BCS Certificate in Information Security Management Principles Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The **BCS Certificate in Information Security Management Principles (CISMP)** provides a comprehensive introduction to the core concepts of information security management. It is designed for professionals who have information security responsibilities within their role, as well as individuals planning to build a career in cybersecurity or information security.

Aligned with the latest **BCS CISMP v10 syllabus**, this official training programme prepares learners for the BCS certification examination. The course includes an official exam voucher together with the latest **BCS CISMP Study Guide (4th Edition)**.

Throughout the course, participants will develop a solid understanding of essential information security concepts, including confidentiality, integrity, availability (CIA), threats, vulnerabilities, risk management, and security controls. Learners will also explore legal and regulatory requirements, governance frameworks, and emerging technologies that influence modern security management.

By applying industry-recognised security principles, participants will be equipped to help protect organisational information assets, strengthen business resilience, and establish a strong foundation for advanced managerial or technical cybersecurity certifications. This qualification is recognised as **NCSC Assured**, providing additional credibility for security professionals.

Prerequisites

There are no formal prerequisites for attending this course.

Who Should Attend

Information security is a business-wide responsibility that extends beyond IT departments. This course is suitable for professionals involved in protecting organisational information, including:

- Information security team members
- IT managers and systems managers
- Information security managers
- Information asset owners
- Business analysts
- Project managers
- Product owners
- Service delivery professionals
- Risk, compliance, and privacy specialists

Continuing Professional Development (CPD)

As an **NCSC Assured** training course, delegates may claim **1 CPD point for each hour of training**, up to a maximum of **15 CPD points**.

BCS Certificate in Information Security Management Principles Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Upon successful completion of this course, learners will be able to:

- Explain the key concepts, principles, and business benefits of information security management.
- Understand legal, regulatory, and ethical requirements related to information security.
- Apply fundamental risk management concepts, including risk assessment and mitigation techniques.
- Recognise how organisational governance, culture, and structure influence security management.
- Identify commonly used security frameworks, standards, technologies, and security controls.
- Explain the information security lifecycle and the role of security within software development processes.
- Describe best practices for incident response, business continuity, and disaster recovery planning.

Outline

Module 1: Information Security Fundamentals

- Core principles of information security
- Information security and data privacy
- Confidentiality, integrity, and availability (CIA)
- Privacy legislation and regulatory considerations

Learning Outcomes

- Define fundamental information security terminology.
- Explain the value of information security within organisations.
- Recognise key privacy and data protection requirements.

Module 2: Information Risk Management

- Understanding information risk
- Risk identification and assessment
- Risk management lifecycle
- Risk treatment and mitigation strategies

Learning Outcomes

- Identify the essential components of risk management.
- Describe the stages involved in managing information security risks.

Module 3: Information Security Frameworks

- Organisational responsibilities
- Policies, standards, and procedures
- Security governance
- Legal and regulatory frameworks
- Information assurance standards

Learning Outcomes

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Explain the importance of organisational governance in information security.
- Describe security policies and assurance principles.
- Identify major information security standards and frameworks.

Module 4: Security Operations

- Information lifecycle management
- Information security management processes
- Technical audits and security reviews
- Secure systems development
- Software Development Lifecycle (SDLC)

Learning Outcomes

- Explain security architecture concepts.
- Describe threat modelling techniques.
- Identify methods for assessing and managing vulnerabilities.
- Recognise common cyber threats and attack types.

Module 5: Security Lifecycle and DevSecOps

- Security lifecycle concepts
- Security architecture
- DevSecOps principles
- Threat modelling
- Vulnerability assessment
- Protection against malware and cyber threats

Learning Outcomes

- Explain the stages of the information security lifecycle.
- Describe the principles and benefits of DevSecOps.

Module 6: Technical Security

- Network and communications security
- Cloud and external service security
- IT infrastructure protection
- Cryptography fundamentals

Learning Outcomes

- Explain the principles of network and communication security.
- Identify technical controls used to secure IT infrastructure.

Module 7: Physical and Environmental Security

- Physical, procedural, and technical security controls
- Clear desk and clear screen policies
- Equipment protection
- Securing delivery and storage areas
- Secure disposal of assets and information

Learning Outcomes

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Identify common physical security controls and industry best practices.

Module 8: Disaster Recovery and Digital Forensics

- Incident response planning
- Business continuity management
- Disaster recovery planning
- Introduction to digital forensics

Learning Outcomes

- Describe the key stages of incident response.
- Explain the principles of disaster recovery.
- Understand the purpose and processes of digital forensics.

Module 9: Emerging Technologies

- Security challenges associated with emerging technologies
- AI governance and AI security
- Internet of Things (IoT)
- Operational Technology (OT) security

Learning Outcomes

- Recognise the security implications of modern and emerging technologies.

Module 10: Practice Examination

- BCS examination guidance
- Exam preparation techniques
- Full-length practice examination
- Review of answers and exam strategies