INFOSECTRAIN

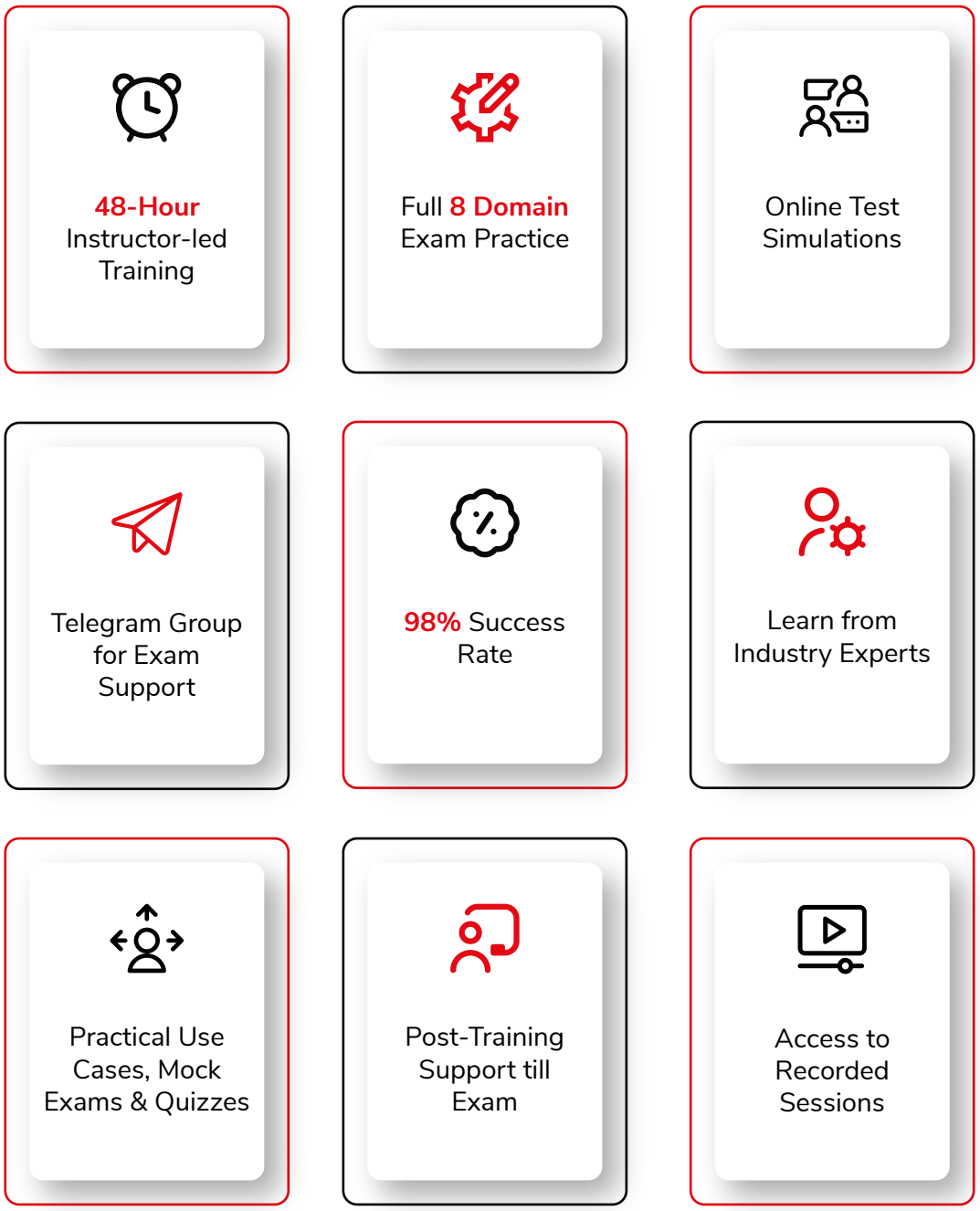
CISSP

Certified Information Systems Security Professional

Certification Training

INFOSECTRAIN

Course Highlights

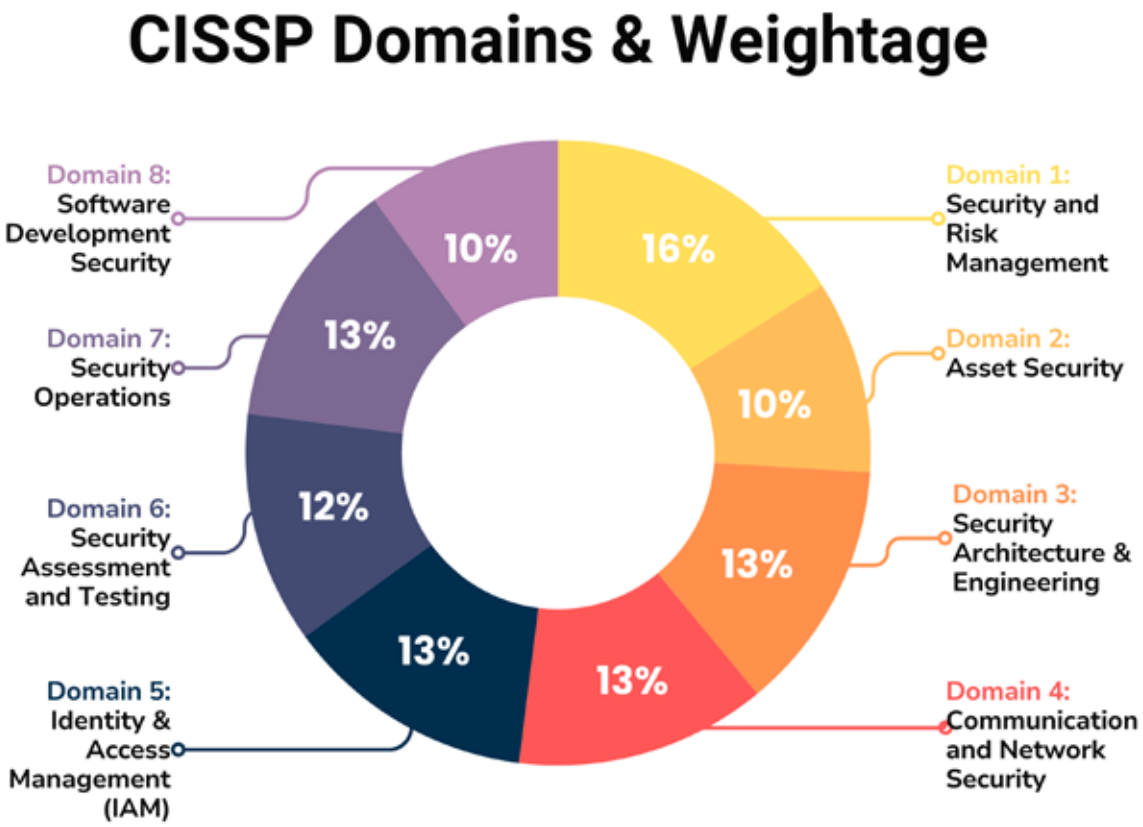


Course Overview

CISSP® is the most renowned certification in the information security domain. Our CISSP® certification training program aims to equip participants with in-demand technical and administrative competence to design, architect, and manage an organization's security posture by applying internationally accepted information security standards.

The latest version (2024) of CISSP enhances the participant's understanding by covering the critical elements of the 8 domains that comprise the Common Body of Knowledge (CBK)®.

(ISC)² 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.



Course Objectives

- 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).

INFOSECTRAIN

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® course 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)² CISSP® Common Body of Knowledge (CBK)
- One-year experience waiver can be earned with a 4-year college degree, or regional equivalent or additional credential from the (ISC)² approved list

Exam Information

Exam Name	**CISSP CAT**
Launch Date	Effective April 15, 2024
Exam Duration	3 hours
Number of Items	100-150
Exam Format	Multiple-choice and advanced innovative items
Passing Score	700 out of 1000 points
Language	English
Testing Center	(ISC)2 Authorized PPC and PVTC Select Pearson VUE Testing Centers

Course Content

Domain 1 Security and Risk Management (16%)

1.1- Understand, adhere to, and promote professional ethics

- ISC2 Code of Professional Ethics
- Organizational code of ethics

1.2 - Understand and apply security concepts

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

1.3 - Evaluate and apply 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))
- Due care/due diligence

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, 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)

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
- Segregation 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 systems
- Edge computing systems
- Virtualized systems

3.6 - Select and determine cryptographic solutions

- 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)

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 - Apply 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
- Services

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 and transition (e.g., people assigned to new roles)
- Privilege escalation (e.g., use of sudo, auditing its use)
- Service accounts management

5.6 – Implement authentication systems

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-premises, 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 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-premises, cloud, hybrid)

Domain 6 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., data, computer, network, mobile device)

7.2 - Conduct logging and monitoring activities

- Intrusion detection and prevention (IDPS)
- Security Information and Event Management (SIEM)
- Continuous monitoring and tuning
- Egress monitoring
- Log management
- Threat intelligence (e.g., threat feeds, threat hunting)
- 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 (SLA)

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 detection 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

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 (CM)
- 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

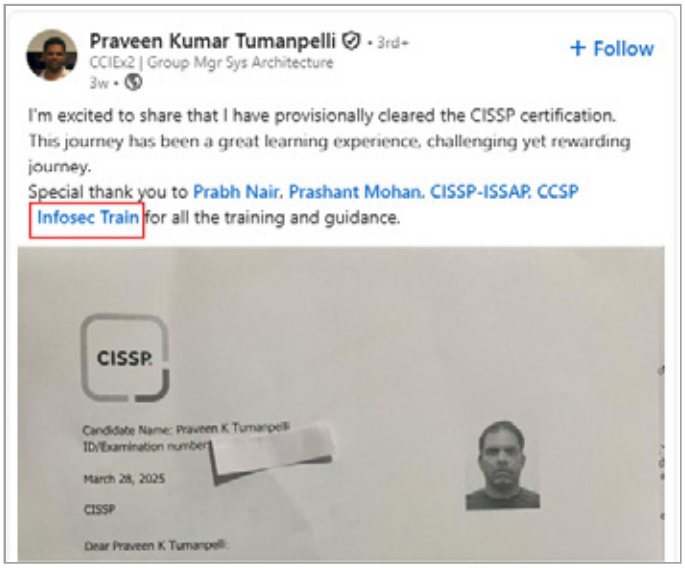
8.4 - Assess security impact of acquired software

- Commercial-off-the-shelf (COTS)
- Open source
- Third-party
- Managed services (e.g., enterprise applications)
- 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

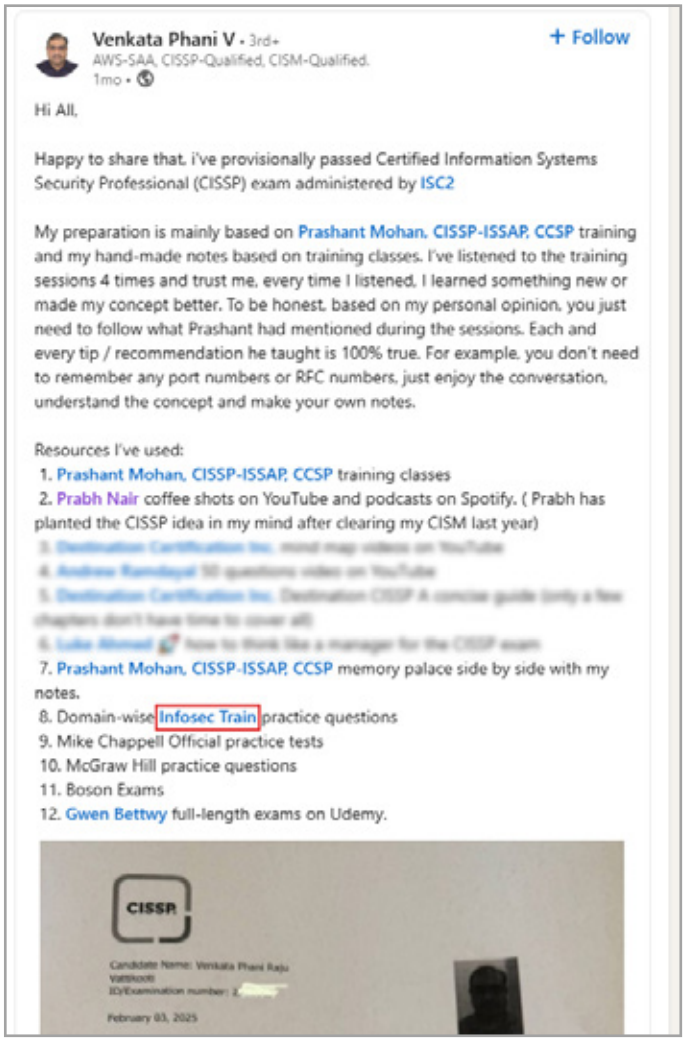
- Security weaknesses and vulnerabilities at the source-code level
- Security of application programming interfaces (API)
- Secure coding practices
- Software-defined security

Words Have Power



Praveen Kumar Tumanpelli • 3rd+
CCIExp2 | Group Mgr Sys Architecture
3w •
+ Follow

I'm excited to share that I have provisionally cleared the CISSP certification. This journey has been a great learning experience, challenging yet rewarding journey.
Special thank you to Prabh Nair, Prashant Mohan, CISSP-ISSAP, CCSP Infosec Train for all the training and guidance.



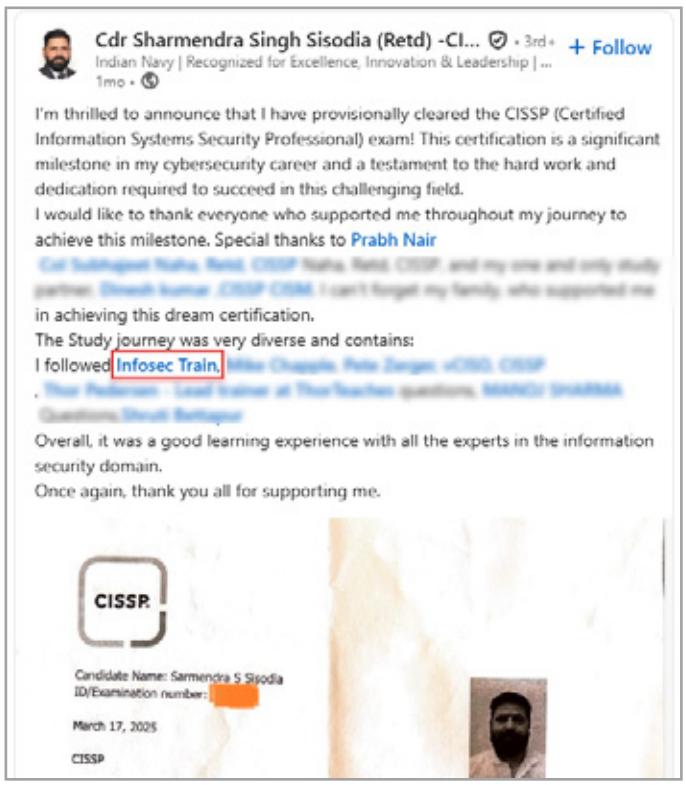
Venkata Phani V • 3rd+
AWS-SAA, CISSP-Qualified, CISM-Qualified.
1mo •
+ Follow

Hi All,

Happy to share that, i've provisionally passed Certified Information Systems Security Professional (CISSP) exam administered by ISC2

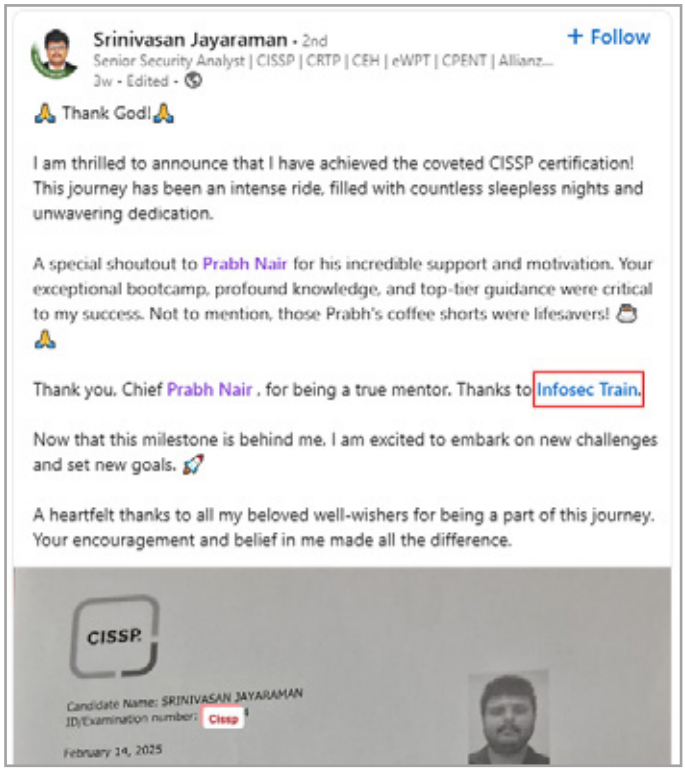
My preparation is mainly based on Prashant Mohan, CISSP-ISSAP, CCSP training and my hand-made notes based on training classes. I've listened to the training sessions 4 times and trust me, every time I listened, I learned something new or made my concept better. To be honest, based on my personal opinion, you just need to follow what Prashant had mentioned during the sessions. Each and every tip / recommendation he taught is 100% true. For example, you don't need to remember any port numbers or RFC numbers, just enjoy the conversation, understand the concept and make your own notes.

Resources I've used:
1. Prashant Mohan, CISSP-ISSAP, CCSP training classes
2. Prabh Nair coffee shots on YouTube and podcasts on Spotify. (Prabh has planted the CISSP idea in my mind after clearing my CISM last year)
3. [redacted]
4. [redacted]
5. [redacted]
6. [redacted]
7. Prashant Mohan, CISSP-ISSAP, CCSP memory palace side by side with my notes.
8. Domain-wise Infosec Train practice questions
9. Mike Chappell Official practice tests
10. McGraw Hill practice questions
11. Boson Exams
12. Gwen Bettwy full-length exams on Udemy.



Cdr Sharmendra Singh Sisodia (Retd) -CI... • 3rd+
Indian Navy | Recognized for Excellence, Innovation & Leadership | ...
1mo •
+ Follow

I'm thrilled to announce that I have provisionally cleared the CISSP (Certified Information Systems Security Professional) exam! This certification is a significant milestone in my cybersecurity career and a testament to the hard work and dedication required to succeed in this challenging field.
I would like to thank everyone who supported me throughout my journey to achieve this milestone. Special thanks to Prabh Nair
[redacted]
in achieving this dream certification.
The Study journey was very diverse and contains:
I followed Infosec Train, [redacted]
Overall, it was a good learning experience with all the experts in the information security domain.
Once again, thank you all for supporting me.



Srinivasan Jayaraman • 2nd
Senior Security Analyst | CISSP | CRTP | CEH | eWPT | CPENT | Allianz...
3w • Edited •
+ Follow

🙏 Thank God! 🙏

I am thrilled to announce that I have achieved the coveted CISSP certification! This journey has been an intense ride, filled with countless sleepless nights and unwavering dedication.

A special shoutout to Prabh Nair for his incredible support and motivation. Your exceptional bootcamp, profound knowledge, and top-tier guidance were critical to my success. Not to mention, those Prabh's coffee shorts were lifesavers! ☕ 🙏

Thank you, Chief Prabh Nair , for being a true mentor. Thanks to Infosec Train.

Now that this milestone is behind me, I am excited to embark on new challenges and set new goals. 🚀

A heartfelt thanks to all my beloved well-wishers for being a part of this journey. Your encouragement and belief in me made all the difference.

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on