Making IT good for society

BCS Level 4 Award in Business Processes Syllabus 603/3215/3

Version 1.0
April 2018

This is a United Kingdom government regulated qualification which is administered and approved by one or more of the following: Ofqual, Qualification in Wales, CCEA or SQA.

Making IT good for society

BCS Level 4 Award in Business Processes

Contents

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
V1.0	Document created.

Introduction

This award is the fourth module of five knowledge modules that are applicable to the level 4 Cyber Intrusion Analyst apprenticeship. This is a general introduction to business processes specific to cyber security, for which apprentices are required to demonstrate their knowledge and understanding.

Objectives

Apprentices should be able to demonstrate an understanding of business processes. Key areas are:

1. Understands lifecycle and service management practices to Information Technology Infrastructure Library (ITIL) foundation level.
2. Capable of advising others on cyber incident response processes, incident management processes and evidence collection / preservation requirements to support incident investigation.

Evidence of lessons learnt in these key areas should be collected and reflected upon when the apprentice is compiling the summative portfolio as the apprentice could identify how the task might be done better / differently with knowledge subsequently gained.

Target Audience

This award is relevant to anyone enrolled on the Level 4 Cyber Intrusion Analyst Apprenticeship programme.

Course Format and Duration

Apprentices can study for this award by attending a training course provided by a BCS accredited Training Provider. The estimated total qualification time for this award is 81 hours.

Eligibility for the Examination

Individual employers will set the selection criteria, but this is likely to include 5 GCSEs (especially English, mathematics and a science or technology subject); other relevant qualifications and experience; or an aptitude test with a focus on IT skills.
Level 2 English and Maths will need to be achieved, if not already, prior to taking the endpoint assessment.

Duration and Format of the Examination

The format for the examination is a one-hour multiple-choice examination consisting of 40 questions. The examination is closed book (no materials can be taken into the examination room). The pass mark is 26/40 (65%).

Additional Time for Apprentices Requiring Reasonable Adjustments Due to a Disability

Apprentices may request additional time if they require reasonable adjustments. Please refer to the Access to Assessment policy for detailed information on how and when to apply.

Additional Time for Apprentices Whose Language Is Not the Language of the Exam

If the examination is taken in a language that is not the apprentice's native / official language, then they are entitled to 25% extra time.

If the examination is taken in a language that is not the apprentice's native / official language, then they are entitled to 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 Training Providers

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. Training providers may spend more time than is indicated and apprentices 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. Apprentices should be encouraged to consider their summative portfolio throughout the modules.

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 Lifecycle and Service Management Practices (25%, K2)

In this topic area, the apprentice will describe and explain the lifecycle and service management practices to Information Technology Infrastructure Library (ITIL). The successful apprentice should be able to:

1.1 Describe the processes and roles within ITIL that are applicable to a cyber intrusion analyst and describe how they fit into their working practices and environment.
- service strategy;
- service design;
- service transition;
- service operation;
- continuous service development.

2 Incident and Management Processes (75%, K2)

In this topic area, the apprentice will describe and explain the different processes for cyber incident response and incident management, as well as how to evidence collection / preservation requirements to support incident investigation. The successful apprentice should be able to:

2.1 Describe what a cyber incident response is, its purpose and how it fits into the corporate or business environment.
- what the incidence response policies and processes are that are relevant to the cyber intrusion analyst's working environment and role;
  - Police and Criminal evidence act 1984 (PACE);
  - GDPR;
  - Computer Misuse Act 1990;
  - Regulation of Investigatory Powers 2000 (RIPA).
- who to interface with during an incident response process and who to contact;
  - people;
  - process;
  - technology;
  - information.

2.2 Describe the cyber incident management processes.

- preparation of an organisation;
  - criticality assessment;
  - complete a cyber security threat analysis;
  - consider the implications of people, process, technology and information;
  - create an appropriate control framework;
  - testing the state of readiness;
- response;
  - identification of security incident;
  - defining objectives and investigate the incident;
  - take appropriate action;
  - recovery of systems, data and connectivity;
- follow-up activities;
  - complete a thorough investigation of the incident;
  - report the incident and findings to relevant stakeholders;
  - complete and record a post incident review;
  - communicate lessons learnt;
  - update key information, controls and processes;
  - complete a trend analysis.

2.3 Explain how the procedure for the collection / preservation of evidence is required to support incident investigation.

- how to collect and handle data to be provided to an investigation;
  - admissibility of evidence – whether or not the evidence can be used;
  - weight of evidence – the quality and completeness of evidence;
- how to meet requirements for evidence preservation in accordance with policies and processes relevant to the cyber intrusion analyst's working environment and role;
  - compliance with Association of Chief Police Officers Guidelines on Computer Evidence (ACPO), and the National Police Chiefs' Council;
  - maintain an action log that should include:
    - identifying information (location, serial number, model number, hostname, Media Access Control addresses, and IP addresses of a hardware);
    - title, name and contact details of every individual involved in collecting or handling the evidence during the investigation;
    - date and time of each handling occurrence;
    - locations where the evidence was stored.

Levels of Knowledge / SFIA Levels

This syllabus will provide apprentices 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 on the website www.bcs.org/levels. The levels of knowledge above will enable apprentices 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

Question Weighting

Syllabus Area	Target Number of Questions
1. Lifecycle and Service Management Practices	10
2. Incident and Management Processes	30
Total	**40 Questions**

Format of Examination

Type	40 Question Multiple Choice.
Duration	1 hour. An additional 15 minutes will be allowed for apprentices sitting the examination in a language that is not their native / mother tongue.
Pre-requisites	Training from a BCS accredited training provider is strongly recommended but is not a pre-requisite.
Supervised	Yes.
Open Book	No.
Pass Mark	26/40 (65%).
Calculators	Calculators cannot be used during this examination.
Total Qualification Time (TQT)	81 Hours, 53 GLH recommended.
Delivery	Online.

Trainer Criteria

Criteria	▪ 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 apprentice ratio	1:16