INFOSECTRAIN

CISSP

Certified Information Systems Security Professional

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...

CISSP Introduction

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 training offers an in-depth understanding of eight domains that comprise CISSP common body knowledge (CBK) and prepares you for the CISSP exam held by the (ISC)2.

(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.

Why CISSP with InfosecTrain

4 hrs/ day in Weekend/ Weekday

Accredited Instructors

Online Test simulation mapped with domains

Access to the recorded sessions

CISSP Exam engine

Full 8 Domain Exam Practice

Telegram Discussion Group

Our Expert Instructors

"

Certified Security specialist having several years of experience in Information Security across all domains including application security, vulnerability assessment, ethical hacking, pen testing and IT risk and compliance and more

PRABH NAIR

CISSP I CCSP I CSSLP I
CRISC I CISM I CISA I CGEITC

"

Ajit has more than 15 years of experience which include Consulting, Network and InfoSec training (CISA, CISM, CISSP, CCSP, Security+, SSCP), Content development, Assessments and auditing and more

AJIT

CISSP I CCSP I CRISC I CISA I CGEITC

"

Prashant is a seasoned Information Security professional with 10+ years of hands on experience in auditing application controls, identifying breaches, communicating gaps and risks to the business and providing solutions in accordance with the policy to the stakeholders.

PRASHANT M

CISSP I CCSP I CRISC | CISA

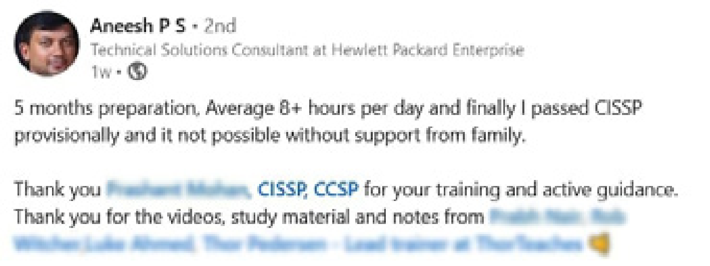
"

After having worked for 20 years in IT, Cyber Security and Consulting, Mathew Ford is enjoying his new career as a Cyber Security instructor. He always knew he will be a teacher and working in InfoSec Train is like a breath of fresh air for him!

MATTHEW FORD

CISSP I CISM

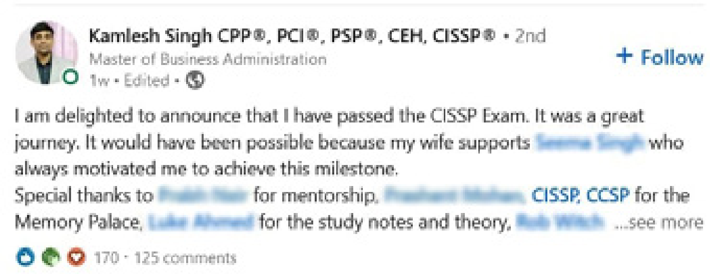
Happy Learners from LinkedIn



Aneesh P S • 2nd
Technical Solutions Consultant at Hewlett Packard Enterprise
1w • 🌐

5 months preparation, Average 8+ hours per day and finally I passed CISSP provisionally and it not possible without support from family.

Thank you [redacted], CISSP, CCSP for your training and active guidance. Thank you for the videos, study material and notes from [redacted]

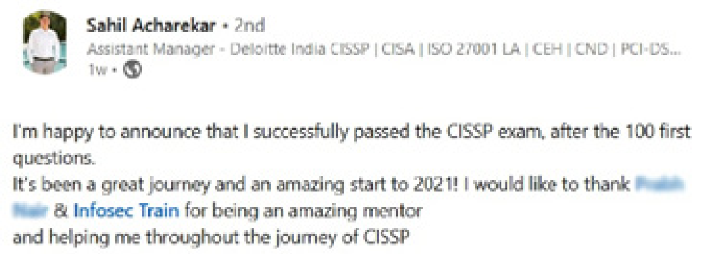


Kamlesh Singh CPP®, PCI®, PSP®, CEH, CISSP® • 2nd
Master of Business Administration
1w • Edited • 🌐

+ Follow

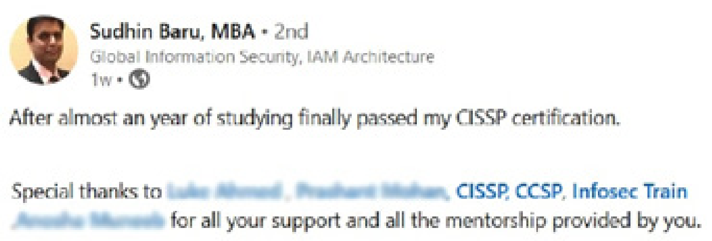
I am delighted to announce that I have passed the CISSP Exam. It was a great journey. It would have been possible because my wife supports [redacted] who always motivated me to achieve this milestone.
Special thanks to [redacted] for mentorship, [redacted], CISSP, CCSP for the Memory Palace, [redacted] for the study notes and theory, [redacted] ...see more

170 · 125 comments



Sahil Acharekar • 2nd
Assistant Manager - Deloitte India CISSP | CISA | ISO 27001 LA | CEH | CND | PCI-DS...
1w • 🌐

I'm happy to announce that I successfully passed the CISSP exam, after the 100 first questions.
It's been a great journey and an amazing start to 2021! I would like to thank [redacted] & Infosec Train for being an amazing mentor and helping me throughout the journey of CISSP

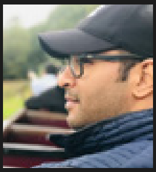


Sudhin Baru, MBA • 2nd
Global Information Security, IAM Architecture
1w • 🌐

After almost an year of studying finally passed my CISSP certification.

Special thanks to [redacted], [redacted], CISSP, CCSP, Infosec Train [redacted] for all your support and all the mentorship provided by you.

Happy Learners from the world



Paul Ebenezer

Senior Consultant | United Kingdom

Infosec Train has an amazing coach, mentor, and a great personality, one of the best IT Security and Technology trainers that currently exists. Trainer's dedication to teach and share knowledge, commitment...

Emily Kong

IT Security | Japan

I had the opportunity to take CISSP lessons. The Trainer has been consistently giving me a lot of mental and material support. I would recommend his mentorship for any aspirant.

Smitha Kurup

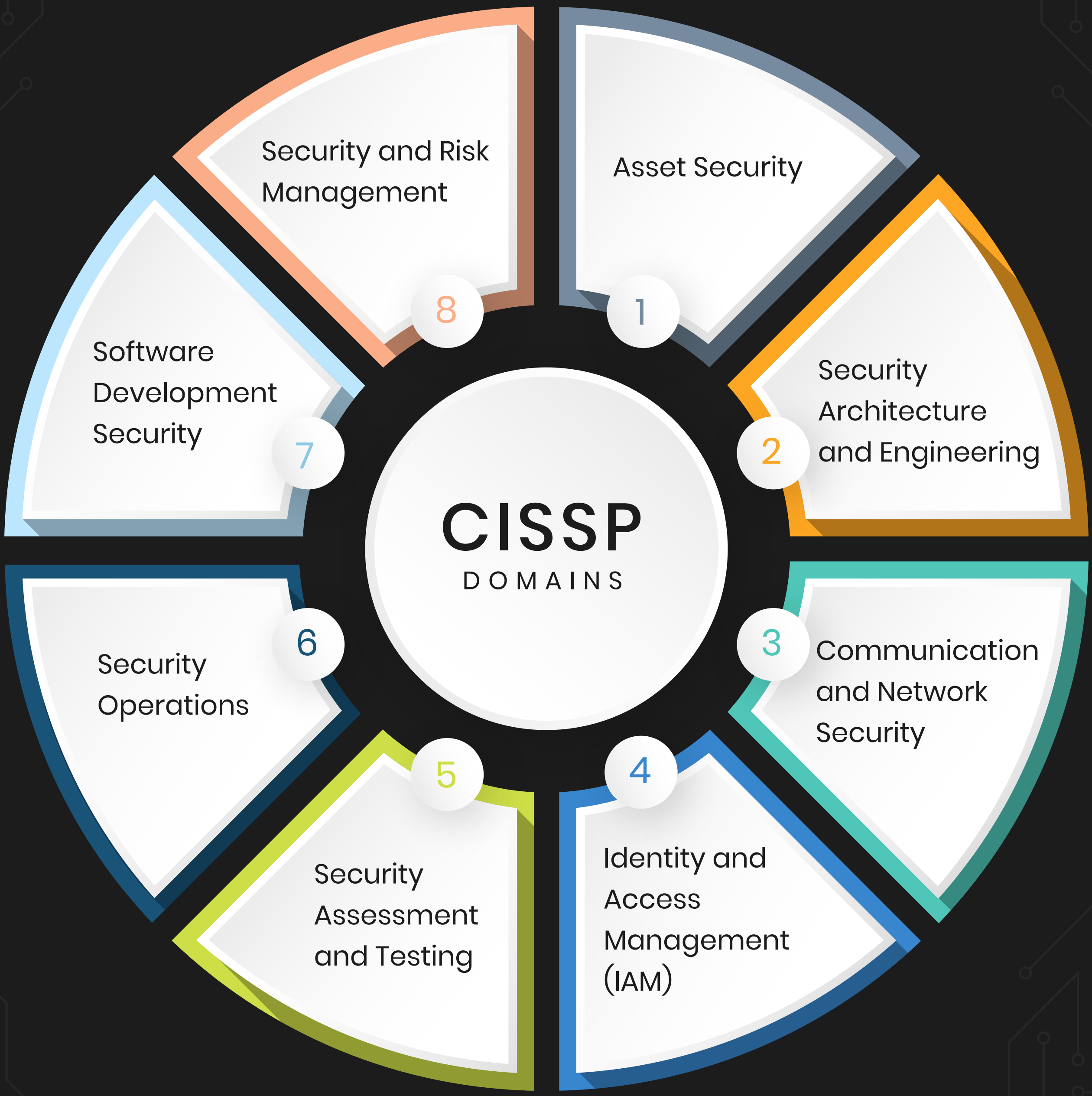
CISSP | USA

I made the right choice, and every session was worth it. Thank you once again. I would highly recommend my friends, the professor has immense knowledge and the subject and was very logical and practical.

Mohit Trehan

CISSP | UAE

Trainer organized the CISSP training session in a well-organized way. Overall Experience with the trainer and the provided training material was Excellent. All the CISSP sessions are very informative and had an explicit knowledge of how to accomplish the certification.



CISSP DOMAINS

1 Asset Security

2 Security Architecture and Engineering

3 Communication and Network Security

4 Identity and Access Management (IAM)

5 Security Assessment and Testing

6 Security Operations

7 Software Development Security

8 Security and Risk Management

Domain 1: Security and Risk Management

1.1 Understand and apply concepts of confidentiality, integrity and availability

1.2 Evaluate and apply security governance principles

- Alignment of security function to business strategy, goals, mission, and objectives
- Organizational processes (e.g., acquisitions, divestitures, governance committees)
- Organizational roles and responsibilities
- Security control frameworks
- Due care/due diligence

1.3 Determine compliance requirements

- Contractual, legal, industry standards, and regulatory requirements
- Privacy requirements

1.4 Understand legal and regulatory issues that pertain to information security in a global context

- Cyber crimes and data breaches
- Licensing and intellectual property requirements
- Import/export controls
- Trans-border data flow
- Privacy

1.5 Understand, adhere to, and promote professional ethics

- (ISC)² Code of Professional Ethics
- Organizational code of ethics

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

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

- Develop and document scope and plan
- Business Impact Analysis (BIA)

1.8 Contribute to and enforce personnel security policies and procedures

- Candidate screening and hiring
- Employment agreements and policies
- Onboarding and termination processes
- Vendor, consultant, and contractor agreements and controls
- Compliance policy requirements
- Privacy policy requirements

1.9 Understand and apply risk management concepts

- Identify threats and vulnerabilities
- Risk assessment/analysis
- Risk response
- Countermeasure selection and implementation
- Applicable types of controls (e.g., preventive, detective, corrective)
- Security Control Assessment (SCA)
- Monitoring and measurement
- Asset valuation
- Reporting
- Continuous improvement
- Risk frameworks

1.10 Understand and apply threat modeling concepts and methodologies

- Threat modeling methodologies
- Threat modeling concepts

1.11 Apply risk- based management concepts to the supply chain

- Risks associated with hardware, software, and services
- Third-party assessment and monitoring
- Minimum security requirements
- Service-level requirements

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

- Methods and techniques to present awareness and training
- Periodic content reviews
- Program effectiveness evaluation

Domain 2: Asset Security

2.1 Identify and classify information and assets

- Data classification
- Asset Classification

2.2 Determine and maintain information and asset ownership

2.3 Protect privacy

- Data owners
- Data processers
- Data remanence
- Collection limitation

2.4 Ensure appropriate asset retention

2.5 Determine data security controls

- Understand data states
- Scoping and tailoring
- Standards selection
- Data protection methods

2.6 Establish information and asset handling requirements

Domain 3: Security Architecture and Engineering

3.1 Implement and manage engineering processes using secure design principles

3.2 Understand the fundamental concepts of security models

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of information systems (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
- Distributed systems
- Internet of Things (IoT)

3.6 Assess and mitigate vulnerabilities in web-based systems

3.7 Assess and mitigate vulnerabilities in mobile systems

3.8 Assess and mitigate vulnerabilities in embedded devices

3.9 Apply cryptography

- Cryptographic life cycle (e.g., key management, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures
- Non-repudiation
- Integrity (e.g., hashing)
- Understand methods of cryptanalytic attacks
- Digital Rights Management (DRM)

3.10 Apply security principles to site and facility design

3.11 Implement 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
- Fire prevention, detection, and suppression

Domain 4: Communication and Network Security

4.1 Implement secure design principles in network architectures

- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) networking
- Implications of multilayer protocols
- Converged protocols
- Software-defined networks
- Wireless networks

4.2 Secure network components

- Operation of hardware
- Transmission media
- Network Access Control (NAC) devices
- Endpoint security
- Content-distribution networks

4.3 Implement secure communication channels according to design

- Voice
- Multimedia collaboration
- Remote access
- Data communications
- Virtualized networks

Domain 5: Identity and Access Management (IAM)

5.1 Control physical and logical access to assets

- Information
- Systems
- Devices
- Facilities

5.2 Manage identification and authentication of people, devices, and services

- Identity management implementation
- Single/multi-factor authentication
- Accountability
- Session management
- Registration and proofing of identity
- Federated Identity Management (FIM)
- Credential management systems

5.3 Integrate identity as a third-party service

- On-premise
- Cloud
- Federated

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)

5.5 Manage the identity and access provisioning lifecycle

- User access review
- System account access review
- Provisioning and deprovisioning

Domain 6: Security Assessment and Testing

6.1 Design and validate assessment, test, and audit strategies

- Internal
- External
- Third-party

6.2 Conduct security control testing

- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing
- Misuse case testing
- Test coverage analysis
- Interface testing

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

6.5 Conduct or facilitate security audits

- Internal
- External
- Third-party

Domain 7: Security Operations

7.1 Understand and support investigations

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures

7.2 Understand requirements for investigation types

- Administrative
- Criminal
- Civil
- Regulatory
- Industry standards

7.3 Conduct logging and monitoring activities

- Intrusion detection and prevention
- Security Information and Event Management (SIEM)
- Continuous monitoring
- Egress monitoring

7.4 Securely provisioning resources

- Asset inventory
- Asset management
- Configuration management

7.5 Understand and apply foundational security operations concepts

- Need-to-know/least privileges
- Separation of duties and responsibilities
- Privileged account management
- Job rotation
- Information lifecycle
- Service Level Agreements (SLA)

7.6 Apply resource protection techniques

- Media management
- Hardware and software asset management

7.7 Conduct incident management

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

7.8 Operate and maintain detective and preventative measures

- Firewalls
- Intrusion detection and prevention systems
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware

7.9 Implement and support patch and vulnerability management

7.10 Understand and participate in change management processes

7.11 Implement recovery strategies

- Backup storage strategies
- Recovery site strategies
- Multiple processing sites
- System resilience, high availability, Quality of Service (QoS), and fault tolerance

7.12 Implement Disaster Recovery (DR) processes

- Response
- Personnel
- Communications
- Assessment
- Restoration
- Training and awareness

7.13 Test Disaster Recovery Plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption

7.14 Participate in Business Continuity (BC) planning and exercises

7.15 Implement and manage physical security

- Perimeter security controls
- Internal security controls

7.16 Address personnel safety and security concerns

- Travel
- Security training and awareness
- Emergency management
- Duress

Domain 8: Software Development Security

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

- Development methodologies
- Maturity models
- Operation and maintenance
- Change management
- Integrated product team

8.2 Identify and apply security controls in development environments

- Security of the software environments
- Configuration management as an aspect of secure coding
- Security of code repositories

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

8.5 Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of application programming interfaces
- Secure coding practices

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com