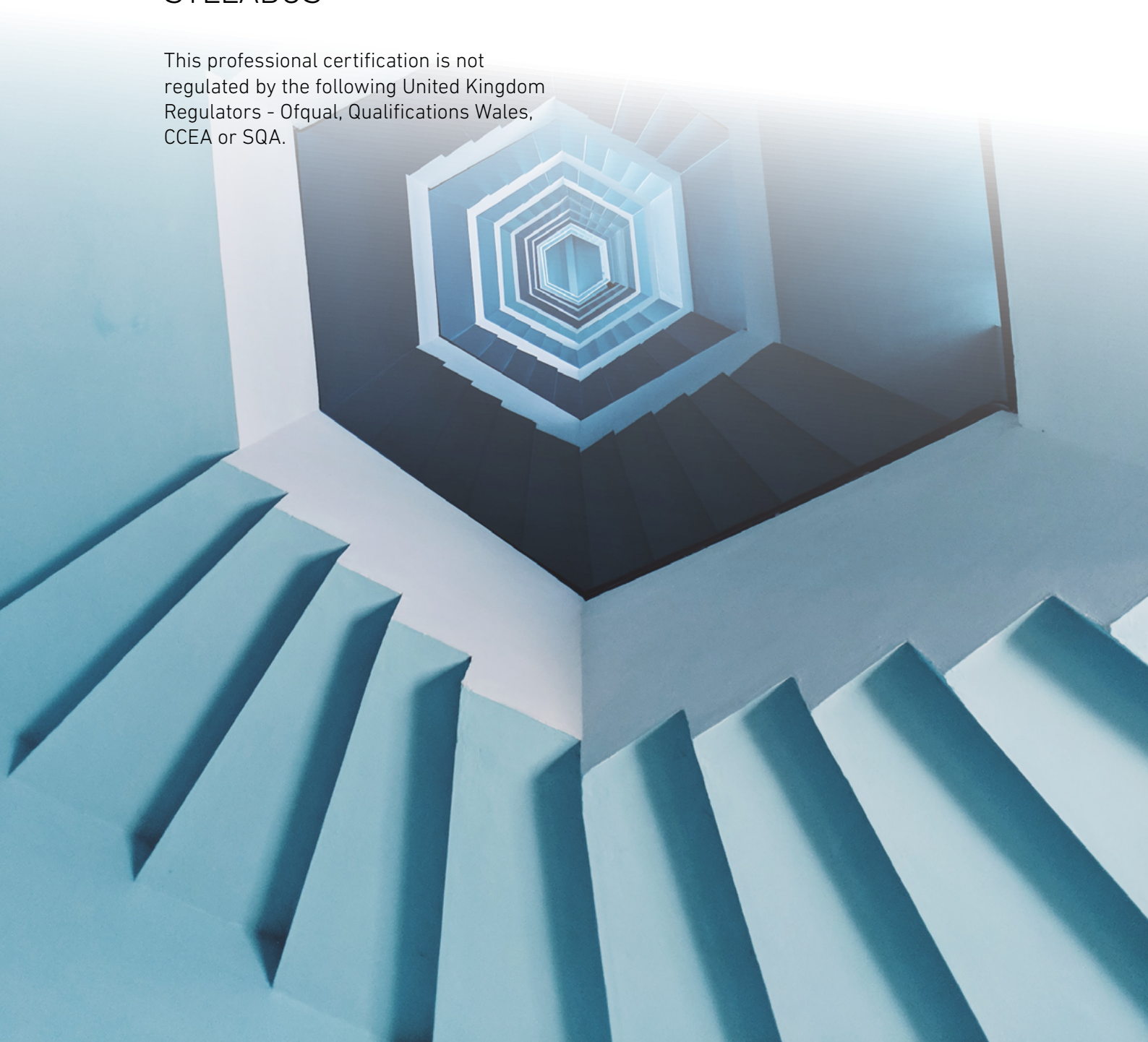
The Chartered Institute for IT

2023 | NOVEMBER V1.0

BCS PRACTITIONER AWARD IN SECURITY ARCHITECTURE

SYLLABUS

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



CONTENTS

INTRODUCTION 04

LEARNING OUTCOMES 04

QUALIFICATION SUITABILITY 05

TRAINER CRITERIA 05

SFIA LEVELS 06

SYLLABUS 08

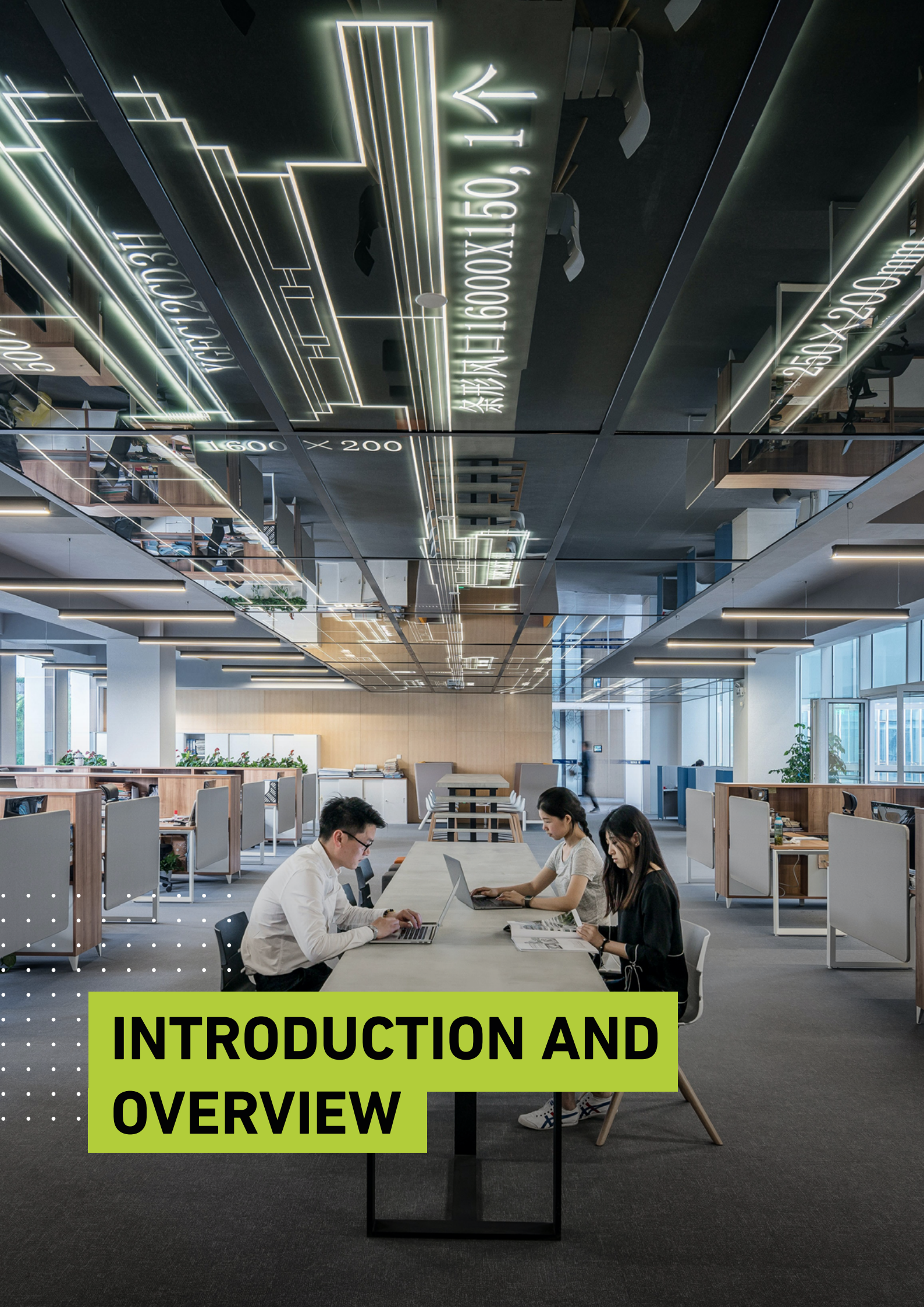
EXAMINATION FORMAT 18

QUESTION WEIGHTING 19

RECOMMENDED READING 20

USING BCS BOOKS 21

DOCUMENT CHANGE HISTORY 21



INTRODUCTION AND OVERVIEW

INTRODUCTION

What is the role of security architecture? How does security architecture sit within the domains? Security architecture is a sub domain within enterprise architecture which focuses the security of structures, processes, and technology necessary to protect assets, data, and systems from threats and risks.

The Practitioner Award in Security Architecture will give candidates an in-depth understanding of the role of security architecture, including the activities undertaken by security architects. It will also explore how the role of security architecture fits in with the other architecture domains.

LEARNING OUTCOMES

Upon completion of the award, candidates will be able to demonstrate a practical understanding of:

- The role of security architecture.
- The relationship between security architecture and the other architecture domains.
- The skills and knowledge required by security architects.
- The activities undertaken by security architects.
- Security architecture governance and decision-making processes.

QUALIFICATION SUITABILITY AND OVERVIEW

Centres must ensure that learners have the potential and opportunity to gain the qualification successfully. Candidates will need to have passed the BCS Foundation Certificate in Architecture Concepts and Domains and have a good standard of written English and Maths.

This qualification is suitable for candidates who are looking to progress their career within a security role. It can be taken in combination with other Practitioner Awards and the Practitioner Certificate in Enterprise and Solution Architecture.

This is an occupationally focused qualification which will:

- Test a learner's ability to recall and apply knowledge in a range of scenarios.
- Demonstrate a practical understanding of key concepts across the topic areas.
- Enable a learner to progress in their career.

Candidates can study for this certificate 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
18 hours	15 hours	2 hours	30 minutes

TRAINER CRITERIA

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

- The BCS Practitioner Award in Security Architecture.
- A minimum of 2 years' training experience or 1 year with a recognised qualification.
- A minimum of 3 years practical experience in the area of IT architecture.

SFIA LEVELS

This award provides candidates with the level of knowledge highlighted within the table, enabling candidates 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 level 4 for an individual working in Security Architecture.

KSCA11

Specialist tools and techniques used in the pursuit of vulnerability management, penetration testing, digital forensics and other security management disciplines for bug-hunting, abstract interpretation and program analysis, binary analysis and reverse-engineering, exploit development, source code analysis, and static and dynamic application security testing (SAST/DAST), etc.

KSC52

The principles and application of cloud/ virtualisation (including ownership, responsibilities and security implications). Use of tools and systems to manage virtualised environments.

KSCA1

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

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.

KSB23

Conveying a level of confidence and professionalism when engaging with stakeholders, influencing positively and persuading others to take a specific course of action when not in a position of authority.

Further detail around the SFIA Levels can be found at www.bcs.org/levels.

SYLLABUS

1. THE ROLE OF SECURITY ARCHITECTURE (10%) K2

1.1 Explain the role of security architecture.

Indicative content

a. Responsibilities of security architecture:
   - Communicate between the technical and non-technical
   - Develop and maintain the organisation's security strategies (e.g. risk assessment, technology evaluation)
   - Define the organisation's security principles, standards, protocols, and technologies
   - Influencing others to execute security principles

b. Understanding security design principles, including:
   - Establish the context before designing a system)
   - Make compromise difficult
   - Make disruption difficult
   - Make compromise detection easier
   - Reduce the impact of compromise

(Source: National Cyber Security Centre, 2019)

Guidance

Candidates should be able to define the role of a security architect and how an architect creates and designs security for a system or service. This includes being able to show an understanding of how a security architect's work impacts the structure and behaviour of an organisation's security processes, information security systems, and people. They should also be able to explain how security principles align with an organisation's mission and strategic plans.

'NOTHING SAYS 'SECURE BY DESIGN', ONE OF THE ACCOUNTABILITY REQUIREMENTS OF GDPR, LIKE AN ENTIRE TEAM DEDICATED TO THE ROLE OF SECURITY TESTING AT ALL STAGES OF PRODUCT DESIGN AND DEVELOPMENT.'

Mike Sheward (2020), Security Operations in Practice

2. SECURITY ARCHITECTURE IN RELATION TO OTHER DOMAINS (15%) K4

2.1 Analyse how security architecture interacts with other domains.

Indicative content

a. Security standards (NIST SP 800-37 & 800-53, ISO 27001, CIS)
b. Solutioning
c. Design
d. Baseline configuration
e. Threat modelling
f. SDLC integration
g. Attack surface management
h. Develop security architecture

Guidance

Candidates should be able to explain and analyse the use of the different security architectural aspects and how they are applied in different contexts. This includes differentiating between general and data-specific frameworks and ensuring the responsibilities of security architecture are well-defined. They need to understand that security architecture is a sub-component of enterprise architecture and ensure it is integrated at the right times and at the right level. They need to understand that security architecture can be considered as part of information security, keeping the processes aligned with the speciality.

2.2 Describe key artefacts used by security architects.

Indicative content

a. Security architecture artefacts:
   - Rules on handling of data/information assets
   - Published security policies and supporting documentation (e.g. information classification and related protective marking rules and guidance)
   - Agreed details of information asset ownership and custody
   - Risk Management regime and documentation

Guidance

Candidates should be able to describe key artefacts used within security architecture. This includes explaining the purpose of each artefact and how they are used across the organisation to contribute towards strategic objectives.

3. SKILLS AND KNOWLEDGE (30%) K4

3.1 Analyse the frameworks used in security architecture.

Indicative content

a. The Zachman Framework
b. COBIT 5
c. OSA
d. TOGAF
e. SABSA

Guidance

Analyse and explain the purposes and chief characteristics of the core security architecture frameworks.

3.2 Analyse methods of communication in specific scenarios to enable effective stakeholder management.

Indicative content

a. Requirements gathering:
   - Interviews
   - Active listening
b. Methods of communication:
   - Written versus oral
   - Level of detail (granularity)
   - Use of technical jargon

Guidance

Candidate should be able to analyse the use of a variety of communication styles that are commonly used in a security architecture environment. Candidate should also develop an understanding of the need for a collaborative and empathetic approach to communicating complex concepts to non-technical stakeholders.

3.3 Evaluate the techniques and tools used by security architects.

Indicative content

a. Content filtering
b. Cryptography
c. Data loss prevention
d. End user devices
e. Firewalls
f. Identity and access management (IDAM)
g. Intrusion detection systems (IDS)/ Intrusion prevention systems (IPS)
h. Malware and malware prevention/management
i. Networks
j. Platforms and operating systems
k. Security information and event management (SIEM) tools
l. Virtualisation
m. Virtual private networks (VPNs)

Guidance

Candidates should be able to identify, explain, and evaluate the use of the techniques and tools that are used by a security architect. This includes the use of operating systems (e.g. Windows, UNIX, and Linux). They should also be able to demonstrate a practical understanding of perimeter security controls including firewalls, IDS/IPS, network access controls, and network segmentation. Furthermore, candidates are expected to be able to evaluate the application of various aspects of wireless security such as routers, switches, and VLAN security.

'THE PURPOSE OF ESTABLISHING AN INFORMATION SECURITY FRAMEWORK IS TO ENSURE THAT APPROPRIATE CONTROL MECHANISMS ARE IN PLACE TO MANAGE EFFECTIVELY THE INFORMATION ASSURANCE ACROSS THE ENTERPRISE.'

Alexander et al. (2021), Information Security Management Principles

3.4 Evaluate the use of risk management approaches in specific scenarios.

Indicative content

a. Key risk management terms:
   - Risk
   - Threat
   - Vulnerabilities
   - Residual risk
   - Risk appetite
   - Risk tolerance
   - Asset
   - Countermeasure
   - Control

b. Five risk management techniques:
   - Avoidance
   - Retention
   - Spreading
   - Loss prevention and reduction
   - Transfer (through insurance and contracts)

c. Analytical tools:
   - Explain decision trees
   - Fishbone analysis
   - SWOT analysis

d. Identify risk methods, including:
   - ISO/IEC 31000
   - ISO/IEC 27005
   - EBIOS
   - SANS Institute six step process: preparation, identification, containment, eradication, recovery, and lessons learnt
   - ISACA's Risk IT framework
   - NIST SP 800-30

Guidance

Candidates should be able to explain how to enable informed risk-based decisions through the use of industry-standard terms, techniques, tools, and methods. This includes identifying the use of different approaches in specific scenarios.

3.5 Explain how sources of industry knowledge can be used in specific scenarios.

Indicative content

a. Sources of information:
   - British Computer Society (BCS)
   - Cloud Security Alliance (CSA)
   - Council on Cyber Security (CCS)
   - Cybersecurity and Infrastructure Security Agency (CISA)
   - European Union Agency for Network and Information Security (ENISA)
   - Information Commissioner's Office (ICO)
   - Information Security Forum (ISF)
   - International Information System Security Certification Consortium (ISC)[2]
   - National Crime Agency (NCA)
   - National Cyber Security Centre (NCSC)
   - National Institute of Standards and Technology (NIST)
   - Open Web Application Security Project (OWASP)
   - SANS Institute

Guidance

Candidates are expected to demonstrate knowledge about relevant public and non-public sources of cyber security information and be able to explain how to use them in specific scenarios, either through direct access or via organisation memberships. This includes national CERTs and professional bodies.

4. ACTIVITIES UNDERTAKEN BY SECURITY ARCHITECTS. (30%) K4

4.1 Analyse how security architecture interacts with stakeholders.

Indicative content

a. Architectural approach to security.
b. Responding to security incidents (e.g., data breaches, viruses, phishing scams, etc.)
c. Providing post-event analysis once an issue is resolved
d. Clarity of communication
e. Use of formal and informal channels

Guidance

Candidates should be able to explain how to apply an architectural approach to real problems and consider all relevant information and apply appropriate rigour to ensure a full solution is designed and strategic and business objectives are met. They need to demonstrate a deep understanding of security concepts and can demonstrably apply them to a technical level. They should be able to communicate security and risk implications clearly to technical and non-technical audiences.

4.2 Analyse the design of different secure systems in specific scenarios.

Indicative content

a. Security architecture frameworks (e.g. COBIT 5, OSA, TOGAF, SABSA)
b. Developing security requirements for routers, firewalls, local area networks (LANs), wide-area networks (WANs), virtual private networks (VPNs), and other related network devices
c. Designing cryptographic solutions including public key infrastructure (PKI), digital signatures, and certification authorities (CA)
d. Specific approaches (e.g. Bastion host, anti-patterns, zero trust, microsegmentation)

Guidance

Candidates should be able to evaluate the use of different secure systems and system architectures through the application of architectural patterns and principles.

4.3 Evaluate sources of research and innovation and how they can be applied to specific scenarios.

Indicative content

a. Public and non-public resources
   - SANS
   - NCSC
   - Vendors
   - Professional groups (ISF, ISC2, BCS)
b. Professional body membership (ISACA, ISF, ISC2, BCS)
c. Attendance at industry events and vendor demonstrations

Guidance

Candidates should be able to identify and evaluate a range of research and innovation related to security architecture. This includes how and where information regarding new security-relevant technologies can be found and the process of how they could be applied in an operational context. Candidates should also be able to explain how to advise on developments to security aspects of changing technology.

4.4 Evaluate the implementation and transformation of security technologies.

Indicative content

a. Reviewing and approving the installation of all firewalls, VPN, routers, servers, and IDS scanning technologies
b. Vulnerability assessment (internal and external)
c. Preparing cost estimates for all cybersecurity measures and identifying any potential integration issues
d. Security testing

Guidance

Candidates should be able to demonstrate a practical understanding of system architectures and security technology. This includes an understanding of the impact of vulnerabilities on existing and future designs, systems, and the associated security implications. Candidates should also be able to demonstrate an understanding of the security implications of transformation, interpretation and application of policy and process, business architecture, and legal and political implications to assist the development of technical solutions or controls.

5.GOVERNANCE (15%) K4

5.1 Analyse how effectively security architecture is governed in accordance with key principles, policies and standards.

Indicative content

a. Core principles of security governance:
   - Systems management
   - SDLC
   - ISMS

b. Relevant standards:
   - OWASP
   - ISO 27000 series of standards
   - ISO/IEC 154081 (Common Criteria)
   - (NIST CSF) – SP 800-12, 800-14, 800-26, 800-64, 800-218
   - FIPS 140
   - Cyber Essentials and Cyber Essentials+
   - BSI IT-Grundschutz
   - PCI-DSS

Guidance

Candidates should be able to explain the importance of keeping up to date with legal, regulatory and technical changes. This includes identifying the use of different methods of governance to support the definition of security policies and procedures. Furthermore, candidates should be able to explain how relevant standards can be used and how they should be deployed in specific scenarios.

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

20 MULTIPLE CHOICE AND MULTIPLE RESPONSE QUESTIONS

DURATION

30 MINUTES

SUPERVISED

YES

THIS AWARD WILL BE SUPERVISED

OPEN BOOK

NO

(NO MATERIALS CAN BE TAKEN INTO THE EXAMINATION ROOM)

PASSMARK

65%

13/20

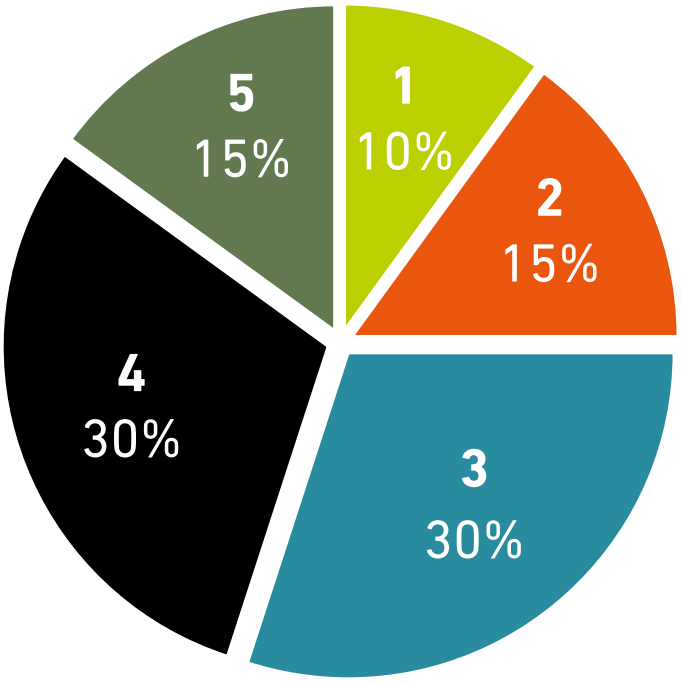
DELIVERY

DIGITAL FORMAT

QUESTION WEIGHTING

Each major 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

1	The Role of Security Architecture
2	The Relationship of Security Architecture to other Disciplines
3	Activities undertaken by Security Architects
4	Skills and Knowledge
5	Governance

Question Type

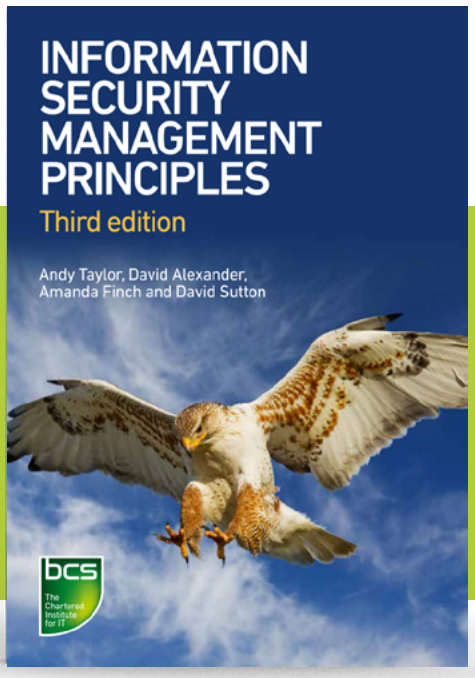
Multiple choice and multiple response questions

RECOMMENDED READING

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

TITLE: Security Operations in Practice
AUTHOR: Mike Sheward
PUBLISHER: Ingram Publisher Services UK - Academic
PUBLICATION DATE: *2020*
ISBN: *9781780175089*

TITLE: Information Security Management Principles
AUTHOR: David Alexander, Amanda Finch, David Sutton, Andy Taylor
PUBLISHER: Ingram Publisher Services UK - Academic
PUBLICATION DATE: *2021*
ISBN: *9781780175201*



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 the syllabus shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

VERSION NUMBER	CHANGES MADE
Version 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