BCS Practitioner Certificate in Business Continuity Management Syllabus

Version 4.5
April 2017

This qualification is not regulated by the following United Kingdom Regulators - Ofqual, Qualification in Wales, CCEA or SQA

BCS Practitioner Certificate in Business Continuity Management Syllabus

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 4.5 April 2017	Standardised new template format adopted, with revised ToC Addition of K levels
Version 4.4 December 2016	Strapline regarding regulated statement has been added
Version 4.3 March 2015	Updated language requirements for extra time and use of dictionaries. Standardised the trainer requirement
Version 4.2 October 2013	Updated trainer requirements to include trainer experience.
Version 4.1	Added new tutor requirement
Version 4.0 May 2013	Entire syllabus revised in the light of the release of ISO 22301:2012, which supersedes BS 25999-2:2012; and the publication of the Business Continuity Institute's Good Practice Guide 2013
Version 3.1 September 2012	Added in specific information about additional time and updated the trainer requirements. Included a section for excerpts from BCS books
Version 3.0 31 May 2012	Document control sheet updated. Reference to ISEB replaced with BCS throughout document. Learning hours added. No change to the content of the syllabus
Version 2.0 March 2011	Added in Classroom Size and Trainer Qualification Criteria. Introduced Knowledge and Skills and Learning Levels. Changed pass rate to 65% for Section A and B (was just Section 1). Minor amendments to Section 4.5 & 4.6 and Section 8.
Version 1.1 January 2010	Reformatted with the BCS branding.

Introduction

This certificate covers the range of concepts, approaches and techniques that are applicable to BCS Practitioner Certificate in Business Continuity Management Syllabus. Candidates are required to demonstrate their knowledge and understanding of these aspects of BCS Practitioner Certificate in Business Continuity Management Syllabus.

The certification contains a number of practical sessions, designed to build on the 'taught' components of the module, and to encourage debate and the sharing of knowledge and experience between candidates.

The certification promotes a hands-on approach to Business Continuity Management, making use of current standards, enabling candidates to make immediate use of the module on their return to their organisations.

Objectives

Candidates should be able to demonstrate knowledge and understanding of Business Continuity Management principles and techniques. Key areas are:

- The function of and the need for Business Continuity Management within an organisation
- The Business Continuity Management life cycle
- The main components of a Business Continuity Management programme
- The need for risk assessment within Business Continuity Management
- The options for development of a Business Continuity Management strategy
- How to prepare and develop plans for Business Continuity Management response
- The need for exercising, maintenance, and review of plans
- The need for embedding Business Continuity Management awareness within the organisation

The module includes a number of practical examples of Business Continuity Management techniques.

Target Audience

The certificate is relevant to anyone requiring an understanding of Business Continuity Management as well as those who are involved in the areas of information security and information assurance.

Course Format and Duration

Candidates can study for this certificate in two ways: by attending an accredited training course provided by Accredited Training Organisation or by self-study. An accredited training course will require a minimum of 36 hours of study run over a minimum of five days.

Eligibility for the Examination

There are no specific pre-requisites for entry to the examination; however, candidates should possess the appropriate level of knowledge to fulfil the objective shown above.

Format of the Examination

- Three hour scenario-based written 'closed book'
- Part A: 10 multiple-choice questions (1 mark each) – answer all questions.
- Part B: 6 Compulsory short narrative questions (5 marks each) – answer all questions.
- Part C: 3 Compulsory essay style questions. (20 marks each) – answer all questions
- Pass mark is 65/100 (65%)

Additional time

For candidates requiring reasonable adjustments

Please refer to the reasonable adjustments policy for detailed information on how and when to apply.

For candidates whose language is not the language of the examination

If the examination is taken in a language that is not the candidate's native/official language, candidates are entitled to:

- 25% extra time
- Use their own **paper** language dictionary (whose purpose is translation between the examination language and another national language) during the examination Electronic versions of dictionaries will **not** be allowed into the examination room

Guidelines for Accredited Training Organisations

Each major subject heading in this syllabus is assigned an allocated time. The purpose of this is two-fold: first, to give both guidance on the relative proportion of time to be allocated to each section of an accredited course and an approximate minimum time for the teaching of each section; second, to guide the proportion of questions in the exam. Accredited Training Organisations may spend more time than is indicated and candidates may spend more time again in reading and research. Courses do not have to follow the same order as the syllabus. Courses may be run as a single module or broken down into two or three smaller modules.

This syllabus is structured into sections relating to major subject headings and numbered with a single digit section number. Each section is allocated a minimum contact time for presentation.

Accredited Training Organisations may include additional exercises where they believe these add value to the training course.

The syllabus contains references to established standards. The use of referenced standards in the preparation of training material is mandatory. Each standard used must be the version quoted in the current version of this syllabus.

The latest version of the syllabus reflects the replacement of BS 25999-2:2007 by ISO 22301:2012 and of the publication of the latest Business Continuity Institute Good Practice Guidelines 2013.

For consistency, the original names of the syllabus modules have been retained, and the revised names from Good Practice Guide 2013 have been added in parentheses.

Use of Calculators

No calculators or mobile technology are acceptable.

Syllabus

For each top-level area of the syllabus a percentage and K level is identified. The percentage is the exam coverage of that area, and the K level identifies the maximum level of knowledge that may be examined for that area.

1.   Introduction to Business Continuity Management (K2, 2 hours)

This section of the module provides a basic introduction to the discipline of Business Continuity Management, describes how it should fit in with the overall strategy of a business, and provides a brief overview of risk management.

1.1   The need for Business Continuity Management
Candidates should be able to explain:

    1.1.1   When and why Business Continuity Management should be used
    1.1.2   How the organisation can make use of Business Continuity Management
    1.1.3   The need for a Business Continuity Management System (BCMS)
    1.1.4   The use of Business Continuity Management standards, (see section 8) or other relevant international standards

1.2   The context of Business Continuity Management in the business
Candidates should be able to explain:

    1.2.1   Why organisations should take account of Business Continuity Management
    1.2.2   The benefits of Business Continuity Management
    1.2.3   The consequences of no Business Continuity Management
    1.2.4   The potential impact of external and internal issues on the organisation
    1.2.5   The potential impact of legal and regulatory requirements

1.3   Leadership and senior management commitment to Business Continuity
Candidates should be able to describe the requirement for:

    1.3.1   Ensuring compatibility between the BCMS and the organisation's strategic direction
    1.3.2   Amalgamating the requirements of the BCMS into the organisation's business processes
    1.3.3   Communicating the importance of the effective Business Continuity Management to the wider audience

1.4   Review of risk management fundamentals
Candidates should be able to describe:

    1.4.1   The concept of threats and hazards
    1.4.2   The concept of vulnerabilities
    1.4.3   The concept of impact or consequences
    1.4.4   The concept of likelihood or probability

1.4.5   The basic principles of business impact analyses

   1.4.6   The basic principles of risk assessment

   1.4.7   The concepts of risk acceptance or tolerance, avoidance or termination, transfer or sharing and reduction or modification

1.5   The Business Continuity Institute's Lifecycle
Candidates should be able to describe the overall relevance of:

   1.5.1   Policy and Programme Management (PP1)

   1.5.2   Embedding Business Continuity (PP2)

   1.5.3   Analysis (PP3)

   1.5.4   Design (PP4)

   1.5.5   Implementation (PP5)

   1.5.6   Validation (PP6)

2.   Business Continuity Policy and Programme Management (K2, 3 hours)

This section of the module describes both the initial stages and the requirements for the on-going management of the Business Continuity Management programme.

2.1   Initial activities
Candidates should be able to describe the requirement for:

   2.1.1   Setting the Business Continuity policy

   2.1.2   Determining the Business Continuity programme objectives

   2.1.3   Determining the Business Continuity programme scope

   2.1.4   Defining governance

   2.1.5   Accountability for the overall Business Continuity programme

   2.1.6   Delegated responsibility for implementation of the individual components of the Business Continuity programme

   2.1.7   Defined roles and responsibilities within the Business Continuity programme

2.2   Implementing the Business Continuity Programme
Candidates should be able to describe the requirement for:

   2.2.1   A properly defined set of Business Continuity Management objectives

   2.2.2   Actions to address risks identified within the Business Continuity Management programme

   2.2.3   Determining the resource requirements for the Business Continuity Management programme

   2.2.4   Determining the competence of people involved in executing the Business Continuity Management programme, the requirement for their training, and the types of training which may be required

   2.2.5   A formal system of operation and control of the Business Continuity Management programme

   2.2.6   Communication of the Business Continuity Management programme to stakeholders

   2.2.7   The review, testing and exercising of Business Continuity capability

2.2.8 Formal reporting of the Business Continuity Management programme status and capability

2.3 Supply Chain Continuity
Candidates should be able to explain:

2.3.1 The need for establishing the Business Continuity capability of key suppliers
2.3.2 How key suppliers can contribute to the organisation's Business Continuity capability
2.3.3 How the information gained from the Business Continuity programme can assist the work of insurance loss adjusters
2.3.4 How evidence must be preserved, collected and used in cases where criminal damage has caused a business interruption
2.3.5 How outsourced activities must be considered within the Business Continuity Management programme

2.4 Documentation
Candidates should be able to explain the requirements for the proper documentation of:

2.4.1 An agreed Business Continuity Management policy
2.4.2 Terms of reference for the Business Continuity Management programme
2.4.3 Business impact analysis
2.4.4 Risk assessments
2.4.5 Business Continuity strategies
2.4.6 A Business Continuity training and awareness programme
2.4.7 Incident management, Business Continuity, disaster recovery and business resumption plans
2.4.8 A Business Continuity testing and exercise schedule
2.4.9 Business Continuity service level agreements and contracts
2.4.10 Secure off-site/dual site storage of vital information and materials

3. Understanding the Organisation (Analysis) (K4, 10 hours)

This section of the module describes how the Business Continuity manager sets about understanding the organisation and initiates the overall Business Continuity Management programme.

3.1 Identification of Business-Critical Areas
Candidates should be able to explain the approach for identifying mission-critical areas of the business by:

3.1.1 Department, e.g. Sales and Marketing, Finance, Production, Human Resources
3.1.2 Product or service, e.g. mainstream versus legacy products
3.1.3 Support capability, e.g. supply chain, energy, distribution

3.2 Terminology
Candidates should be able to understand the concepts of:

3.2.1 Maximum Tolerable Period of Disruption (MTPD), also known as Maximum Acceptable Outage (MAO)
3.2.2 Recovery Time Objective (RTO)
3.2.3 Maximum Tolerable Data Loss (MTDL)
3.2.4 Recovery Point Objective (RPO)
3.2.5 Minimum Business Continuity Objective (MBCO)

3.3 Business Impact Analysis
Candidates should be able to explain the process for arriving at a Business Impact Analysis in terms of:

3.3.1 Financial impacts, e.g. revenue streams, cashflow, litigation
3.3.2 Non-financial loss, e.g. brand, share value, customer confidence
3.3.3 Other impacts, e.g. legal and regulatory

3.4 Continuity Requirements Analysis
Candidates should be able to explain how a Business Continuity plan must take into account:

3.4.1 Staff
3.4.2 Premises
3.4.3 Supporting technology
3.4.4 Information
3.4.5 External services and supplies

3.5 Threat and Vulnerability Assessments
Candidates should be able to describe the process for assessing threats, hazards, and vulnerabilities, including environmental, people, premises, process, supply chain, fire, natural hazards, deliberate and accidental releases of toxic chemicals:

3.5.1 Identifying threats, hazards and vulnerabilities
3.5.2 Analysing threats, hazards and vulnerabilities
3.5.3 Evaluating threats, hazards and vulnerabilities

3.6 Horizon Scanning
Candidates should be able to explain the advantages of horizon scanning to identify early warnings of potential:

3.6.1 Threats, e.g. virus and denial of service attacks, disaffected staff
3.6.2 Hazards, e.g. severe weather, pandemics

3.7 Risk Assessment
Candidates should be able to explain the process of risk assessment:

3.7.1 Likelihood or probability

      3.7.2   Levels of impact
      3.7.3   Quantitative risk assessments
      3.7.4   Qualitative risk assessments
      3.7.5   Proximity of risk
      3.7.6   Single points of failure in premises, systems and people
      3.7.7   Risk matrices

3.8   Evaluation of Options
     Candidates should be able to explain how each risk can be categorised in terms of:

      3.8.1   Acceptance or tolerance
      3.8.2   Avoidance or termination
      3.8.3   Transfer or sharing
      3.8.4   Reduction or modification
      3.8.5   Describe the need for a cost/benefit analysis where the costs of controls are similar to the potential losses

3.9   Business Cases and Programme Sign-Off
     Candidates should be able to describe the key components of a business case:

      3.9.1   Management summary
      3.9.2   Impact statement (business impact analysis)
      3.9.3   Risk assessment
      3.9.4   Options and recommendations
      3.9.5   Supporting material, including costs and timescales
      3.9.6   Formal presentation of a business case and the need for approval and sign-off by senior management

4.   **Determining the Business Continuity Strategy (Design) (K4, 8 hours)**

This section of the module describes how the organisation develops an overall Business Continuity strategy.

4.1   Strategic Options
     Candidates should be able to outline:

      4.1.1   The strategic option to avoid or terminate a risk
      4.1.2   The strategic option to share or transfer a risk
      4.1.3   The strategic option to reduce or modify a risk
      4.1.4   The strategic option to accept or tolerate a risk
      4.1.5   The concept of costs versus benefits in the implementation of Business Continuity strategies
      4.1.6   The possible consequences of inaction on business impact analysis
      4.1.7   The advantages of emergency packs
      4.1.8   The need for accurate inventories of assets

4.1.9 The need to take local, regional, national and industry sector legislation into account

4.2 People
Candidates should be able to explain:

4.2.1 The benefits of multi-skill training of both permanent and contract staff
4.2.2 The benefits of the physical separation of staff with core skills
4.2.3 The advantages (and disadvantages) of using third party staff
4.2.4 The need for succession planning
4.2.5 The need for knowledge retention and management
4.2.6 Types of team, including response, recovery, public relations, welfare
4.2.7 The need for staff welfare arrangements during and following an incident, including stress and trauma counselling

4.3 Premises
Candidates should be able to explain:

4.3.1 The benefits of using alternative premises owned by the organisation and those of other organisations and third-parties
4.3.2 The benefits of home or teleworking and those of working from remote premises
4.3.3 The benefits of moving workload to existing alternative premises

4.4 Processes and Procedures
Candidates should be able to explain:

4.4.1 The need to document and store the way in which mission-critical processes and procedures are carried out
4.4.2 Understanding the legal implications, including consequential loss, legal action and third party losses

4.5 Technology
Candidates should be able to explain:

4.5.1 How the geographical separation of technology solutions improves resilience
4.5.2 How previously-used equipment can be retained for disaster recovery purposes
4.5.3 How lead times must be taken into account in planning technology recovery
4.5.4 The impact of distance between main and standby premises
4.5.5 Remote access considerations
4.5.6 The use of "hot", "warm" and "cold" sites, both manned and unmanned or dark sites
4.5.7 The need for careful provisioning of telecommunications facilities
4.5.8 The differences between resilience, redundancy and separacy
4.5.9 The various mechanisms for achieving failover to standby premises
4.5.10 The importance of considering connectivity to third parties
4.5.11 Links with information security strategies

4.6 Information
Candidates should be able to review the need for and importance of:

4.6.1 Confidentiality
4.6.2 Integrity
4.6.3 Availability
4.6.4 Authentication
4.6.5 Non-repudiation
4.6.6 Describe the concept of currency of information
4.6.7 Describe the various methods of information storage
4.6.8 Explain the need for efficient backup, off-site storage and retrieval of information, bearing in mind the RTO and RPO

4.7 Supply Chain
Candidates should be able to discuss:

4.7.1 The advantages of storing supplies and materials at alternative locations
4.7.2 The benefits of supplier arrangements which allow short-notice ordering and delivery and the service level agreements which underpin these
4.7.3 The diversion of just-in-time deliveries to alternative locations
4.7.4 The transfer of operations to those locations having supplies and materials
4.7.5 Identification of potential alternative suppliers and materials
4.7.6 The advantages of sourcing suppliers and materials from multiple suppliers
4.7.7 Ensuring that key suppliers have appropriate levels of Business Continuity themselves

4.8 Stakeholders
Candidates should be able to explain the requirement to take into consideration the relationship with key stakeholders:

4.8.1 Parent organisations
4.8.2 Shareholders
4.8.3 Customers
4.8.4 Suppliers and outsourced organisations
4.8.5 Business partners
4.8.6 Contractors
4.8.7 Industry regulators (where applicable)

4.9 Civil Emergencies
Candidates should be able to explain:

4.9.1 The need for an awareness of civil contingency requirements
4.9.2 The possible need for the production, maintenance and testing of on-site or off-site emergency plans
4.9.3 The need for warning and informing staff about civil emergencies which might affect them
4.9.4 The need for an awareness of the ongoing recovery arrangements following a civil emergency

4.9.5 The integration and inter-dependency of organisational plans and those of other emergency responders

5. Business Continuity Response (Implementation) (K3, 6 hours)

This section of the module describes how the organisation develops and implements the Business Continuity response.

5.1 Overall Incident Response Structure
Candidates should be able to describe how the organisation should develop a formal incident response structure, which will permit the organisation to:

5.1.1 Confirm the nature and extent of the incident
5.1.2 Take control of the situation and determine the most appropriate response
5.1.3 Contain and manage the incident
5.1.4 Communicate with internal and external stakeholders

5.2 Types of Plan
Candidates should be able to describe the various types of plan, including:

5.2.1 Incident response and management plans
5.2.2 Business Continuity plans, including technical and business plans and individual employee instructions
5.2.3 Disaster recovery plans
5.2.4 Business resumption plans
5.2.5 The generic content of plans, e.g. purpose and scope; roles and responsibilities; invocation process; contact details; plan version history, revision date and ownership; references
5.2.6 Involvement of key departments of the organisation in verifying the suitability of plans
5.2.7 Links and inter-dependencies between departmental and organisational plans
5.2.8 The involvement of third parties in disaster recovery and Business Continuity plans
5.2.9 The use of service level and contingency agreements to activate disaster recovery and Business Continuity plans
5.2.10 The advantages of disaster recovery companies and their services
5.2.11 The need for off-site storage of plans, including multiple media types
5.2.12 The advantages of a pre-equipped emergency operations centre
5.2.13 Planning for renewal of staff resources during incident response and the effects of stress on individual members of response teams
5.2.14 Planning for escalation of issues requiring senior management decisions
5.2.15 The need to consider different durations of disruption

5.3 Incident Management Plans
Candidates should be able to describe the contents of an incident management plan over and above those found in 5.2.5:

5.3.1 Task and action lists

5.3.2 Emergency contact details; details of the incident management location

5.3.3 Activities, including people, process and technology

5.3.4 Communications, including internal, media, emergency responders, voluntary services and stakeholders

5.3.5 Annexes, including photographs, maps and charts; third party response documentation; site access information; insurance claim procedures

5.4 Business Continuity Plans

Candidates should be able to describe the contents of a Business Continuity plan over and above those found in 5.2.5:

5.4.1 Task and action lists, including invocation procedures; locations of key people and resources; procedures for disaster recovery and alternative working

5.4.2 Resource requirements, including people, premises, processes and procedures, technology, information, supply chain and stakeholders

5.4.3 Person(s) responsible for the management of the response and recovery operations

5.4.4 Checklists, forms and annexes, including activity log form

5.5 Disaster Recovery Plans

Candidates should be able to describe the contents of a disaster recovery plan over and above those found in 5.2.5:

5.5.1 Task and action lists

5.5.2 Emergency contact details; details of the incident management location

5.5.3 Activities, including people, process and technology

5.5.4 Communications, including internal and stakeholders

5.5.5 Annexes, including details of third party contacts and invocation procedures, site access information

5.6 Business Resumption Plans

Candidates should be able to describe the contents of a business resumption plan over and above those found in 5.2.5:

5.6.1 Task and action lists

5.6.2 Ownership and management of the business resumption process

5.6.3 High-level options for longer-term replacement of key staff, premises, systems, services, equipment and machinery

5.6.4 Salvage and recovery of assets from premises affected by an incident

5.6.5 Insurance claims for assets lost or destroyed by an incident

5.6.6 Communications, including internal and stakeholders

5.6.7 The subsequent impact of an incident on cashflow, staff, customers, insurance premiums

6. Exercising, maintenance and review (Validation) (K2, 4 hours)

This section of the module describes the overall Business Continuity exercising, maintenance and review programme.

6.1 Exercising and Testing of Plans
Candidates should be able to explain the concept of Business Continuity exercising, maintenance and review:

6.1.1 Types of test and exercise, including communications, documentation walk-through; table-top simulation; partial test; full failover test; building evacuation/redeployment test
6.1.2 Developing an exercise programme
6.1.3 Developing an exercise
6.1.4 Post-exercise reviews and audit
6.1.5 Programme of remedial work to implement improvements raised by a post-exercise review or audit
6.1.6 Training and education programme for staff already involved in the Business Continuity programme and for new staff who will be involved
6.1.7 The need to decide when to test or exercise plans – during normal working hours, out of normal working hours, tests and exercises which overlap two or more changes of staff (e.g. shift changes)
6.1.8 The need for change control of plans

6.2 Maintenance of Plans
Candidates should be able to explain the need for and frequency of regular updates to the plans for:

6.2.1 Names of key individuals
6.2.2 Contact details
6.2.3 Photographs, maps and charts
6.2.4 Third party response documentation
6.2.5 Site access information
6.2.6 Insurance claim procedures
6.2.7 Communication procedures
6.2.8 Links into the organisation's change management process

6.3 Review of Plans
Candidates should be able to explain the need for and frequency of regular reviews of:

6.3.1 Mission-critical activities
6.3.2 Impact analyses
6.3.3 Vulnerabilities
6.3.4 Threats and hazards
6.3.5 The overall Business Continuity strategy
6.3.6 The organisation's risk appetite
6.3.7 The organisation's Business Continuity capability

6.3.8 The degree to which Business Continuity solutions remain appropriate

6.3.9 The progress of testing, exercising and training

6.3.10 Independent audit of Business Continuity plans

7. Embedding Business Continuity Awareness in the Organisation (K3, 3 hours)

This section of the module describes how Business Continuity awareness should be embedded into the organisation.

7.1 Overall Awareness
Candidates should be able to describe how Business Continuity awareness can be achieved through:

7.1.1 Consultation with key departments within the organisation

7.1.2 Aligning awareness to the organisation's culture

7.1.3 Articles on Business Continuity within the organisation's newsletters, briefings, intranet pages and through the organisation's induction programme

7.1.4 Business Continuity Management workshops, which examine lessons learnt from real-life internal and external incidents

7.1.5 Inclusion in team meeting and project meeting agenda

7.1.6 Involvement of deputising staff in tests and exercises

7.1.7 Structured advice to all staff on what to do or where to report in the event of an incident

7.1.8 Establishing and maintaining an awareness campaign

7.2 Skills Training
Candidates should be able to explain the need for and benefits of training of key staff for:

7.2.1 Business Continuity programme management

7.2.2 Business impact analyses and risk assessments

7.2.3 Developing and implementing Business Continuity plans

7.2.4 Taking part in and/or running Business Continuity tests and exercises

7.2.5 Communications with the media

7.2.6 Establishing a training programme

Glossary of Terms and Definitions

Refer to Glossary of Terms from:

8.1.1 BS 25999-1:2006 – Business Continuity Management – Code of practice

8.1.2 ISO 22300:2012 – Societal security – Terminology

8.1.3 ISO Guide 73:2009 – Risk management – Vocabulary – Guidelines for use in standards

8.1.4 ISO 19011:2011 – Guidelines for auditing management systems

References

8.2.1 ISO/IEC 20000-:2011 Service management system requirements

8.2.2 ISO/IEC 20000-2:2012 Guidance on the application of service management systems

8.2.3 ISO/IEC 27000:2009 - Information technology - Security techniques - Information security management systems - Fundamentals and vocabulary

8.2.4 ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

8.2.5 ISO 22301:2012 – Societal security – Business Continuity Management systems – Requirements.

8.2.6 BS 25999-1:2006 Business continuity management – Code of practice

8.2.7 The Business Continuity Institute Good Practice Guidelines 2013.

Levels of Knowledge / SFIA Levels

This course will provide candidates with the levels of difficulty / knowledge skill highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated.

The levels of knowledge and SFIA levels are explained in on the website www.bcs.org/levels.

The levels of knowledge above will enable candidates to develop the following levels of skill to be able to operate at the following levels of responsibility (as defined within the SFIA framework) within their workplace:

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

Format of Examination

Type	10 multiple choice questions, 6 short answer questions and 3 essay style questions (all compulsory)
Duration	3 Hours. An additional 45 minutes will be allowed for candidates sitting the examination in a language that is not their native /mother tongue.
Pre-requisites	Accredited training is strongly recommended but is not a pre-requisite
Supervised	Yes
Open Book	No
Pass Mark	65/100 (65%)
Calculators	Calculators cannot be used during this examination.
Learning Hours	36 Hours
Delivery	Paper based examination

Trainer Criteria

Criteria	- Hold the BCS Practitioner Certificate in Business Continuity Management - Have 10 days' training experience or have a train the trainer qualification - Have a minimum of 3 years' practical experience in the subject area

Classroom Size

Trainer to candidate ratio	1:16