# Qualification Specification for:

## OCN NI Level 4 Certificate in Cyber Security

➢ **Qualification No: 610/0201/X**

# Qualification Regulation Information

**OCN NI Level 4 Certificate in Cyber Security**
Qualification Number: **610/0201/X**

Operational start date: 01 December 2021
Operational end date: 30 November 2026
Certification end date: 30 November 2030

Qualification operational start and end dates indicate the lifecycle of a regulated qualification. The operational end date is the last date by which learners can be registered on a qualification. The certification end date is the last date by which learners have to complete the qualification and claim their certificate.

All OCN NI regulated qualifications are published to the Register of Regulated Qualifications ( **http://register.ofqual.gov.uk/** ). This site shows the qualifications and awarding organisations regulated by CCEA Regulation and Ofqual.

**OCN NI Contact Details**

Open College Network Northern Ireland (OCN NI)
Sirius House
10 Heron Road
Belfast
BT3 9LE

Phone: 028 90463990
Web: **www.ocnni.org.uk**

# Foreword

This document explains OCN NI's requirements for the delivery and assessment of the following regulated qualification:

→ **OCN NI Level 4 Certificate in Cyber Security**

This specification sets out:

- Qualification features
- Centre requirements for delivering and assessing the qualifications
- The structure and content of the qualifications
- Unit Details
- Assessment requirements for the qualification
- OCN NI's quality assurance arrangements for the qualifications
- Administration

OCN NI will notify centres in writing of any major changes to this specification. We will also publish changes on our website at **www.ocnni.org.uk**

This specification is provided online, so the version available on our website is the most up to date publication. It is important to note that copies of the specification that have been downloaded and printed may be different from this authoritative online version.

# Contents

## About Regulation

### OCN NI

Open College Network Northern Ireland (OCN NI) is a regulated Awarding Organisation based in Northern Ireland. OCN NI is regulated by CCEA Regulation to develop and award professional and technical (vocational) qualifications from Entry Level up to and including Level 5 across all sector areas. In addition, OCN NI is regulated by Ofqual to award similar qualification types in England.

### The Regulated Qualifications Framework: an overview

The Regulated Qualifications Framework (RQF) was introduced on 1st October 2015: the RQF provides a single framework for all regulated qualifications.

**Qualification Level**
The level indicates the difficulty and complexity of the knowledge and skills associated with any qualification. There are eight levels (Levels 1-8) supported by three 'entry' levels (Entry 1-3).

**Qualification Size**
Size refers to the estimated total amount of time it could typically take to study and be assessed for a qualification. Size is expressed in terms of Total Qualification Time (TQT), and the part of that time typically spent being taught or supervised, rather than studying alone, is known as Guided Learning Hours (GLH).

## Qualification Features

### Sector Subject Area

6.1 ICT for Practitioners

This qualification relates to the following National Occupational Standards:

**NOS - Information Technology**

### Qualification Aim

The aim of the OCN NI Level 4 Certificate in Cyber Security qualification is to develop the skills and knowledge of learners to monitor, maintain and enhance the security of information technology systems.

### Qualification Objectives

The objectives of the OCN NI Level 4 Certificate in Cyber Security are to enable the learner to carry out the following on information technology systems:

- penetration testing
- management of governance and security
- security programming techniques, configuration and management processes
- data examination, recovery and forensic analysis
- perimetral security

### Grading

Grading for this qualification is pass/fail.

### Qualification Target Group

The OCN NI Level 4 Certificate in Cyber Security is suitable for learners who work in or intend to work in roles as information technology professionals.

### Progression Opportunities

The OCN NI Level 4 Certificate in Cyber Security will enable learners to progress to higher level qualifications in the areas of information technology and/or cyber security. This qualification may also assist learners gain employment in occupations requiring the safe and secure use of information technology.

## Entry Requirements

Learners must be at least 18 years of age and have a level three qualification in information technology or related subjects or have relevant information technology experience equivalent to at least a level three qualification in information technology.

## Qualification Support

A Qualification Support pack is available for OCN NI centres within the login area of the OCN NI website (https://www.ocnni.org.uk/my-account/), which includes additional support for teachers, eg planning and assessment templates, guides to best practice, etc.

## Delivery Languages

This qualification is available in English only at this time. If you wish to offer the qualification in Welsh or Irish (Gaeilge) then please contact OCN NI who will review demand and provide as appropriate.

## Centre Requirements for Delivering the Qualification

### Centre Recognition and Qualification Approval

New and existing OCN NI recognised centres must apply for and be granted approval to deliver these qualifications prior to the commencement of delivery.

### Centre Staffing

Centres are required to have the following roles in place as a minimum, although a member of staff may hold more than one role*:

- Centre contact
- Programme co-ordinator
- Assessor
- Internal Verifier

*Note: A person cannot be an internal verifier for any evidence they have assessed.

Centres must ensure that staff delivering, assessing and internally verifying qualifications are both qualified to teach in Northern Ireland and competent to do so.

### Tutors

Tutors delivering the qualification should be occupationally competent, qualified to at least one level higher than the qualification and have a minimum of one year's experience in information technology network management and / or cybersecurity.

### Assessors

The qualifications are assessed within the centre and are subject to OCN NI's quality assurance processes. Units are achieved through internally set, internally assessed, and internally verified evidence.

***Assessors must:***

- be occupationally competent and qualified to at least one level higher than the qualification
- have a minimum of one year's experience in information technology network management and / or cybersecurity
- have direct or related relevant experience in assessment
- assess all assessment tasks and activities

## Internal Verification

OCN NI qualifications must be scrutinised through the centre's internal quality assurance processes as part of the recognised centre agreement with OCN NI. The centre must appoint an experienced and trained internal verifier whose responsibility is to act as the internal quality monitor for the verification of the delivery and assessment of the qualifications.

The centre must agree a working model for internal verification with OCN NI prior to delivery of the qualification.

***Internal Verifiers must:***

- have at least one year's occupational experience in the areas they are internally verifying
- attend OCN NI's internal verifier training if not already completed

Internal verifiers are required to:

- support tutors and assessors
- sample assessments according to the centre's sampling strategy
- ensure tasks are appropriate to the level being assessed
- maintain up-to-date records supporting the verification of assessment and learner achievement

## Structure and Content

**OCN NI Level 4 Certificate in Cyber Security**

To achieve the OCN NI Level 4 Certificate in Cyber Security learners must successfully complete all five units – 26 credits.

Total Qualification Time (TQT) for this qualification: 260 hours
Guided Learning Hours (GLH) for this qualification: 100 hours

| Unit Reference Number | OCN NI Unit Code | Unit Title | Credit Value | GLH | Level |
|---|---|---|---|---|---|
| F/650/0765 | CBF619 | Information Technology Systems Penetration Testing | 4 | 14 | Four |
| H/650/0766 | CBF620 | Management and Governance of Information Technology Security | 4 | 11 | Four |
| J/650/0767 | CBF621 | Security Development for Information Technology | 8 | 32 | Four |
| K/650/0768 | CBF622 | Data Examination, Recovery and Forensic Analysis of Information Technology Systems | 6 | 28 | Four |
| T/650/0770 | CBF623 | Information Technology System Perimetral Security | 4 | 15 | Four |

## Unit Details

| | |
|---|---|
| Title | Information Technology Systems Penetration Testing |
| Level | Four |
| Credit Value | 4 |
| Guided Learning Hours (GLH) | 14 |
| OCN NI Unit Code | CBF619 |
| Unit Reference No | F/650/0765 |
| *Unit purpose and aim(s):* This unit will enable the learner to understand penetration testing including being able to test for vulnerabilities in information technology (IT) systems and report on testing. | |

| Learning Outcomes | Assessment Criteria |
|---|---|
| 1. Understand the cyber security audit process. | 1.1. Explain the stages involved in the cyber security audit process and the importance of each. |
| 2. Be able to search and identify vulnerabilities in an organisation's IT systems. | 2.1. Explain the main steps involved in determining IT hardware and software compliance with an organisation's requirements.<br>2.2. Demonstrate how to test IT hardware and software to ensure compliance with a given organisation's requirements.<br>2.3. Select with justification and use an appropriate scanning device, to identify possible vulnerabilities in a given organisation's IT system. |
| 3. Know how to report on identified vulnerabilities in an organisation's IT systems and provide appropriate guidance. | 3.1. Report the findings of the scan undertaken in AC 2.3 in an appropriate format to include:<br>a) vulnerability name and date of discovery<br>b) description of the vulnerability<br>c) possible impacts of the vulnerability<br>d) guidance for addressing identified vulnerabilities |

**Assessment Guidance**

The following assessment method/s may be used to ensure all learning outcomes and assessment criteria are fully covered.

| Assessment Method | Definition | Possible Content |
|---|---|---|
| Portfolio of evidence | A collection of documents containing work undertaken to be assessed as evidence to meet required skills outcomes<br>OR<br>A collection of documents containing work that shows the learner's progression through the course | Learner notes/written work<br>Learner log/diary<br>Record of observation<br>Record of discussion |
| Practical demonstration/assignment | A practical demonstration of a skill/situation selected by the tutor or by learners, to enable learners to practise and apply skills and knowledge | Record of observation<br>Learner notes/written work<br>Learner log |

| | | |
|---|---|---|
| Coursework | Research or projects that count towards a learner's final outcome and demonstrate the skills and/or knowledge gained throughout the course | Record of observation<br>Learner notes/written work<br>Tutor notes/record<br>Learner log/diary |
| E-assessment | The use of information technology to assess learners' work | Electronic portfolio<br>E-tests |

| | |
|---|---|
| Title | Management and Governance of Information Technology Security |
| Level | Four |
| Credit Value | 4 |
| Guided Learning Hours (GLH) | 11 |
| OCN NI Unit Code | CBF620 |
| Unit Reference No | H/650/0766 |
| *Unit purpose and aim(s):* This unit will enable the learner to understand the management and governance of information technology (IT) security. The learner will be able to apply IT management techniques, implement information security management system (ISMS) and carry out risk assessment to enhance the security of IT systems. | |
| **Learning Outcomes** | **Assessment Criteria** |
| 1. Understand information security standards and best practice in the use of IT management techniques. | 1.1. Explain the Information Technology Infrastructure Library (ITIL) framework and how it can be used to enhance the security of IT systems.<br>1.2. Explain the following information security management standards and their application:<br>a) ISO/IEC 27001<br>b) ISO/IEC 27002<br>1.3. Explain using examples, best practice in applying IT management techniques to enhance the security of IT systems. |
| 2. Understand IT security governance. | 2.1. Explain what is meant by IT security governance and how it can be used to enhance the security of IT systems. |
| 3. Be able to implement information security management system (ISMS). | 3.1. Explain the key features of an effective ISMS.<br>3.2. Implement ISMS on a given IT system. |
| 4. Be able to carry out and report on a risk assessment of an organisation's IT system and data. | 4.1. Summarise the key steps involved in carrying out a risk assessment on an organisation's IT system and data.<br>4.2. Carry out a risk assessment on a given organisation's IT system and data.<br>4.3. Develop a report based on outcomes of risk assessment carried out in AC 3.2 to include any recommendations regarding system weaknesses.<br>4.4. Explain the importance of adhering to security regulations when reporting on IT system and data risk assessments. |

| Assessment Guidance | | |
|---|---|---|
| The following assessment method/s may be used to ensure all learning outcomes and assessment criteria are fully covered. | | |
| **Assessment Method** | **Definition** | **Possible Content** |
| Portfolio of evidence | A collection of documents containing work undertaken to be assessed as evidence to meet required skills outcomes<br>OR<br>A collection of documents containing work that shows the learner's progression through the course | Learner notes/written work<br>Learner log/diary<br>Record of observation<br>Record of discussion |
| Practical demonstration/assignment | A practical demonstration of a skill/situation selected by the tutor or by learners, to enable learners to practise and apply skills and knowledge | Record of observation<br>Learner notes/written work<br>Learner log |
| Coursework | Research or projects that count towards a learner's final outcome and demonstrate the skills and/or knowledge gained throughout the course | Record of observation<br>Learner notes/written work<br>Tutor notes/record<br>Learner log/diary |
| E-assessment | The use of information technology to assess learners' work | Electronic portfolio<br>E-tests |

| | |
|---|---|
| Title | Security Development for Information Technology |
| Level | Four |
| Credit Value | 8 |
| Guided Learning Hours (GLH) | 32 |
| OCN NI Unit Code | CBF621 |
| Unit Reference No | J/650/0767 |
| *Unit purpose and aim(s):* This unit will enable the learner to understand how to carry out security programming techniques, configuration and management processes and incorporate security measures when developing applications. | |

| Learning Outcomes | Assessment Criteria |
|---|---|
| 1. Understand secure programming techniques, security configuration and management processes. | 1.1. Explain what is meant by and the key features of secure programming. techniques, security configuration and security management processes. |
| 2. Be able to apply secure programming techniques and security management processes. | 2.1. Demonstrate how to apply security management processes to enhance the security of given information technology (IT) systems and data.<br>2.2. Select with justification and apply appropriate secure programming techniques to enhance the security of a given IT system.<br>2.3. Demonstrate the application of secure configuration management processes to minimise intrusion events. |
| 3. Be able to incorporate appropriate security measures when developing applications. | 3.1. Explain the security measures that should be incorporated and tested when developing applications.<br>3.2. Develop an application incorporating appropriate security configuration.<br>3.3. Demonstrate how to ensure the application developed in AC 3.2 is secure. |

**Assessment Guidance**

The following assessment method/s may be used to ensure all learning outcomes and assessment criteria are fully covered.

| Assessment Method | Definition | Possible Content |
|---|---|---|
| Portfolio of evidence | A collection of documents containing work undertaken to be assessed as evidence to meet required skills outcomes<br>OR<br>A collection of documents containing work that shows the learner's progression through the course | Learner notes/written work<br>Learner log/diary<br>Record of observation<br>Record of discussion |
| Practical demonstration/assignment | A practical demonstration of a skill/situation selected by the tutor or by learners, to enable learners to practise and apply skills and knowledge | Record of observation<br>Learner notes/written work<br>Learner log |

| | | |
|---|---|---|
| Coursework | Research or projects that count towards a learner's final outcome and demonstrate the skills and/or knowledge gained throughout the course | Record of observation<br>Learner notes/written work<br>Tutor notes/record<br>Learner log/diary |
| E-assessment | The use of information technology to assess learners' work | Electronic portfolio<br>E-tests |

| | |
|---|---|
| Title | Data Examination, Recovery and Forensic Analysis of Information Technology Systems |
| Level | Four |
| Credit Value | 6 |
| Guided Learning Hours (GLH) | 28 |
| OCN NI Unit Code | CBF622 |
| Unit Reference No | K/650/0768 |
| *Unit purpose and aim(s):* This unit will enable the learner to understand how to examine and recover data, create clones of devices, carry out forensic analysis and address malicious activities that may compromise an information Technology (IT) system's security. | |

| Learning Outcomes | Assessment Criteria |
|---|---|
| 1. Be able to examine and recover data and create clones of devices. | 1.1. Summarise how to examine and recover system data.<br>1.2. Demonstrate how to examine data which has been the source of an intrusion.<br>1.3. Select with justification and use an appropriate data extraction and recovery tool.<br>1.4. Demonstrate how to create duplicates of hard drives and other removeable media. |
| 2. Be able to carry out a forensic analysis on an IT system. | 2.1. Explain the stages involved in the forensic analysis of an IT system.<br>2.2. Analyse given IT system log files and associated evidence to determine appropriate methods to identify possible network intrusions.<br>2.3. Carry out a forensic analysis on a given IT system and produce a report on findings in an appropriate format. |
| 3. Be able to address malicious activities identified in IT system log files. | 3.1. Summarise options for addressing malicious activities identified in IT system log files and associated evidence.<br>3.2. Demonstrate how to address malicious activities identified in the analysis of IT system log files and associated evidence carried out in AC 2.2. |

**Assessment Guidance**

The following assessment method/s may be used to ensure all learning outcomes and assessment criteria are fully covered.

| Assessment Method | Definition | Possible Content |
|---|---|---|
| Portfolio of evidence | A collection of documents containing work undertaken to be assessed as evidence to meet required skills outcomes<br>OR<br>A collection of documents containing work that shows the learner's progression through the course | Learner notes/written work<br>Learner log/diary<br>Record of observation<br>Record of discussion |
| Practical demonstration/assignment | A practical demonstration of a skill/situation selected by the tutor or by learners, to enable learners to practise and apply skills and knowledge | Record of observation<br>Learner notes/written work<br>Learner log |

| | | |
|---|---|---|
| Coursework | Research or projects that count towards a learner's final outcome and demonstrate the skills and/or knowledge gained throughout the course | Record of observation<br>Learner notes/written work<br>Tutor notes/record<br>Learner log/diary |
| E-assessment | The use of information technology to assess learners' work | Electronic portfolio<br>E-tests |

| | |
|---|---|
| Title | Information Technology System Perimetral Security |
| Level | Four |
| Credit Value | 4 |
| Guided Learning Hours (GLH) | 15 |
| OCN NI Unit Code | CBF623 |
| Unit Reference No | T/650/0770 |
| *Unit purpose and aim(s):* This unit will enable the learners to understand perimetral security and be able to secure information technology (IT) systems. | |

| Learning Outcomes | Assessment Criteria |
|---|---|
| 1. Understand perimetral security. | 1.1. Explain what is meant by perimetral security and how it is applied to IT systems including:<br>a) email and web services<br>b) firewall configuration<br>c) print servers<br>1.2. Explain how to effectively inform others of security requirements. |
| 2. Be able to secure IT systems. | 2.1. Demonstrate how to secure email and web services on a given organisation's IT system.<br>2.2. Demonstrate how to securely configure firewall technology on a given organisation's IT system. |

**Assessment Guidance**

The following assessment method/s may be used to ensure all learning outcomes and assessment criteria are fully covered.

| Assessment Method | Definition | Possible Content |
|---|---|---|
| Portfolio of evidence | A collection of documents containing work undertaken to be assessed as evidence to meet required skills outcomes<br>OR<br>A collection of documents containing work that shows the learner's progression through the course | Learner notes/written work<br>Learner log/diary<br>Record of observation<br>Record of discussion |
| Practical demonstration/assignment | A practical demonstration of a skill/situation selected by the tutor or by learners, to enable learners to practise and apply skills and knowledge | Record of observation<br>Learner notes/written work<br>Learner log |
| Coursework | Research or projects that count towards a learner's final outcome and demonstrate the skills and/or knowledge gained throughout the course | Record of observation<br>Learner notes/written work<br>Tutor notes/record<br>Learner log/diary |
| E-assessment | The use of information technology to assess learners' work | Electronic portfolio<br>E-tests |

## Quality Assurance of Centre Performance

### External Verification

All OCN NI recognised centres are subject to External Verification. External verification visits and monitoring activities will be conducted annually to confirm continued compliance with the conditions of recognition, review the centre's risk rating for the qualification and to assure OCN NI of the maintenance of the integrity of the qualification.

The External Verifier will review the delivery and assessment of this qualification. This will include the review of a sample of assessment evidence and evidence of the internal verification of assessment and assessment decisions. This will form the basis of the External Verification report and will inform OCN NI's annual assessment of centre compliance and risk. The External Verifier is appointed by OCN NI.

### Standardisation

As a process, standardisation is designed to ensure consistency and promote good practice in understanding and the application of standards. Standardisation events:

- make qualified statements about the level of consistency in assessment across centres delivering a qualification
- make statements on the standard of evidence that is required to meet the assessment criteria for units in a qualification
- make recommendations on assessment practice
- produce advice and guidance for the assessment of units
- identify good practice in assessment and internal verification

Centres offering units of an OCN NI qualification must attend and contribute assessment materials and learner evidence for standardisation events if requested.

OCN NI will notify centres of the nature of sample evidence required for standardisation events (this will include assessment materials, learner evidence and relevant assessor and internal verifier documentation). OCN NI will make standardisation summary reports available and correspond directly with centres regarding event outcomes.

## Administration

### Registration

A centre must register learners within 20 working days of commencement of a qualification.

### Certification

Certificates will be issued to centres within 20 working days of receipt of correctly completed results marksheets. It is the responsibility of the centre to ensure that certificates received from OCN NI are held securely and distributed to learners promptly and securely.

### Charges

OCN NI publishes all up to date qualification fees in its Fees and Invoicing Policy document. Further information can be found on the centre login area of the OCN NI website.

### Equality, Fairness and Inclusion

OCN NI has considered the requirements of equalities legislation in developing the specification for these qualifications. For further information and guidance relating to access to fair assessment and the OCN NI Reasonable Adjustments and Special Considerations policies, centres should refer to the OCN NI website.

### Retention of Evidence

OCN NI has published guidance for centres on the retention of evidence. Details are provided in the OCN NI Centre Handbook and can be accessed via the OCN NI website.

**OCN NI Level 4 Certificate in Cyber Security**
**Qualification Number: 610/0201/X**

| | |
|---|---|
| Operational start date: | 01 December 2021 |
| Operational end date: | 30 November 2026 |
| Certification end date: | 30 November 2030 |

Open College Network Northern Ireland (OCN NI)
Sirius House
10 Heron Road
Belfast
BT3 9LE

Phone: 028 90463990
Web: www.ocnni.org.uk