



## Qualification Specification for:

**OCN NI Level 5 Certificate in Cyber Security**  
➤ **Qualification No: 610/0598/8**

## Qualification Regulation Information

---

### OCN NI Level 5 Certificate in Cyber Security

Qualification Number: 610/0598/8

Operational start date: 15 March 2022

Operational end date: 28 February 2027

Certification end date: 28 February 2032

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](http://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 5 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.ocni.org.uk](http://www.ocni.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

---

<b>About Regulation .....</b>	<b>5</b>
OCN NI.....	5
<b>Qualification Features.....</b>	<b>6</b>
Sector Subject Area .....	6
Qualification Aim .....	6
Grading .....	6
Qualification Target Group .....	6
Progression Opportunities.....	7
Entry Requirements.....	7
Qualification Support.....	7
Delivery Languages.....	7
<b>Centre Requirements for Delivering the Qualification .....</b>	<b>8</b>
Centre Recognition and Qualification Approval .....	8
Centre Staffing .....	8
Tutors .....	8
Assessors.....	8
Internal Verification.....	9
<b>Structure and Content .....</b>	<b>10</b>
<b>Unit Details.....</b>	<b>11</b>
<b>Quality Assurance of Centre Performance .....</b>	<b>15</b>
External Verification .....	15
Standardisation .....	15
<b>Administration .....</b>	<b>16</b>
Registration .....	16
Certification .....	16
Charges.....	16
Equality, Fairness and Inclusion.....	16
Retention of Evidence .....	16

## 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 1<sup>st</sup> 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:

TECIS600201 - [Identify cyber security threats and vulnerabilities - National Occupational Standards \(ukstandards.org.uk\)](https://www.ukstandards.org.uk/standards/TECIS600201)

TECDT80844 - [Develop and implement cryptographic methods - National Occupational Standards \(ukstandards.org.uk\)](https://www.ukstandards.org.uk/standards/TECDT80844)

TECIS600202 - [Protect against cyber security threats - National Occupational Standards \(ukstandards.org.uk\)](https://www.ukstandards.org.uk/standards/TECIS600202)

TECIS60443 - [Carry out infrastructure penetration testing - National Occupational Standards \(ukstandards.org.uk\)](https://www.ukstandards.org.uk/standards/TECIS60443)

### Qualification Aim

The aim of the OCN NI Level 5 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 5 Certificate in Cyber Security are to enable the learner to carry out the following:

- application of computer security principles using current technologies and management tools
- planning, implementation and monitoring of system and software security
- network security management
- application of cryptographic algorithms and network security
- security penetration tests
- network security logging and monitoring services to be utilised

### Grading

Grading for this qualification is pass/fail.

### Qualification Target Group

The OCN NI Level 5 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 5 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 to 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.

### 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 cyber security.

### 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 cyber security
- 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 5 Certificate in Cyber Security

To achieve the OCN NI Level 5 Certificate in Cyber Security learners must successfully complete both units – 14 credits.

Total Qualification Time (TQT) for this qualification: 140 hours  
 Guided Learning Hours (GLH) for this qualification: 64 hours

Unit Reference Number	OCN NI Unit Code	Unit Title	Credit Value	GLH	Level
<a href="#">D/650/1673</a>	CBF776	Computer System and Software Security	7	32	Five
<a href="#">F/650/1674</a>	CBF777	Network Security and Management	7	32	Five

## Unit Details

Title	Computer System and Software Security
Level	Five
Credit Value	7
Guided Learning Hours (GLH)	32
OCN NI Unit Code	CBF776
Unit Reference No	D/650/1673
<i>Unit purpose and aim(s):</i> This unit will enable the learner to understand how to secure computer networks. The learner will also understand cyber security from both defensive and offensive perspectives.	
Learning Outcomes	Assessment Criteria
1. Understand the technologies and management tools used in computer security.	1.1. Explain current computer security technologies and management tools relating to the following and the principles and standards on which they are based: a) encryption b) authentication c) access control d) database security e) malicious software f) Intrusion Detection Systems (IDS) g) Denial of Service (DOS) attacks
2. Understand software security.	2.1. Explain with examples what is meant by the following and how they impact on the security of computer systems: a) system overflows b) software security c) system security d) trusted security
3. Understand the main phases involved in the implementation of system and software security across different operating systems.	3.1. Explain the main phases involved in the implementation of system and software security. 3.2. Critically compare the implementation of security across at least three different operating systems used in the following a) system b) network c) application d) user security e) cloud f) encryption and data services
4. Understand how to carry out the plan phase of a system and software security implementation.	4.1. Explain how to carry out the plan phase of a system and software security implementation.
5. Be able to carry out the identification and implementation phase of a system and software security implementation.	5.1. Carry out the identification and implementation phase of system and software security implementation on a given system using appropriate software to include: a) development of rules-based filtering across hardware and software b) approval and implementation of baseline configurations for browser settings, group policy, password complexity, local permissions,

	patching, application control, software restrictions
6. Be able to carry out the controlling of configuration changes phase of a system and software security implementation.	6.1. Carry out the controlling of configuration changes phase of a system and software security implementation to include: <ul style="list-style-type: none"> <li>a) maintaining secure, approved baseline configurations</li> <li>b) monitoring adherence to established policies, procedures, and approved baseline configurations</li> <li>c) identification of unauthorised system components</li> <li>d) identification of misconfigurations or vulnerabilities</li> <li>e) identification of system modifications to reduce risk</li> </ul>

### 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 OR A collection of documents containing work that shows the learner's progression through the course	Learner notes/written work Learner log/diary Peer notes Record of observation 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 Learner notes/written work 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 Learner notes/written work Tutor notes/record Learner log/diary
E-assessment	The use of information technology to assess learners' work	Electronic portfolio E-tests

Title	Network Security and Management
Level	Five
Credit Value	7
Guided Learning Hours (GLH)	32
OCN NI Unit Code	CBF777
Unit Reference No	F/650/1674
<i>Unit purpose and aim(s):</i> This unit will enable the learner to understand how to implement and manage the security of computer networks.	
Learning Outcomes	Assessment Criteria
1. Understand network security management.	1.1. Explain using examples what is meant by network security management and its role within an organisation. 1.2. Research and evaluate the physical and infrastructure security options available for a given network including: a) surveillance b) access control c) protection of people, property, and physical assets from actions and events that could cause damage or loss 1.3. Explain how human resource security policies and practices can form part of network management including: a) employment b) e-mail usage c) internet usage
2. Understand cryptographic algorithms and network security.	2.1. Explain how the following can be used to enhance network security: a) cryptographical algorithms b) public-key cryptography and message authentication c) secure hash functions d) hash-based message authentication code
3. Be able to carry out security penetration tests.	3.1. Carry out the following security tests on a given network: a) network sniffing using a network protocol analyser b) connecting to a Transmission Control Protocol and User Datagram Control Protocol (TCP/UDP) port with Netcat and transfer files c) using an intrusion detection system (IDS) d) completing a brute force dictionary attack e) investigating cross site scripting cross sites scripting (XSS) attacks f) deploying information gathering tools g) cracking Wired Equivalent Privacy (WEP)
4. Be able to determine network security logging and monitoring services to be utilised.	4.1. Determine for a given network, how security logging and monitoring services may be used to enhance network security management including: a) audit trail analysis b) detection of security breaches

- c) event reconstruction
- d) use of security logging and monitoring for faster recovery

### 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 OR A collection of documents containing work that shows the learner's progression through the course	Learner notes/written work Learner log/diary Peer notes Record of observation 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 Learner notes/written work 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 Learner notes/written work Tutor notes/record Learner log/diary
E-assessment	The use of information technology to assess learners' work	Electronic portfolio 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 5 Certificate in Cyber Security**  
**Qualification Number: 610/0598/8**

---

Operational start date: 15 March 2022  
Operational end date: 28 February 2027  
Certification end date: 28 February 2032

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

Phone: 028 90463990  
Web: [www.ocnni.org.uk](http://www.ocnni.org.uk)