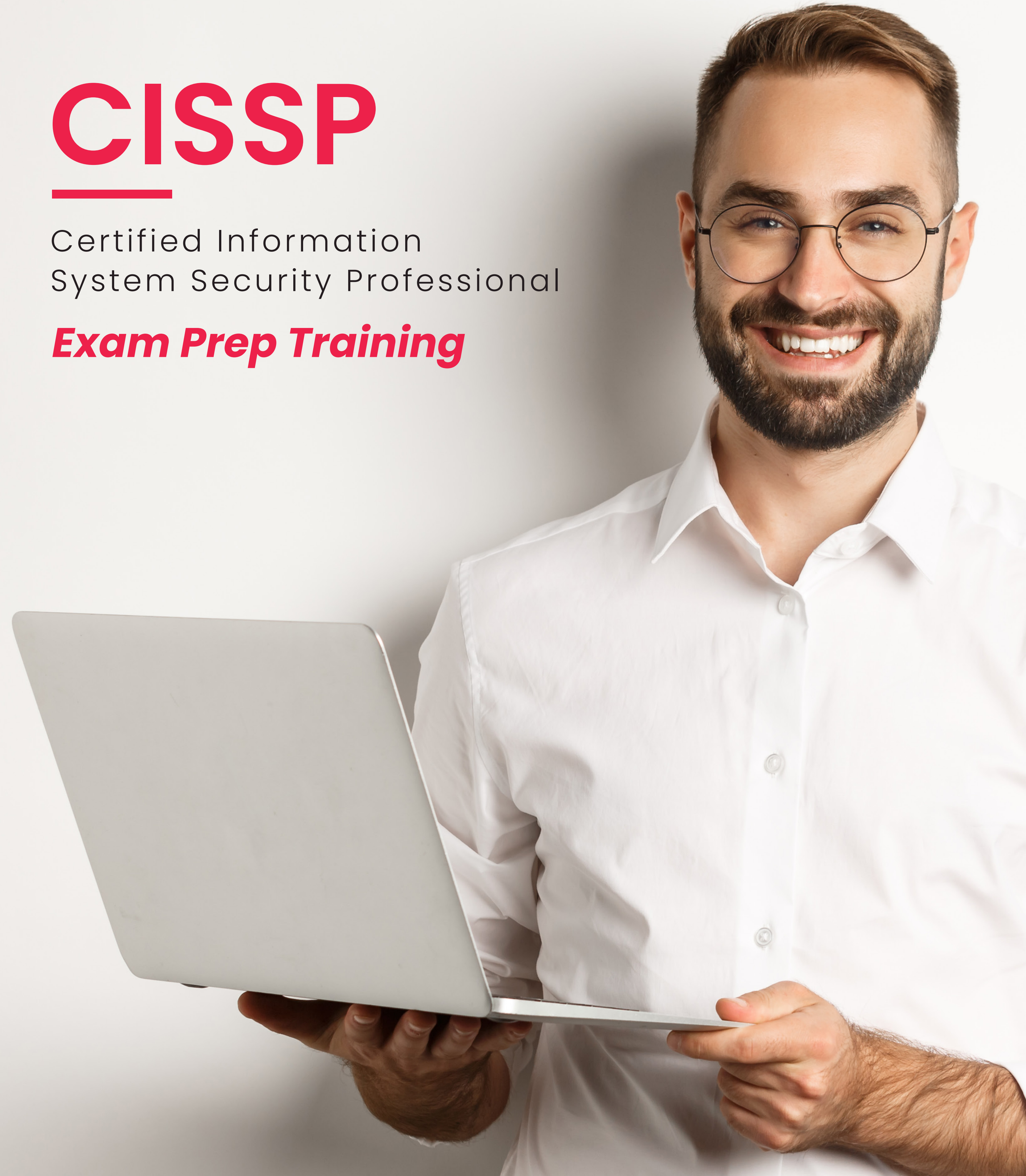
INFOSECTRAIN

CISSP

Certified Information System Security Professional

Exam Prep Training



CISSP Program 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 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.

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

CISSP Course Highlights

48-Hrs
Instructor-led Training

Full **8-Domain**
Exam Practice

Accredited
Instructors

CISSP
Exam Engine

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
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

Domains	Average Weight
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	13%
5. Identity and Access Management (IAM)	13%
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	11%
	Total: 100%

About the CISSP Exam

Duration	**4** Hours
Number of questions	**175**
Question format	Multiple Choice
Passing marks	**700** out of **1000**
Exam language	English, French, German, Brazilian,Portuguese, Spanish, Japanese, Simplified Chinese, Korean, Visually Impaired
Delivery Method	CAT

Pre-Requisites

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

Our Expert Instructors

Prabh Nair

17+ Years Of Experience

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

Prashant M

11+ Years Of Experience

Security Architect CISSP, CCSP, C|EH & CPISI

KK Singh

18+ Years Of Experience

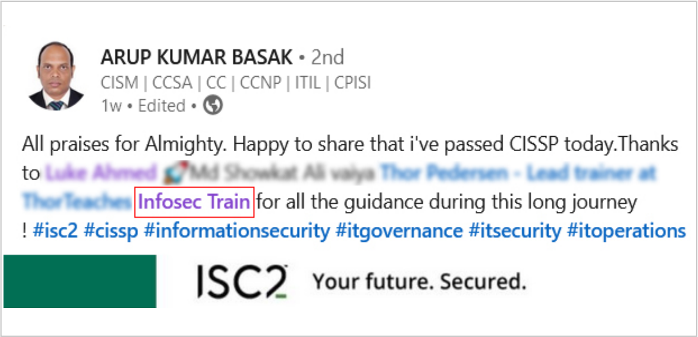
CISSP | CCSP | CISM | CRISC | CISA | CCSK | CCAK | CEH | RHCSA

Sujay

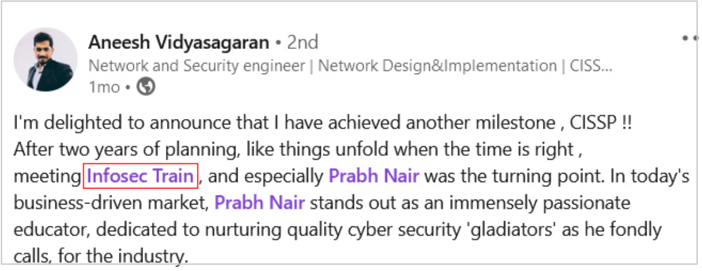
15+ Years Of Experience

CSOA | CCSP | CISSP | ISO 27001 Lead Auditor | ITIL v3

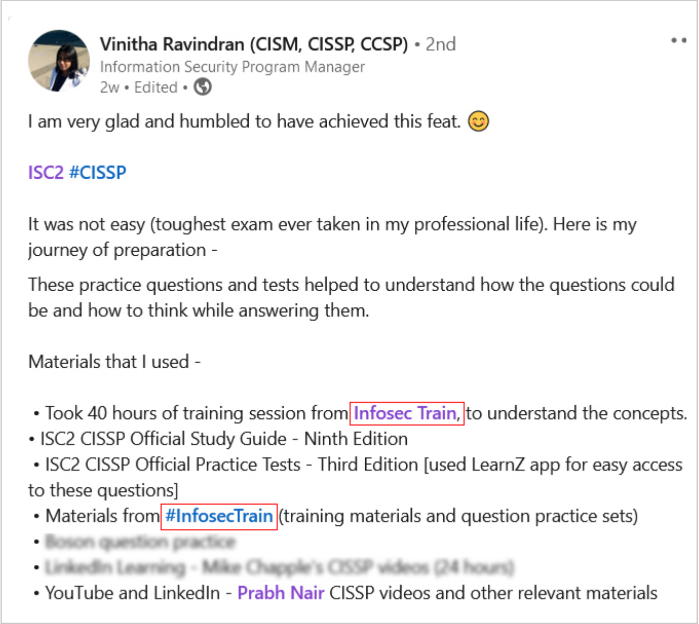
Happy Learners Across the World


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 [redacted] Infosec Train for all the guidance during this long journey ! #isc2 #cissp #informationsecurity #itgovernance #itsecurity #itoperations


Aneesh Vidyasagaran • 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. 😊

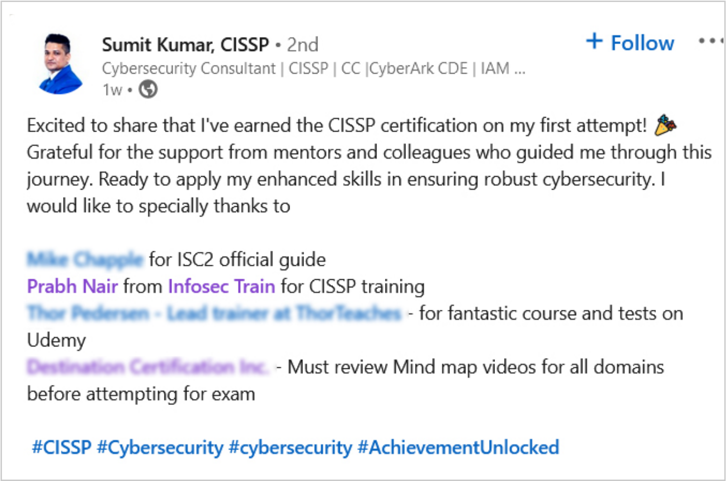
ISC2 #CISSP

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)
- [redacted]
- [redacted]
- YouTube and LinkedIn - Prabh Nair CISSP videos and other relevant materials

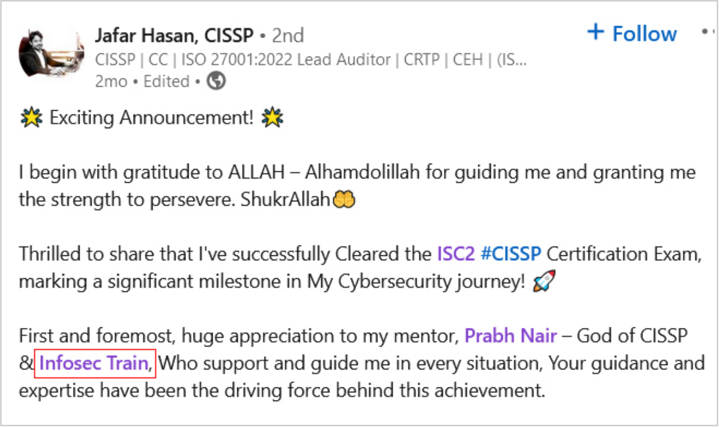

Sumit Kumar, CISSP • 2nd
Cybersecurity Consultant | CISSP | CC |CyberArk CDE | IAM ...
1w •

+ 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

[redacted] for ISC2 official guide
Prabh Nair from Infosec Train for CISSP training
[redacted] - for fantastic course and tests on Udemy
[redacted] - 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 •

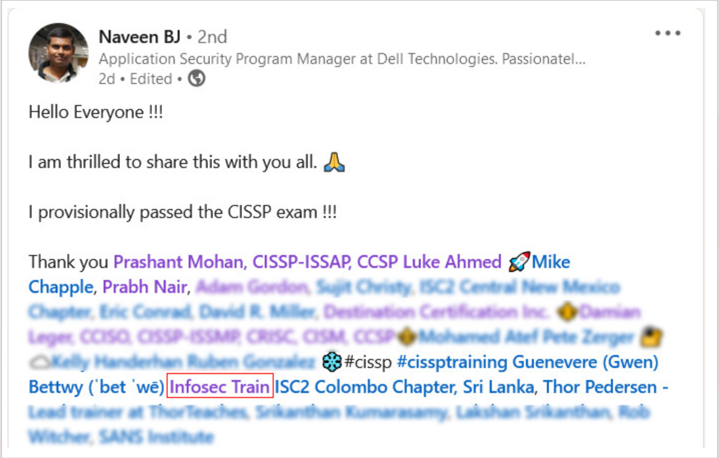
+ Follow

🌟 Exciting Announcement! 🌟

I begin with gratitude to ALLAH – Alhamdolillah 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, [redacted] ❄️#cissp #cissptraining Guenevere (Gwen) Bettwy (ˈbet ˈwē) Infosec Train ISC2 Colombo Chapter, Sri Lanka, Thor Pedersen - [redacted]

CISSP Domains

Domain 1: Security and Risk Management

Domain 2: Asset Security

Domain 3: Security Architecture and Engineering

Domain 4: Communication and Network Security

Domain 5: Identity and Access Management (IAM)

Domain 6: Security Assessment and Testing

Domain 7: Security Operations

Domain 8: Software Development Security

Domain 1
Security and Risk Management

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

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

» Due care/due diligence

1.4 Determine compliance and other requirements

» Contractual, legal, industry standards, and regulatory requirements

» Privacy requirements

1.5 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

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

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

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

» Business Impact Analysis (BIA)

» Develop and document the scope and the plan

1.9 Contribute to and enforce personnel security policies and procedures

» Candidate screening and hiring

» Employment agreements and policies

» Onboarding, transfers, and termination processes

» Vendor, consultant, and contractor agreements and controls

» Compliance policy requirements

» Privacy policy requirements

1.10 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)

» Control assessments (security and privacy)

» Monitoring and measurement

» Reporting

» Continuous improvement e.g., Risk maturity modeling)

» Risk frameworks

1.11 Understand and apply threat modeling concepts and methodologies

1.12 Apply Supply Chain Risk Management (SCRM) concepts

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

1.13 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

Domain 2
Asset Security

2.1 Identify and classify information and assets

» Data classification

» Asset Classification

2.2 Establish information and asset handling requirements

2.3 Provision resources 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

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

» Zero Trust

» Privacy by design

» Trust but verify

» Shared responsibility

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,

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

» Containerization

» Serverless

» Embedded systems

» High-Performance Computing (HPC) 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)

» Key management practices

» Digital signatures and digital certificates

» Non-repudiation

» Integrity (e.g., hashing)

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

» Fire prevention, detection, and suppression

» Power (e.g., redundant, backup)

Domain 4
Communication and Network Security

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) 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)

4.2 Secure network components

- Operation of hardware (e.g., redundant power, warranty, support)
- Transmission media
- Network Access Control (NAC) devices
- Endpoint security

4.3 Implement secure communication channels according to design

- Voice
- Multimedia collaboration
- Remote access
- Data communications
- Virtualized networks
- Third-party connectivity

Domain 5 Identity and Access Management (IAM)

5.1 Control physical and logical access to assets

» Information

» Systems

» Devices

» Facilities

» Applications

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

» Identity Management (IdM) implementation

» Single/Multi-Factor Authentication (MFA)

» Accountability

» Session management

» Registration, proofing, and establishment of identity

» Federated Identity Management (FIM)

» Credential management systems

» Single Sign On (SSO)

» Just-In-Time (JIT)

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

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)

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

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

» 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

» External

» Third-party

Domain 7
Security Operations

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
- » Security Information and Event Management(SIEM)
- » Continuous monitoring
- » 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

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
- » Recovery site strategies
- » 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
- » Assessment
- » Restoration
- » Training and awareness
- » Lessons learned

7.12 Test Disaster Recovery Plans (DRP)

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

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
- » Emergency management
- » Duress

Domain 8
Software Development Security

8.1 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)

8.2 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), DynamicApplication Security Testing (DAST))

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)

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 security