CISSP EXAM PREPARATION TRAINING

NAVEG Academy

CISSP Certification Overview

Certified Information Systems Security Professional (CISSP) is an independent information security certification developed by (ISC)2, the world's leading cyber-security association, this international certification is key for professionals aiming for senior roles cyber security. It provides information security professionals with an objective measure of competence and a globally recognised standard of achievement.

CISSP certified professionals are considered authorities on key security issues including managing an enterprise security programme, security governance, risk management, asset security, application development security, cloud computing, among others.

Individuals possessing this vendor neutral credential are high in demand by corporations all over the world who want to protect their organizations from a growing spurt of sophisticated cyber-attacks especially during and post COVID-19.

Who is CISSP training for?

The CISSP certification is ideal for those working in positions such as (but not limited to):

- Security Consultant
- Security Analyst
- Security Manager
- Security Systems Engineer
- IT Director/Manager
- Chief Information Security Officer
- Security Auditor
- Director of Security
- Security Architect
- Network Architect

Training course outline

The accelerated CISSP exam preparation course teaches you everything you need to know in just five days.

The CISSP curriculum is comprised of an information security common body of knowledge (CBK), which is divided into eight domains:

1. Security and Risk Management
2. Asset Security
3. Security Engineering
4. Communications and Network Security

5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

With engaging, knowledgeable and highly experienced trainers, you'll be confident in joining the 140,000+ qualified CISSP professionals who have proven experience and a higher earning potential in roles such as CISO, CPO, CSO and senior security manager.

What are the prerequisites for CISSP?

To qualify for the CISSP certification, you must:

- Have a minimum of five years' experience in two or more of the eight CBK domains.
- Pass the CISSP examination.
- Complete the endorsement process and subscribe to the $(ISC)^2$ Code of Ethics.
- Maintain certification through continuing professional education (CPE) credits.

What's included in this course?

- Professional training venue with lunch and refreshments.
- Comprehensive revision documentation (digital copy provided as PDF file.)
- A Free copy of the $(ISC)^2$ CISSP Certified Information Systems Security Professional Official Study Guide, 8th Edition textbook.
- Collection of other available learning materials & resources.
- Certificate of attendance.

Why study with us?

There several reasons why you should study your course with us

1. **Learn from anywhere** – We provide Classroom or Live Online delivery and blended option that enables you to attend either in person or online.
2. Keeping travel and costs down to a minimum by attending live online training
3. **Accelerated 5 days training with** CISSPs & industry experts – our trainers are working consultants with years of practical, hands-on experience.
4. **Pass first time or try again for free.** This is our guarantee. We're confident you'll pass your course first time. But if not, come back within a year and only pay for accommodation, exams and incidental costs
5. **You'll learn faster.** Chances are, you'll have a different learning style to those around you. We combine visual, auditory and tactile styles to deliver the material in a way that ensures you will learn faster and more easily
6. We will provide you with **continued support** during the crucial exam preparation period, which means you will have email, WhatsApp & telephone call access to the trainer, who will answer any last-minute questions as required.

For more information contact our Academy Team

Telephone: +27 11 678 0653 | WhatsApp: +27 78 178 3979
Email: training@naveg.co.za | www.naveg-academy.com

CISSP Training Programme

DAY 1

1. Introduction
    - CISSP requirements
    - CISSP exam and exam process
    - Security Fundamentals

2. Security and Risk Management

- Governance principles
- Compliance
- Legal and regulatory issues
- Professional ethics
- Security policy, standards, and guidelines
- Business Continuity requirements
- Personnel security policies
- Risk management concepts
- Threat modeling
- Security in acquisition strategy
- Information security education programs

DAY 2

3. Asset Security

- Information classification
- Data and system ownership
- Privacy protection
- Retention policies
- Data security controls (data at rest/transit)
- Media handling requirements

4. Security Engineering

- Secure engineering process
- Security models
- Security control selection (eval. methods)
- Information system security capabilities
- Security architecture vulnerabilities per type (e.g., client/server, industrial)
- Web-based vulnerabilities
- Mobile system vulnerabilities
- Embedded device vulnerabilities
- Applied Cryptography
- Site and facility design
- Design and implement physical security

DAY 3

5. Communication and Network Security

- Secure design principles
    - OSI and TCP/IP models
    - IP networking
    - Multi-layer models
    - Converged protocols
    - Software-defined networks
        - Wireless networks
        - Communications cryptography
- Secure network components
- Secure communication channels
- Network attacks

DAY 4

6. Identity and Access Management

- Physical and logical access
- Identification and authentication
- Identity as a service (e.g. cloud identity)
- Third-party identity services
- Authorization mechanisms
- Access control attacks
- Identity and access provisioning lifecycle

7. Security Assessment and Testing

- Assessment and test strategies
- Security control testing
- Security process data
- Test outputs
- Internal and third party audits

DAY 5

8. Security Operations

- Investigations
- Logging and monitoring
- Secure resource provisioning
- Operational security concepts and principles
- Resource protection techniques
- Incident management
- Preventative measures (e.g. firewalls, IDS, honeypots)
- Patch and vulnerability management
- Change management process
- Recovery strategies
- Disaster recovery planning and testing
- Physical security (access control)
- Personnel safety concerns (e.g., duress, travel)

9. **Software Development Security**

- Security in the SDLC
- Security in developmental environment
- Software security assessment
- Security impact of acquired software

10. Review and Q&A Session

- Review concepts
- Tips for additional CISSP exam preparation
- Techniques for scoring well on the exam