Making IT
good for
society

# BCS Level 4 Award in Operating Systems (Cyber Intrusion Analyst) Syllabus
# 603/2894/0

## Version 1.2
## February 2019

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.

# BCS Level 4 Award in Operating Systems (Cyber Intrusion Analyst)

## 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. |
| V1.1 | Title and contents pages updated with certification |
| V1.2 | Minor correction to number of questions in exam. |
| | |
| | |

# Introduction

This award is the second module of five knowledge modules that are applicable to the level 4 Cyber Intrusion Analyst apprenticeship. It covers the range of concepts, approaches and techniques that are applicable to operating systems, for which apprentices are required to demonstrate their knowledge and understanding.

# Objectives

Apprentices should be able to demonstrate an understanding and utilise three different operating systems. Key areas are:

1. Knows how to configure an OS firewall with rationale
2. Knows how to configure user / file access control list, user groups with rationale
3. Knows how to enable / disable OS services for security reasons with rationale
4. Knows how to implement a patching policy
5. Knows how to configure OS security policies with rationale
6. Able to contrast the security features in 2 different OS (e.g. Linux, Windows, iOS)
7. Able to contrast the security features implemented in server and client

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 68.5 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 60-minute 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 reasonable adjustments 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 Configuring an Operating System's Firewall (37.5%, K2)

In this topic area, the apprentice will describe and explain the common configurations of operating system's (OS) firewalls. The successful apprentice should be able to:

1.1 Explain how to configure an OS firewall.

- OS Linux;
- IOS;
- Windows.

1.2 Explain the rational for configuring an OS firewall.

- OS Linux;
- IOS;
- Windows.

1.3 Describe how to enable / disable OS services for security reasons.

- OS Linux;
- IOS;
- Windows.

1.4 Explain the rationale for enabling / disabling OS services for security reasons.

- OS Linux;
- IOS;
- Windows.

## 2 Configuring User Groups and Access Control Lists (25%, K2)

In this topic area, the apprentice will be able to explain the differences between user and file access control lists and how to configure them. The successful apprentice should be able to:

2.1 Describe how to configure user / file access control list.

- Active Directory;
- Group Policy;
- Share Permissions;
- local NTFS files and folders;
- registry;
- printers.

2.2 Explain how to add and remove domain users and groups.

2.3 Explain the rationale for adding and removing domain users and groups.

## 3 Security Features (20%, K2)

In this topic area, the apprentice will explain the security features of OS, servers and clients. The successful apprentice should be able to:

3.1 Compare and contrast the security features in the following operating systems:

- Linux;
  - user accounts;
  - file and directory permissions;
  - data verification;
  - secure remote access with OpenSSH;
  - system recovery;
  - resource allocation controls;
  - monitoring and audit facilities;
  - firewall;
  - NFS;
- Windows;
  - Windows Defender;
  - Device Guard;
  - Windows Hello;
  - Secure Boot;
  - Widows Passport;
  - firewall;
  - Network Access Policy (NAP);
  - DirectAccess;
  - App Locker;
  - Data Execution Prevention (DEP);
  - address space layout randomisation (ASLR);
  - Structured Exception Handler Overwrite Protection (SEHOP);
  - User Account Control (UAC);
  - DNS Security Extensions (DNSSEC);
- iOS;
  - system security;
  - network security;
  - encryption and data protection;
  - internet services;
  - privacy controls.

3.2 Describe the security features implemented in a server and client.

- server;
  - password authentication;
  - firewalls;
  - auditing and accounting;
  - resource sharing;
  - public key infrastructure and SSL / TLS encryption;
- client;
  - protection;
  - control;
  - reporting.

## 4 Policies (17.5%, K2)

In this topic area, the apprentice will show an understanding of the need for OS security policies and how to implement a patching policy. The successful apprentice should be able to:

4.1 Describe how to implement a patching policy.

- detect;
- assess;
- acquire;
- test;
- deploy;
- maintain.

4.2 Explain the rational and describe how to configure OS security policies for the following:

- audit policy settings;
- remote desktop service;
- system services;
- patch management settings;
- firewall.

## 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. Configuring an Operating System’s Firewall | 15 |
| 2. Configuring User Groups and Access Control Lists | 10 |
| 3. Security Features | 8 |
| 4. Policies | 7 |
| **Total** | **40 Questions** |

## Format of Examination

| | |
|---|---|
| Type | 40 Question Multiple Choice. |
| Duration | 60 minutes. An additional 25% 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) | 68.5 Hours, 37.5 GLH recommended. |
| Delivery | Online. |

## Trainer Criteria

| | |
|---|---|
| Criteria | ▪ Have 10 days' training experience or have a Train the Trainer qualification.<br>▪ Have a minimum of 3 years' practical experience in the subject area. |

## Classroom Size

| | |
|---|---|
| Trainer to apprentice ratio | 1:16 |