Information Security Strategic Solutions

Mastering CISSP

M-CISSP

Information Security Strategic Solutions

London, UK Dubai, UAE Chennai, India

www.isss.co.in, www.infosecss.com

training@isss.co.in, training-me@infosecss.com

+91 99405 87544, +44 7723 433 145

Time to win the world

Information Security Strategic Solutions

Certified Information System Security Professional (CISSP), There could be 100 of certification in Cyber Security, but none to match this one. That is true. ☺

Welcome to one of the worlds best training for CISSP.

The one that can hand hold you until you clear your certification.

We are assigning you a master who has been delivering this training from 2008 in Europe and then to Middle East and now in India.

With a 97% global pass rate… you are joining us for launching your InfoSec career with CISSP.

We promise to deliver the best CISSP training in the world for you.

This is our promise. And …

Welcome On-board!

Time to win the world

Information Security Strategic Solutions

Agenda:

Domain 1: Security Risk Management

Understand, adhere to, and promote professional ethics

ISC)2 Code of Professional Ethics
Organizational code of ethics

Understand and apply security concepts

Confidentiality, integrity, and availability, authenticity and nonrepudiation

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
Due care/due diligence

Determine compliance and other requirements

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

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

Cybercrimes and data breaches
Licensing and Intellectual Property (IP) requirements
Import/export controls
Transborder data flow
Privacy

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

Time to win the world

Information Security Strategic Solutions

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

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

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

Contribute to and enforce personnel security policies and procedures
Candidate screening and hiring
Compliance policy requirements
Employment agreements and policies
Privacy policy requirements
Onboarding, transfers, and termination processes
Vendor, consultant, and contractor agreements and controls

Understand and apply risk management concepts

Identify threats and vulnerabilities
Control assessments (security and privacy)
Risk assessment/analysis
Monitoring and measurement
Risk response
Reporting
Countermeasure selection and implementation
Continuous improvement
Applicable types of controls (e.g., preventive,
Risk frameworks

Understand and apply threat modeling concepts and methodologies

Apply Supply Chain Risk Management (SCRM) concepts

Time to win the world

Information Security Strategic Solutions

Risks associated with hardware, software and services

Minimum security requirements

Service level requirements

Third-party assessment and monitoring

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

Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)

Periodic content reviews

Program effectiveness evaluation

Information Security Strategic Solutions

Domain 2: Asset Security

Identify and classify information and assets

Data classification

Asset Classification

Establish information and asset handling requirements

Provision resources securely

Information and asset ownership

Asset inventory (e.g., tangible, intangible)

Asset management

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

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

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))

Time to win the world

Information Security Strategic Solutions

Domain 3: Security Architecture and Engineering

Research, implement and manage engineering processes using secure design principles

Threat modeling
Keep it simple
Least privilege
Zero Trust
Defense in depth
Privacy by design
Secure defaults
Trust but verify
Fail securely
Shared responsibility
Separation of Duties (SoD)

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

Select controls based upon systems security requirements

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

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))

Time to win the world

Information Security Strategic Solutions

Distributed systems
Internet of Things (IoT)
Microservices
Containerization
Serverless
Embedded systems
High-Performance Computing (HPC) systems
Edge computing systems
Virtualized systems

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)
Key management practices
Digital signatures and digital certificates
Non-repudiation
Integrity (e.g., hashing)

Understand methods of cryptanalytic attacks

Brute force
Fault injection
Ciphertext only
Timing
Known plaintext
Man-in-the-Middle (MITM)
Frequency analysis
Pass the hash
Chosen ciphertext
Kerberos exploitation
Implementation attacks
Ransomware
Side-channel

Time to win the world

Information Security Strategic Solutions

Apply security principles to site and facility design

Design site and facility security controls

Wiring closets/intermediate distribution facilities

Utilities and Heating, Ventilation, and Air Conditioning (HVAC)

Server rooms/data centers

Environmental issues

Media storage facilities

Fire prevention, detection, and suppression

Evidence storage

Power (e.g., redundant, backup)

Information Security Strategic Solutions

Domain 4: Communication and Network Security

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) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)

Secure protocols

Implications of multilayer protocols

Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))

Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))

Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)

Cellular networks (e.g., 4G, 5G)

Content Distribution Networks (CDN)

Secure network components

Operation of hardware (e.g., redundant power, warranty, support)

Network Access Control (NAC) devices

Endpoint security

Transmission media

Implement secure communication channels according to design

Voice

Data communications

Multimedia collaboration

Virtualized networks

Remote access

Third-party connectivity

Time to win the world

Information Security Strategic Solutions

Domain 5: Identity and Access Management

Control physical and logical access to assets

Information
Facilities
Systems
Applications
Devices

Manage identification and authentication of people, devices, and services

Identity Management (IdM) implementation
Federated Identity Management (FIM)
Single/Multi-Factor Authentication (MFA)
Credential management systems
Accountability
Single Sign On (SSO)
Session management
Just-In-Time (JIT)
Registration, proofing, and establishment of identity

Federated identity with a third-party service

On-premise
Hybrid
Cloud

Implement and manage authorization mechanisms

Role Based Access Control (RBAC)
Discretionary Access Control (DAC)
Rule based access control
Attribute Based Access Control (ABAC)
Mandatory Access Control (MAC)
Risk based access control

Time to win the world

Information Security Strategic Solutions

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)

Implement authentication systems

OpenID Connect (OIDC)/Open Authorization (Oauth)
Security Assertion Markup Language (SAML)
Kerberos

Information Security Strategic Solutions

Domain 6: Security Assessment and Testing

Design and validate assessment, test, and audit strategies

Internal
External
Third-party

Conduct security control testing

Vulnerability assessment
Misuse case testing
Penetration testing
Test coverage analysis
Log reviews
Interface testing
Synthetic transactions
Breach attack simulations
Code review and testing
Compliance checks

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)

Analyze test output and generate report

Remediation
Exception handling
Ethical disclosure

Conduct or facilitate security audits

Internal
External
Third-party

Time to win the world

Information Security Strategic Solutions

Domain 7: Security Assessment and Testing

Understand and comply with investigations

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

Conduct logging and monitoring activities

Intrusion detection and prevention
Security Information and Event Management (SIEM)
Continuous monitoring
Egress monitoring
Log management
Threat intelligence (e.g., threat feeds, threat hunting)
User and Entity Behavior Analytics (UEBA)

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

Apply foundational security operations concepts

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

Apply resource protection

Media management
Media protection techniques

Conduct incident management

Detection
Recovery
Response
Remediation

Time to win the world

Information Security Strategic Solutions

Mitigation
Lessons learned
Reporting

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

Implement and support patch and vulnerability management

Understand and participate in change management processes

Implement recovery strategies

Backup storage strategies

System resilience, High Availability (HA), Quality of Service (QoS), and fault tolerance
Recovery site strategies
Multiple processing sites

Implement Disaster Recovery (DR) processes

Response
Restoration
Personnel
Training and awareness
Communications
Lessons learned
Assessment

Time to win the world

Information Security Strategic Solutions

Test Disaster Recovery Plans (DRP)

Read-through/tabletop

Parallel

Walkthrough

Full interruption

Simulation

Participate in Business Continuity (BC) planning and exercises

Implement and manage physical security

Perimeter security controls

Internal security controls

Address personnel safety and security concerns

Travel

Emergency management

Security training and awareness

Duress

Information Security Strategic Solutions

Domain 8: Software Development Security

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

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

Identify and apply security controls in software development ecosystems

Programming languages
Libraries
Tool sets
Integrated Development Environment (IDE)
Runtime
Continuous Integration and Continuous Delivery (CI/CD)
Security Orchestration, Automation, and Response (SOAR)
Software Configuration Management (SCM)
Code repositories
Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))

Assess the effectiveness of software security

Auditing and logging of changes
Risk analysis and mitigation

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))

Time to win the world

Information Security Strategic Solutions

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 security

Time to win the world

Information Security Strategic Solutions

Benefits:

- Trainer with more than 180 deliveries across the world.
- Trainer for United Nations Support Base, Valentia, Spain and Brindisi, Italy
- Complete hand holding until certification
- Regular Connect Classes
- Recorded sessions
- Free to join further CISSP sessions

Time to win the world

Information Security Strategic Solutions

Schedule:

4th,5th,11th,12th,18th and 19th September
0930-1700 IST
Online

Time to win the world