Qualification Specification:

OCN NI Level 4 Certificate in Cyber Security

- **Qualification No: 610/0201/X**

Version: 2.0

1. Specification Updates

Key changes have been listed below:

Section	Detail of change	Version and date of Issue
Specification	On new format	2.0 December 2025
Qual extended	Qualification extended to 30 November 2031	2.0 December 2025

2. Contents

3. Introduction to Open College Network Northern Ireland (OCN NI)

The Open College Network Northern Ireland (OCN NI) is a UK recognised awarding organisation based in Northern Ireland. We are regulated by CCEA Regulation to develop and award regulated professional and technical (vocational) qualifications from Entry Level up to and including Level 5 across all sector areas. In addition, OCN NI is also regulated by Ofqual to award qualifications in England.

OCN NI is also an educational charity that advances education by developing nationally recognised qualifications and recognising the achievements of learners. We work with centres such as Further Education Colleges, Private Training Organisations, Voluntary & Community Organisations, Schools, SME's and Public Sector bodies to provide learners with opportunities to progress into further learning and/or employment. OCN NI's Strategic Plan can be found on the OCN NI website www.ocnni.org.uk.

For further information on OCN NI qualifications or to contact us, you can visit our website at www.ocnni.org.uk. The website should provide you with details about our qualifications, courses, contact information, and any other relevant information you may need.

OCN NI Contact Details

Open College Network Northern Ireland
Sirius House
10 Heron Road
Belfast
BT3 9LE

Phone: 028 90 463990
Website: **www.ocnni.org.uk**
Email: info@ocnni.org.uk

4. About this Specification

This specification details OCN NI's specific requirements for the delivery and assessment of the **OCN NI Level 4 Certificate in Cyber Security.**

This specification will provide guidelines for centres to ensure the effective and correct delivery of this qualification. OCN NI qualification specifications are based on research and engagement with the practitioner community to ensure they provide appropriate skills and knowledge for learners.

The qualification specification will detail the following aspects of the OCN NI Level 4 Certificate in Cyber Security.

- **Qualification Features**: this includes the key characteristics and features of this qualification, such as its intended audience, purpose, and credit value.

- **Centre Requirements:** this details the prerequisites and obligations that centres must fulfil to be eligible to deliver and assess this qualification. These include guidelines on staff qualifications, resources, and required procedures.

- **Structure and Content:** this details the structure and content of the qualification including units, and any specific content that learners will be required to study.

- **Assessment Requirements:** this details assessment criteria and assessment methods for this qualification, ensuring that summative assessment approaches are clear.

- **Quality Assurance:** the quality and consistency of delivery and assessment of this qualification are of paramount importance to OCN NI. The mandatory quality assurance arrangements including processes for internal and external quality assurance that all centres offering this qualification must adhere to are detailed.

- **Administration:** guidance on the administrative aspects of delivering this qualification, including registration, certification and record-keeping.

- Reference to other handbooks and policies as appropriate to the qualifications.

It is important to note that OCN NI will communicate any significant updates or changes to this specification in writing to our centres. Additionally, we will make these changes available on our official website at www.ocnni.org.uk.

To stay current, please refer to the online version of this specification as it is the most authoritative and up-to-date publication. Be aware that downloaded and printed copies may not reflect the latest revisions.

4.1 Additional Support

OCN NI offers a comprehensive range of support services designed to assist centres in meeting the delivery and quality assurance requirements of OCN NI qualifications. These services include:

- **Learner Assessment Booklets**: These booklets are created to assist learners in demonstrating the fulfilment of assessment criteria and organising the quality assurance prerequisites for each individual unit.

- **Specimen Assessment Materials**: These booklets are created to assist learners in demonstrating the fulfilment of assessment criteria and organising the quality assurance prerequisites for each individual unit.

- **Qualification Support Pack**: A support pack has been developed to support centres in the delivery of this qualification. The pack includes planning and assessment templates, guides to best practice, etc.

- **Professional Development for Educators**: OCN NI provides opportunities for professional development tailored to meet the various needs of practitioners and quality assurance staff. Centres can join our training sessions, available in both face-to-face and online formats, or explore a wealth of training materials by visiting www.ocnni.org.uk

- **OCN NI Subject Advisors**: Our team of subject advisors offers vital information and support to centres. They provide guidance on specification details, non-exam assessment advice, updates on resource developments, and various training opportunities. They actively engage with subject communities through an array of networks to facilitate the exchange of ideas and expertise, to support practitioners to provide quality education programs to learners.

All centres can access information, support and guidance to support the delivery and quality assurance of this qualification by contacting their designated Business Development Advisor or by contacting us on Contact Us | OCN NI

5. About this Qualification

5.1 Qualification Regulation Information

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

Operational start date: 01 December 2021
Review date: 30 November 2031

The qualification's operational start and end dates define the regulated qualification's lifecycle. The operational end date is the final date for learner registration, while learners have until the certificate end date to complete the qualification and receive their certificates.

It is important to note that all OCN NI regulated qualifications are listed on the Register of Regulated Qualifications (RQF), which can be found at Ofqual Register. This register is maintained by Ofqual in England and CCEA Regulation in Northern Ireland. It contains information about qualifications that are regulated and accredited. It is a key resource for learners, employers, and educational institutions to verify the status and recognition of qualifications.

Centres must adhere to administrative guidelines diligently, with special attention to the fact that fees, registration, and certification end dates for the qualification may be subject to changes. It is a centre's responsibility to make itself aware of updates on any modifications to ensure compliance with the latest requirements. OCN NI provides centres with timely updates through various channels including website, newsletters and through this specification. Information on qualification fees can be found on the Centre Login section of the OCN NI website www.ocnni.org.uk .

5.2 Sector Subject Area

A subject sector area is a specific category used to classify academic and vocational qualifications. Subject sector areas are part of the educational and qualifications framework to organise and categorise qualifications. The sector subject for this qualification is:

Subject Area: 6.1 – Digital technology (practitioners)

NOS:

TECIS60443 Carry out infrastructure penetration testing
TECIS60131 Contribute to information security governance activities
TECIS60141 Carry out information security governance activities
TECIS60151 Manage information security governance activities
TECDT80651 Develop and implement strategies for privacy and data protection compliance
TECDT61251 Manage digital forensic activities
TECHDUDS3 Apply enhanced security procedures to protect data

5.3 Grading

Grading for this qualification is pass/fail.

5.4 Qualification's Aim and Objectives

Qualification's Aim

The aim of the OCN NI Level 4 Certificate in Cyber Security is to provide individuals with the knowledge and skills to accurately monitor, maintain and enhance the security of information technology systems.

Qualification's Objectives

The objectives of the OCN NI Level 4 Certificate in Cyber Security are to enable learners 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

5.5 Target Learners

This qualification is targeted at individuals who work in or intend to work in roles as information technology professionals.

5.6 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.

5.7 Progression

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.

5.8 Delivery Language

This qualification is exclusively available in English. If there is a desire to offer this qualification in Welsh or Irish (Gaeilge), we encourage you to get in touch with OCN NI. They will assess the demand for such provisions and, if feasible, provide the qualification in the requested language as appropriate.

6. Centre Requirements for Delivering this Qualification

6.1 Centre Recognition

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

6.2 Qualification Approval

Once a centre has successfully undergone the Centre Recognition process, it becomes eligible to apply for qualification approval. The centre's capability to meet and sustain the qualification criteria will be assessed. Throughout the qualification approval process, OCN NI will aim to ensure that:

- centres possess suitable physical resources (e.g., equipment, IT, learning materials, teaching rooms) to support qualification delivery and assessment
- centre staff involved in the assessment process have relevant expertise and/or occupational experience
- robust systems are in place for ensuring ongoing professional development for staff delivering the qualification
- centres have appropriate health and safety policies concerning learner equipment use
- qualification delivery by centres complies with current equality and diversity legislation and regulations
- as a part of the assessment process for this qualification it may be useful for learners to have access to a practical work setting

6.3 Centre Staffing

To offer this qualification centres are mandated to establish the following roles as a minimum, although a single staff member may serve in more than one capacity*:

- Centre contact
- Programme Co-ordinator
- Assessor
- Internal Quality Assurance (IQA)

*Note: An individual cannot serve as an IQA for their own assessments.

6.4 Tutor Requirements

Tutors responsible for delivering this qualification are expected to possess a high degree of occupational competency. They should meet the following criteria:

- **Occupational Competency:** Tutors should demonstrate a clear understanding of the subject matter, including up-to-date knowledge. They should also have a minimum of one year's experience in information technology network management and / or cybersecurity. This competence should enable them to effectively impart knowledge and practical skills to learners.

- **Qualifications:** Tutors should hold qualifications at a level that is at least one level higher than the qualification they are teaching. This ensures that they have the necessary academic foundation to provide in-depth guidance and support to learners.

These requirements collectively ensure that learners receive instruction from highly qualified and experienced instructors, thereby enhancing the quality and effectiveness of their educational experience.

6.5 Assessor Requirements

The assessment of this qualification takes place within the centre and is subjected to OCN NI's rigorous quality assurance procedures. The achievement of individual units is based on the criteria defined in each unit.

Assessors play a pivotal role in ensuring the validity and fairness of assessments. They are required to meet the following criteria:

- **Occupational Competency:** Assessors should possess a high degree of occupational competency in the relevant subject matter. This expertise enables them to accurately evaluate and measure a learner's knowledge and skills. Additionally, they should hold qualifications at a level that is at least one level higher than the qualification they are assessing, ensuring their in-depth understanding of the subject matter.

- **Assessment Expertise:** Assessors should have a minimum of one year's experience in information technology network management and/or cybersecurity. This includes knowledge of best practices in designing, conducting, and grading assessments. Their expertise ensures that assessments are both fair and valid.

- **Assessors Qualification:** Assessors should hold or be currently undertaking a recognised assessor's qualification; or must have attended the OCN NI Assessment Training.

- **Comprehensive Assessment Oversight:** Assessors are responsible for evaluating all assessment tasks and activities comprehensively. They must thoroughly review and assess each element to ensure a fair and accurate representation of a learner's skills and knowledge.

These rigorous requirements uphold the quality and integrity of the qualification's assessment process, ensuring that learners receive a fair and reliable evaluation of their competencies.

6.6 Internal Quality Assurer Requirements

The Internal Quality Assurer plays a crucial role in the centre's internal quality assurance processes. The centre must designate a skilled and trained IQA who assumes the role of an internal quality monitor responsible for verifying the delivery and assessment of the qualification.

The Internal Quality Assurer for this qualification must meet the following criteria:

- **IQA Expertise:** IQA should have direct or related experience in the field of internal assurance and have at least one year's occupational experience in the areas they are internally quality assuring. This includes knowledge of best practices in designing, conducting, and grading assessments. Their expertise ensures that assessments are both fair and valid.
- **IQA Qualification:** IQA should hold or be currently undertaking a recognised IQA qualification or must have attended the OCN NI IQA Training.
- **Thorough Evaluation of Assessment Tasks and Activities:** IQAs are tasked with conducting in-depth reviews and assessments of all assessment tasks and activities. Their responsibility is to ensure a comprehensive and meticulous oversight of each element to guarantee a just and precise reflection of a learner's abilities and knowledge and to ensure that all assessment and quality assurance requirements are fulfilled.

7. Qualification Structure

7.1 Qualification Purpose

The OCN NI Level 4 Certificate in Cyber Security is a unitised qualification on a scale of pass or fail. Learners are expected to demonstrate a comprehensive understanding of the subject matter, ensuring a level of proficiency. The qualification will provide individuals with the knowledge and skills to accurately monitor, maintain and enhance the security of information technology systems.

7.2 Qualification Level

In the context of the OCN NI Level 4 Certificate in Cyber Security it is essential to understand the significance of qualification levels, as they play a pivotal role in assessing the depth and complexity of knowledge and skills required for successful attainment. This qualification aligns with Level 4, which signifies a complex level of difficulty and intricacy. It's important to note that qualification levels in the educational framework range from Level 1 to Level 8, complemented by three 'entry' levels, namely Entry 1 to Entry 3.

7.3 Qualification Size

Total Qualification Time (TQT)

This represents the total amount of time a learner is expected to spend to complete the qualification successfully. It includes both guided learning hours (GLH) and independent study or additional learning time.

Guided Learning Hours (GLH)

These are the hours of guided instruction and teaching provided to learners. This may include classroom instruction, tutorials, or other forms of structured learning.

OCN NI Level 4 Certificate in Cyber Security	
Total Qualification Time (TQT):	260 hours
Total Credits Required:	26 credits
Guided Learning Hours (GLH):	100 hours

7.4 How to Achieve the Qualification

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

8. Assessment Structure

This qualification is assessed through internal assessment and each unit is accompanied by specific assessment criteria that define the requirements for achievement.

8.1 Assessment Guidance: Portfolio

The portfolio for this qualification is designed to provide a comprehensive view of a learner's skills and knowledge. It is a holistic collection of evidence that may include a single piece of evidence that satisfies multiple assessment criteria. There is no requirement for learners to maintain separate evidence for each assessment criterion.

When learners are creating their portfolio, they should refer to the assessment criteria to understand the evidence required.

It is essential that the evidence in the portfolio reflects the application of skills in real-world situations. Learners should ensure that they provide multiple examples or references whenever the assessment criteria require it.

8.2 Understanding the Units

The units outlined in this specification establish clear assessment expectations. They serve as a valuable guide for conducting assessments and ensuring quality assurance efficiently. Each unit within this specification follows a consistent structure. This section explains the operational framework of these units. It is imperative that all educators, assessors, Internal Quality Assurers, and other personnel overseeing the qualification review and familiarise themselves with this section to ensure a comprehensive understanding of how these units function.

- **Title:** The title will reflect the content of the unit and should be clear and concise.
- **Level:** A unit can have one of six RQF levels: Entry, One, Two, Three, Four or Five. All units within this qualification are Level 4.
- **Credit Value:** This describes the number of credits ascribed to a unit. It identifies the number of credits a learner is awarded upon successful achievement of the unit. One credit is awarded for the learning outcomes which a learner, on average, might reasonably be expected to achieve in a notional 10 hours of learning.
- **Learning Outcome:** A coherent set of measurable achievements.
- **Assessment Criteria:** These enable a judgement to be made about whether or not, and how well, the students have achieved the learning outcomes.
- **Assessment Guidance and Methods:** These detail the different assessment methods within the unit that may be used.
- **Unit Content:** This provides indicative content to assist in teaching and learning.

9. Qualification Summary by Unit

OCN NI Level 4 Certificate in Cyber Security

In order to achieve the OCN NI Level 4 Certificate in Cyber Security the learner 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

10. Unit Content

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. 2.2. Demonstrate how to test IT hardware and software to ensure compliance with a given organisation's requirements. 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: a) vulnerability name and date of discovery b) description of the vulnerability c) possible impacts of the vulnerability d) guidance for addressing identified vulnerabilities

Assessment Guidance
NOS: TECIS60443 NOS - Carry out infrastructure penetration testing

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 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	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. 1.2. Explain the following information security management standards and their application: a) ISO/IEC 27001 b) ISO/IEC 27002 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. 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. 4.2. Carry out a risk assessment on a given organisation's IT system and data. 4.3. Develop a report based on outcomes of risk assessment carried out in AC 3.2 to include any recommendations regarding system weaknesses. 4.4. Explain the importance of adhering to security regulations when reporting on IT system and data risk assessments.

Assessment Guidance
NOS: TECIS60131 Contribute to information security governance activities
TECIS60141 Carry out information security governance activities
TECIS60151 Manage information security governance activities

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 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	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. 2.2. Select with justification and apply appropriate secure programming techniques to enhance the security of a given IT system. 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. 3.2. Develop an application incorporating appropriate security configuration. 3.3. Demonstrate how to ensure the application developed in AC 3.2 is secure.

Assessment Guidance
NOS: TECDT80651 -Develop and implement strategies for privacy and data protection compliance

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 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	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. 1.2. Demonstrate how to examine data which has been the source of an intrusion. 1.3. Select with justification and use an appropriate data extraction and recovery tool. 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. 2.2. Analyse given IT system log files and associated evidence to determine appropriate methods to identify possible network intrusions. 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. 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
NOS: TECDT61251 Manage digital forensic activities

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 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	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: a) email and web services b) firewall configuration c) print servers 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. 2.2. Demonstrate how to securely configure firewall technology on a given organisation's IT system.

Assessment Guidance
NOS: TECHDUDS3 Apply enhanced security procedures to protect data

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 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

11. Quality Assurance of Centre Performance

11.1 Internal Quality Assurance

When delivering and assessing this qualification, centres must align with stakeholders' expectations and address learners' needs by implementing a practical and applied programme. Centres have the flexibility to customise programmes to meet local requirements and establish connections with local employers and the broader vocational sector.

The Assessor should work with the Internal Quality Assurer to ensure that the assessment is planned in line with OCN NI requirements. Assessment Plans must be developed and approved by the Internal Quality Assurer prior to the delivery of the qualification.

All units within this qualification must undergo internal assessment. Learners must provide evidence that they have appropriately met all assessment criteria required for that grade.

The assessment format for all units involves a task conducted after the delivery of the unit's content, or part of it, if multiple tasks are used. Tasks may exhibit in various forms, encompassing practical and written types. Please refer to 'OCN NI's Assessment Definitions Guide' for additional details.

A task constitutes a distinct activity completed independently by learners, separated from teaching, practice, exploration, and other activities guided by tutors. Tasks are assigned to learners with a specified start date, completion date, and explicit requirements for the evidence to be produced. Some tasks may include observed practical components and require diverse forms of evidence.

A valid assignment will enable a clear and formal assessment outcome which meets the requirements of the assessment criteria. Assessment decisions are based on the specific assessment criteria given in each unit and set at each grade level. The way in which individual units are written provides a balance of assessment of understanding, practical skills and vocational attributes appropriate to the purpose of qualification.

It is the Assessor's role to ensure that learners are appropriately prepared for assessment, this begins from induction onwards. Assessors should ensure that learners understand how assessment tasks are used to determine the award of credit, the importance of meeting assessment timelines, and that all learners work must be independently created, where source documents are used this should be appropriately referenced, learners should be aware of what would constitute plagiarism and the possible consequences.

When conducting the assessment, Assessors must ensure they do not provide direct input, instructions or specific feedback which may compromise the authenticity of the work submitted.

Once the Assessor has authenticated the learners work, they must transparently demonstrate the rationale behind their assessment decisions. Once a learner completes all assigned tasks for a unit, the Assessor will allocate a grade for the unit. Refer to the 'Unit Grading Matrix' for additional information on the grading process.

Once the Assessor has completed the assessment process for the task, the assessment decision is recorded formally, and feedback is provided to the learner. The feedback should show the learner the outcome of the assessment decision, how it was determined or where the criteria has been met, it may indicate to the learner why achievement of the assessment criteria has not been met. It must be clear to the learner that this Assessment outcome is subject to verification.

For further information on assessment practice, please see the 'OCN NI Centre Handbook'. Assessment Training is also available and can be booked through the OCN NI Website.

11.2 Internal Quality Assurance

The role of the Internal Quality Assurer is to ensure appropriate internal quality assurance processes are carried out. The Internal Quality Assurer must oversee that assessments are conducted in accordance with relevant OCN NI policies, regulations, and this specification.

The Internal Quality Assurer must ensure assessments are fair, reliable, and uniform, thereby providing a consistent standard for all learners.

Internal Quality Assurers are required to provide constructive feedback to Assessors, identifying areas of strength and those that may require improvement. This feedback contributes to the ongoing professional development of Assessors.

Contributing to the standardisation of assessment practices within the centre is an important function of this role. This entails aligning assessment methods, grading criteria, and decision-making processes to maintain fairness and equity.

Internal Quality Assurers will actively engage in the sampling and monitoring of assessments to ensure the consistency and accuracy of assessment decisions. This process helps identify trends, areas for improvement, and ensures the robustness of the overall assessment system.

For further information on Internal Quality Assurance practice, please see the 'OCN NI Centre Handbook'. Internal Quality Assurance Training is also available and can be booked through the OCN NI Website.

11.3 Documentation

For internal quality assurance processes to be effective, the internal assessment and Internal Quality Assurance team needs to keep effective records.

- The programme must have an assessment and Internal Quality Assurance plan. When producing a plan, they should consider:
    - the time required for training and standardisation activities
    - the time available to undertake teaching and carry out assessment,
    - consider when learners may complete assessments and when quality assurance will take place
    - the completion dates for different assessment tasks
    - the date by which the assignment needs to be internally verified
    - sampling strategies
    - how to manage the assessment and verification of learners' work so that they can be given formal decisions promptly
    - how resubmission opportunities can be scheduled.

The following documents are available from OCN NI and document templates can be found in the Centre Login section of the OCN NI website www.ocnni.org.uk:

- A1 – Learner Assessment Record per Learner
- Learner Authentication Declarations
- Records of any reasonable adjustments applied for and the outcome – please see 'OCN NI's Reasonable Adjustments and Special Consideration Policy' for further information
- M1 Internal Quality Assurance Sample Record
- M2 Feedback to Assessor
- Records of any complaints or appeals

11.4 External Quality Assurance

All OCN NI recognised centres are subject to External Quality Assurance. External quality assurance activities will be conducted to confirm continued compliance with the CCEA Regulation General Conditions of Recognition, OCN NI terms and conditions and the requirements outlined within this qualification specification.

The External Quality Assurer is assigned by OCN NI. The External Quality Assurer will review the delivery and assessment of this qualification. This will include, but is not limited to, the review of a sample of assessment evidence and evidence of the internal quality assurance of assessment and assessment decisions. This will form the basis of the External Quality Assurance report and will help OCN NI determine the centre's risk.

The role of the External Quality Assurer serves as an external overseer of assessment quality, working to uphold consistency, compliance, and continuous improvement within the assessment process. Their role is crucial in ensuring that assessments are valid, reliable, fair, and aligned with the required standards and regulations.

For further information on OCN NI Centre Assessments Standards Scrutiny (CASS) Strategy, please see the OCN NI Centre Handbook.

11.5 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 Quality Assurance

Centres offering this qualification must carry out internal standardisation activities prior to the claim for certification.

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 Quality Assurer documentation). OCN NI will make standardisation summary reports available and correspond directly with centres regarding event outcomes.

12. Administration

12.1 Registration

A centre must register learners for this qualification within 20 days of commencement of the delivery of the programme.

For further information on learner registration please see the OCN NI Centre Handbook and the QuartzWeb Manual, available through the Centre Login section of the OCN NI website. Administration training is also available and can be booked through www.ocnni.org.uk.

12.2 Certification

Once all internal quality assurance activities have been successfully completed, the centre can claim certification for the learner(s).

Certificates will be issued to centres within 20 working days from completion of a satisfactory external quality assurance activity, if appropriate, alternatively from the submission of an accurate and complete marksheet.

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.

For further information on the uploading of results please see the QuartzWeb Manual for guidance, administration training is also available and can be booked through OCN NI

12.3 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.

12.4 Equality, Fairness and Inclusion

OCN NI's are committed to ensuring all learners have an equal opportunity to access our qualifications and assessment, and that our qualifications are awarded in a way that is fair to every learner.

OCN NI is committed to making sure that:

- learners with a protected characteristic are not, when they are undertaking one of our qualifications, disadvantaged in comparison to learners who do not share that characteristic
- all learners achieve the recognition they deserve for undertaking a qualification and that this achievement can be compared fairly to the achievement of their peers

For information on reasonable adjustments and special considerations please see the OCN NI Centre Handbook and Reasonable Adjustments and Special Considerations Policy held in the back office of the OCN NI website.

12.5 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
Review date: 30 November 2031

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

Phone: 028 90 463990
Email: info@ocnni.org.uk
Web: www.ocnni.org.uk