BCS PRACTITIONER CERTIFICATE

INFORMATION ASSURANCE ARCHITECTURE

SYLLABUS

November 2021 v1.0

bcs
The Chartered Institute for IT

CONTENTS

Introduction

In today's information age, keeping organisations' data assets secure is a vital responsibility. An Information Assurance (IA) architect provides a framework to successfully manage complexity. Although many designers will need to work together as a project becomes bigger and more complex, a well-built system will have the appearance of being designed by a single authority.

This Level 4 module covers the key concepts, skills and tools required of anyone working in the role of an IA architect. They will be able to successfully undertake the tasks required for the development of IA architecture to support complex systems while considering an organisation's goals, environmental factors and technical capabilities.

This certificate covers the range of concepts, approaches and techniques used in information management. It promotes a hands-on approach to information risk management, using current standards and enabling candidates to make immediate use of the module content in their own context.

Candidates will be required to demonstrate their knowledge and practical application of these concepts by undertaking a scenario-based online assessment.

Qualification Suitability and Overview

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

This course is suitable for security professionals interested in the technical and business aspects of the profession or anyone looking to work in the field of security architecture. They could be either within a dedicated security team or as part of a more general Enterprise Architecture (EA) team.

This is an occupationally-focused qualification which will test a learner's ability to:

- Apply knowledge and concepts relating to Information Security Architecture principles.
- Demonstrate a practical understanding of the business environment and available technical controls.
- Demonstrate knowledge of how to provide a multi-layered set of defences and how to implement cost-effective security controls.
- Demonstrate an understanding and knowledge of Information Assurance methodologies.

Candidates can study for this certification 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
56 hours	**40 hours**	**16 hours**	**1.5 hours**

* Examples of Independent Learning include reading of articles or books, watching videos, attendance of other types of training or work shadowing.

Trainer Criteria

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

- 1 year training experience.
- An Information Assurance Architecture or similar qualification.
- 1 year experience working in an information risk management role in any business area or the ability through experience to contextualise.

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 Skill 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 information assurance architecture.

KSB 16 – Persistence

Meeting targets, acting and/or fulfilling agreements, even when adverse circumstances prevail.

KSB 18 – Organisational awareness

Understanding the hierarchy and culture of own, customer, supplier and partner organisations and being able to identify decision makers and influencers.

KSB 22 – Interacting with People

Establishing relationships, contributing to an open culture, and maintaining contacts with people from a variety of backgrounds and disciplines. Effective, approachable, and sensitive communicator in different communities and cultures. Ability to adapt style and approach to meet the needs of different audiences.

KSC 08 –Infrastructure Architecture

The frameworks and principles on which networks, systems, equipment, and resources are based, both on-premises and cloud-based. E.g. AWS and VMWare. Conceptual models and standards may include SOA and ISO standards.

KSC 15 – Operating Systems

System software which controls activities such as input, output, dynamic resource allocation, and error reporting, within the operation of a computer configuration, e.g. Windows and cloud services.

KSC 19 – Corporate, Industry and Professional Standards

Applying standards, practices, codes, and assessment and certification programmes relevant to the IT industry and the specific organisation or business domain.

KSC 20 – Telecommunications Protocols

Rules for the inter-operation of networking components. E.g. TCP/IP and IP suite.

KSC 28 – Business Continuity Planning

Methods and techniques for risk assessment, business impact analysis, establishment of countermeasures and contingency arrangements relating to the serious disruption of IT services. E.g. data replication and contingency plan testing.

KSD 11 – Legislation

Relevant national and international legislation, e.g. GDPR (General Data Protection Act) and the Computer Misuse Act. For certain industries specific legislation requires conformance to the destruction of information and also the recording and safe transfer and storage of data for a defined period of time.

KSD 60 – Network Data Gathering Techniques

The selection, implementation and application of network data gathering methods, tools and techniques which are appropriate to the information required and the sources available. E.g. network management and monitoring, statistical analysis.

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

Learning Outcomes

Upon completion of this module, candidates will be able to:

- Understand the skills, including those of communication and influencing required by an IA architect is to provide a framework within which complexity can be managed successfully.
- Describe the business environment, the risks that apply to it, and the impact of Security in improving its governance.
- Identify information risks that arise from potential solution architectures.
- Develop and implement architectures that mitigate the risks posed by modern technologies and business practices
- Use the concept of architecture to integrate solutions to a diverse range of complex needs, and to manage that complexity.
- Apply 'standard' security techniques and architectural reference models to mitigate security risks.
- Provide consultancy and advice to explain Information Assurance and architectural problems.
- Securely configure ICT systems in compliance with their approved security architectures.

Syllabus

1. The Basics of Information Assurance (IA) Architecture (15%, K2)

Candidates will be able to:

1.1 Describe the concepts of IA and cyber security, the role of the IA architect and the concepts of security architectures.

Indicative content

a. IA concepts, e.g. integrity, availability, authentication, confidentiality, non-repudiation.
b. Cyber security concepts, e.g. threat identification, information protect, attack and intrusion, detection and response, recovering security and defences.
c. The role of the IA architect and their responsibility for architecture, design, interface definition, and implementation.

Guidance

Before exploring the detail of IA architecture, candidates will be expected to understand the contextual framework for thinking about IA and Cyber security, as well as how the IA architect's role fits into an organisation.

1.2 Describe the knowledge, skills and experience an IA architect must possess.

Indicative content

a. Soft skills, e.g. communication, influencing.
b. Information architecture methods.
c. Business technology planning.
d. IT infrastructure, architecture operations and investment decision-making.
e. Implementing security initiatives.

Guidance

Candidates will be expected to have a thorough understanding of the business strategy, on-going security initiatives, relationships, risks, constraints, and enablers, as this is key to the success of the IA architecture's activity. Successful delivery also depends on the architect's interpersonal skills that will ensure that stakeholders are fully on-board and open to change.

1.3 Explain the concepts and design principles used by IA architects when designing and assuring systems.

Indicative content

a. Implementing concepts of least privilege, segregation of duties, privacy by design.
b. Implementing concepts and principles of classifying data.
c. Ethics, e.g. CIA triad (confidentiality, integrity, availability).
d. Concepts of defence.

Guidance

Candidates should be able to demonstrate their understanding of the several well-known and established principles of IA that may help IA architects in their initiatives. They should also consider how and why ethics are a key consideration in development and design.

1.4 Describe security architectures at a high level using appropriate contextual terms and architectural concepts related to security concerns.

Indicative content

a. Multi-layering security, e.g. organisation, procedures, physical, application.
b. Multi-tiered incident handling, e.g. prevention, containment, detection, recovery.
c. Security infrastructure layered architecture, e.g. platform security, network security, application security.
d. Integrated applications architectures, e.g. micro services, event-driven architectures.

Guidance

Candidates are expected to be able to demonstrate a thorough understanding of appropriate architectural concepts, in order to provide a framework for application.

1.5 Explain the importance of design patterns and conceptual architectures.

Indicative content

a. Concepts of reusability.
b. Security patterns to promote consistency and cost-effectiveness across an organisation.
c. Communication, connectivity and composition, data management, event-driven architecture, stream processing, and API management and consumption.

Guidance

Candidates are expected to be able to understand the important role patterns play in the design of systems and defining and documenting common solutions to recurring design problems.

1.6 Describe the methods and techniques used for risk assessment, business impact analysis, and establishing countermeasures and contingency plans.

Indicative content

a. Risk assessment frameworks, e.g. ISO/IEC 27005, ISO 31000 series, NIST Cybersecurity Framework, OCTAVE, RiskIT, SABSA, Open FAIR, COSO.
b. Assess and manage IA risks.
c. Risk mitigation plan, e.g. control, transfer, avoid, delay, compensate etc.
d. Enabling benefits.

Guidance

Candidates are expected to be able to follow appropriate risk methodologies that support the business and enable risks to be effectively managed using appropriate methodologies and frameworks.

2. Innovation and Business Improvement (15%, K2, K3 and K5)

Candidates will be able to:

2.1 Evaluate the security implications and governance of business transitions.

Indicative content	Guidance
a. Internal growth, e.g. franchising, opening new operations, e-commerce, outsourcing. b. External growth, e.g. mergers, takeover, horizontal integration, vertical integration, forward vertical integration, conglomerate integration.	Candidates are expected to have a full understanding of how growth or contraction to the business can impact its security and governance.

2.2 Explain the nature of organisational risk, culture, appetite and risk tolerance.

Indicative content	Guidance
a. The reference environment, sector, district, industry, or value chain. b. Identifying stakeholders, e.g. SRE, governance teams. c. Principle-based risk management approach tailored to the organisation's needs, structure and purpose. d. Organisations' corporate risk appetite. e. Acceptable risk threshold.	Candidates should be able to identify the key stakeholders and ensure that development and implementation of the IA architecture is within the overall business appetite.

2.3 Evaluate how security is a business enabler.

Indicative content

a. Context for risk assessments.
b. Complying with control framework.
c. Justifying security measures.

Guidance

Candidates are expected to be able to justify security measures and ensure that these align with business objectives and the control framework being followed.

2.4 Describe continuous improvement as a philosophy.

Indicative content

a. Six Sigma and continuous improvement as part of the Plan-Do-Check-Act cycle.
b. Agile principles to adapt to changing requirements and customer needs.
c. Lean principles such as adding value and eliminating waste (e.g. Muda).
d. Kanban, e.g. focusing on visualisation, flow, and limiting work in progress.

Guidance

Candidates should ensure that any ongoing improvement initiatives are leveraged and be able to explain how they may adapt these initiatives according to change.

2.5 Apply the techniques that can be used to measure security maturity levels.

Indicative content

a. Security KPIs.
b. ISO/IEC 21827:2008 Systems Security Engineering - Capability Maturity Model® (SSE-CMM®).
c. Cybersecurity Capability Maturity Model (C2M2).

Guidance

Maturity models should be aligned with and have buy-in from the business leaders. Candidates are expected to be able to demonstrate their understanding of how relevant KPIs should be incorporated into the IA architecture design.

3. Advanced Security Architecture Concepts (35%, K2, K3, K4 and K5)

Candidates will be able to:

3.1 Evaluate available security monitoring, response solutions and security services.

Indicative content

a. Security policies covering information security, physical security, remote access, network, application.
b. Security services covering prevention, containment, event collection and tracking, recovery and restoration, assurance.
c. On-premises security solutions and services.
d. Cloud security solutions and services.
e. The integration of information risk management into business-as-usual operations.
f. The proper assignment of resources to undertake an information risk management programme.
g. Regular communications and reporting.

Guidance

As the main goal is to enhance security, candidates should be able to demonstrate their understanding of how to follow security policies and standards, ensuring that both on premises and cloud-based activities are addressed.

3.2 Describe the role of directories and how they can be used in authentication and authorisation.

Indicative content

a. Representing business entities and their relationships through a directory infrastructure.
b. Covering people, equipment, organisations, business roles, cloud.
c. Considering design aspects, e.g. naming standards, physical storage resilience, access protocols.
d. Cloud, e.g. setting up federation between Active Directory or Azure Active directory, enabling single sign-on using appropriate SSO protocols such as SAML 2.0, OpenID Connect, LDAP.

Guidance

Candidates are expected to be able to explain how IA architects should make use of directories to ensure all parts of the business, including in the Cloud, are included when designing the IA architecture.

3.3 Demonstrate the functions of security management within the organisation.

Indicative content

a. Integrated programme of operational security management, based on ISO/IEC 27001:2013 framework.
b. Culture of shared responsibility for organisation's security.
c. Segregating duties to mitigate elevated risk of abusing privilege.
d. Managing physical and environmental security.
e. Using a change management programme.
f. Protecting live IT production systems environment.

Guidance

Candidates should be able to demonstrate an understanding of the security management principles to be followed and design an architecture in line with them.

3.4 Evaluate the main network technologies, associated security controls and the threats they counter.

Indicative content

a. IThreats relating to all the layers of the TCP/IP and OSI models, e.g. MAC flooding, session hijacking, IP spoofing, Denial of Service, UDP flooding, SYN flooding.
b. Countermeasures, e.g. port security, encryption, authentication, string as session key, regeneration of session key, router filtering, intrusion detection, DDoS mitigation, Security as a Service (SaaS).

Guidance

Candidates are expected to be able to understand how risks posed by current threats can be reduced by IA architecture, as well as how architecture can be made be robust enough to withstand any emerging security threats.

3.5 Illustrate the main methods for resilience, recovery capabilities and techniques.

Indicative content

a. Designing IT structure, infrastructure, equipment and processes to be resistant to interruption using data replication, fault tolerance, redundancy of equipment and networks.
b. Using back-ups and logs to recover data and systems.
c. Using business continuity and disaster recovery to help recovery using hot, cold, and warm sites.

Guidance

Candidates should be able to consider how IA architecture should be designed for resilience, depending on the risks assessed, in order to ensure continuity of operations and reduce the impact to the business of any unforeseen events.

3.6 Illustrate the main characteristics of virtualisation, cloud platforms and their security aspects.

Indicative content

a. Types of service model, e.g. SaaS, PaaS, IaaS, STaaS, SECaaS, DaaS, TEaaS, BaaS.
b. Characteristics of virtualisation in cloud computing, e.g. partitioning, isolation, encapsulation.
c. Virtualisation applications, e.g. memory, networks, storage, hardware.
d. Cloud deployment models, e.g. private, public, community, hybrid, multi-cloud.
e. Forms of virtualisation, e.g. virtual memory, software.
f. IT governance in cloud computing, e.g. ensuring IT assets are implemented and used according to policies and procedures.

Guidance

Candidates are expected to be able to demonstrate a thorough understanding of cloud operations and be able to communicate their implications to business stakeholders.

3.7 Illustrate the threats to Industrial Control Systems and appropriate countermeasures.

Indicative content

a. Industrial control systems, e.g. Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Safety Instrumented Systems (SIS).
b. Characterising an attack on an Industrial Control System.
c. Standards and procedures used for securing Industrial Control Systems, e.g. ISA/IEC-62443 (formerly ISA-99), NIST Special Publication 800-82.
d. Prioritising security areas within Industrial Control Systems.

Guidance

Candidates should be able to explain how any new systems may have to interface with older technologies, in such a way as to minimise threats to critical systems.

3.8 Demonstrate the purpose of Digital Right Managements (DRM), Data Loss Prevention (DLP), and their main standards and technologies.

Indicative content

a. Addressing unauthorised copying using digital rights management (DRM) systems, e.g. MPEG-21, Rights Expression Languages (RELs).
b. Data loss categories, e.g. leakage, disappearance or damage.
c. Components of DLP systems, e.g. DLP management console, DLP endpoint agent, DLP network gateway, data discovery agent (or appliance).
d. DLP methods, e.g. content matching, learning method (LM).

Guidance

To protect intellectual assets, candidates will need to consider and make use of DRM and DLP technologies in designing IA architecture.

3.9 Illustrate the threats to an organisation when implementing and managing microprocessor-controlled devices.

Indicative content

a. Type of micro-processor devices, e.g. smart devices in the workplace, in transport systems, MFDs.
b. Privacy issues.
c. Compliance issues.
d. Controls, e.g. passwords, restricting physical access, configuration, patching, disposal.
e. Risk of remote attack, e.g. on devices with networking capability.
f. Additional controls for networked devices, e.g. firewalls, private IP address, encrypting data, auditing, monitoring.

Guidance

Candidates should be able to consider the potential threats which such devices can pose, but equally will need to understand mitigation strategies, as the introduction of microprocessor-controlled devices should not compromise the security of the IA architecture.

3.10 Evaluate common mobile platforms and technologies, their management, and their potential risks.

Indicative content

a. Concepts and principles of managing mobile devices (BYOD).
b. Mobile device management (MDM) solutions and platforms.
c. Mobile device threats and their associated risks.
d. Protecting mobile devices.

Guidance

Similarly to micro-processor controlled devices, candidates will be expected to be able to demonstrate their understanding of BYODs and the processes for avoiding compromise of the IA architecture's security.

3.11 Apply appropriate security mechanisms for a given scenario or organisation.

Indicative content

a. Implementing appropriate technical and organisational controls, e.g. based on risks, policies and standards.
b. Tools and techniques for implementing security services, e.g. cryptography, access control.

Guidance

Candidates will be expected to be able to actively use appropriate technologies to ensure security within the organisation.

3.12 Implement application security measures and adhere to appropriate frameworks to secure them.

Indicative content

a. Application security features, e.g. authentication, authorisation.
b. Common application and software weaknesses and how to mitigate them.
c. Main tools, methodologies, and frameworks to assess application security, e.g. OWASP, static or dynamic testing.
d. Appropriate controls to secure applications.

Guidance

Candidates should be able to use appropriate security frames to ensure the security of applications systems.

3.13 Apply appropriate cryptographic mechanisms and techniques.

Indicative content

a. Security mechanisms and services that can be provided by cryptography, e.g. encryption, hashing, key management.
b. Encryption algorithms and how they can be used to provide security.
c. Key management and PKI services.

Guidance

Candidates should be familiar with appropriate cryptographic techniques, tools and products and be able to implement them seamlessly within the IA architecture.

3.14 Evaluate the use of threat modelling techniques.

Indicative content

a. Threat modelling techniques, e.g. STRIDE, OCTAVE, attack trees.
b. Identifying threats and mitigations using threat modelling techniques.
c. Conducting a threat analysis using best practice methodologies.

Guidance

Candidates are expected to be able to demonstrate a full understanding of threat modelling techniques and ensure the IA architecture is designed to minimise the impact of threats.

3.15 Illustrate security design patterns, common threats, and security controls that can be used to counter them.

Indicative content

a. Design patterns used in industry and related security, e.g. software design patterns.
b. Developing security patterns to solve security issues.
c. Security architectural frameworks, e.g. SABSA.
d. Analysing systems to identify common threats and risks.
e. Aligning security patterns to appropriate policies and standards.
f. Implementing controls using industry standards, e.g. ISO27701/2, COBIT.

Guidance

Candidates should be able to explain how to make the best use of secure design patterns, as these will ensure the reliability of the resulting IA architecture.

3.16 Evaluate supplier assurance frameworks and how supplier services can be securely acquired and managed.

Indicative content

a. Interpreting reports and documents for supplier assurance purposes, e.g. SOC1, SOC2.
b. Securely managing suppler services.
c. Tools and techniques for assuring and acquiring supplier services, e.g. contracts, assessments, audits.
d. Evaluating supplier risks.
e. Validating controls and mitigations.

Guidance

As the use of external suppliers is so prevalent, candidates should be able to explain the process of fully assessing third party audit reports such as SOC1 and SOC2, so that the IA architecture is appropriately protected.

3.17 Evaluate the main authentication, authorisation, and accounting (AAA) techniques and how to implement them.

Indicative content

a. Authentication services, e.g. MFA, SSO, directory services, federation.
b. Authorisation services, e.g. access control (RBAC, ABAC).
c. Accounting services, e.g. logging.

Guidance

Candidates should be able to demonstrate an appreciation of new authentication and authorisation services which have evolved to counter the current threat landscape. They should also be able to describe how they would implement the most appropriate techniques based on the threat level faced by the organisation.

3.18 Demonstrate how new and emerging technologies impact on security.

Indicative content

a. Cloud services, e.g. IaaS, PaaS, SaaS.
b. Containerisation technologies and how they can be managed using Kubernetes and the Open Group's Collaboration Oriented Architectures (COA) framework for cloud.
c. Basics of machine learning and related security concerns.
d. Zero Trust as a target architectural approach.

Guidance

Candidates will need to be able to demonstrate their ability to look beyond the organisation, understand how new and emerging technologies are being used, and ensure that IA architecture incorporates them in an optimal manner.

3.19 Analyse how operational changes can be managed, controlled and assured.

Indicative content

a. Change management methodologies, e.g. ITIL.
b. Evaluating changes for security, validity, and effectiveness.
c. Reviewing change management plans.
d. Reviewing changes throughout their lifecycles to ensure that changes are aligned to an organisation's security objectives.

Guidance

As the IA architect typically brings in many changes, candidates should demonstrate their understanding of how to mitigate the associated risks by using tried and tested methodologies, and avoid introducing new threats to the organisation.

4. Information Assurance Methodologies (20%, K3, K4 and K5)

Candidates will be able to:

4.1 Apply the main information assurance and enterprise architecture methodologies and frameworks.

Indicative content

a. Improving IA across an organisation using appropriate methodologies.
b. Comparing enterprise architecture frameworks, e.g. SABSA, TOGAF, SOA.

Guidance

Candidates should be able to practically demonstrate a solid understanding of enterprise and IA architecture frameworks and the principles underpinning these.

4.2 Evaluate methods, tools and techniques for identifying potential vulnerabilities.

Indicative content

a. Types of vulnerabilities, e.g. technological and organisational vulnerabilities.
b. Vulnerability management standards and frameworks, e.g. those defined by SANS, IASME, Cyber Essentials Plus.
c. Conducting vulnerability assessments using various tools and methodologies, e.g. OpenVas, Nessus.
d. Assessing and prioritising vulnerabilities.
e. Frameworks used for scoring vulnerabilities, e.g. CVE, CVSS.
f. Potential for exploiting vulnerabilities using appropriate frameworks, e.g. CAPEC, ATT&CK.

Guidance

Candidates should be able to demonstrate a clear understanding of how to identify, analyse and manage vulnerabilities related to the organisation and technology.

4.3 Evaluate methods, tools and techniques used for penetration testing.

Indicative content

a. Different types of penetration tests, e.g. black box, white box.
b. Stages of a penetration test.
c. Penetration testing methods, e.g. external, internal.
d. Testing frameworks, e.g. OSSTMM.
e. Developing rules for penetration test engagements.
f. Reporting penetration test results.
g. Remediation plans based on penetration test results.

Guidance

Candidates will be expected to have a solid grasp of how penetration tests can help secure organisations and how they can be used to identify threats and vulnerabilities within systems and services.

4.4 Analyse vulnerability and penetration testing programs.

Indicative content

a. Scoping a vulnerability and penetration test.
b. Appropriate roles and responsibilities for a testing program.
c. Appropriate components for the tests, e.g. agreeing appropriate disclosure requirements, setting up accounts, agreeing appropriate tools.
d. Tracking and reporting testing results.
e. Analysing different methods and their appropriateness to the organisation.

Guidance

IA architects will have a vested interest in these programs as they will provide vital information about threats and vulnerabilities, which can then be managed and shared with appropriate stakeholders.

Candidates will need to be able to compare the features of various programs and consider how they can be implemented.

4.5 Analyse frameworks and tools that can be used to secure code.

Indicative content

a. Best practice for securing code, e.g. OWASP.
b. Code testing methodologies, e.g. static and dynamic testing.
c. Code review methodologies, e.g. code inspection, pair programming, walk throughs.
d. Tools for reviewing code.

Guidance

Candidates should be able to understand the approaches used to secure code and promote good secure coding practices within the organisation, as well as to compare the characteristics and benefits of the most common methodologies and tools.

4.6 Demonstrate an understanding of product evaluation and maturity models.

Indicative content

a. Product evolution models, e,g, TCSEC, evaluation assurance levels, common criteria, ITSEC.
b. Maturity models, e.g. CMM, CMMC, NIST maturity framework.
c. Level of IA maturity within an organisation.

Guidance

Candidates will be expected to be able to recommend appropriate products that meet the security requirements and security goals of the organisation.

4.7 Demonstrate an understanding of cryptographic assurance frameworks and standards.

Indicative content

a. Operations that underpin cryptography.
b. Classical and modern ciphers that can be used in cryptography.
c. Cryptography techniques, e.g. key/secrets management, stream and block ciphers, symmetric and asymmetric encryption.
d. Cryptography concepts, e.g. hashing and digital signatures.
e. Recommendations, standards and frameworks related to cryptography, e.g. FIPS, foundation or prime profiles.
f. FIPS 140 certification levels, e.g. FIPS 140-2, FIPS 140-3.

Guidance

Candidates will need to recommend appropriate ciphers and understand how and which cryptographic solutions can be used to solve business problems and meet regulatory and compliance requirements.

5. Security Across the Lifecycle (15%, K2, K3 and K5)

Candidates will be able to:

5.1 Explain the roles and responsibilities related to Information Assurance Architecture development.

Indicative content

a. Key areas required to develop a successful assurance program, e.g. leadership, governance, monitoring, compliance.
b. Core principles of developing an IA strategy.
c. Organisational needs for IA.
d. Concepts and requirements for developing an IA architect's terms of reference.

Guidance

Candidates will be expected to be able to demonstrate their understanding of how IA architects contribute and develop IA strategies which complement and help the business achieve its objectives.

5.2 Illustrate the importance of embedding security throughout the development process.

Indicative content

a. Information life cycles and how they relate to IA.
b. Process models to help embed security throughout the various lifecycles, e.g. PDCA.
c. Security management activities at strategic, tactical, and operational levels.
d. Tactics, techniques and procedures for enhancing visibility of threats, e.g. Kill chain.
e. Security throughout software development lifecycles, e.g. SDLC, Lean, Waterfall, Agile.
f. Concept of DevOps and DevSecOps.

Guidance

Candidates should be able to discuss the importance of working with appropriate stakeholders like developers to integrate information security and assurance throughout all of an organisation's activities.

5.3 Demonstrate the main concepts and techniques of auditability and traceability.

Indicative content

a. Concepts of traceability.
b. Governance and auditability requirements for IA.
c. Information flows within a system and how they can be secured.
d. Traceability methodologies, e.g. those described in SABSA.

Guidance

Candidates will be expected to be able to contextualise the assurance activities to the business needs, ensuring that security goals are linked to business goals and that security activities are auditable.

5.4 Explain the core types of design artefacts at the conceptual, logical and physical layers.

Indicative content

a. Fundamental types of EA artefacts and their key properties using appropriate models, e.g. CSVLOD model.
b. Artefacts related to principles of IA.
c. Technology reference artefacts.
d. Solution design artefacts, e.g. HLDs, LLDs.
e. Additional artefacts, e.g. standards, guidelines, business capability models, roadmaps, landscape diagrams.
f. Artefact classes under TOGAF.

Guidance

IA architects should follow appropriate guidelines when dealing with artefacts. Therefore candidates will need to be familiar with a range of artefacts as they will be involved in reviewing and creating these.

5.5 Evaluate the security issues associated with commercial systems, applications and products.

Indicative content

a. Security issues and risks related to off-the-shelf products and COTS.
b. Security issues and risks related to outsourcing.
c. Security issues and risks related to offshoring.
d. Security issues and risks related to cloud services, e.g. IaaS, PaaS, SaaS.

Guidance

Candidates should be able to demonstrate an awareness of security issues and risks in a wide range of technologies and solutions.

5.6 Demonstrate the importance of systems hardening.

Indicative content

a. Types of system hardening, e.g. server, database hardening.
b. Standards for system hardening, e.g. CIS benchmarks, NIST special publications.
c. Techniques used for system hardening, e.g. patch management, changing default passwords, encryption, controlling privileged users.
d. How system hardening can reduce risks.

Guidance

Candidates must be able to discuss methods of hardening systems and services based in best practice, as well as how to align these so that a business can meet its objectives.

5.7 Explain the role and value of information security architecture within the overall business process.

Indicative content

a. Concepts of Enterprise Information Security Architectures (EISA).
b. How EISA can align to and enable the business.
c. Methodologies for aligning IAA to the business, e.g. SABSA.
d. Using appropriate frameworks to develop IAA, e.g. TOGAF.
e. Monitoring, measuring and reporting architecture development progress.

Guidance

Candidates should be able to demonstrate their understanding of how IA enables the business objectives and aligns to the goals of the organisation. Monitoring, measuring and reporting these will be a crucial part of these as this will raise awareness and provide the justifications for the assurance activities.

Examination Format

This certificate is assessed through completion of an invigilated online exam which candidates will only be able to access at the date and time they are registered to attend.

Type	A two-part exam containing a knowledge section (comprising ten 1-mark multiple choice questions and ten 2-mark multiple response questions) and a scenario-based section (containing four scenarios, each with five 2-mark questions).
Duration	90 minutes
Supervised	Yes
Open Book	No (no materials can be taken into the examination room)
Passmark	45/70 (65%)
Delivery	Digital format only.

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.

Question Weighting

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

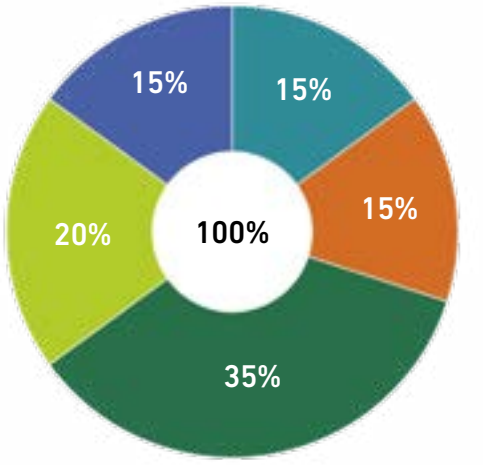
1. Guidance on the proportion of content allocated to each topic area of an accredited course.
2. Guidance on the proportion of questions or marks in the exam.

Syllabus Area

1. The Basics of Information Assurance (IA) Architecture	**15%**
2. Innovation and Business Improvement	**15%**
3. Advanced Security Architecture Concepts	**35%**
4. Information Assurance Methodologies	**20%**
5. Security Across the Lifecycle	**15%**

Question types

A mix of question types will be used including multiple choice, multiple response, fill in the blanks, ordering and matching.



Syllabus Weighting

Recommended Reading

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

Books

Title	Information Risk Management: A Practitioner's Guide
Authors	David Sutton
Publisher	BCS, Learning and Development Limited
Publication Date	November 2014 (Second edition due for publication in late 2021)
ISBN	978-1-78017-265-1

Title	Information Security Management Principles
Authors	David Alexander, Amanda Finch, David Sutton, Andy Taylor
Publisher	BCS, Learning and Development Limited
Publication Date	January 2020 - 3rd edition
ISBN	978-1-78017-518-8

Legislation

Data Protection Act 2018. Her Majesty's Stationery Office.	https://www.gov.uk/government/collections/data-protection-act-2018
The General Data Protection Regulation (GDPR).	https://ec.europa.eu/info/law/law-topic/data-protection_en
The Computer Misuse Act 1990. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/1990/18/contents
The Police and Criminal Evidence Act 1984. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/1984/60/contents
The Official Secrets Act 1989. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/1989/6/contents
The Freedom of Information Act 2000. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/2000/36/contents

The Regulation of Investigatory Powers Act 2000. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/2000/23/contents
The Copyright, Designs and Patents Act 1988. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/1988/48/contents
Control Of Major Accident Hazards Regulations 2015. Health and Safety Executive	http://www.legislation.gov.uk/uksi/2015/483/contents/made
Civil Contingencies Act 2004. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/2004/36/contents

Codes of Practice

Good Practice Guidelines 2018. The Business Continuity Institute.	https://www.thebci.org/training-qualifications/good-practice-guidelines.html

Guidance

The Traffic Light Protocol (TLP). European Network and Information Security Agency (ENISA).	https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol
The Capability Maturity Model. Carnegie Mellon University.	https://www.itgovernance.co.uk/capability-maturity-model
Critical Security Controls Version 7.1. The Centre for Internet Security.	https://cybernetsecurity.com/industry-papers/CIS-Controls%20Version-7-cc-FINAL.PDF
The IISP Skills Framework. The Chartered Institute of Information Security (CIISec).	https://www.ciisec.org/Skills_Framework
The IISP Knowledge Framework. The Chartered Institute of Information Security (CIISec).	https://www.ciisec.org/Knowledge_Framework
The IISP Roles Framework. The Chartered Institute of Information Security (CIISec).	https://www.ciisec.org/Roles_Framework

A Structured Approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. The Federation of European Risk Management Associations (FERMA).	https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf
The Standard for Information Assurance for Small and Medium Sized Enterprises (IASME).	https://iasme.co.uk

Websites

HMG Cyber Essentials Scheme from the Department for Digital, Culture, Media & Sport (DCMS).	https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
10 Steps to Cyber Security, produced by the National Cyber Security Centre (NCSC).	https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security
CORAS Risk Assessment Platform. SourceForge	http://coras.sourceforge.net/index.html
FAIR (Factor Analysis of Information Risk). Risk Management Insight.	https://www.fairinstitute.org

The OCTAVE Method (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

The OCTAVE-S Method – designed for use by smaller organisations.

The OCTAVE Allegro Method, a streamlined approach for information security assessment and assurance. Carnegie Mellon University.

Details of all three Octave methodologies are available from the Carnegie Mellon University:	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=309051
SABSA (Sherwood Applied Business Security Architecture). The SABSA Institute.	http://www.sabsa.org/

Information Risk Management Standards

A number of standards have been developed worldwide which aim to assist organisations to implement risk management systematically and effectively.
The different standards reflect the different motivations and technical focus of their developers and may be appropriate for different organisations and situations. Standards are normally voluntary, although adherence to a standard may be required by regulators or by contract.
Commonly used standards include:

- ISO 31000:2018 - Risk Management Principles and Guidelines
- The Risk Management Standard
- ISO31010:2019 - Risk Management - Risk Assessment Techniques
- COSO 2017 - Enterprise Risk Management Integrated Framework (due to be updated in 2015)
- OCEG Red Book 2009 A Governance, Risk and Compliance Capability Model
- ISO Guide 73:2009 Definitions of generic terms related to Risk Management.
- ISO 27005:2018 Guidelines for information security risk management.
- ISO 27001:2017 A specification for an information security management system
- BS 31100:2011

ISO Standards are available for purchase from.	https://www.iso.org/store.html or https://shop.bsigroup.com/
The Risk Management Standard can be downloaded from	https://www.theirm.org/what-we-do/what-is-enterprise-risk-management/irms-risk-management-standard/
The COSO Enterprise Risk Management document can be obtained from	https://www.coso.org/pages/erm-integratedframework.aspx
The OCEG Capability Model can be downloaded from	https://go.oceg.org/grc-capability-model-red-book (registration is required)
The BS 31100:2011 Standard may be purchased from	https://shop.bsigroup.com/

Using BCS Books

Accredited Training Organisations may include excerpts from BCS books in the course materials. If you wish to use excerpts from the books you will need a license from BCS. To request a licence, please contact 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 **November 2021**	Document Creation

CONTACT

For further information please contact:

BCS
The Chartered Institute for IT
3 Newbridge Square
Swindon
SN1 1BY

T +44 (0)1793 417 445

www.bcs.org

The Chartered Institute for IT