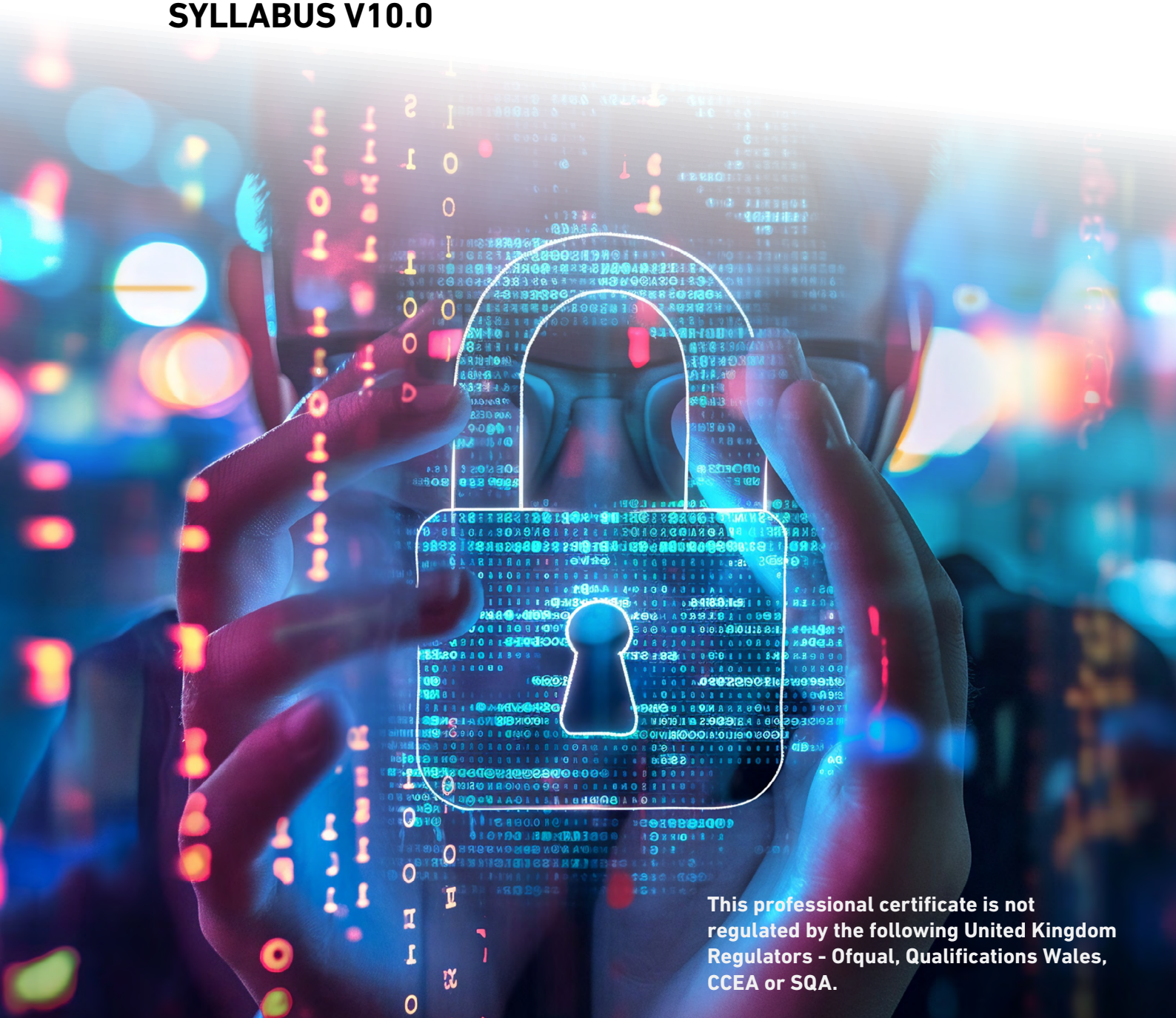
The Chartered Institute for IT

BCS FOUNDATION CERTIFICATE IN INFORMATION SECURITY MANAGEMENT PRINCIPLES

SYLLABUS V10.0



This professional certificate is not regulated by the following United Kingdom Regulators - Ofqual, Qualifications Wales, CCEA or SQA.

CONTENTS

INTRODUCTION 04

LEARNING OUTCOMES 04

QUALIFICATION 05

TRAINER CRITERIA 05

SFIA LEVELS 06

SYLLABUS 09

EXAMINATION FORMAT 26

QUESTION WEIGHTING 27

RECOMMENDED READING 28

DOCUMENT CHANGE HISTORY 30

INTRODUCTION AND OVERVIEW

INTRODUCTION

In today's digital world, ever-evolving technologies offer a wealth of opportunity for both individuals and organisations, but they also give rise to new and increasingly more advanced cyberattacks. The widespread use of digital systems to store and share information comes with an increased vulnerability to attacks that can lead to severe consequences, including financial loss, reputational damage, and violations of personal privacy.

Robust information security management helps protect against these threats by implementing measures that prevent unauthorised access, ensuring that the confidentiality, integrity and availability of data is maintained, and that organisations can meet their legal and ethical obligations.

This foundation level certificate covers the fundamental concepts, technologies and principles of information security management that are so important in helping to safeguard information technology infrastructure and the data it houses.

LEARNING OUTCOMES

Upon completion of this certificate candidates will be able to demonstrate an understanding of:

- Concepts and benefits of information security management.
- Principles of risk management.
- The role of organisational culture and governance in information security management.
- Models and technologies used in information security architecture.
- The key considerations of information security lifecycle management.
- Activities involved in planning for and recovering from security incidents.

QUALIFICATION SUITABILITY AND OVERVIEW

The BCS Foundation Certificate in Information Security Management Principles is relevant to anyone starting work, or looking to start work, in a cyber or information security role, or a related function. It also provides the opportunity for those already within such a role to refresh, enhance and demonstrate their knowledge, and gives a firm foundation for anyone wishing to explore further or higher-level qualifications.

There are no mandatory requirements to be able to undertake this certificate qualification, although candidates will need a good standard of written English. Centres must ensure that candidates have the potential and opportunity to gain the qualification successfully.

This is a foundation level certificate that will:

- develop knowledge of fundamental concepts associated with information security management.
- explore risk management and information lifecycles.
- develop an understanding of information governance and assurance.
- build knowledge of common cyber threats, vulnerabilities and attacks.
- explore how different types of controls can be used to create a layered defence.

Candidates can study for this award by attending a training course provided by a BCS-accredited training provider, or through self-study.

TOTAL QUALIFICATION TIME	GUIDED LEARNING HOURS	INDEPENDENT LEARNING	ASSESSMENT TIME
30 hours	18 hours	11 hours	60 minutes

TRAINER CRITERIA

It is recommended that to deliver this award effectively, trainers should possess:

- BCS Foundation Certificate in Information Security Management Principles
- Ten days' training experience, or have a 'train the trainer' qualification
- A minimum of three years' practical experience in the subject area

SFIA LEVELS

This award provides candidates with the level of knowledge highlighted within the table, enabling them to develop the skills to operate successfully at the levels of responsibility indicated.

LEVEL	LEVELS OF KNOWLEDGE	LEVELS OF SKILLS AND RESPONSIBILITY (SFIA)
K7		Set strategy, inspire and mobilise
K6	Evaluate	Initiate and influence
K5	Synthesise	Ensure and advise
K4	Analyse	Enable
K3	Apply	**Apply**
K2	**Understand**	**Assist**
K1	**Remember**	**Follow**

SFIA*PLUS*

This syllabus has been linked to the SFIA knowledge, skills and behaviours required at levels 2 and 3 for an individual working in information security.

KSC13

Aware of current and emerging standards associated with IT practice nationally and internationally, published by authorities such as IEEE, IEC, BSI, ISO.

KSC14

Aware of the planning and management of the interaction between two or more networking systems, computers or other intelligent devices.

KSC27

Aware of any tool or system which provides security access control (i.e. prevents unauthorised access to systems).

KSC42

Aware of knowledge and understanding of infrastructure configurations.

KSCA1

Familiar with network security and threat mitigation, including physical, electronic, firewalling, encryption, access, and authorisation; protecting data at rest and in transit; defending against viruses and malware; the impact of big data; and the integration of robust security controls into enterprise services and policies.

KSCA2

Familiar with the security threats and vulnerabilities that impact and/or emanate from system hardware, software and other infrastructure components, and relevant strategies, controls and activities to prevent, mitigate, detect and resolve security incidents affecting system hardware, software and other infrastructure components.

KSCA11

Familiar with specialist tools and techniques used in the pursuit of vulnerability management, penetration testing, digital forensics and other security management disciplines.

KSD11

Aware of relevant national and international legislation.

KSD21

Aware of methods and techniques for the assessment and management of business risk including safety-related risk.

For further information regarding the SFIA Levels, please visit:
https://www.bcs.org/it-careers/sfiaplus-it-skills-framework/

SYLLABUS

SYLLABUS

1. INFORMATION SECURITY PRINCIPLES (10%) K2

Recommended reading for this key topic:
Information Security Management Principles (4th Edition), Chapter 1.

1.1 Describe terms and concepts associated with information security management.

Indicative content

a. Information assurance:
   - Confidentiality, integrity, availability and non-repudiation
b. Assets and asset types
c. Threat, vulnerability, risk, and impact
d. Risk appetite and risk tolerance
e. Identity, authentication and authorisation
f. Information governance
g. Accountability, audit and compliance
h. The Information Security Management System (ISMS)

Guidance

Candidates should understand the key concepts associated with information security management, as listed, and be able to recognise definitions, descriptions and examples of each concept.

1.2 Explain the need for, and benefits of, information security.

Indicative content

a. Information security as part of a whole business model:
   - Build information security into business processes
   - Information security professionalism and ethics

b. Different business models and their impact on security

c. Balancing the cost and impact of security with the reduction in risk

d. Security awareness and training

Guidance

Candidates should understand the role and significance of information security and be able to articulate its benefits, such as risk reduction and protection of assets. They should be able to explain how different business models impact security requirements, the importance of balancing security costs with benefits, and the need for ongoing security awareness and training of staff within an organisation.

1.3 Describe the terms and principles associated with personal data privacy legislation and considerations.

Indicative content

a. GDPR data protection principles:
   - Lawfulness, fairness and transparency
   - Purpose limitation
   - Data minimisation
   - Accuracy
   - Storage limitation
   - Integrity and confidentiality
   - Accountability

b. GDPR key terms and definitions:
   - Personal data
   - Data processing
   - Data subject
   - Data controller
   - Data processor

c. The Data Protection Act 2018:
   - Coverage and objectives
   - Four data protection regimes

Guidance

Candidates should understand and be able to describe key terms, definitions and principles of the data protection and privacy legislation and considerations, as listed.

SYLLABUS

2. INFORMATION RISK (15%) K2

Recommended reading for this key topic:
Information Security Management Principles (4th Edition), Chapter 2.

2.1 Describe the key components of risk management.

Indicative content

a. Threat categorisation:
   - Physical threats, cyber threats, legal and contractual threats
   - Accidental threats, deliberate threats

b. Types of operational control:
   - Physical, technical, procedural

c. Control categories:
   - Preventive, detective, corrective, compensating, deterrent, directive

d. Identifying and accounting for the value of information assets:
   - Asset inventory
   - Data classification

e. Risk register

Guidance

Candidates should be able to describe concepts associated with risk management, such as the different types of threats an organisation may face, and the controls that may be used to mitigate and manage them, including identifying examples of different types of control.

Candidates should also be able to describe how both tangible and intangible assets can be identified, classified and valued, and how a risk register can be used to identify, assess and manage risks.

2.2 Explain the processes involved in the risk management lifecycle.

Indicative content

a. Risk identification
b. Risk analysis:
   - Impact and likelihood
   - Business impact analysis (BIA)
   - Risk analysis methods - risk matrix, ISACA risk formula, qualitative and quantitative methods, single loss expectancy, annual rate of occurance, annual loss expectancy
c. Risk treatment:
   - Avoid, transfer, mitigate, accept
d. Communication and consultation
e. Monitoring and review

Guidance

The purpose of risk management is to mitigate risk and reduce potential harm to the organisation.

Candidates should be able to explain the different processes within the risk management lifecycle and the different methods or options that might be employed within each process, including the use of the listed risk analysis methods within an organisation.

SYLLABUS

3. INFORMATION SECURITY FRAMEWORKS (15%) K2

Recommended reading for this key topic:
Information Security Management Principles (4th Edition), Chapter 3.

3.1 Describe key components of organisational structure and policy in managing information security.

Indicative content

a. Typical information and cyber security roles and responsibilities
b. Responsibilities across the business
c. Statutory, regulatory and advisory requirements
d. Creating a culture of good information security practice
e. Organisational security policies, standards, procedures, and guidelines
f. Balancing physical, procedural and technical controls
g. End-user codes of practice

Guidance

Candidates should be able to define and describe the various elements, as listed, that can be used in combination to establish an effective organisational structure for managing information security.

3.2 Explain the principles of information security governance and information assurance.

Indicative content

a. Information security charter
b. Review of security policy
c. Security audits and reviews
d. Checking and reporting on compliance status
e. Protection of data:
   - Classification systems and levels
   - Rules associated with assets of each classification level
f. Implementing information assurance
g. Legal principles relating to information assurance management:
   - Protection of personal data
   - Computer misuse
   - Intellectual property
   - Contractual safeguards
   - Records retention
   - Securing digital signatures
   - The use of cryptography technology

Guidance

Candidates should be able to explain the scope and purpose of activities associated with information security governance, such as auditing and reviewing security policy to ensure organisations are meeting their data protection obligations.

Candidates should also be able to explain how information assurance measures can be planned and implemented to fit within an organisation's architectural and strategic requirements.

3.3 Describe security standards, procedures and frameworks.

Indicative content

a. Baseline controls
b. Configuration management and change control
c. Information security frameworks:
   - NIST Cybersecurity Framework
   - ISO27001
   - CIS 18
   - Cyber Essentials and Cyber Essentials Plus

Guidance

Externally produced standards and frameworks can be adopted by organisations to demonstrate, structure and enhance their information security practices.

Candidates should be able to describe the purpose, scope and high-level processes and controls of the standards, procedures and frameworks listed.

SYLLABUS

4. SECURITY OPERATIONS (15%) K2

Recommended reading for this key topic:
Information Security Management Principles (4th Edition), Chapter 4.

4.1 Explain concepts, models and technologies associated with security architecture and operations.

Indicative content

a. Security architecture:
   - Layered defence
   - Defence in depth and breadth
   - Least privilege
   - Separation of duties
   - Authentication and authorisation mechanisms

b. Technical components of security operations:
   - Security Information and Event Management (SIEM)
   - Security Orchestration, Automation and Response (SOAR)
   - Network Security Monitoring (NSM)
   - Endpoint security, including anti-virus
   - Vulnerability management
   - Incident response
   - Threat intelligence, including the threat intelligence lifecycle
   - Access control

Guidance

Security architecture is a set of models, methods, and principles that serve as a blueprint for ensuring the protection of data, systems, and networks against cyber threats.

Candidates should be able to explain different architectural concepts, as well as being able to explain and give examples of technical components used in security operations.

4.2 Explain threat modelling and common threat modelling frameworks.

Indicative content

a. The definition and purpose of threat modelling
b. Threat modelling frameworks:
   - Attack trees
   - STRIDE
   - MITRE ATT&CK
c. Threat informed defence
d. Information warfare

Guidance

A business needs to understand the threat landscape and what could happen should a threat be realised. By modelling a threat, a business can then plan appropriate protection.

Candidates should be able to explain threat modelling and the purpose, scope and high-level processes of the common frameworks listed. They should also be able to explain the concepts of information warfare and threat informed defence.

4.3 Explain techniques for identifying, assessing and managing security vulnerabilities.

Indicative content

a. Systems for identifying and rating vulnerabilities:
   - Vulnerability monitoring
   - Common Vulnerabilities & Exposure (CVE)
   - Common Vulnerability & Scoring System (CVSS)
b. Ethical hacking and penetration testing
c. Red teaming

Guidance

In order for security vulnerabilities to be appropriately managed, they first need to be identified and assessed.

Candidates should be able to explain the different methods and systems listed for identifying and understanding the severity of vulnerabilities that exist in an organisation's cyber and information security.

4.4 Describe common types of cyberattacks and threats to systems.

Indicative content

a. Common types of attack:
   - Denial-of-Service (DoS)
   - Spoofing
   - Identity-based attacks, e.g. credential stuffing, brute force attacks
   - Code injection attacks, e.g. SQL injection, cross-site scripting (XSS)
   - DNS tunnelling

b. Common threats:
   - Passwords, e.g. the threat of bad passwords, advice on good passwords, use of multi-factor authentication
   - Insider threats
   - Malware, e.g. viruses, worms, ransomware, rootkits, backdoors, spyware, trojans, logic bombs, keyloggers, infostealer
   - Zero Day exploits
   - Social engineering and phishing

Guidance

Candidates should be able to define, describe and recognise examples and typical behaviours of different types of common cyberattacks and threats, as listed.

SYLLABUS

5. THE SECURITY LIFECYCLE AND DEVSECOPS (10%) K2

Recommended reading for this key topic:
Information Security Management Principles (4th Edition), Chapter 5.

5.1 Explain stages and considerations of information security lifecycle management.

Indicative content

a. The information lifecycle:
   - Creation, storage, usage, archive, destruction

b. Effective testing of systems:
   - Planning
   - Execution
   - Post-execution
   - Use of control frameworks

c. Security issues associated with software:
   - Commercial off-the-shelf (COTS)
   - Free and open-source software (FOSS)

d. Shadow IT

e. Cybersecurity Supply Chain Risk Management (C-SCRM)

Guidance

All information needs to be managed carefully throughout its lifecycle, from creation to destruction, to ensure its confidentiality, integrity and availability.

Candidates should be able to explain the relevant considerations at each stage of the information lifecycle. This includes identifying and managing unauthorised data sources and applications, understanding how security can be integrated into system design, and how system security can be tested. Candidates should also understand the importance of managing risk within the supply chain.

5.2 Describe the key terms, features and benefits of DevSecOps.

Indicative content

a. The definition and purpose of DevSecOps
b. Benefits of DevSecOps
c. Stages in the DevSecOps pipeline:
   - Plan, code, build, test, release, deploy
d. Secure by design
e. Agile development:
   - Sprint planning
   - Daily scrum
   - Sprint review
   - Backlog refinement

Guidance

DevSecOps is a collaborative approach that integrates security practices into the software development and operations process, ensuring security is implemented at each stage of development and that adequate testing is carried out.

Candidates should be able to describe the concept of DevSecOps and why and how it is used, as well as the key concepts of Agile development, as listed.

SYLLABUS

6. TECHNICAL SECURITY (15%) K2

Recommended reading for this key topic:
Information Security Management Principles (4th Edition), Chapter 6.

6.1 Describe key concepts associated with networks and network security.

Indicative content

a. Network topologies:
   - Bus, star, mesh, hybrid
b. Network types
c. IP address
d. Common protocols:
   - FTP/SFTP, SSH, SMTP, DNS, HTTP/HTTPS, Kerberos
e. Network components and security technologies:
   - Switch, router, firewall
   - Wi-Fi
   - Intrusion detection system (IDS)
   - Intrusion prevention System (IPS)
   - Wi-Fi Protected Access (WPA)
   - Virtual private network (VPN
   - Internet Protocol Security (IPSec)
   - Data loss prevention (DLP)
   - Demilitarized zone (DMZ)
   - Cryptography, including hashing
f. Cloud computing:
   - Infrastructure-as-a-service (IaaS)
   - Platform-as-a-service (PaaS)
   - Software-as-a-service (SaaS)
   - Cloud deployment models
   - Cloud security
g. Containers:
   - Microservices
   - Docker

Guidance

Candidates should be able to define, describe and recognise examples of different network topologies, types, protocols, and components, as listed.

They should also be able to describe different cloud computing models and their security considerations, as well as understanding containers and their common vulnerabilities.

6.2 Describe technical strategies and measures to secure IT infrastructure.

Indicative content

a. Zero trust
b. Privileged access management (PAM)
c. Separation of systems
d. Data backups:
   - Common approaches
   - Checking integrity of restored data
   - Storage of backups

Guidance

A number of different strategies, practices and technologies can be implemented to increase cyber and information security, such as zero trust, privileged access management, and separation of systems.

Candidates should understand and be able to describe the strategies listed, as well as the importance of, and best practice approaches to, data backups.

SYLLABUS

7. PHYSICAL AND ENVIRONMENTAL SECURITY (5%) K2

Recommended reading for this key topic:
Information Security Management Principles (4th Edition), Chapter 7.

7.1 Describe common physical security controls.

Indicative content

a. Physical security measures and concerns:
   - Controlling access to buildings
   - Securing entry points and storage facilities
   - Electronic entry controls
   - Tailgating
   - Monitoring and detection tools

b. Protecting equipment:
   - Security marking
   - Backup generators and uninterruptible power supplies (UPS)
   - Maintenance contracts and service level agreements (SLAs)
   - Security of mains electricity and network cabling

c. Clear screen and desk policy

d. Moving property on and off site:
   - Asset registers
   - Staff procedures
   - Bring your own device (BYOD)
   - Security requirements in delivery and loading areas

e. Secure disposal of equipment and other assets:
   - Disposal methods
   - IEEE P2883 standard for sanitising storage

Guidance

From controlling access to buildings, to the disposal of equipment, physical security considerations are an important area of security within any organisation.

Candidates should be able to define, describe and recognise examples of the physical aspects of security that contribute to a multi-layered defence.

SYLLABUS

8. DISASTER RECOVERY AND DIGITAL FORENSICS (10%) K2

Recommended reading for this key topic:
Information Security Management Principles (4th Edition), Chapter 8.

8.1 Describe activities involved in incident response.

Indicative content

a. The incident response plan
b. Stages of NIST 800-61 incident response:
   - Preparation
   - Detection and analysis
   - Containment, eradication and recovery
   - Post-incident activity
c. The roles of incident response team personnel

Guidance

Incident response is a structured approach to managing the aftermath of an incident to reduce damage, and recovery time and costs.

Candidates should be able to describe the different components and activities involved in incident response, as well as the typical roles and responsibilities undertaken by those in the response team.

8.2 Explain terms associated with disaster recovery.

Indicative content

a. Disaster recovery, the business continuity plan, and the business impact analysis
b. Resilience metrics:
   - Recovery time objective (RTO)
   - Recovery point objective (RPO)
   - Maximum tolerable outage (MTO)
c. The disaster recovery plan

Guidance

Candidates should be able to explain how disaster recovery fits in with the business continuity plan, and how the business impact analysis helps inform both of these processes.

Candidates should also be able to explain the resilience metrics associated with disaster recovery, and the purpose and content of an effective disaster recovery plan.

8.3 Describe the process and principles of digital forensics.

Indicative content

a. Uses of digital forensics:
   - Criminal investigations
   - Root cause analysis

b. The digital forensic process

c. Four principles of the NPCC Good Practice Guide for Computer Based Electronic Evidence

d. Types of digital evidence and examples of devices where evidence may be found:
   - Volatile data
   - Non-volatile data

e. The chain of custody

Guidance

Digital forensics involves the investigation and analysis of digital devices and data to uncover and preserve evidence.

Candidates should understand the reasons why digital forensics might be used, and be able to describe the typical processes, devices and types of evidence involved. Candidates should also understand the importance of maintaining chain of custody for legal investigations.

SYLLABUS

9. EMERGING AND GROWING TECHNOLOGIES (5%) K2

Recommended reading for this key topic:
Information Security Management Principles (4th Edition), Chapter 9.

9.1 Describe common security concerns associated with emerging and growing technologies.

Indicative content

a. Security concerns associated with AI:
   - AI privacy, data collection and security
   - Transparency and explainability
   - Bias in data and outcomes
   - Misuse
   - Deepfakes

b. Ethical considerations of AI

c. Security risks associated with IoT devices:
   - Increased attack surface
   - Default settings and passwords
   - Unencrypted data transfer

d. Operational technology:
   - Security considerations
   - ISA/IEC 62443

Guidance

New technologies can present organisations and society with new opportunities and improved ways of operating. However, they can also present new threats that may be exploited to introduce previously unconsidered risks.

Candidates should be able to recognise examples of emerging and growing technologies, as listed, as well as being able to describe the security considerations and concerns associated with them.

EXAMINATION FORMAT

This award is assessed by completing an invigilated online exam that candidates will only be able to access at the date and time they are registered to attend.

Adjustments and/or additional time can be requested in line with the BCS reasonable adjustments policy for candidates with a disability or other special considerations, including English as a second language.

TYPE

40 MULTIPLE CHOICE QUESTIONS

DURATION

60 MINUTES

SUPERVISED

YES

THIS AWARD WILL BE SUPERVISED

OPEN BOOK

NO

(NO MATERIALS CAN BE TAKEN INTO THE EXAMINATION ROOM)

PASSMARK

(65%)

26/40

DELIVERY

ONLINE FORMAT

QUESTION WEIGHTING

Each primary subject heading in this syllabus is assigned a percentage weighting. The purpose of this is:

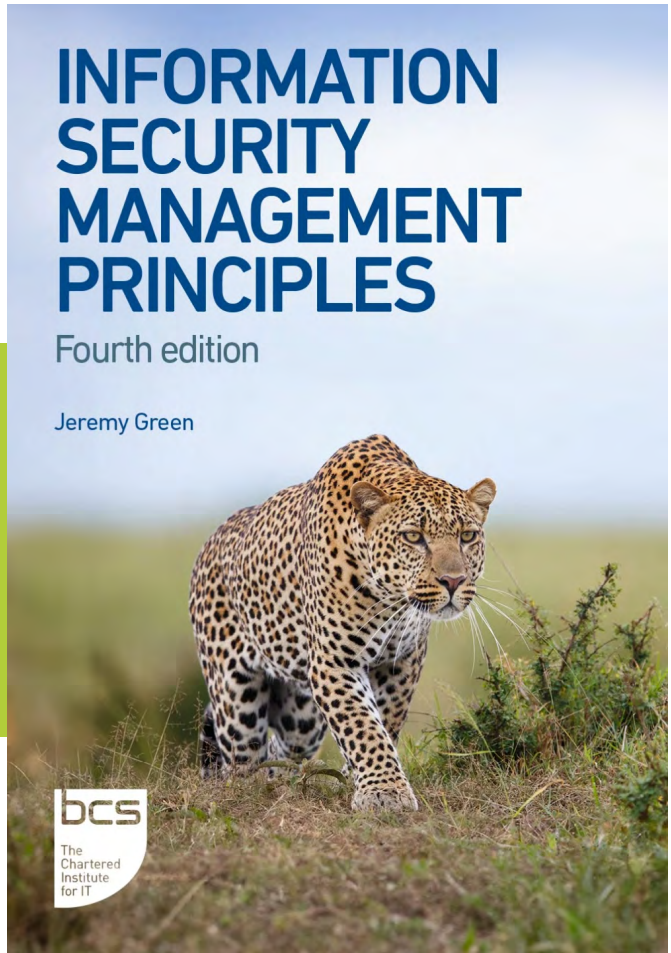
- Guidance on the proportion of content allocated to each topic area of an accredited course.
- Guidance on the proportion of questions in the exam.

Syllabus Area		Weighting
1	Information security principles	10%
2	Information risk	15%
3	Information security frameworks	15%
4	Security operations	15%
5	The security lifecycle and DevSecOps	10%
6	Technical security	15%
7	Physical and environmental security	5%
8	Disaster recovery and digital forensics	10%
9	Emerging and growing technologies	5%

RECOMMENDED READING

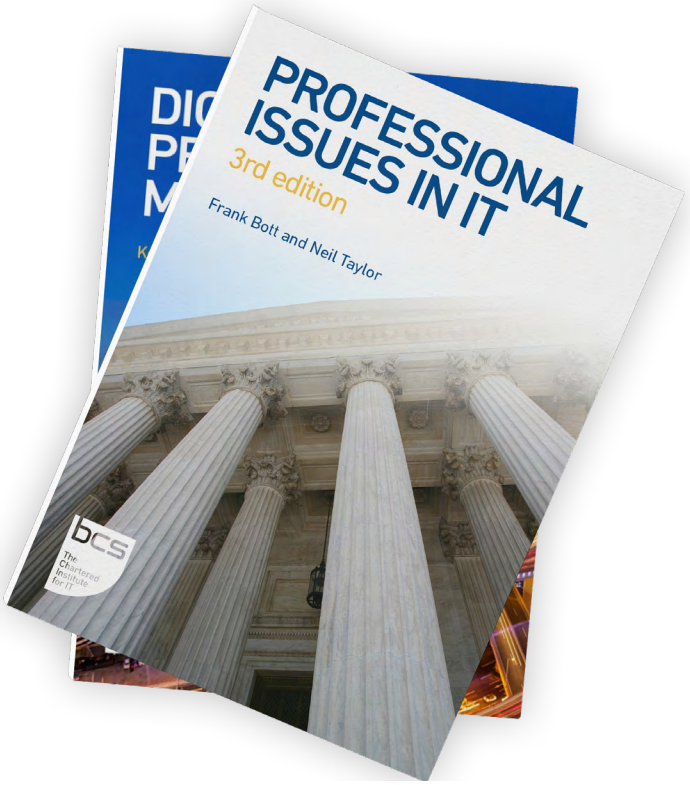
The following titles are suggested reading for anyone undertaking this certificate. Candidates are also be encouraged to explore other available sources.

TITLE: Information Security Management Principles, Fourth Edition
AUTHOR: Jeremy Green
PUBLISHER: BCS
PUBLICATION DATE: November 2024
ISBN: 978-780175-18-8



USING BCS BOOKS

Accredited Training Organisations may include excerpts from BCS books in the course materials. If you wish to use quotes from the books, you will need a licence from BCS. To request an appointment, please get in touch with the Head of Publishing at BCS, outlining the material you wish to copy and the use to which it will be put.



DOCUMENT CHANGE HISTORY

Any changes made to this syllabus document shall be clearly recorded with a change history log. This shall include the latest document version number and details of changes made.

SYLLABUS V10.0	
DOCUMENT VERSION	**NOTES**
1.0	Document created.

For further information please contact:
BCS
The Chartered Institute for IT
3 Newbridge Square
Swindon
SN1 1BY
T +44 (0)1793 417 417
www.bcs.org