| | |
|---|---|
| **Course Title**: Certified Information Systems Security Professional (CISSP) | **Course Duration**: 5.0 Days |
| **Exam**: Included | **Exam Type**: Proctored Exam |
| **Qualification**: ISC Certified Information Systems Security Professional (CISSP) Certificate | |

## Course Syllabus

Our Certified Information Systems Security Professional (CISSP) training course will cover the following modules:

Module 1: Security and Risk Management

- Understand, adhere to, and promote professional ethics
- Understand and apply security concepts
- Evaluate and apply security governance principles
- Determine compliance and other requirements
- Understand legal and regulatory issues that pertain to information security in a holistic context
- Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyse, and prioritise Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modelling concepts and methodologies
- Apply Supply Chain Risk Management (SCRM) concepts
- Establish and maintain a security awareness, education, and training programme

Module 2: Asset Security

- Identify and classify information and assets
- Establish information and asset handling requirements
- Provision resources securely
- Manage data lifecycle
- Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))
- Determine data security controls and compliance requirements

Module 3: Security Architecture and Engineering

- Research, implement and manage engineering processes using secure design principles
- 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
- Select and determine cryptographic solutions
- Understand methods of cryptanalytic attacks

- Apply security principles to site and facility design
- Design site and facility security controls

Module 4: Communication and Network Security

- Assess and implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

Module 5: Identity and Access Management (IAM)

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Federated identity with a third-party service
- Implement and manage authorisation mechanisms
- Manage the identity and access provisioning lifecycle
- Implement authentication systems

Module 6: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyse test output and generate a report
- Conduct or facilitate security audits

Module 7: Security Operations

- Understand and comply with investigations
- Conduct logging and monitoring activities
- Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
- Apply foundational security operations concepts
- Apply resource protection
- Conduct incident management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

Module 8: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in software development ecosystems
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure code

## Course Overview

Our five-day Certified Information Systems Security Professional (CISSP) training course will cover the latest developments in information security, including the requirements for operating systems and the impact of data breaches on sensitive information. Participants will learn about social engineering and the importance of a comprehensive information security programme.

Our Certified Information Systems Security Professional (CISSP) training course will prepare individuals for the CISSP Certified Information Systems Security Professional exam. The course covers various aspects of information security, including security measures, data security, and system security. The curriculum also includes a focus on security architecture, application security, and cryptographic keys.

The Certified Information Systems Security Professional (CISSP) certification is recognised as the 'must have' requirement for the development of a Senior Career in Information Security, Audit and IT Governance Management.

## Course Learning Outcomes

Our Certified Information Systems Security Professional (CISSP) training course will teach you to become proficient in the following:

- Manage security and risk.
- Practice securing assets.
- Design security framework.
- Secure communication and networks.
- Securely develop software.
- Learn from official ISC2 real-world instructors using ISC2 course materials with a preferred official partner.
- Get practical insights into the 8 domains of the CISSP CBK (Common Body of Knowledge).
- Create a test study strategy by assessing strengths and weaknesses.
- Access to ISC2 Official flashcards for use in exam prep.
- Receive a voucher for the CISSP certification exam included with the course tuition.
- Continue learning and face new challenges with after-course one-on-one instructor coaching.

## Audience

Our Certified Information Systems Security Professional (CISSP) training course is suitable for mid and senior-level IT and security managers who are working towards or have already achieved a position such as:

- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)
- Senior Security Engineer
- Security Consultant
- Security Manager
- Security Auditor
- Security Director
- Security Architect
- Network Architect
- IT Director/Manager
- Security Analyst
- Security Systems Engineer

## Entry-Level Requirements

Our Certified Information Systems Security Professional (CISSP) requires attendees to have a minimum 5 years of experience.

## Recommended Reading

It is recommended you read one of the following:

- An Introduction to Information Security and ISO27001:2013
- Assessing Information Security
- Information Security - A Practical Guide

## What's Included

Our Certified Information Systems Security Professional (CISSP) training course includes the following:

- Certificate of attendance.
- 5-day instructor-led training course
- Includes a CISSP exam voucher that allows you to take the exam at any Pearson VUE Test Center.
- After-course coaching available
- Pre-reading
- Course Manuel
- Quizzes
- Exercises

## Exam Information

**Certified Information Systems Security Professional (CISSP) Examination:**

- Duration: 4 hours.
- Format: Multiple Choice.
- Number of questions: 125-175
- Pass Mark: 700

## What's Next

Our Certified Information Systems certificates have emerged as key qualifications for Security Professionals. More and more organisations are demanding experienced Information Security Professionals with the qualifications to prove that you can protect their valuable information and assets. It is the ideal time to achieve and maintain up to date qualifications. Purple Griffon currently offer the following Certified Information Systems classroom-based training courses:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- BCS Certificate In Information Security Management Principles (CISMP)
- Certified In Risk & Information Systems Control (CRISC)

## Additional Information

With over 30,000 qualified professionals worldwide, our Certified Information Systems Security Professional (CISSP) Certification demonstrates proven experience and is the key to a higher earning potential in roles that include:

- CISO
- CSO
- Senior Security Manager