detection, and suppression
- » Power (e.g., redundant, backup)

#### **3.10 Manage the information system lifecycle**

- » Stakeholders needs and requirements
- » Requirements analysis
- » Architectural design
- » Development /implementation
- » Integration
- » Verification and validation
- » Transition/deployment
- » Operations and maintenance/sustainment
- » Retirement/disposal



## Domain 4

# Communication and Network Security (13%)

### 4.1 Assess and implement secure design principles in network architectures

- » Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- » Internet Protocol (IP) version 4 and 6 (IPv6) (e.g., unicast, broadcast, multicast, anycast)
- » Secure protocols (e.g., Internet Protocol Security (IPSec), Secure Shell (SSH), Secure Sockets Layer (SSL)/Transport Layer Security (TLS))
- » Implications of multilayer protocols
- » Converged protocols (e.g., Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP), InfiniBand over Ethernet, Compute Express Link)
- » Transport architecture (e.g., topology, data/control/management plane, cut-through/store-and-forward)
- » Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)
- » Traffic flows (e.g., north-south, east-west)
- » Physical segmentation (e.g., in-band, out-of-band, air-gapped)
- » Logical segmentation (e.g., virtual local area networks (VLANs), virtual private networks (VPNs), virtual routing and forwarding, virtual domain)
- » Micro-segmentation (e.g., network overlays/encapsulation; distributed firewalls, routers, intrusion detection system (IDS)/intrusion prevention system (IPS), zero trust)
- » Edge networks (e.g., ingress/egress, peering)
- » Wireless networks (e.g., Bluetooth, Wi-Fi, Zigbee, Satellite)
- » Cellular/mobile networks (e.g., 4G, 5G)
- » Content distribution networks (CDN)
- » Software-defined networks (SDN) (e.g., application programming interface (API), Software-Defined Wide-Area Network, network functions virtualization)
- » Virtual Private Cloud (VPC)
- » Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)

## 4.2 Secure network components

- » Operation of infrastructure (e.g., redundant power, warranty, support)
- » Transmission media (e.g., physical security of media, signal propagation quality)
- » Network Access Control (NAC) systems (e.g., physical and virtual solutions)
- » Endpoint security (e.g., host-based)

## 4.3 Implement secure communication channels according to design

- » Voice, video, and collaboration (e.g., conferencing, Zoom rooms)
- » Remote access (e.g., network administrative functions)
- » Data communications (e.g., backhaul networks, satellite)
- » Third-party connectivity (e.g., telecom providers, hardware support)



## Domain 5

# Identity and Access Management (IAM) (13%)

---

### 5.1 Control physical and logical access to assets

- » Information
- » Systems
- » Devices
- » Facilities
- » Applications

### 5.2 Design identification and authentication strategy (e.g., people, devices, and services)

- » Groups and Roles
- » Authentication, Authorization and Accounting (AAA) (e.g., multi-factor authentication (MFA), password-less authentication)
- » Session management
- » Registration, proofing, and establishment of identity
- » Federated Identity Management (FIM)
- » Credential management systems (e.g., Password vault)
- » Single sign-on (SSO)
- » Just-In-Time

### 5.3 Federated identity with a third-party service

- » On-premise
- » Cloud
- » Hybrid

## 5.4 Implement and manage authorization mechanisms

- » Role Based Access Control (RBAC)
- » Rule based access control
- » Mandatory Access Control (MAC)
- » Discretionary Access Control (DAC)
- » Attribute Based Access Control (ABAC)
- » Risk based access control
- » Access policy enforcement (e.g., policy decision point, policy enforcement point)

## 5.5 Manage the identity and access provisioning lifecycle

- » Account access review (e.g., user, system, service)
- » Provisioning and deprovisioning (e.g., on /off boarding and transfers)
- » Role definition (e.g., people assigned to new roles)
- » Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)
- » Service accounts management

## 5.6 Implement authentication systems

- » OpenID Connect (OIDC)/Open Authorization (Oauth)
- » Security Assertion Markup Language (SAML)
- » Kerberos
- » Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)





## Domain 6

# Security Assessment and Testing (12%)

---

### 6.1 Design and validate assessment, test, and audit strategies

- » Internal (e.g., within organization control)
- » External (e.g., outside organization control)
- » Third-party (e.g., outside of enterprise control)
- » Location (e.g., on-premise, cloud, hybrid)

### 6.2 Conduct security control testing

- » Vulnerability assessment
- » Penetration testing (e.g., red, blue, and/or purple team exercises)
- » Log reviews
- » Synthetic transactions /benchmarks
- » Code review and testing
- » Misuse case testing
- » Coverage analysis
- » Interface testing (e.g., user interface, network interface, application programming interface (API))
- » Breach attack simulations
- » Compliance checks

### 6.3 Collect security process data (e.g., technical and administrative)

- » Account management
- » Management review and approval
- » Key performance and risk indicators
- » Backup verification data
- » Training and awareness
- » Disaster Recovery (DR) and Business Continuity (BC)

## 6.4 Analyze test output and generate a report

- » Remediation
- » Exception handling
- » Ethical disclosure

## 6.5 Conduct or facilitate security audits

- » Internal (e.g., within organization control)
- » External (e.g., outside organization control)
- » Third-party (e.g., outside of enterprise control)
- » Location (e.g., on-premise, cloud, hybrid)



## Domain 7 Security Operations (13%)

---

### 7.1 Understand and comply with investigations

- » Evidence collection and handling
- » Reporting and documentation
- » Investigative techniques
- » Digital forensics tools, tactics, and procedures
- » Artifacts (e.g., computer, network, mobile device)

### 7.2 Conduct logging and monitoring activities

- » Intrusion detection and prevention system (IDPS)
- » Security Information and Event Management (SIEM)
- » Security orchestration, automation, and response (SOAR)
- » Continuous monitoring and tuning
- » Egress monitoring
- » Log management
- » Threat intelligence (e.g., threat feeds, threathunting)
- » User and Entity Behavior Analytics (UEBA)

### 7.3 Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)

### 7.4 Apply foundational security operations concepts

- » Need-to-know/least privilege
- » Separation of Duties (SoD) and responsibilities
- » Privileged account management
- » Job rotation
- » Service Level Agreements (SLAs)

### 7.5 Apply resource protection

- » Media management
- » Media protection techniques
- » Data at rest/data in transit

## 7.6 Conduct incident management

- » Detection
- » Response
- » Mitigation
- » Reporting
- » Recovery
- » Remediation
- » Lessons learned

## 7.7 Operate and maintain detective and preventative measures

- » Firewalls (e.g., next generation, web application, network)
- » Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- » Whitelisting/blacklisting
- » Third-party provided security services
- » Sandboxing
- » Honeypots/honeynets
- » Anti-malware
- » Machine learning and Artificial Intelligence (AI) based tools

## 7.8 Implement and support patch and vulnerability management

## 7.9 Understand and participate in change management processes

## 7.10 Implement recovery strategies

- » Backup storage strategies (e.g., cloud storage, onsite, offsite)
- » Recovery site strategies (e.g., cold vs. hot, resource capacity agreements)
- » Multiple processing sites
- » System resilience, High Availability (HA), Quality of Service (QoS), and fault tolerance

### **7.11 Implement Disaster Recovery (DR) processes**

- » Response
- » Personnel
- » Communications (e.g., methods)
- » Assessment
- » Restoration
- » Training and awareness
- » Lessons learned

### **7.12 Test Disaster Recovery Plans (DRP)**

- » Read-through/tabletop
- » Walkthrough
- » Simulation
- » Parallel
- » Full interruption
- » Communications (e.g., stakeholders, test status, regulators)

### **7.13 Participate in Business Continuity (BC) planning and exercises**

### **7.14 Implement and manage physical security**

- » Perimeter security controls
- » Internal security controls

### **7.15 Address personnel safety and security concerns**

- » Travel
- » Security training and awareness (e.g., insider threat, social media impacts, two-factor authentication (2FA) fatigue)
- » Emergency management
- » Duress



## Domain 8

# Software Development Security (10%)

### 8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

- » Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps Scaled Agile Framework)
- » Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
- » Operation and maintenance
- » Change management
- » Integrated Product Team

### 8.2 Identify and apply security controls in software development ecosystems

- » Programming languages
- » Libraries
- » Tool sets
- » Integrated Development Environment
- » Runtime
- » Continuous Integration and Continuous Delivery (CI/CD)
- » Software Configuration Management
- » Code repositories
- » Application security testing (e.g., static application security testing (SAST), dynamic application security testing (DAST), software composition analysis, Interactive Application Security Test (IAST))

### 8.3 Assess the effectiveness of software security

- » Auditing and logging of changes
- » Risk analysis and mitigation

#### 8.4 Assess security impact of acquired software

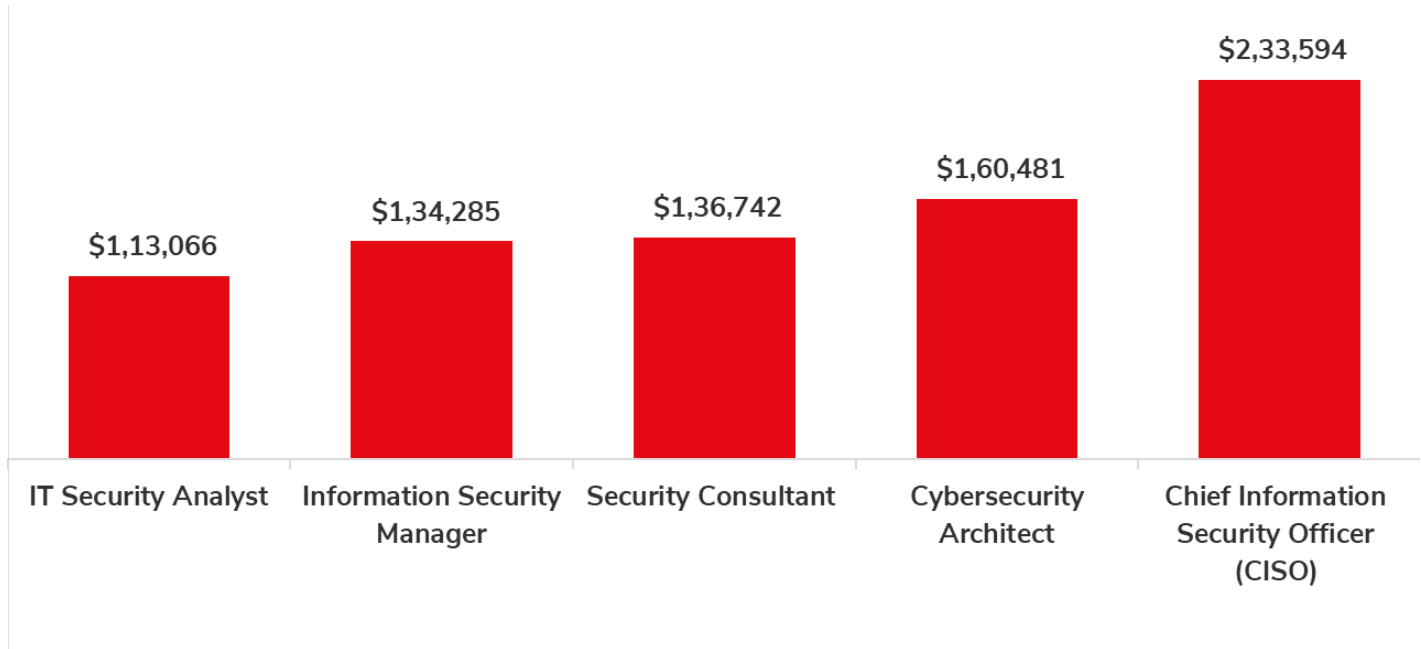
- » Commercial-off-the-shelf (COTS)
- » Open source
- » Third-party
- » Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- » Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

#### 8.5 Define and apply secure coding guidelines and standards

- » Security weaknesses and vulnerabilities at the source-code level
- » Security of Application Programming Interfaces (APIs)
- » Secure coding practices
- » Software-defined secure use this information and write course overview



## CISSP® Course Benefits



### HIRING COMPANIES



"Source: Glassdoor, Indeed"



[www.infosectrain.com](http://www.infosectrain.com) | [sales@infosectrain.com](mailto:sales@infosectrain.com)