The Chartered Institute for IT

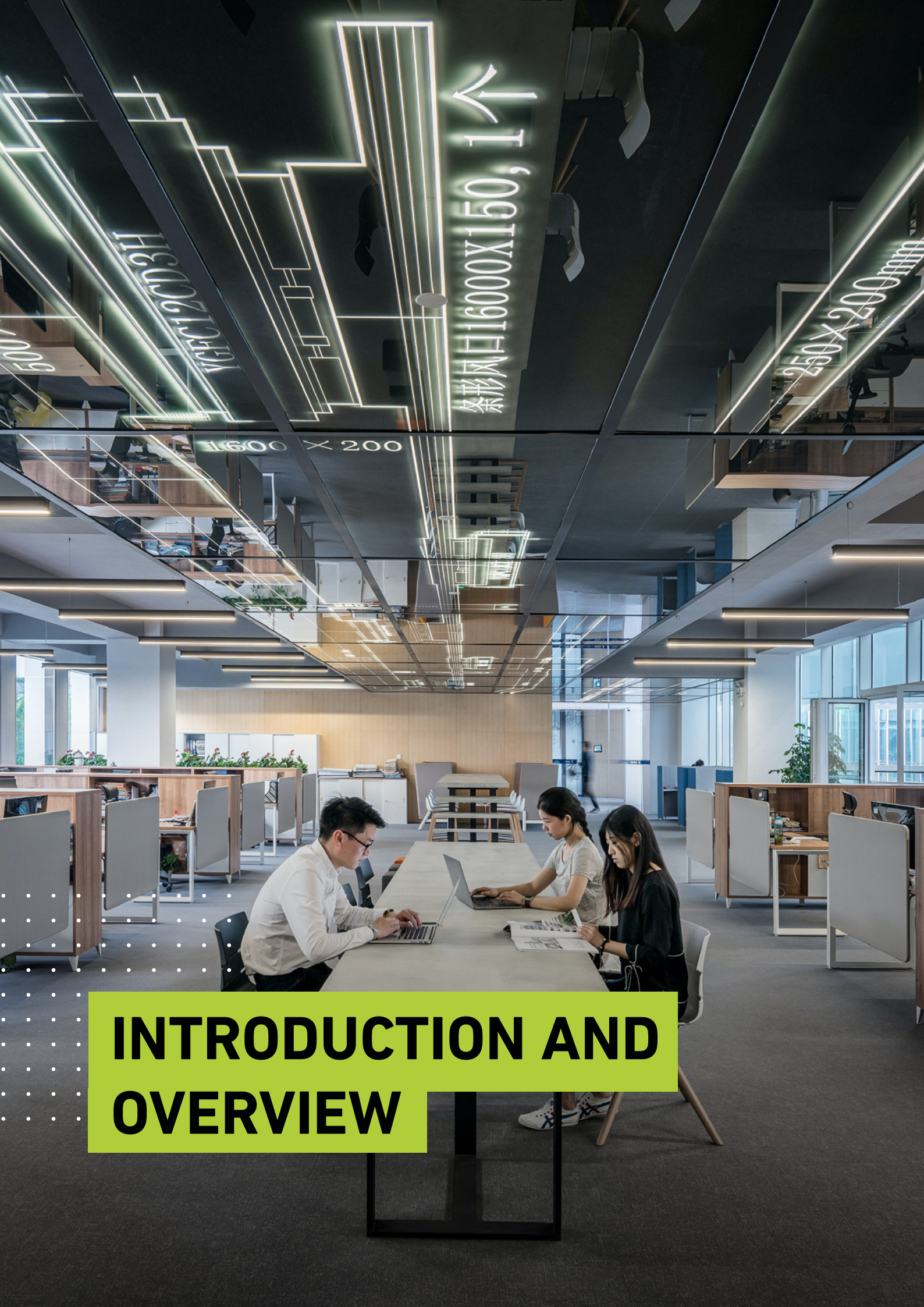
2023 | NOVEMBER V1.0

BCS PRACTITIONER AWARD IN CLOUD INFRASTRUCTURE ARCHITECTURE

SYLLABUS

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

CONTENTS



INTRODUCTION AND OVERVIEW

INTRODUCTION

Cloud infrastructure architecture defines the design and structure of an organisation's technological foundation. This includes hardware, software, networking, and cloud services. A cloud infrastructure architect is responsible for establishing a strategic framework to optimise IT sources, enhance performance, improve scalability, and mitigate security threats.

The Practitioner Award in Cloud Infrastructure Architecture will give candidates an in-depth understanding of the role of cloud infrastructure architecture, including the responsibilities and activities undertaken by a cloud infrastructure architect, its relation to other architectural domains, and the common tools, techniques, and frameworks that are used to create a robust IT infrastructure.

LEARNING OUTCOMES

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

- The role of cloud infrastructure architecture.
- The relationship of cloud infrastructure architecture to other domains.
- The activities undertaken by cloud infrastructure architects.
- Cloud infrastructure architecture: skills and knowledge.
- How cloud infrastructure architecture is governed.

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.

The qualification is suitable for candidates who are looking to progress their career within a cloud infrastructure role. It can be taken in combination with other practitioner awards and the Practitioner Certificate in Enterprise and Solutions 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 Cloud Infrastructure 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 cloud infrastructure architecture.

KSC08

The frameworks and principles on which networks, systems, equipment and resources are based both on premises and cloud-based.

KSC21

Knowledge of the IT/IS infrastructure and the IT applications and service processes used within own organisation, including those associated with sustainability and efficiency.

KSC22

Methods and techniques for structured reviews, including reviews of technical work products, test plans, business cases, architectures and any other key deliverables.

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.

KSC52

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

KSC42

Knowledge and understanding of infrastructure configurations.

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

SYLLABUS

1. THE ROLE OF CLOUD INFRASTRUCTURE ARCHITECTURE (15%) K4

1.1 Explain the role of cloud infrastructure architecture.

Indicative content

a. The definition of:
   - Cloud: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (NIST, 2011 cited in Morris, 2023)

   - Infrastructure architecture: "The architecture of the technology infrastructure of an organisation for enterprise that supports the delivery of business activities." (Mark Lovatt, 2021).

b. Characteristics of cloud computing:
   - Multi-tenancy
   - Resource pooling
   - Elasticity
   - Scalability

c. Cloud Secure Data Lifecycle (CSDL)

Guidance

The candidate should be able to explain the role of cloud infrastructure architecture and its relationship to an organisation. This includes understanding cloud-related definitions and roles based on ISO 1778 and 22123. The candidate should also be able to explain the key characteristics and principles that are unique to cloud infrastructure (e.g. the steps required in the CSDL).

1.2 Analyse how architectural frameworks and standards are used in specific scenarios.

Indicative content

a. Frameworks:
   - National Institute of Standards and Technology (NIST)
   - Information Technology Infrastructure Library (ITIL)
   - TOGAF
   - SANS Institute
   - Center for Internet Security (CIS)

b. Standards:
   - ISO 27001
   - ISO 27017
   - ISO 17789

Guidance

The candidate should be able to analyse various situations related to cloud infrastructure architecture and be able to apply 'Best Practices' with a strong emphasis on the security issues facing cloud deployments. The candidate should be able to identify relevant IT architectural frameworks, security standards, and how they are applied in the design, management, and control of a cloud deployment.

2. CLOUD INFRASTRUCTURE ARCHITECTURE IN RELATION TO OTHER DOMAINS (10%) K4

2.1 Analyse how cloud infrastructure architecture interacts with other domains.

Indicative content

a. Domains:
- Enterprise
- Business
- Data
- Application / Solution
- Technology
- Security

Guidance

The candidate should be able to analyse specific scenarios and identify how the cloud infrastructure architecture influences other domains. For example, the candidate should be able to identify and explain how certain capabilities and limitations of cloud infrastructure impact how data is handled in an organisation.

2.2 Describe key artefacts used by cloud infrastructure architects.

Indicative content

a. Artefacts:
- Infrastructure diagrams
- Network topology diagrams
- Deployment models and flowcharts
- Capacity planning and performance models (component, service, business)

Guidance

Candidates should be able to describe key artefacts used within cloud infrastructure architecture. This includes explaining the purpose of each artefact and how they contribute towards an organisation's IT architecture.

3. SKILLS AND KNOWLEDGE (30%) K4

3.1 Analyse the implementation of cloud environments and components.

Indicative content

a. Physical components:
- Virtualisation
- Hypervisors
- Networking (LAN/WAN technologies: Layer 2, Layer 3, VNets, VCLAN, NVGRE)

b. Approaches to cloud implementation:
- Virtual machines and containers
- Cloud native, "lift and shift", refactoring
- Cloud services (e.g. Azure, AWS, GCP)
- Private, public, hybrid

Guidance

Candidates should be able to explain and analyse the use of different components and approaches used in cloud infrastructure. This includes the ability to evaluate the advantages and disadvantages of various aspects of cloud environments and having an understanding of the differences between traditional security practices in a standard data centre system and those required for a cloud environment (e.g. the loss of direct control of the physical environment).

3.2 Evaluate the use of different storage options in specific scenarios.

Indicative content

a. Types of storage:
- Infrastructure as a Service (IaaS): volume and object
- Platform as a Service (PaaS): structured and unstructured
- Software as a Service (SaaS)
- Hosted object storage service
- File storage
- Block storage

Guidance

The candidate should have an understanding of different types of storage (e.g. Azure Archive, Amazon Glacier, GCP Cloud Storage) and how the storage requirements differ for cloud-based infrastructure. This includes the ability to analyse specific scenarios and identify and recommend the most appropriate approach to managing data.

3.3 Identify the use of the Shared Resource and Responsibility Model in specific scenarios.

Indicative content

a. Cloud service provider responsibilities
b. Customer responsibilities

Guidance

The candidate should be able to identify the principles of the Shared Resource and Responsibility Model required by public and private cloud implementations. They should have knowledge of references such as Open Alliance for Cloud Adoption (OACA), and vendor-specific models such as AWS, Azure, Google.

3.4 Explain security concepts related to cloud computing.

Indicative content

a. Data
b. Communications (checksums, hashes, digital signing)
c. Cryptography

Guidance

The candidate should be able to explain the importance of identity and access management (IAM), Data Loss Prevention (DLP), Security Information and Event Management (SIEM) and Business Continuity. They should also have an understanding of the core aspects of information security governance including ISO 27001, risk mitigation, and control implementation such as SOC2. The candidate should also be able to explain encryption standards and techniques in relation to cloud environments. This includes the understanding of Key Management and the challenges of using encryption in cloud environments (e.g. protecting short-lived data, long-term data, data at rest, and data in flight).

3.5 Explain the impact of emergent related technologies on cloud infrastructure.

Indicative content

a. Artificial Intelligence
b. Machine Learning
c. Internet of Things
d. Blockchain
e. Robotics
f. Augmented Reality

Guidance

The candidate should be cognisant of the impact of emerging and related technologies and the increasing role they play in cloud computing infrastructure.

4. THE ACTIVITIES UNDERTAKEN BY CLOUD INFRASTRUCTURE ARCHITECTS. (30%) K4

4.1 Analyse the use of design considerations and standards for private cloud operation.

Indicative content

a. Logical design (virtualisations, multi-latency, access control, application programming interface)
b. Physical design (location, buy or build)
c. Environment design: heating, ventilation and air conditioning, power, physical access (HVAC)

Guidance

The candidate should have an understanding of the unique design considerations pertaining to a private cloud data centre, such as the cloud model being offered, regulatory controls, jurisdictions, and target customer(s). They should also possess an understanding of the differences between public and private cloud data centres. Candidates will need to understand both logical and physical design, including environmental considerations such as cooling, power consumption and physical access to a facility.

4.2 Analyse the specific risks and appropriate strategies in specific scenarios.

Indicative content

a. Risk assessment and analysis

b. Virtualisation functions (e.g. NIST SP800-125A) and risks:
   - Compromise of neighbouring tenancies
   - Share infrastructure
   - Control plane (private, public, or community)
   - Hardware vulnerabilities (e.g. CPU)

c. Risk mitigation strategies:
   - Avoid, transfer, mitigate, accept
   - Role-Based Access Control (RBAC)
   - Security Information and Event Management (SIEM)
   - Minimum Viable Product (MVP)

Guidance

The candidate should have an understanding of risks associated with IT systems and applications, with an increased level of knowledge pertaining to the additional risks specific to cloud computing and hosting (e.g. increasing the attack surface areas, increasing the number of people with access, etc.).

4.3 Analyse the use of Business Continuity and Disaster Recovery (BCDR) in specific scenarios.

Indicative content

a. Business requirements and cloud environment.
b. Risks
c. BCDR strategy
d. Recovery objectives:
   - Recovery Point Objective (RPO)
   - Recovery Time Objective (RTO)
   - Recovery Service Level (RSL)

Guidance

The candidate should be able to identify BCDR processes in specific scenarios related to cloud environments. For example, an organisation that has primary computing and hosting capabilities in the cloud versus a system or application already cloud-hosted and has an additional cloud provider for BCDR support. They should also be able to explain how the tools provided by cloud implementation (such as on-demand elasticity) and DevOps can address these challenges. The candidate should also be able to identify BCDR continual process strategies in specific scenarios as well as the different strategies available to achieve effective business continuity and a disaster recovery stance (e.g. restore versus rebuild).

4.4 Analyse the use of auditing mechanisms in specific scenarios.

Indicative content

a. Sources of auditing mechanisms:
   - Internal security policy
   - Contractual requirements
   - Regulatory requirements
   - Industry standards
   - Organisational standards

b. Cloud compliance programs

c. Auditing techniques:
   - Log collection
   - Correlation
   - Threat analysis
   - Control identification
   - Continuous improvement

Guidance

The candidate should be able to identify various sources of auditing mechanisms and how they can be applied to measure effective security controls for a system or application. This includes identifying elements of cloud compliance programs and specific auditing techniques available to mitigate potential risks and threats. Candidates should have knowledge of a variety of cloud services, e.g. Azure, AWS, GCP.

5. GOVERNANCE (15%) K3

5.1 Understand and be able to explain governance concerns.

Indicative content

a. Legal frameworks
b. eDiscovery – ISO 27050
c. Forensics requirements
d. Laws pertaining to Personally Identifiable Information (PII), e.g. GDPR, UK DPA
e. Cloud auditing processes and best practices: Cloud Security Alliance (CSA), Cloud Control Matrix (CCM), Center for Digital Government (CDG)
f. Risk management in a cloud environment (e.g. RACI)
g. Outsourcing and overseeing cloud contracts

Guidance

The candidate should be able to show an understanding that IT environments, especially cloud, often cross jurisdictional lines and naturally generate complex issues centred around applicable laws and regulations both from policy and technology perspectives for data collection and discovery requirements.

'IF YOU DO NOT HAVE A HANDLE ON GOVERNANCE, RISK MANAGEMENT AND REGULATORY COMPLIANCE INTERNALLY, MOVING TO THE CLOUD WILL EXPOSE YOUR VULNERABILITY EXTERNALLY.'

BCS (2012), Cloud Computing

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

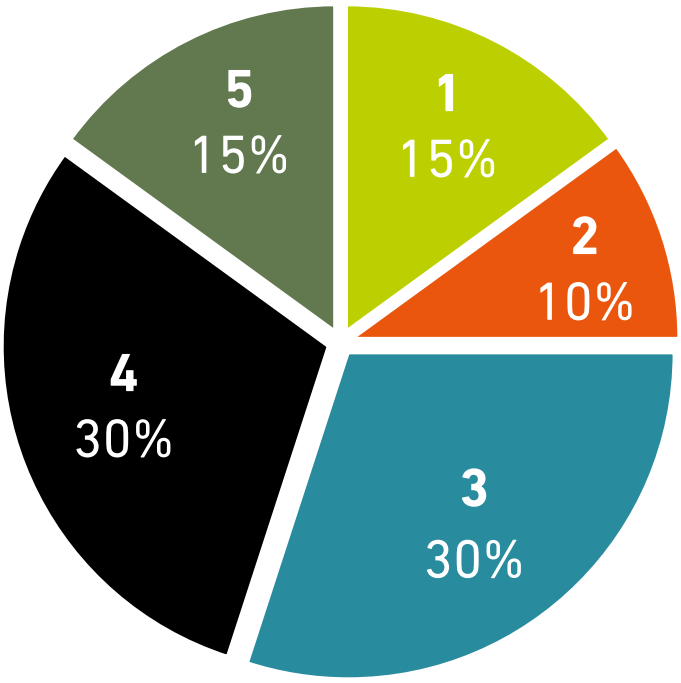
DELIVERY

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 Cloud Infrastructure Architecture
2	Cloud Infrastructure Architecture in Relation to Other Domains
3	Skills and Knowledge
4	The Activities Undertaken by Cloud Infrastructure Architects
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: Cloud Computing
AUTHOR: BCS (Editor)
PUBLISHER: Ingram Publisher Services UK - Academic
PUBLICATION DATE: *2012*
ISBN: *9781780171319*

TITLE: Moving to the Cloud
AUTHOR: Johnny Morris
PUBLISHER: BCS
PUBLICATION DATE: *2023*
ISBN: *9781780176260*

TITLE: The Evolution of Cloud Computing
AUTHOR: Clive Longbottom
PUBLISHER: Ingram Publisher Services UK - Academic
PUBLICATION DATE: *2017*
ISBN: *9781780173603*

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