CAMBRIDGE
ADVANCED
NATIONALS

OCR
Oxford Cambridge and RSA

DRAFT

Specification

Cambridge Advanced National in Cyber Security and Networks

OCR Level 3 Alternative Academic Qualification
Cambridge Advanced National in Cyber Security and Networks

Certificate H037
Extended Certificate H137
For first teaching in 2026

Version 1.0 (April 2025)
ocr.org.uk/cambridge-advanced-nationals

Tell us what you think

Your feedback plays an important role in how we develop, market, support and resource qualifications now and into the future. We want you and your students to enjoy and get the best out of our qualifications and resources, but to do that we need your honest opinions to tell us whether we're on the right track or not.

You can email your thoughts to support@ocr.org.uk or visit our feedback page to learn more about how you can help us improve our qualifications.

Designing and testing in collaboration with you and your students

Helping young people develop an ethical view of the world

Equality, diversity, inclusion and belonging (EDIB) are part of everything we do

Are you using the latest version of this specification?

The latest version of our specifications will always be on our website and may differ from printed versions. We will inform centres about changes to specifications.

This qualification is in draft form and has not yet been accredited by the regulator, Ofqual. It is published to enable teachers to have an early sight of our proposed approach to this qualification. Further changes may be required, and no assurance can be given at this time that the proposed qualification will be made available in its current form, or that it will be accredited in time for first teaching in 2026.

Contents

1 Qualifications at a glance

1.1 Qualification structures

Key to units for these qualifications:

EA = External Assessment	We set and mark the exams for these units.
NEA = Non Examined Assessment	We set the assignment for these units. You assess the assignment and we moderate the assessment.
M = Mandatory	Students must complete these units.
O = Optional	Students must complete some of these units.
GLH = Guided Learning Hours	The teacher contact time needed to teach the content, plus the assessment time for the unit.

OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate)

For this qualification, students must complete two units:

- One mandatory externally assessed unit
- One mandatory NEA unit

OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate)

For this qualification, students must complete five units:

- Two mandatory externally assessed units
- One mandatory NEA unit
- Two optional NEA units

Unit no	Unit title	Unit ref no (URN)	Guided learning hours (GLH)	Assessment method	Certificate	Extended Certificate
F193	Fundamentals of cyber security	TBC	75	E	M	M
F194	Fundamentals of networks	TBC	70	E	-	M
F195	Preventing cyberattacks	TBC	75	N	M	M
F196	Digital forensic investigation	TBC	70	N	-	O
F197	Penetration testing and incident response	TBC	70	N	-	O
F198	Implementing secure local area networks (LANs)	TBC	70	N	-	O
F199	Designing and communicating secure global computing systems	TBC	70	N	-	O

1.2 Comparison between the Cambridge Advanced Nationals Qualifications and the Level 3 Cambridge Technicals qualification model

	Area of comparison	Approach used in these Level 3 Cambridge Advanced Nationals qualifications	Approach used in the Level 3 Cambridge Technicals qualification model	Reasons for the change
1	The size of the qualifications	Qualifications are available in two sizes • 150 GLH • 360 GLH The 150 GLH qualification includes nested units from the 360 GLH qualification.	Qualifications are typically available in the following sizes: • 180 GLH • 360 GLH • 540 GLH • 720 GLH • 1080 GLH	For this subject, the Department for Education allows: • a maximum size of 360 GLH for these qualifications. • a maximum of two qualification sizes.
2	Number and duration of external assessments	150 GLH qualification: • One externally assessed unit • Exam is 1 hour 15 minutes 360 GLH qualification: • Two externally assessed units • Exams are 1 hour 15 minutes	There are no exams in the 2012 qualifications. In the 2016 suite, there is a minimum requirement of 30% external assessment.	It is an Ofqual requirement to have 40% external assessment in these qualifications. The exam design is intended to aid accessibility and encourage student engagement while easing the exam burden for students and timetabling.
3	Format of the exam	Each exam is available in January and June and is paper-based.	Each exam is available in January and June and is mainly paper-based.	It is an Ofqual requirement to have two assessment opportunities per assessment.
4	Setting the NEA assignment	We will set all NEA assignments.	We provide a model assignment, or centres can set their own.	This is a requirement of our Regulator, Ofqual.
5	Lifespan of the assignment	Each assignment will remain live for **two** years, with a new assignment being released every year.	Assignments can be used for a number of years.	This is a requirement of our Regulator, Ofqual.
6	The approach to achieving unit grades on the NEA units and its impact on qualification outcomes	These take a 'compensatory' approach. This means that: • the unit grade students achieve is based on the **total** number of criteria achieved for that unit.	These take a 'hurdles' approach. This means students must achieve: • all Pass criteria to achieve a unit Pass • all Pass and Merit criteria to achieve a unit Merit.	The Cambridge Advanced Nationals qualifications are designed for academic progression. A compensatory approach rewards students for what they can do by

		• the total number can come from any combination of the Pass, Merit or Distinction criteria. • students do not have to achieve all criteria for a grade to achieve that grade (e.g. all Pass criteria to achieve a unit Pass). • if students do not achieve enough total criteria for a unit Pass, the criteria they do achieve will still earn uniform marks (UMS) which will count towards their qualification outcome. • The qualification outcome is based on the combined total UMS achieved for all units. This means that students may still pass the qualification if they achieve enough total marks, even if they do not pass all units. Every mark counts!	• all Pass, Merit and Distinction criteria to achieve a unit Distinction. • At least a Pass for each NEA unit to achieve the qualification (along with at least a near pass in the examined unit/s).	combining marks achieved to calculate a qualification outcome.
7	Number of NEA Assessment Criteria	Each NEA unit of the same size has a fixed and consistent number of Pass, Merit and Distinction assessment criteria, within and across qualifications.	The number of Pass, Merit and Distinction assessment criteria differs across units and qualifications.	This is to: • ensure a consistent approach to the awarding of units within each qualification and across qualifications in the suite. • aid familiarity of approach for teachers and students.
8	NEA Assessment Criteria design	There will be 24 assessment criteria for each NEA unit. Each assessment criterion is designed to: • assess one discrete task or activity • provide a yes/no approach to decision-making and achievement	There may be fewer assessment criteria for each unit, but these are typically broader, and may assess several tasks or activities in one criterion.	This is to: • ensure clarity of requirements for students in the form of discrete tasks or activities that they should evidence • simplify decision-making for teachers assessing students' work.

9	Introduced Performance Objectives for each unit	Each exam question and each Assessment Criterion in the NEA units is mapped to one of our four performance objectives.	These qualifications do not contain performance objectives.	To aid consistency of approach and demand to exams and assignments over time.
10	Moderation opportunities for the NEA assignments	Moderation is available twice each year in windows.	Moderation is available on-demand.	Typically, Level 3 Cambridge Advanced Nationals will be delivered in two years. This allows you the opportunity for two moderation activities in each academic year.
11	Moderation approach	Moderation takes the form of face-to-face or virtual visits between the centre and our moderator.	Moderation takes the form of face-to-face or virtual visits between the centre and our moderator.	We have kept this the same to reflect the most requested approach to moderation from centres since the pandemic This is to ease the moderation burden on centres, while still providing direct interaction with our moderator.
12	SAMs for NEA	Sample assignments are available for you to use as practice materials with students.	We do not provide sample assignments for practice purposes.	This is to ensure that students have access to sample assessment material for both the EA and NEA units.

2 Why choose OCR?

Choose OCR and you've got the reassurance that you're working with one of the UK's leading exam boards. We've developed our specifications in consultation with teachers, employers, subject experts and higher education institutions (HEIs) to give students a qualification that's relevant to them and meets their needs.

We're part of Cambridge University Press & Assessment. We help millions of people worldwide unlock their potential. Our qualifications, assessments, academic publications and original research spread knowledge, spark curiosity and aid understanding around the world.

We work with a range of education providers in both the public and private sectors. These include schools, colleges, HEIs and other workplaces. Over 13,000 centres choose our A Levels, GCSEs and vocational qualifications including Cambridge Nationals and legacy Cambridge Technicals.

2.1 Our specifications

We provide specifications that help you bring the subject to life and inspire your students to achieve more.

We've created teacher-friendly specifications based on extensive research and engagement with the teaching community. Our specifications are designed to be straightforward to deliver and accessible for students. The design allows you to tailor the delivery of the course to suit your needs.

2.2 Our support

We provide a range of support services to help you at every stage, from preparation to delivery:

- A wide range of high-quality creative resources including resources created by leading organisations in the industry.
- Textbooks and teaching and learning resources from leading publishers. The Cambridge Advanced Nationals page on our website has more information about all the published support for the qualifications that we have endorsed.
- Professional development for teachers to meet a range of needs. To join our training (either face-to-face or online) or to search for training materials, go to the Professional Development page on our website.
- Active Results which is our free results analysis service. It helps you review the performance of individual students or whole groups.
- ExamBuilder which is our free question-building platform. It helps you to build your own tests using past OCR exam questions.
- Our Subject Advisors, who give information and support to centres. They can help with specification and non examined assessment (NEA) advice, updates on resources developments and a range of training opportunities. They use networks to work with subject communities and share ideas and expertise to support teachers.

2.2.1 More help and support

Whether you are new to OCR or already teaching with us, you can find useful information, help and support on our website . Or get in touch:

support@ocr.org.uk
@ocrexams
01223 553998

2.3 People and Planet

We are part of Cambridge University Press & Assessment, which has clear commitments to champion sustainability, diversity, trust and respect for our people and planet.

We are committed to supporting a curriculum that helps young people develop an ethical view of the world. This enables them to take social responsibility, understand environmental issues and prepare them for the green jobs of the future.

Our equality, diversity, inclusion and belonging principles are that we:

- are respectful and considerate
- celebrate differences and promote positive attitudes to belonging
- include perspectives that reflect the diverse cultural and lifestyle backgrounds of our society
- challenge prejudicial views and unconscious biases
- promote a safe and supportive approach to learning
- are accessible and fair, creating positive experiences for all
- provide opportunities for everyone to perform at their best
- are contemporary, relevant and equip everyone to live and thrive in a global, diverse world
- create a shared sense of identity in a modern mixed society with one humanity.

To learn more, including our work on accessibility in our assessment materials, visit our People and Planet page.

2.4 Aims and learning outcomes

Our Cambridge Advanced Nationals in Cyber Security and Networks will encourage students to:

- develop key knowledge, understanding and skills, relevant to the subject
- think creatively, innovatively, analytically, logically and critically
- develop valuable communication skills that are important in all aspects of further study and life
- develop transferable learning and skills, such as communication, critical thinking, independent learning, planning, problem solving, research skills, resilience and time management that are important for progression to HE and can be applied to real-life contexts and work situations
- develop independence and confidence in applying the knowledge and skills that are vital for progression to HE and relevant to the digital technology (practitioners) sector and more widely.

2.5 What are the key features of this specification?

The key features of our Cambridge Advanced Nationals in Cyber Security and Networks for you and your students are:

- a simple and intuitive assessment model, that has:
    - externally assessed units, which focus on subject knowledge and understanding
    - applied and practical non examined assessment units (NEA)
    - optional NEA units to provide flexibility
- a specification developed with teachers specifically for teachers. The specification lays out the subject content, assessment criteria, teacher guidance and delivery requirements clearly
- a flexible support package made based on teachers’ needs. The support package will help teachers to easily understand the qualification and how it is assessed
- a team of Subject Advisors who directly support teachers
- a specification designed to:
    - complement A Levels and/or other Level 3 qualifications in a Post-16 study programme
    - develop wider transferable skills, knowledge and understanding desired by HEIs. More detail about the transferable skills these qualifications may develop is in Section 6.3

All Cambridge Advanced National qualifications offered by OCR are regulated by Ofqual, the Regulator for qualifications offered in England.

The qualification numbers for OCR’s Alternative Academic Qualification Cambridge Advanced Nationals in Cyber Security and Networks are:

- Certificate: QN TBC
- Extended Certificate: QN TBC

2.6 Acknowledgements

We would like to acknowledge the following Higher Education Providers for their input and support in designing these qualifications:
Anglia Ruskin University
Liverpool John Moores University
Manchester Metropolitan University
Nottingham Trent University
Staffordshire University
The University of Buckinghamshire

3 Qualification overview

3.1 OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate) overview

Qualification number	TBC
First entry date	01 September 2026
Guided learning hours (GLH)	150
Total qualification time (TQT)	200
OCR entry code	H037
Approved age range	16-18, 18+, 19+
Offered in	England only
Performance table information	This qualification is designed to meet the Department for Education's requirements for qualifications in the Alternative Academic Qualifications category of the 16-19 performance tables.
Eligibility for funding	This qualification meets funding approval criteria.
UCAS Points	This qualification is recognised in the UCAS tariff tables. You'll find more information on the UCAS website .
This qualification is suitable for students who:	• are age 16-19 and on a full-time study programme • want to develop applied knowledge and skills in cyber security and networks • want to progress onto other related study, such as higher education courses in computer science with cyber security, cyber security, cyber security and digital forensics and cyber security management.
Entry requirements	There is no requirement for students to achieve any specific qualifications before taking this qualification
Qualification requirements	Students must complete two units: • one externally assessed unit • one NEA unit
Assessment method/model	Unit F193 is assessed by an exam and marked by us. You will assess the NEA unit and we will moderate it. The NEA assignments are live for two years. The front cover details the intended cohort. You must make sure you use the live assignment that relates to the student's cohort for assessment and submit in the period in which the assignments are live. For example, a cohort beginning a two-year course in September 2026 should use the set of assignments marked as being for 2026-

	2028 so that whatever order assignments are taken in, they will be able to re-submit improved work on the same NEA assignment if they wish to during their study of the qualification. Centres should avoid allowing new cohorts to use assignments which have already been live for a year, e.g. students who start the course in September 2027 using assignments for the 2026-2028 cohorts. Centres must have suitable controls in place to ensure that NEA assignment work is completed by each student independently and must not allow previously completed work for assignments which are still live to be shared as examples with other students.
Exam series each year	• January • June
Exam resits	Students can resit the examined unit twice before they complete the qualification.
NEA submission	There are two windows each year to submit NEA outcomes and request a moderation visit. You must make unit entries for students before you can submit outcomes for a visit. All dates are on our administration pages.
Resubmission of students' NEA work	If students have not performed at their best in the NEA assignments, they can improve their work and submit it to you again for assessment. They must have your agreement and you must be sure it is in the student's best interests. We use the term 'resubmission' when referring to student work that has previously been submitted for moderation. Following moderation, a student can attempt to improve their work for you to assess and provide the final mark to us. There is one resubmission opportunity per NEA assignment. All work submitted (or resubmitted) must be based on the assignment that is live for assessment. For information about feedback see Section 7.3. The final piece of work must be completed solely by the student and teachers must not detail specifically what amendments should be made.
Grading	Information about unit and qualification grading is in Section 6.

3.2 OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate) overview

Qualification number	TBC
First entry date	01 September 2026
Guided learning hours (GLH)	360
Total qualification time (TQT)	500
OCR entry code	H137
Approved age range	16-18, 18+, 19+
Offered in	England only
Performance table information	This qualification is designed to meet the Department for Education's requirements for qualifications in the Alternative Academic Qualifications category of the 16-19 performance tables.
Eligibility for funding	This qualification meets funding approval criteria.
UCAS Points	This qualification is recognised in the UCAS tariff tables. You'll find more information on the UCAS website.
This qualification is suitable for students who:	• are age 16-19 and on a full-time study programme • want to develop applied knowledge and skills in cyber security and networks • want to progress onto other related study, such as higher education courses in computer networks, computer networks and cyber security, computer science with cyber security, cyber security, cyber security and digital forensics, cyber security management and ethical hacking and cyber security.
Entry requirements	There is no requirement for students to achieve any specific qualifications before taking this qualification
Qualification requirements	Students must complete five units: • two externally assessed units • three NEA units
Assessment method/model	Units F193 and F194 are assessed by an exam and marked by us. You will assess the NEA units and we will moderate them. The NEA assignments are live for two years. The front cover details the intended cohort. You must make sure you use the live assignment that relates to the student's cohort for assessment and submit in the period in which the assignments are live.

	For example, a cohort beginning a two-year course in September 2026 should use the set of assignments marked as being for 2026-2028 so that whatever order assignments are taken in, they will be able to re-submit improved work on the same NEA assignment if they wish to during their study of the qualification. Centres should avoid allowing new cohorts to use assignments which have already been live for a year, e.g. students who start the course in September 2027 using assignments for the 2026-2028 cohorts. Centres must have suitable controls in place to ensure that NEA assignment work is completed by each student independently and must not allow previously completed work for assignments which are still live to be shared as examples with other students.
Exam series each year	• January • June
Exam resits	Students can resit each examined unit twice before they complete the qualification.
NEA Submission	There are two windows each year to submit NEA outcomes and request a moderation visit. You must make unit entries for students before you can submit outcomes for a visit. All dates are on our administration pages.
Resubmission of students' NEA work	If students have not performed at their best in the NEA assignments, they can improve their work and submit it to you again for assessment. They must have your agreement and you must be sure it is in the student's best interests. We use the term 'resubmission' when referring to student work that has previously been submitted for moderation. Following moderation, a student can attempt to improve their work for you to assess and provide the final mark to us. There is one resubmission opportunity per NEA assignment. All work submitted (or resubmitted) must be based on the assignment that is live for assessment. For information about feedback see Section 7.3 . The final piece of work must be completed solely by the student and teachers must not detail specifically what amendments should be made.
Grading	Information about unit and qualification grading is in Section 6.

3.3 Purpose statement – Certificate

OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate)

Qualification number: TBC

Overview

Who this qualification is for

The OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate) is for students aged 16-19 years old. It will develop knowledge, understanding and skills that will help prepare you for progression to undergraduate study when taken alongside other qualifications and are relevant to the digital technology (practitioners) sector.

You might be interested in this qualification if you want a small qualification that builds applied or practical skills, to take alongside and enhance your A Levels or other Level 3 qualifications. You will have the opportunity to apply what you learn to real-life contexts, such as:

- Assessing for risks to networks, devices and applications and creating risk assessments.
- Auditing the measures used to prevent cyberattacks.
- Designing policies that control access to systems and educate users in cyberattack prevention.

This qualification will help you develop independence and confidence in using skills that are relevant to the sector and that prepare you for progressing to university courses where independent study skills are needed. You will develop the following transferable skills that can be used in both higher education and other life and work situations:

- Critical thinking and problem solving. You will explore the options, tools and techniques to tackle problems and use critical thinking skills to select the most appropriate solution. You will assess/audit current practices and design solutions, checking the outcome to see if the problem has been resolved.
- Independent learning and research skills. You will spend time outside of lessons learning about the latest cyber security threats and the measures used to prevent cyberattacks.
- Time management. It is important both in higher education and the digital technology (practitioners) sector that projects are delivered on time. You will learn techniques to effectively complete projects on time.

This qualification will complement other learning that you're completing at Key Stage 5. If you are a full-time student, it will be part of your studies along with your A Levels and/or other Level 3 qualifications.

What you will study when you take this qualification

Through a combination of theoretical study and hands-on experience, you will develop the necessary knowledge and skills that can support progression to higher education study in cyber security and networks.

In the examined unit, you will study key knowledge and understanding relevant to cyber security and networks. In the non examined assessment (NEA) unit, you will demonstrate knowledge and skills you learn by completing an applied assignment. More information about the knowledge and skills you will develop is below.

All units in the qualification are mandatory. You must take **all** of these units:

- F193: Fundamentals of cyber security

  This unit is assessed by an exam.

  In this unit you will learn why cyber security is important to us all and the motivations of different threat actors. You will learn what cyber security threats look like, how threats function and the steps that can be taken by individuals and organisations to protect, detect and respond to them. Topics include:

  - Topic Area 1 The cyber security landscape
  - Topic Area 2 Cyber security vulnerabilities
  - Topic Area 3 Impact of cyber security events
  - Topic Area 4 Cyber security mitigations
  - Topic Area 5 Policies, procedures, and event handling
  - Topic Area 6 Job roles and responsibilities

- F195: Preventing cyberattacks

  This unit is assessed by an assignment.

  In this unit you will learn techniques to assess for risks to networks, devices and applications and produce risk assessments. You will learn how to audit the measures used to prevent cyberattacks, design policies that control access to systems and educate users in cyberattack prevention. Topics include:

  - Topic Area 1 Cyber security aims and threats
  - Topic Area 2 Identify risks to networks and data
  - Topic Area 3 Audit and improve cyberattack prevention measures
  - Topic Area 4 Design access control policies
  - Topic Area 5 Design written user policies
  - Topic Area 6 Review designed cyberattack prevention measures

The subjects that complement this qualification

- Business
- Computer Science
- Design and Technology
- Engineering
- Information technology
- Maths.

The types of courses you may progress to

Both the subject-specific knowledge, understanding and skills, and broader transferable skills developed in this qualification will help you progress to further study in related areas such as:

- BSc (hons) Computer Networks and Cyber Security
- BSc (hons) Computer Science with Cyber Security
- BSc (hons) Cyber Security
- BSc (hons) Cyber Security and Digital Forensics
- BSc (hons) Cyber Security Management.

Why you should take the OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate)

There are two qualifications available in **Cyber Security and Networks**. These are:

OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate) – this is 150 GLH in size.

OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate) – this is 360 GLH in size.

You should take this Certificate qualification if you want a small Level 3 qualification that builds some applied knowledge and skills in cyber security and networks. This qualification is an Alternative Academic Qualification that is the same size as an AS Level qualification. It is half the size of an A Level. It could be taken alongside A Levels and/or other Level 3 qualifications to enhance your learning helping you to build broader knowledge and skills that are valued in undergraduate study, and relevant for progression to higher education. You would take this qualification alongside A Levels and/or other Level 3 qualifications as part of your study programme at Key Stage 5.

More information

More information about this qualification is in these documents:

- Sample Assessment Material (SAM) Question Papers:
  - Unit F193: <<insert link>>
- Guides to our SAM Question Papers:
  - Unit F193: <<insert link>>
- SAM Set Assignment(s):
  - Unit F195: <<insert link>>
- Student Guide to NEA Assignments: <<insert link>>

3.4 Purpose statement – Extended Certificate

OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate)

Qualification number: TBC

Overview

Who this qualification is for

The OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate) is for students aged 16-19 years old. It will develop knowledge, understanding and skills that will help prepare you for progression to undergraduate study and are relevant to the digital technology (practitioners) sector.

You might be interested in this qualification if you want to apply what you learn to practical, real-life contexts, such as:

- Assessing for risks to networks, devices and applications and creating risk assessments.
- Auditing the measures used to prevent cyberattacks.
- Designing policies that control access to systems and educate users in cyberattack prevention.
- Planning digital forensic investigations and using software tools to extract evidence.
- Planning authorised exploits on vulnerable systems.
- Creating cyber security incident response plans, incident playbooks and maintenance plans.
- Planning, designing, implementing, securing and testing local networks that meet client and user requirements.
- Planning, scoping, designing and securing global computing systems that meet client and user requirements.

This qualification will help you develop independence and confidence in using skills that are relevant to the sector and that prepare you for progressing to university courses where independent study skills are needed. You will develop the following transferable skills that can be used in both higher education and other life and work situations:

- Communicating effectively with individuals or groups. Communicating effectively with clients, users and other stakeholders is important in the digital technology (practitioners) sector. It is also a vital life-skill and important for progressing to and in, higher education.
- Critical thinking and problem solving. You will explore the options, tools and techniques to tackle problems and use critical thinking skills to select the most appropriate way to proceed. You will assess/audit current practices and design solutions, checking the outcome to see if the problem has been resolved.
- Independent learning and research skills. You will spend time outside of lessons learning about the latest cyber security threats and the measures used to prevent cyberattacks.
- Time management. It is important both in higher education and the digital technology (practitioners) sector that projects are delivered on time. You will learn techniques to effectively complete projects on time.

This qualification will complement other learning that you're completing at Key Stage 5. If you are a full-time student, it will be part of your studies along with A Levels and/or other Level 3 qualifications.

What you will study when you take this qualification

Through a combination of theoretical study and hands-on experience, you will develop the necessary knowledge and skills that can support progression to higher education study in cyber security and networks.

In the examined units, you will study key knowledge and understanding relevant to cyber security and digital networking. In the non examined assessment (NEA) units, you will demonstrate knowledge and skills you learn by completing applied or practical assignments. More information about the knowledge and skills you will develop is below.

The qualification has three mandatory units and four optional units.

These are the **mandatory** units – you must take **all** these units:

- F193: Fundamentals of cyber security

  This unit is assessed by an exam.

  In this unit you will learn why cyber security is important to us all and the motivations of different threat actors. You will learn what cyber security threats look like, how threats function and the steps that can be taken by individuals and organisations to protect, detect and respond to them. Topics include:

  - Topic Area 1 The cyber security landscape
  - Topic Area 2 Cyber security vulnerabilities
  - Topic Area 3 Impact of cyber security events
  - Topic Area 4 Cyber security mitigations
  - Topic Area 5 Policies, procedures, and event handling
  - Topic Area 6 Job roles and responsibilities

- F194: Fundamentals of networks

  This unit is assessed by an exam.

  In this unit you will learn about the fundamental concepts of networks, including different models, addressing techniques and protocols. You will also learn about the different hardware devices that are used in a network and how those devices are connected. Topics include:

  - Topic Area 1 Network types, models, topologies and services
  - Topic Area 2 Network layers, protocols and addressing
  - Topic Area 3 Wired network components
  - Topic Area 4 Mobile and wireless networks
  - Topic Area 5 Network Performance
  - Topic Area 6 Cloud networks

- F195: Preventing cyberattacks

  This unit is assessed by an assignment.

  In this unit you will learn techniques to assess for risks to networks, devices and applications and produce risk assessments. You will learn how to audit the measures used to prevent cyberattacks, design policies that control access to systems and educate users in cyberattack prevention. Topics include:

  - Topic Area 1 Cyber security aims and threats
  - Topic Area 2 Identify risks to digital networks and data
  - Topic Area 3 Audit and improve cyberattack prevention measures
  - Topic Area 4 Design access control policies
  - Topic Area 5 Design written user policies
  - Topic Area 6 Review designed cyberattack prevention measures

- F196: Digital forensic investigation

  This unit is assessed by an assignment.

  In this unit you will learn about digital forensics including the processes followed when completing digital forensic investigations. You will plan digital forensic investigations and use software tools to extract evidence and present evidence ready for use in court. Topics include:

  - Topic Area 1 Fundamentals of digital forensics
  - Topic Area 2 Plan digital forensic investigations
  - Topic Area 3 Collect, preserve and analyse digital evidence
  - Topic Area 4 Report digital forensic investigation findings
  - Topic Area 5 Review digital forensic investigations

- F197: Penetration testing and incident response

  This unit is assessed by an assignment.

  In this unit you will learn about penetration testing strategies and plan penetration tests. You will learn how to undertake planned exploits on vulnerable systems, using specific methods and tools. You will create cyber security incident response plans, incident playbooks and maintenance plans to build and upkeep incident response capability. Topics include:

  - Topic Area 1 Introduction to penetration testing
  - Topic Area 2 Plan penetration testing
  - Topic Area 3 Implement penetration testing scoping plans
  - Topic Area 4 Incident response planning
  - Topic Area 5 Develop cyber security incident response capability
  - Topic Area 6 Review penetration testing and incident response capability

- F198: Implementing secure local area networks (LANs)

  This unit is assessed by an assignment.

  In this unit you will learn the purpose and components of local area networks (LANs). You will then plan, design, implement, secure and test local networks that meet client and user requirements. Topics include:

  - Topic Area 1 Purpose and components of local area networks (LANs)
  - Topic Area 2 Design secure local area networks (LANs)
  - Topic Area 3 Implement and secure local area networks (LANs)
  - Topic Area 4 Test local area networks (LANs)
  - Topic Area 5 Review and maintain local area network (LAN) performance and security

- F199: Designing and communicating secure global computing systems

  This unit is assessed by an assignment.

  In this unit you will learn about technologies that allow networked computing systems to interconnect across multiple sites. You will plan, scope and design secure global computing systems that meet client and user requirements and use software simulators to test the intended function. You will also learn how to communicate effectively with clients. Topics include:

  - Topic Area 1 Fundamentals of secure global computing systems
  - Topic Area 2 Plan and scope secure global computing systems
  - Topic Area 3 Design secure global computing systems
  - Topic Area 4 Simulate and test secure global computing systems
  - Topic Area 5 Communicate and review secure global computing systems

The subjects that complement this qualification

- Business
- Computer Science
- Design and Technology
- Engineering
- Information technology
- Maths.

The types of courses you may progress to

Both the subject-specific knowledge, understanding and skills, and broader transferable skills developed through these units, will help you progress to further study in related areas such as:

- BSc (hons) Computer Networks
- BSc (hons) Computer Networks and Cyber Security
- BSc (hons) Computer Networks Engineering
- BSc (hons) Computer Networks and Security
- BSc (hons) Computer Science with Cyber Security
- BSc (hons) Cyber Security
- BSc (hons) Cyber Security and Digital Forensics
- BSc (hons) Cyber Security Management
- BSc (hons) Ethical Hacking and Cyber Security.

Why you should take the OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate)

There are two qualifications available in Cyber Security and Networks. These are:

OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate) – this is 150 GLH in size

OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate) – this is 360 GLH in size

You should take this Extended Certificate qualification if you want a Level 3 qualification that builds applied knowledge and skills in cyber security and networks. This qualification is an Alternative Academic Qualification that is the same size as an A Level. When it is taken alongside other Level 3 qualifications, it will complement them, helping you to build broader knowledge and skills that are valued in undergraduate study, and relevant for progression to higher education. You would take this qualification alongside other Level 3 qualifications as part of your study programme at Key Stage 5.

More information

More information about this qualification is in these documents:

- Sample Assessment Material (SAM) Question Papers:
  - Unit F193: <<insert link>>
  - Unit F194: <<insert link>>
- Guides to our SAM Question Papers:
  - Unit F193: <<insert link>>
  - Unit F194: <<insert link>>
- SAM Set Assignment(s):
  - Unit F195: <<insert link>>
  - Unit F196: <<insert link>>
  - Unit F197: <<insert link>>
  - Unit F198: <<insert link>>
  - Unit F199: <<insert link>>
- Student Guide to NEA Assignments: <<insert link>>

4 About these qualifications

4.1 Qualification size

The size of each qualification is described in terms of Guided Learning Hours (GLH) and Total Qualification Time (TQT).

GLH indicates the approximate time (in hours) you will spend supervising or directing study and assessment activities. We have worked with people who are experienced in delivering related qualifications to determine the content that needs to be taught and how long it will take to deliver.

TQT includes two parts:

- GLH
- an estimate of the number of hours a student will spend on unsupervised learning or assessment activities (including homework) to successfully complete their qualification.

The OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate) is 150 GLH and 200 TQT.

The OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate) is 360 GLH and 500 TQT.

4.2 Availability and language

The Level 3 Alternative Academic Qualification Cambridge Advanced Nationals are available in England only. They are **not** available in Wales or Northern Ireland.

The qualifications and their assessment materials are available in English only. We will only assess answers written in English.

4.3 Prior knowledge and experience

Recognition of prior learning (RPL) is the process for recognising learning that never received formal recognition through a qualification or certification. It includes knowledge and skills gained in school, college or outside of formal learning situations. These may include:

- domestic/family life
- education
- training
- work activities
- voluntary activities.

In most cases RPL will not be appropriate for directly evidencing the requirements of the NEA assignments for the Cambridge Advanced National qualifications. However, if you feel that your student could use RPL to support their evidence, you must follow the guidance provided in our RPL Policy.

5 Units

5.1 Guidance on unit content

This section describes what must be taught so that students can access all available marks and meet assessment criteria.

5.1.1 Externally assessed units (F193 and F194)

The externally assessed units contain a number of topic areas.

For each topic area, we list the **teaching content** that must be taught and give information on the **breadth and depth** of teaching needed.

Teaching content

Questions can be asked about anything in the teaching content or breadth and depth columns

Breadth and depth

The breadth and depth column:

- clarifies the breadth and depth of teaching needed
- indicates the range of knowledge and understanding that can be assessed in the exam
- confirms any aspects that you do not need to teach as 'does not include' statements.

Teaching must cover **both** the **teaching content** and **breadth and depth** columns.

Knowledge and understanding

This is what we mean by knowledge and understanding:

Knowledge	• Be able to identify or recognise an item, for example on a diagram. • Use direct recall to answer a question, for example the definition of a term.
Understanding	• To assess and evidence the perceived meaning of something in greater depth than straight identification or recall. • Understanding will be expressed and presented using terms such as: how; why; when; reasons for; advantages and disadvantages of; benefits and limitations of; purpose of; suitability of; recommendations for improvement; appropriateness of something to/in different contexts.

Students will need to **understand** the content, unless the breadth and depth column identifies it as knowledge only.

Any item(s) that should be taught as **knowledge** only will start with the word 'know' in the breadth and depth column.

All other content must be taught as understanding.

5.1.2 NEA units (F195-F199)

The NEA units contain a number of topic areas.

For each topic area, we list **teaching content** that must be taught and give **exemplification**. The exemplification shows the teaching expected to equip students to successfully complete their assignments.

5.1.3 Command words

Appendix B gives information about the command words that will be used in the external assessments and the NEA assessment criteria.

5.1.4 Performance objectives (POs):

Each Cambridge Advanced National qualification has four Performance Objectives.

PO1	Show knowledge and understanding
PO2	Apply knowledge and understanding
PO3	Analyse and evaluate knowledge, understanding and performance
PO4	Demonstrate and apply skills and processes relevant to the subject

PO1 is assessed in the externally assessed unit only.

PO4 is assessed in the NEA units only.

The weightings of the Performance Objectives across the units in the **Certificate** qualification are:

Performance Objective	**Externally Assessed unit (range)**	**NEA unit**	**Overall weighting**
PO1	16.7-25%	n/a	16.7-25%
PO2	12.5-20.8%	16.7%	29.2-37.5%
PO3	12.5%	16.7%	29.2%
PO4	n/a	16.7%	16.7%
Overall weighting of assessments	**50%**	**50%**	**100%**

The weightings of the Performance Objectives across the units in the **Extended Certificate** qualification are:

Performance Objective	**Externally Assessed unit (range)**	**NEA units**	**Overall weighting**
PO1	13.3%-20%	n/a	13.3%-20.0%
PO2	10-16.7%	18.3%-20.8%	28.3%-37.5%
PO3	10%	17.5%-20.8%	27.5%-30.8%
PO4	n/a	18.3%-24.2%	18.3%-24.2%
Overall weighting of assessments	**40%**	**60%**	**100%**

5.2 Externally assessed units

5.2.1 Unit F193: Fundamentals of cyber security

Unit aim

Individuals and organisations are more connected than ever before and more and more of our everyday activities are being completed using digital devices. This has led to an increase in the risk that our data and information is being accessed, destroyed and used without our knowledge. Protecting this data and information has become an area of major importance. As a result, cyber security is now one of the biggest employment growth areas in the IT sector. Understanding how data and information can be protected, and how threats can be detected is now a highly desirable skill set.

In this unit you will learn why cyber security is important to us all and how to identify possible vulnerabilities to individuals and organisations. You will learn about the different actors who threaten the cyber security of individuals and organisations and their motivations for doing it. You will also learn what threats look like, how they function and the steps that can be taken by individuals and organisations to protect, detect and respond to them. Finally, you will learn about some of the job roles involved in cyber security and the skills required to work in these roles.

Unit F193: Fundamentals of cyber security	
Topic Area 1: The cyber security landscape	
Teaching content	**Breadth and depth**
1.1 Importance and key concepts of cyber security	
1.1.1 Cyber security □ Definition □ Importance	To include: □ Know what cyber security is □ Know the importance of cyber security for individuals □ Know the importance of cyber security for organisations and society
1.1.2 CIA triad □ Confidentiality □ Integrity □ Availability	To include: □ Know what the CIA triad is □ How CIA can be applied to security systems □ The importance of maintaining CIA
1.1.3 IAAA principles □ Identification □ Authentication □ Authorisation □ Accountability	To include: □ Know what the IAAA is □ Know the purpose of IAAA □ The benefits of how IAAA enhances cyber security
1.1.4 Risk management □ Threats and vulnerabilities □ Impact of threats and vulnerabilities □ Probability □ Mitigations • Proactive • Reactive	To include: □ Know the purpose of risk management □ Know how to identify threats and vulnerabilities □ The benefits and limitations of risk management □ The process of carrying out risk management

1.2 Types of cyber security incidents	
□ Destruction of data □ Environmental/physical □ Inaccessibility of data □ Information disclosure □ Modification of data □ Theft • Finance • Identity • Industrial secrets • Military secrets □ Unauthorised access/hacking	To include: □ Know what each incident type is □ Know how each type of incident can take place □ That cyber security incidents can be accidental in nature □ That cyber security incidents can be deliberate in nature □ The purpose of each incident type
1.3 Targets of cyber security incidents	
1.3.1 Human □ Individuals □ Organisations □ Nation states	To include: □ How individuals are targeted □ Why individuals are targeted □ How organisations are targeted □ Why organisations are targeted □ How nation states are targeted □ Why nation states are targeted Does not include: □ Details of methods of attack
1.3.2 System □ Data/information • Business • Classified • Financial • Personal • Public • At rest • In transit □ Infrastructure • Devices ○ Console ○ Desktop ○ Laptop ○ Smartphone ○ Tablet/hybrid ○ Servers ▪ Database ▪ File ▪ Hypervisor ▪ Mail ▪ Network ▪ Web • Networking and communications ○ Wired ○ Wireless	To include: □ Know what parts of a system can be targeted □ Know how parts of systems can be targeted □ Why different parts of a system may be attacked Does not include: □ Details of methods of attack

□ Data Storage Location • Onsite • Cloud ○ Private ○ Public ○ Hybrid ○ Community	
1.4 Actors and motivations	
1.4.1 Actors □ Competitor □ Cyber criminal □ Cyber terrorist □ Hacker • White hat • Grey hat • Black hat □ Hacktivist □ Insider □ Nation state □ Phisher □ Scammer □ Script kiddie	To include: □ The characteristics and traits of each type of actor
1.4.2 Motivations □ Accidental □ Intentional • Espionage • Revenge ○ Right perceived wrong ○ Score settling • Publicity • Fraud • Thrill • Income generation • Political gain	To include: □ Why different actors are motivated to carry out cyberattacks □ The features and characteristics of each motivation

Topic Area 2: Cyber security vulnerabilities	
Teaching content	**Breadth and depth**
2.1 Vulnerability vectors	
□ Cloud □ Direct access to network □ Email/social media □ Removable media □ Third party access • Suppliers/vendors • Workers □ Wireless networks	To include: □ How access can be gained to data by different vulnerability vectors □ The advantages and disadvantages of each vulnerability vector
Physical vulnerabilities	
2.2.1 Human based □ Not following policies □ Competency levels □ Poor Policies □ Poor screening □ Poor data habits □ Malicious employees	To include: □ The features and characteristics of each vulnerability □ How human mistakes cause vulnerabilities in digital systems □ How humans are manipulated to create vulnerabilities in digital systems

□ Disguised criminals □ State sponsored □ Targeted attack □ Social engineering □ Access controls • Poor door access control • Recycled codes • Poor monitoring of access/areas • Unnecessary access rights	□ How humans can deliberately create vulnerabilities in digital systems □ How each vulnerability causes increased cyber security risks
2.2.2 Natural disasters □ Earthquakes □ Fire □ Severe weather events	To include: □ Know how natural disasters can impact cyber security □ The importance of considering natural disasters when planning cyber security
2.3 System vulnerabilities	
Digital methods □ Botnets □ Malware □ Denial of Service (DoS) □ Distributed Denial of Service (DDoS) □ Hacking □ Lack of supplier support □ Malicious spam □ Man in the middle □ Out of date • Software • Hardware • Firmware	To include: □ The purpose of each digital method □ The features and characteristics of each digital methods □ How the different digital methods create vulnerabilities in a digital system □ What vulnerabilities vectors can be attacked by each digital method

Topic Area 3: Impact of cyber security events	
Teaching content	**Breadth and depth**
3.1 Disruption	
□ Financial disruption □ Information disruption □ Operational disruption □ Service disruption	To include: □ Know how cyber security events cause disruption to a range of targets □ The effects of disruption on a range of targets
3.2 Loss	
□ Data availability □ Financial □ Identity □ Integrity □ Reputation/customer confidence	To include: □ Know how cyber security events result in different types of loss to a range of targets □ The effects of loss on a range of targets in the short and long term
3.3 Safety	
□ Financial □ Personal safety □ Society □ Transport systems □ Utilities/services	To include: □ Know how cyber security events cause safety issues to a range of targets

Topic Area 4: Cyber security mitigations	
Teaching content	**Breadth and depth**
4.1 Endpoint mitigation measures	
□ Air gap □ Anomaly based system □ Anti-malware □ Anti-virus □ Backup □ Cryptography □ Encryption • At rest • In transit □ Firewalls • Hardware • Software □ Identity and access controls • Access rights • Levels of privilege • Password • Separation of duties □ Machine Learning (ML) and Artificial Intelligence (AI) systems □ Network segregation • Virtual Local Area Network (VLAN) • Physical separation • Offline network □ Physical controls • Alarm • Biometrics • Cable locks • Cameras • Locks • Radio-Frequency Identification (RFID) • Safe • Swipe cards □ Physical location • On site • Remote • Above floor levels □ Quantum cryptography □ Two-Factor Authentication (2FA) □ Virtual Private Network (VPN) □ Whitelist/blacklist	To include: □ Know what endpoint mitigation is □ Know the risk each mitigation can counter □ The features and characteristics of each mitigation method which enable them to counter risks □ The advantages and disadvantages of each mitigation method

4.2 Detection measures	
□ Behavioural analytics □ Emerging technologies □ Honeypot □ Intrusion detection systems • Intrusion Detection System (IDS) • Network Intrusion Detection System (NIDS) • Host Intrusion Detection System (HIDS) • Decentralised Intrusion Detection System (DIDS) □ Intrusion prevention systems □ Network monitoring □ Vulnerability testing	To include: □ Know the risk each mitigation can counter □ Know the features and characteristics of each detection method □ The advantages and disadvantages of each detection method
4.3 Intelligence assessment	
□ Human intelligence □ Open-source intelligence	To include: □ The purpose and use of each intelligence form □ The features and characteristics of each intelligence form □ How each intelligence form can be used in cyber security mitigation

Topic Area 5: Policies, procedures and event handling	
Teaching content	**Breadth and depth**
5.1 Policies and procedures	
□ AUP (Acceptable Use Policy) □ BYOD (Bring Your Own Device) policy □ Credential management policy □ Information security policy □ Remote working policy □ Staff training	To include: □ What a policy is □ Why policies are required □ The purpose and use of each policy □ The procedures covered in each policy □ How each policy improves cyber security Does not include: □ Details of each policy's contents
5.2 Event handling	
□ Responsibilities □ Roles □ Procedures □ Incident report • Title and date of incident • Target • Category ○ Critical ○ Significant ○ Minor ○ Negligible • Description of incident • Type of attacker(s) • Attack vector attacked • Attack method used by attacker(s) • Effect/impact of incident	To include: □ Know how to respond to a cyber security event □ Know the roles and responsibilities of individuals when responding to a cyber security event □ The procedures followed after a cyber security event has been identified □ Know the components of a cyber security incident report □ How a cyber security incident report is used Does not include: □ The creation of cyber security incident reports from scratch

• Responses required ○ Internal stakeholder notifications ○ External stakeholder notifications ○ Mitigations • Future management ○ Recommendations for change	
5.3 Legislation, regulations and standards	
Legislation/regulations □ Computer Misuse Act (CMA) □ Data Protection Act (DPA) □ UK General Data Protection Regulation (UK GDPR) Standards □ ISO 27001 Information security management	To include: □ Know what the latest version of each Act/regulation is □ Know the main purpose(s) of each Act/regulation □ How each Act/regulation impacts cyber security □ The steps that must be taken to comply with each Act/regulation □ The consequences of not complying with each Act/regulation □ The main purpose of the standard □ How the standard impacts cyber security □ The steps that must be taken to comply with the standard □ The benefits of meeting the standard Does not include: □ Knowing the detailed content of each Act/regulation or standard

Topic Area 6: Job roles and responsibilities	
Teaching content	**Breadth and depth**
6.1 General cyber security roles	
□ Computer forensic engineer □ Cyber security analyst □ Cyber security officer □ IT security compliance analysts □ Network security engineer □ Penetration tester	To include: □ Know the main responsibilities of job roles in cyber security prevention and response Does not include: □ Detailed job description for each job role and qualifications required
6.2 Communication skills	
□ Verbal □ Written □ Non-verbal □ Appropriate language to meet the needs of the audience □ Questioning techniques to elicit specific information	To include: □ How communication skills increase cyber security risks □ How communication skills contribute to cyber security mitigation development □ Know how communication skills can be used in a cyber security incident response

Assessment guidance

This unit is assessed by an exam. The exam is 1 hour and 15 minutes and has **60** marks in total. All questions in the exam are compulsory.

The exam will **always** have:

A short scenario	• This will develop through the paper.
Questions to assess Performance Objectives 1, 2, and 3	• PO1: these questions will require students to recall generic knowledge and understanding. • PO2: these questions will require students to apply knowledge and understanding. • PO3: these questions will require students to analyse and evaluate knowledge, understanding and performance in relation to the scenario.
A range of question types	• Forced choice/controlled response questions. • Short answer, closed response questions. • Extended constructed response questions with points-based marks schemes. • Extended constructed response questions with levels of response marks schemes. • One six mark and one nine mark extended constructed response question with a levels of response marks scheme
Questions relating to each Topic Area	• Content will be sampled from all topic areas, with at least one question or part question relating to each topic area.

This will be conducted under examination conditions. For more details refer to the Administration area.

The guide to our Sample Assessment Material for this unit gives more information about the layout and expectations of the exam.

The exam for this unit assesses the following Performance Objectives:

- PO1 – Show knowledge and understanding
- PO2 – Apply knowledge and understanding
- PO3 – Analyse and evaluate knowledge, understanding and performance.

Synoptic assessment

This unit allows students to gain underpinning knowledge and understanding relevant to the qualification and sector. The NEA units draw on and strengthen this learning with students applying their learning in an applied and practical way.

The following NEA units have synoptic links with this unit. The synoptic grids at the end of these NEA units show these synoptic links.

- F195: Preventing cyberattacks
- F196: Digital forensic investigation
- F197: Penetration testing and incident response
- F198: Implementing secure local area networks (LANs)
- F199: Designing and communicating secure global computing systems

More information about synoptic assessment in these qualifications can be found in Section 6.2 Synoptic Assessment.

5.2.2 Unit F194: Fundamentals of networks

Unit aim

Networks are one of the main areas targeted by cyber criminals and to be proactive in preventing attacks, a solid understanding of network fundamentals and concepts is needed. It is not possible to plan, design, build, support and keep a network secure unless the key concepts are known and understood. Unfortunately, cyber criminals have often learned these concepts to use in their attacks. This means it is critical that those wanting to protect networks are equally, if not better, equipped with the key knowledge and skills to prevent them.

In this unit you will learn the underpinning fundamentals and concepts of networks, including different models, addressing techniques and protocols. You will learn about the different hardware devices that are used in a network and how those devices are connected. To truly understand networks, you need to understand different number systems, how to convert between them and how they are used in network data transfer. This is where an understanding of some underlying mathematical concepts is required. Networks extend beyond physical boundaries of an office or site, and you will also learn about mobile and cloud computing environments.

Unit F194: Fundamentals of networks	
Topic Area 1: Network types, models, topologies and services	
Teaching content	**Breadth and depth**
1.1 Network types	
□ Personal Area Network (PAN) □ Local Area Network (LAN) • Intranet • Extranet □ Wireless Local Area Network (WLAN) □ Metropolitan Area Network (MAN) □ Wide Area Network (WAN) □ Storage Area Network (SAN) □ Virtual Private Network (VPN)	To include: □ The purpose and use of each network type □ The features and characteristics of each network type □ The advantages and disadvantages of each network type
1.2 Network models	
□ Client-server □ Peer-to-peer □ Thin client	To include: □ The purpose and use of each network model □ The features and characteristics of each network model □ The advantages and disadvantages of each network model
1.3 Network topologies	
□ Hybrid □ Partial mesh □ Point-to-point □ Star • Distributed star □ Tree □ Wireless	To include: □ The use of each topology □ The characteristics of each topology □ The advantages and disadvantages of each topology □ The difference between a logical and physical topology Does not include: □ Bus □ Ring

1.4 Network Services	
□ Domain controller □ Domain Name System (DNS) □ Email □ Firewall □ Internet access □ Intrusion detection systems (IDS) □ Intrusion prevention systems (IPS) □ Proxy □ Routing □ Voice □ VPN termination	To include: □ The roles of each service □ The use of each service in a network

Topic Area 2: Network layers, protocols and addressing	
Teaching content	**Breadth and depth**
2.1 Network layers	
□ Transmission Control Protocol/Internet Protocol (TCP/IP) layer model • Application layer • Transport layer • Internet layer • Network access layer	To include: □ The features and characteristics of the TCP/IP layer model □ The features, characteristics and function of the layers □ How data is transmitted between the layers □ The process of encapsulation and decapsulation Does not include: □ The OSI model
2.2 Network protocols	
□ Dynamic Host Configuration Protocol (DHCP) □ File Transfer Protocol (FTP) □ Hypertext Transfer Protocol (HTTP) □ Hypertext Transfer Protocol Secure (HTTPS) □ Internet Message Access Protocol (IMAP) □ Internet Protocol (IP) □ Network Time Protocol (NTP) □ Post Office Protocol (POP) □ Secure Socket Layer (SSL) □ Simple Mail Transfer Protocol (SMTP) □ Voice Over Internet Protocol (VOIP) □ Transport Control Protocol (TCP) □ User Datagram Protocol (UDP) □ Ethernet	To include: □ The features and characteristics of each protocol □ The use of each protocol □ The terminology associated with each protocol

2.3 Network Addressing	
□ Media Access Control (MAC) □ Internet Protocol Version 4 (IP V4) □ Internet Protocol Version 6 (IP V6) □ IP Addressing • Network classes ○ A, B and C ○ D and E • Automatic Private IP Addressing (APIPA) • Classless • Dynamic/static • Loopback • Network Address Translation (NAT) • Private/public • Reservations □ Subnetwork/subnet • Subnet mask/netmask □ Default gateway address	To include: □ The features and characteristics of each type of addressing method □ The use of each type of addressing method □ The purpose of each type of addressing method □ The differences between each type of addressing method □ The advantages and disadvantages of each type of addressing method □ How devices obtain IP addresses □ Default subnet masks for each network class □ How to complete subnet calculations

Topic Area 3: Wired network components	
Teaching content	**Breadth and depth**
3.1 Communications media	
Network transmission media □ Copper media • Coaxial • Twisted pair ○ Shielded Twisted Pair (STP) ○ Unshielded Twisted Pair (UTP) □ Optical media • Fibre optics	To include: □ The categories of transmission media □ The purpose and use of each type of transmission media □ The features and characteristics of each type of transmission media □ The advantages and disadvantages of each type of transmission media
3.2 Network connection devices	
□ Bridge • Source routing • Transparent □ Brouter (Bridging router) □ Gateway □ Network Interface Card (NIC) □ Repeater □ Router □ Switch • Layer 2 • Layer 3	To include: □ The purpose and use of each device □ The features and characteristics of each device □ The advantages and disadvantages of each device

3.3 Host devices	
□ Laptops □ Mobile handheld devices □ PCs □ Printers □ Servers • Application • Database • Email • File • Hypervisor (virtual machine monitor) • Print • Web □ VOIP Phones	To include: □ The purpose and use of each device □ The features and characteristics of each device

Topic Area 4: Mobile and wireless networks	
Teaching content	**Breadth and depth**
4.1 Transmission media	
□ Microwave transmission □ Wireless media • Bluetooth • Infra-red • Laser • Radio	To include: □ The purpose and use of each transmission media □ The features and characteristics of each transmission media □ The differences between each transmission media □ The advantages and disadvantages of each transmission media
4.2 Connectivity	
4.2.1 Technologies used in connecting cellular/mobile networks □ Advance mobile phone service (AMPS) □ Code-division multiple access (CDMA) □ Global System for Mobile Communications (GSM) □ Long Term Evaluation (LTE) □ Time-division multiple access (TDMA)	To include: □ The purpose and use of each technology □ The features and characteristics of each technology
4.2.2 Hardware used in connecting mobile/wireless networks □ Wireless Access Point (WAP) □ Wireless Network Interface Controller (WNIC)	To include: □ The purpose and use of each item of hardware □ The features and characteristics of each item of hardware

4.3 Concepts of mobile and wireless networks	
4.3.1 Mobile and wireless network concepts □ Access Points (APs)/Wireless Access Point (WAP) □ Bands and Channels □ Frequencies □ Service Set Identifier (SSIDs) □ Wireless Security • Security protocols • Authentication ○ WPA/WPA2 Enterprise (Radius) ○ WPA/WPA2 Personal (WPA-PSK) ○ WPA3 • Authorisation	To include: □ The purpose and use of each concept □ The features and characteristics of each concept □ The advantages and disadvantages of each concept
4.3.2 Radio Frequency (RF) concepts □ Amplitude □ Attenuation □ Bandwidth □ Modulation □ Phase □ Wavelength	To include: □ The purpose and use of each RF concept □ The features and characteristics of each RF concept
4.3.3 Mobile Network Antennas □ Bi-directional □ Omni-directional □ Semi-directional	To include: □ The purpose and use of each type of antennae □ The features and characteristics of each type of antennae □ The advantages and disadvantages of each type of antennae □ The differences between each type of antennae
4.4 Networking standards	
4.4.1 Mobile networking standards □ Broadband cellular network generation technology standards □ Wideband wireless digital communication systems • Code Division Multiple Access (CDMA) • Orthogonal Frequency Division Multiplexing (OFDM)	To include: □ The purpose and use of each mobile networking standard □ The features, characteristics, and properties of each mobile networking standard □ The differences between each mobile networking standard □ The purpose and use of each wideband wireless digital communication system □ The features, characteristics, and properties of each wideband wireless digital communication system □ The differences between wideband wireless digital communication systems
4.4.2 Wireless Networking Standards □ Bluetooth □ Institute of Electrical and Electronics Engineers IEEE 802.11 (WIFI)	To include: □ The purpose and use of each wireless networking standard □ The features, characteristics, and properties of each wireless networking standard □ The differences between each wireless networking standard

4.5 Global Positioning System (GPS)	
□ Global Positioning System (GPS)	To include: □ The purpose and use of GPS □ The features, characteristics and properties of GPS □ The advantages and disadvantages of GPS

Topic Area 5: Network Performance	
Teaching content	**Breadth and depth**
5.1 Network performance indicators	
□ Bandwidth □ Data Transfer Rate (DTR) □ Latency □ Throughput	To include: □ The purpose and use of each indicator □ The features and characteristics of each indicator
5.2 Network data transfer rate measurement	
5.2.1 Units of data transfer rate measurement □ Data Transfer Rate (DTR) □ Bits per second (bps) □ Bit, nibble (4 bits) and byte (8 bits) □ Binary units • Kibibyte (KiB) • Mebibyte (MiB) • Gibibyte (GiB) • Tebibyte (TiB) • Pebibyte (PiB) • Exbibyte (EiB) □ Metric/decimal units • Kilobyte (KB) • Megabyte (MB) • Gigabyte (GB) • Terabyte (TB) • Petabyte (PB) • Exabyte (EB)	To include: □ Know the meaning of data transfer rate □ Know what a good data transfer rate is □ The range of data transfer rates through different network types and media □ Know different units of data transfer □ Know what bit, nibble and byte are □ The difference between binary and metric measurements • 1 KiB = 1024 bytes (binary) • 1 KB = 1000 bytes (metric) □ How to convert between different units of DTR measurement
5.2.2 Network Performance Calculations □ Bandwidth requirements □ Data transfer speed □ Duration of data transfer (time)	To include: □ Know the formulas • Bandwidth requirements: ○ For each application: application requirement * simultaneous users ○ Add each application together • Data transfer speed = size of data / transfer time • Duration of data transfer (time) = data size / speed □ The difference between best and typical DTR calculations □ How to complete best and typical DTR calculations

5.3 Factors affecting network performance	
□ Bandwidth □ Data Transfer Rate (DTR) □ Distance □ Environmental □ Interference □ Intervening objects □ Jitter □ Latency □ Medium □ Reliability □ Signal strength □ Throughput	To include: □ How each factor affects network performance □ How network performance issues caused by each factor can be resolved

Topic Area 6: Cloud networks	
Teaching content	**Breadth and depth**
6.1 Cloud environments	
6.1.1 Cloud types □ Community □ Hybrid □ Private □ Public	To include: □ The purpose and use of each cloud type □ The features and characteristics of each cloud type □ The differences between each cloud type □ The advantages and disadvantages of each cloud type
6.1.2 Cloud service models □ Anything (or everything)-as-a-Service (Xaas) □ Communication-as-a-Service (CaaS) □ Infrastructure-as-a-Service (IaaS) □ Platform-as-a-Service (PaaS) □ Software-as-a-Service (SaaS)	To include: □ The purpose and use of each model □ The features and characteristics of each model □ The differences between the types of model
6.1.3 Cloud computing techniques □ Cloud Automation □ Cloud Bursting □ Cloud Elasticity □ Cloud Orchestration □ Clustering □ Multi-tenancy □ Resource pooling • Computer • Networks • Storage □ Ubiquitous network access	To include: □ The purpose and use of each cloud computing technique □ The features and characteristics of each cloud computing technique
6.2 Network virtualisation	
6.2.1 Types of virtualisation □ Application virtualisation □ Data virtualisation □ Desktop virtualisation □ Network virtualisation • External • Internal □ Server virtualisation □ Storage virtualisation	To include: □ The purpose and use of each type of virtualisation □ The features and characteristics of each type of virtualisation □ The differences between the virtualisation types □ The advantages and disadvantages of each type of virtualisation

Assessment guidance

This unit is assessed by an exam. The exam is 1 hour and 15 minutes and has **60** marks in total. All questions in the exam are compulsory.

The exam will **always** have:

A short scenario	• This will develop through the paper.
Questions to assess Performance Objectives 1, 2, and 3	• PO1: these questions will require students to recall generic knowledge and understanding. • PO2: these questions will require students to apply knowledge and understanding. • PO3: these questions will require students to analyse and evaluate knowledge, understanding and performance in relation to the scenario.
A range of question types	• Forced choice/controlled response questions. • Short answer, closed response questions. • Short answer questions with calculation/working • Extended constructed response questions with points-based marks schemes. • Extended constructed response questions with levels of response marks schemes. • One six mark and one nine mark extended constructed response question with a levels of response marks scheme
Questions relating to each Topic Area	• Content will be sampled from all topic areas, with at least one question or part question relating to each topic area.

This will be conducted under examination conditions. For more details refer to the Administration area.

The guide to our Sample Assessment Material for this unit gives more information about the layout and expectations of the exam.

gives more information about the layout and expectations of the exam.

The exam for this unit assesses the following Performance Objectives:

- PO1 – Show knowledge and understanding
- PO2 – Apply knowledge and understanding
- PO3 – Analyse and evaluate knowledge, understanding and performance.

Synoptic assessment

This unit allows students to gain underpinning knowledge and understanding relevant to the qualification and sector. The NEA units draw on and strengthen this learning as students will apply their learning to practical and applied tasks.

The following NEA units have synoptic links with this unit. The synoptic grids at the end of these NEA units show these synoptic links.

- F195: Preventing cyberattacks
- F196: Digital forensic investigation
- F197: Penetration testing and incident response
- F198: Implementing secure local area networks (LANs)
- F199: Designing and communicating secure global computing systems

More information about synoptic assessment in these qualifications can be found in Section 6.2 Synoptic Assessment.

5.3 NEA Units

5.3.1 Unit F195: Preventing cyberattacks

Unit Aim

When connected to the internet, networks, devices, applications and data face significant risk from cyber security threats daily. However, there are practical steps that can be taken to reduce the impact of cyberattacks and other security breaches. These can help to keep critical networks, devices, and applications operational and data safe.

In this unit you will learn concepts of cyber security, threats that can compromise networks and countermeasures that can prevent cyberattacks. Your learning will help you understand how to assess for risks to networks, devices and applications and produce risk assessments. You will also learn how to audit the measures used on networks, devices, and applications to prevent cyberattacks, making recommendations, and demonstrating how these can be improved. Finally, you will learn how to design policies which control access to systems and educate users in cyberattack prevention.

Unit F195: Preventing cyberattacks	
Topic Area 1: Cyber security aims and threats	
Teaching content	**Exemplification**
1.1 Concepts of cyber security	
1.1.1 Three pillars of information security □ People □ Process □ Technology	To include: □ The different areas to be considered when discussing cyber security □ How the different pillars impact cyber security planning
1.1.2 Application of cyber security concepts □ Confidentiality, Integrity and Availability (CIA) Triad □ Identification, Authentication, Authorisation and Accountability (IAAA)	To include: □ How CIA and IAAA impact on cyber security planning
1.2 Threats against cyber security and countermeasures	
1.2.1 Threats against cyber security □ Threat types • Active and passive • Internal and external □ Threat impacts • Denial of Service (DoS) • Destruction, corruption and disclosure of information • Elevation of privilege • Theft □ Threat information sources • Common Vulnerabilities and Exposures (CVE) lists • National Cyber Security Centre (NCSC) threat reports	To include: □ How security experts can learn about current cyber security threats □ How to use threat information sources to learn about current cyber security threats □ The current cyber security threats and the potential impact each has on networks and data security

1.2.2 Countermeasures □ Preventative • Security policies and procedures • Testing of systems and staff • Pen testing □ Detective • Pen testing • Digital forensics □ Corrective • Business continuity plan • Cyber security insurance	To include: □ The features and characteristics of each countermeasure □ How each countermeasure impact cyberattack prevention

Topic Area 2: Identify risks to networks and data	
Teaching content	**Exemplification**
2.1 Risks to digital networks and data	
2.1.1 Risks □ Contractor access □ Employee access □ Internet of Things (IoT) devices □ Network access □ Robotic Process Automation (RPAs)/Internet Robots (Bots) □ Serverless functions □ Service accounts	To include: □ The potential impact each risk has on an organisation's operations □ The potential impact each risk has on an organisation's network(s) and data security
2.1.2 Reasons for performing security risk assessments □ Cost justification □ Create awareness of hazards and risks □ Identify who may be at risk/self-analysis □ Meet legal requirements where applicable □ Prioritise hazards/risks and control measures □ Productivity	To include: □ The purpose of completing security risk assessments □ How security risk assessments impact organisations
2.2 Tools and techniques to identify and record risks	
□ Risk assessments • Risk assessment types • Risk assessment stages ○ Risk identification ○ Risk analysis ○ Risk evaluation ○ Risk treatment ○ Risk review and monitoring □ Risk matrix • Risk matrix format ○ Impact of event ○ Likelihood of event	To include: □ The purpose and use of risk assessments in cyber security □ The purpose and use of different risk assessment types □ The format and layout of different risk assessment types □ The stages of risk assessment □ How to create risk assessments □ The purpose and use of risk matrices in risk assessment □ How to use a risk matrix to define the severity level of risks found Examples of **types of risk assessment** may include: □ Qualitative □ Quantitative

Topic Area 3: Audit and improve cyberattack prevention measures	
Teaching content	**Exemplification**
3.1 Tools and techniques to audit and improve cyberattack prevention measures	
Preparing security audits □ Internal • First party audits □ External • Second party audits • Third party audits □ Audit process □ Audit findings • Points of strength • Observations • Gaps • Non-conformity (NCR) – minor/major • Opportunities for improvement □ Reports and corrective actions □ Types of recommendations	To include: □ The purpose and use of security audits in preventing cyberattacks □ The format and layout of security audits □ How to complete security audits
3.2 Methods of network access control	
3.2.1 Firewalls □ Firewall types • Packet-filtering firewall • Proxy firewall/application-level gateways □ Methods of packet inspection • Stateful packet Inspection • Stateless packet Inspection □ Firewall Rules Management □ Network Address Translation (NAT)	To include: □ How firewalls allow or prevent traffic through a network □ The difference between stateful and stateless packet inspection □ The role of NAT and how it improves network security □ The strengths and weaknesses of firewall types and configurations □ How to audit firewall use □ How to design, create and manage firewall rules □ The impact firewall rules have on system users
3.2.2 De-Militarized Zone (DMZ) □ Three-tire design (Trusted, Semi-trusted, Untrusted networks) □ Single and Dual Firewall DMZ design □ Security policies	To include: □ The purpose and use of DMZs □ The features and characteristics of DMZs □ The role of firewalls within DMZs □ The type of security policies used in DMZs □ The strengths and weaknesses of DMZ designs and configurations □ How to audit DMZ use □ How to design diagrams that illustrate DMZ use □ How DMZs are implemented □ The impact DNZs have on system users

3.2.3 Wireless network security □ Encryption standards □ Access restrictions • Media Access Control (MAC) address filtering • Guest access □ Service Set Identifier (SSID) protection • Hide SSID • Change default SSID names and passwords	To include: □ The current encryption standards used in wireless networking □ How access restrictions are used to secure wireless networks □ How protecting SSIDs can secure wireless networks □ The strengths and weaknesses of wireless network security types and configurations □ How to audit wireless network security □ How to configure wireless network security □ The impact wireless network security has on system users
3.2.4 Other network hardening techniques □ Backup resources on-demand □ Firmware □ Web filtering	To include: □ The use of web filtering in networks □ How web filtering prevents cyber threats □ The importance of keeping firmware up to date □ The types of backup resources that can be used against cyber threats □ The strengths and weaknesses of network hardening techniques and configurations □ How to audit network hardening techniques used □ How to implement and configure network hardening techniques □ The impact network hardening techniques have on system users
3.3 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)	
□ Intrusion Detection System (IDS) • Detection types ○ Anomaly-based detection ○ Signature-based detection • Deployment methods ○ Network ○ Host ○ Distributed ○ Gateway ○ Application • Components ○ Sensors ○ Analysers ○ User Interface □ Intrusion Prevention System (IPS) • Deployment methods ○ Network ○ Host ○ Wireless	To include: □ The difference between IDS and IPS □ How IDS and IPS detect and react to intrusions □ The strengths and weaknesses of different IDS configurations □ The strengths and weaknesses of different IPS configurations □ How to audit IDS and IPS use □ How to set up and configure IDP/IPS □ The impact IDP/IPS have on system users

Topic Area 4: Design access control policies	
Teaching content	**Exemplification**
4.1 Access control	
4.1.1 Access control models □ Types of access control • Mandatory Access Control (MAC) • Discretionary Access Control (DAC) • Role Based Access Control (RBAC) • Attribute-based Access Control (ABAC) • Policy-based Access Control (PBAC) □ Access control administration • Centralised • Co-operative • Decentralised • Hierarchical • Ownership-based □ Types of access control • Physical • Logical	To include: □ The strengths and weaknesses of different types of access control □ How access controls are administered □ The principles used for administering access control □ The strengths and weaknesses of different physical access controls that limit access □ The strengths and weaknesses of different logical access controls that limit connections to computer networks, system files and data □ How access control models influence the design of policies that improve cyberattack prevention □ The impact each types of access control model has on system users
4.1.2 Principles of user access control □ Group policy management □ Principle of least privilege □ Privilege escalation □ Segregation of Duties (SoD)	To include: □ The importance of controlling privilege levels □ How privilege escalation can happen □ How the principle of least privilege relates to cyber security □ The different permissions that can be given to users and groups □ How group policy management can be used to manage access to systems and resources □ How principles of user access control influence the design of policies that improve cyberattack prevention □ The impact each principles of user access control has on system users
4.1.3 User authentication methods □ Passwords □ Biometrics • Fingerprints • Facial • Voice • Iris • Finger or palm vein patterns • Facial recognition □ Tokens □ Multi-factor authentication (MFA)	To include: □ The strengths and weaknesses of different authentication methods □ The features and characteristics of strong passwords □ The implications of weak passwords □ The purpose and use of multi-factor authentication □ How tokens can be used during authentication □ How methods of user authentication influence the design of policies which improve cyberattack prevention □ The impact each user authentication method has on system users

4.1.4 Physical security methods □ Deterrence □ Delay □ Detection □ Denying a breach □ Perimeter Intrusion Detection (PID) • Closed Circuit Television (CCTV) • Biometrics	To include: □ The features and characteristics of each physical security method □ How physical security methods impact cyber security threats □ How physical security methods influence the design of policies which improve cyberattack prevention □ The impact each physical security method has on system users
4.2 Access control policies	
□ Access control policy content • Business/client requirements • User needs • Access control models • User access control • User authentication • Physical security	To include: □ The purpose, structure and content of access control policies □ How to design access control policies □ The impact each access control policy has on system users

Topic Area 5: Design written user policies	
Teaching content	**Exemplification**
5.1 Policy writing considerations	
□ Establish the policy goals □ Break into manageable pieces □ Analyse impacts before setting rules □ Structure and clarity □ Feedback from other stakeholders □ Review regularly □ Format of policy • On screen • Paper • Digital	To include: □ That policies should include more DOs than DON'Ts □ How each policy writing consideration affects the writing of user policies □ How written policies can be implemented and shared with users
5.2 Written user policies	
□ Acceptable Use Policy (AUP) • Device use • Email, internet and social media use • Data use • Consequences of misuse □ Remote Access Policy • Procedure for remote network access when offsite • Options and use of remote connections • Email, extranet and data use • Consequences of misuse □ Bring Your Own Device (BYOD) policy • SSID and wired connection use • Data/network access • Device monitoring • Consequences of misuse □ Password Management Policy • Password requirement • How passwords are administered and managed • Consequences of misuse	To include: □ The purpose and use of each written user policy □ The structure, layout, content and format of each written user policy □ How to design each written user policy □ The impact each written user policy has on system users

Topic Area 6: Review designed cyberattack prevention measures	
Teaching content	**Exemplification**
6.1 Techniques to review the success of designed cyberattack prevention measures	
□ Accessibility/user friendliness of policies □ Conformation with CIA and IAAA concepts □ Suitability of planned cyberattack measures	To include: □ How to assess the appropriateness and effectiveness of planned cyberattack prevention measures

Assessment criteria

The table below gives the assessment criteria for the tasks in the set assignment for this unit. The assessment criteria indicate what is required in these tasks.

This qualification has a compensatory approach. This means that the unit grade awarded is based on the **total** number of achieved criteria for the unit (see Section 6.4). Students do **not** have to achieve **all** criteria for a specific grade to achieve that unit grade (e.g. achieve all Pass criteria to achieve a Pass grade).

Section 7.4 provides full information on how to assess the NEA units and apply the assessment criteria. Students' work must show that all aspects of a criterion have been met in sufficient detail for it to be **successfully achieved** (see Section 7.4.1). If a student's work does not fully meet a criterion, you must not award that criterion.

The command words used in the assessment criteria are defined in Appendix B.

Pass	**Merit**	**Distinction**
P1: Create a risk assessment appropriate for the organisation.	**M1: Explain** how the risks identified could impact the network and data security of the organisation.	**D1: Evaluate** the tools and techniques used to identify risks and their level of severity.
P2: Use a risk matrix to define the severity level of each risk identified.		
P3: Identify three assumptions made when defining the severity of the risks.	**M2: Justify** the assumptions identified when defining the severity of the risks.	
P4: Complete an audit of the existing cyberattack prevention methods used.	**M3: Assess** the strengths and weaknesses of the existing cyberattack policies, procedures and methods identified in the audit.	**D2: Discuss** how each improvement to the organisation's cyber security policies, procedures and methods will enhance their cyber security.
P5: Identify the gaps in the existing cyberattack policies, procedures and methods used.	**M4: Describe** improvements to each of the existing cyberattack policies, procedures and methods used.	
P6: Design access control policies for external access to systems/networks.	**M5: Design** cyber security prevention measures which make use of Intrusion	**D3: Justify** how each cyber security prevention policy and

Pass	Merit	Distinction
P7: Design access control policies for internal access to systems/networks.	Detection System (IDS) and Intrusion Prevention System (IPS).	measure designed relate to the concepts of cyber security.
P8: Design access control policies for access rights of different user groups.		
P9: Design written user policies which outline how technology should be used in the organisation.		
P10: Describe the purpose of each policy and measure designed.	**M6: Explain** how each policy and measure designed could be implemented.	**D4: Discuss** the impact of implementing each policy and measure designed on the users of the organisation's system.
P11: Explain how each policy and measure designed prevents exposure to cyber security threats.	**M7: Analyse** the advantages and disadvantages of each policy and measure designed.	**D5: Evaluate** the effectiveness of each policy and measure designed in reducing the cyber security risks identified.
P12: Explain how each policy and measure designed reduces the likelihood and severity of cyber security risk.		

Assessment guidance

This assessment guidance gives you information relating to the assessment criteria. There might not be additional assessment guidance for each assessment criterion. It is included only where it is needed.

Assessment Criteria	Assessment guidance
P1	• Students **must** use appropriate tools and techniques to create their risk assessment. The risk assessment must cover **all** risks detailed in the scenario. • Students **must not** be given a template to complete this task.
P2	• Students **must** define the severity of all risks identified in P1. To define each risk's severity, students **could** use the risk matrix format from Topic Area 2.2 or another standard risk matrix format they have been taught.
P3	• There is no additional assessment guidance for this criterion.
M1	• Students **must** explain how the risks detailed in P1 and P2 could impact the organisation's network(s) and data security.
M2	• There is no additional assessment guidance for this criterion.

D1	• Students **must** include in their evaluations an assessment of the effectiveness of the tools and techniques they used to identify risks and their level of severity.
P4	• Students **must** audit **all** the existing cyberattack policies, procedures and methods used by the organisation in the scenario.
P5	• Students **must** identity where the existing cyberattack policies, procedures and methods, used by the organisation in the scenario, do not sufficiently protect them from the risks identified in Task 1.
M3	• M3 builds on P4. For **each** cyberattack measure identified in the audit, students **must** assess how well it protects the organisation in the scenario from cyberattacks. Where weaknesses and/or any non-conformities (NCR) are found, students **must** include the impact these could have on the organisation's operations.
M4	• M4 builds on P5. Students **must** describe at least **one** specific improvements to each existing cyberattack policy, procedure and method used by the organisation in the scenario.
D2	• D2 builds on M3 and M4. Students **must** discuss how the recommended improvements will: o reduce the risk to the organisation's network data security and o improve the organisation's overall cyber security.
P6	• Students **must** choose appropriate methods and use them to design policies which will improve the organisation in the scenario's cyber security. Students **could** use content from Topic Areas 3 and 4. • Designs **must** include how the policies will be setup/configured and **could** include diagrams as well as written text. • There is no requirement for students to implement any of their policies, however if centres have facilities to do this, students **could** demonstrate their policies as part of their evidence.
P7	
P8	
M5	
P9	• Students **must** design written user policies which will indicate how users from the organisation should and shouldn't use the network. Topic Area 5 contains common written user policies and students only need to design those which are appropriate to/relevant for the organisation in the scenario.
D3	• Students **must** use the content in Topic Area 1.1 to help them discuss how well each of the cyber security prevention policies and measures designed relates to the concepts of cyber security,
P10	• Students **must** describe the purpose of each policy and measure designed in Task 3.
P11	The focus of P11 and P12 is different. • P11 focuses on how each policy and measure designed in Task 3 aims to eliminate the exposure to cyber security threats that pose a potential loss. • P12 focuses on how each policy measure designed in Task 3 reduces the likelihood and severity of a possible loss from cyber security threats.
P12	

M6	• Students **must** explain how the organisation in the scenario would implement policies they designed in Task 3. The implementation explanations **must** be at a high level rather than a step-by-step guide. Students **must** also explain how they would "roll out" their written policies to staff.
M7	• There is no assessment guidance for this criterion.
D4	• D4 builds on M6. Students **must** discuss how users will be impacted by the implementation of the policies designed in Task 3. This **must** include how their "usage" may change and any negative impact they may experience.
D5	• Students **must** evaluate how well their policies and measures ensure that the more severe risks identified in Task 1 and insufficiencies/gaps in protection identified in Task 2 are mitigated. If any insufficiencies/gaps in protection remain, students **must** justify why these have not been addressed.

Synoptic assessment

Some of the knowledge, understanding and skills needed to complete this unit will draw on the learning in Units F193 and F194.

This table details these synoptic links.

Unit F195: Preventing cyberattacks		Unit F193: Fundamentals of cyber security	
Topic Area		Topic Area	
1	Cyber security aims and threats	1 2 6	The cyber security landscape Cyber security vulnerabilities Job roles and responsibilities
2	Identify risks to networks and data	1 2 3 5	The cyber security landscape Cyber security vulnerabilities Impact of cyber security events Policies, procedures, and event handling
3	Audit and improve cyberattack prevention measures	2 4 5	Cyber security vulnerabilities Cyber security mitigations Policies, procedures, and event handling
4	Design access control policies	2 4 5	Cyber security vulnerabilities Cyber security mitigations Policies, procedures, and event handling
5	Design user policies	5	Policies, procedures, and event handling
6	Review planned cyberattack prevention measures	1	The cyber security landscape

Unit F195: Preventing cyberattacks		Unit F194: Fundamentals of networks	
Topic Area		Topic Area	
1	Cyber security aims and threats	1 3 4 6	Network types, models, topologies, and services Wired network components Mobile and wireless networks Cloud networks
2	Identify risks to networks and data	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks
3	Audit and improve cyberattack prevention measures	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks
4	Design access control policies	1 3 4 6	Network types, models, topologies, and services Wired network components Mobile and wireless networks Cloud networks
5	Design user policies	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks
6	Review planned cyberattack prevention measures	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks

More information about synoptic assessment in these qualifications can be found in Section 6.2 Synoptic assessment.

5.3.2 Unit F196: Digital forensic investigation

Unit Aim

Digital forensics focuses on the recovery and investigation of material found in digital devices related to cyber crime. It is the process of identifying, preserving, collecting, analysing, documenting, and reporting digital evidence. This is done so that critical evidence can be presented in a court of law when needed.

In this unit you will learn the fundamentals of digital forensics, including the process followed, where it is used and the implications of carrying out digital forensic investigations. You will learn how to plan digital forensic investigations, including methods to identify evidence and make sure it is preserved. Finaly, you will learn how to use different software tools to extract evidence and how to present evidence ready for use in court.

Unit F196: Digital forensic investigation	
Topic Area 1: Fundamentals of digital forensics	
Teaching content	**Exemplification**
1.1 Applications of digital forensics	
1.1.1 Introduction to digital forensics □ Purpose and use of digital forensics • Investigating criminal activity • Incident response ○ Internal incidents ○ External incidents □ Parties involved • Victims • Perpetrators • Investigators □ Digital forensic process • Identification • Collection/extraction • Preservation • Analysis • Documenting/reporting	To include: □ What digital forensics are □ Why and when digital forensic investigations are carried out □ The role each party plays in digital forensic investigations □ How each stage of the digital forensic process contributes towards digital forensic investigations Examples of **internal incidents** may include: □ Inappropriate data handling □ Mishandling security credentials □ Acceptable use policy violations □ Unauthorised access Examples of **external incidents** may include: □ Hacking □ Phishing □ Malware/ransomware attack □ Denial-of-Service (DoS) attack □ Serious vulnerability discovered
1.1.2 Factors of digital forensics □ Preservation of digital evidence • Do not alter evidence • Only access evidence if competent • Record all actions taken • Lead investigator has overall responsibility □ Legal admissibility □ Repeatability □ Volatility of digital data □ False positives	To include: □ The features and characteristics of each factor □ How each factor contributes towards digital forensic investigations □ The importance of each factor when completing digital forensic investigations

1.2 Digital forensic investigation considerations and challenges	
1.2.1 Legal considerations □ Data Protection Act (DPA) □ UK General Data Protection Regulation (UK GDPR) □ Data Retention and Investigatory Powers Act (DRIPA) □ Computer Misuse Act (CMA) □ Regulation of Investigatory Powers Act (RIPA)	To include: □ The latest version of each act and regulation □ The main purpose(s) of each act and regulation in relation to digital forensic investigations Does not include: □ The detailed content of each act and regulation
1.2.2 Ethical considerations □ A sense of community □ Consistency □ Diligence □ Good reputation □ Honesty and fairness □ Maintain objectivity □ Present accurate findings □ Proficiency	To include: □ How each ethical consideration impacts digital forensic investigations □ How each ethical consideration impacts individuals and society during digital forensic investigations
1.2.3 Digital forensic challenges □ Acquisition of evidence □ Readability of evidence □ Data hiding and encryption technique □ Evidence preservation □ Size and distribution of the evidence □ Rise of anti-forensic techniques	To include: □ How each digital forensic challenge impacts digital forensic investigations

Topic Area 2: Plan digital forensic investigations	
Teaching content	**Exemplification**
2.1 Techniques to plan digital forensic investigations	
Digital forensic investigation plans □ Investigation purpose • Aim • Scope • Scene □ Evidence requirements • Source • Collection • Preservation □ Resources required • Tool and techniques to handle evidence □ Potential issues • Involvement of legal authority • Involvement of corporate personnel management • Record keeping • Time constraints • Diligence	To include: □ The content of digital forensic investigation plans □ The conventions and layout of digital forensic investigation plans □ How to plan digital forensic investigations

2.2 Crime scenes and digital evidence	
2.2.1 Crime scenes □ Types • Physical scene • Non-physical/virtual scene □ Management	To include: □ The features and characteristics of each crime scene type □ The differences between each crime scene type □ How crime scenes are managed to prevent contamination and preserve evidence
2.2.2 Digital evidence □ Digital evidence classifications • Visible • Invisible □ Digital evidence types • Active data • Archived files • Logs • Metadata • Replicant data • Residual data • Video footage and images • Volatile data □ Digital evidence sources • Standalone computers or devices • Mobile devices • Internet based	To include: □ The features and characteristics of each digital evidence classification □ The differences between each digital evidence classification □ The features and characteristics of each digital evidence type □ The differences between each digital evidence type □ How each digital evidence type should be handled □ The data/information which could be found in each digital evidence type □ The type of digital evidence which is likely to be found on each digital evidence source Examples of data/information found within **digital evidence types** may include: □ Contents of open applications □ Encrypted traffic □ Local user account data □ Network connection information □ Operating system data □ Passwords □ Running processes Examples of **digital evidence sources** may include: □ PC/laptops □ Mobile phones/tablets □ Cloud □ Internet of Everything (IoE) devices □ Network attached storage (NAS) □ Portable storage devices □ Servers □ Virtual machines □ Wearable technology

2.3 Techniques to handle evidence	
2.3.1 Evidence collection □ First Response □ Scoping the scene □ Search and seizure □ Evidence collection • Creation of images • Disk cloning • Live imaging • Data acquisition • Drive imaging • Chain of custody • Hash value • Asset management □ Evidence assessment □ Securing of the evidence • Physical scene ○ Powered-off devices ○ Powered-on devices ○ Mobile devices ○ Media • Non-physical scene	To include: □ How investigators initially survey scenes on arrival □ The process of deciding what evidence to collect □ How to safely and securely collect and record evidence
2.3.2 Preservation of evidence □ Transportation □ Storage □ Maintaining integrity • Not working directly on the original evidence • Recording actions taken	To include: □ How digital evidence is transported to digital forensic laboratories □ The advantages and disadvantages of evidence transportation method □ How digital evidence is stored □ The advantages and disadvantages of evidence storage methods □ How evidence integrity is maintained and proven

Topic Area 3: Collect, preserve and analyse digital evidence	
Teaching content	**Exemplification**
3.1 Principles of data storage	
3.1.1 File systems and properties □ File systems • File Allocation Table (FAT) • New Technology File System (NTFS) • Apple File System (APFS) • Hierarchical File System Plus (HFS+) □ File system properties • Partitions • Volume • Redundant Array of Independent Disks (RAID) • Master Boot Record (MBR) • Disk geometry • Sectors • Clusters/allocation units • Slack space • File deletion in FAT and NTFS	To include: □ The purpose and use of file systems □ File systems used by different operating systems □ The properties of each file system □ How data is recorded and accessed by different file systems □ How disk drives can be configured □ How files can be written over multiple disks, sectors, volumes, and the implications of this during digital forensic investigations □ How file systems mark files as deleted rather than removing them

3.1.2 File Signatures □ File carving □ Known file filters □ Deleted files □ Complications with file signatures □ Deleted file systems and related complications	To include: □ The importance of file signatures for digital forensic investigations □ The methods of carving files from disk drives □ How to find files based on their file signature when they are deleted □ The issues with file systems and file signatures
3.1.3 Transforming and hiding data □ Methods to transformation data • Encoding ○ Base64 ○ Unicode Transformation Format (UTF)-8 ○ Endianness • Encryption • Hashing • Steganography □ Methods to hide data • Encryption ○ Disk ○ File • Encoding/cryptography • Virtual Private Network (VPN) • Steganography • The Onion Router (Tor) • Reversable Data Handling (RDH) • Fileless Malware □ Complications	To include: □ The difference between transforming and hiding data □ How each method is used to transform data □ How each method is used to hide data □ How data can be hidden in other files □ The issues with decoding and decrypting data Does not include: □ Technical understanding of how each method functions
3.1.4 Digital imaging □ Image types • Bit by bit copy • Live imaging • Dead imaging • Physical imaging • Logical imaging □ Hash types • Acquisition hash • Verification hash	To include: □ How images of storage devices can be created □ The importance of acquisition and verification hashes during digital forensic investigations

3.2 Tools to collect and preserve digital forensic evidence	
3.2.1 Grab bag tools □ Tools and equipment □ Stationary	To include: □ The typical contents of an investigator’s grab bag □ The purpose and use of grab bag tools □ How to safely use grab bag tools to collect and preserve digital forensic evidence Examples of **grab bag tool use** may include: □ Using cameras to record the visual layout of the scene □ Using write blockers to prevent changes to non-volatile storage □ Using disk duplication and sterile media to create images of evidence □ Completing chain of custody forms
3.2.2 Forensic software tools □ Disk Imaging software □ Live CD/USB □ Tools for viewing files/information on disk images □ Hex editor and disk editor □ Recovery software • Deleted data/files • Hidden data/files • Transformed data/files □ File carving software □ Memory forensic tools	To include: □ The purpose and use of forensic software □ How to use digital forensic software tools to collect and preserve digital forensic evidence Examples of **forensic software tool use** may include: □ Creating disk and memory images (ISO) □ Capturing live images on running systems to create a forensic image file □ Using Live CD/USB to collect volatile data □ Processing and parsing of collected disk images □ Decrypting encrypted disks and files □ Analysing evidence □ Collating evidence for use in the reporting phase □ Viewing deleted or hidden files on a disk image □ Searching for file signatures □ File carving deleted files □ Capturing and viewing information in memory
3.2.3 Mobile device forensic tools □ Data extraction □ Password recovery	To include: □ The purpose and use of mobile device forensic tools □ How to use mobile device forensic tools to collect and preserve digital forensic evidence Examples of **mobile device forensic tool use** may include extracting: □ Call information □ Global Positioning System (GPS) data □ Application data □ Text messages □ Photos and videos

3.2.4 Network forensic tools □ Encrypted traffic analysis tools □ Log viewer □ Network taps □ Packet capture tools □ Wireless traffic analysis tools	To include: □ The purpose and use of network forensic tools □ How to use network forensic tools to collect and preserve digital forensic evidence Examples of **network forensic tool use** may include: □ Acquiring network traffic □ Viewing data packet streams □ Capturing encrypted traffic □ Capturing wireless network traffic □ Using connection event logs to track network activity
3.3 Techniques to record investigation outcomes	
□ Photos and screen recordings □ Video recordings □ Written records • Evidence form • Observation record • Table • Written statement	To include: □ The format, structure, content and use of techniques to record investigation outcomes □ How to record investigation outcomes
3.4 Digital forensic investigation evidence integrity and accuracy	
□ Methods of checking • Checklist • Hash values □ Elements of digital forensic investigations to check • Evidence preservation • Chain of custody • Accuracy of evidence • Evidence meets the needs of the investigation • Integrity of the evidence □ Tools and techniques to check integrity and accuracy	To include: □ The structure, content and use of checklists □ How to record check results □ How to check elements of digital forensic investigations □ How to use tools and techniques to confirm the integrity and accuracy of digital forensic evidence
3.5 Stages of evidence analysis	
□ Data reconstruction □ Data analysis □ Evidence assessment □ Crime Scene reconstruction from recovered data □ Summarise and draw conclusions	To include: □ How to analyse evidence found during digital forensic investigations

Topic Area 4: Report digital forensic investigation findings	
Teaching content	**Exemplification**
4.1 Digital forensic investigation findings report	
□ Findings report sections • Introduction • Executive summary of findings • Acquisition and chain of custody • Tools and techniques used • Findings and evidence • Conclusions • Appendices □ Finding reports presentation considerations • Content depth • Format • Layout • Style • Technical language	To include: □ The structure, content and use of digital forensic investigation findings reports □ How the intended audience affects the presentation of digital forensic investigation findings reports □ How to create digital forensic investigation findings reports

Topic Area 5: Review digital forensic investigations	
Teaching content	**Exemplification**
5.1 Techniques to review digital forensic investigations	
□ Effectiveness of digital forensic investigation planning □ Accuracy, reliability and repeatability □ Processes followed • Tools and techniques • Skills used	To include: □ How to assess the suitability and effectiveness of digital forensic investigation planning □ How to assess accuracy and reliability of the results during digital forensic investigations □ How to assess the suitability of the processes followed to complete digital forensic investigations
5.2 Digital forensic investigation constraints	
□ Abilities of the investigator □ Technical constraints □ Time	To include: □ How to assess constraints that impact digital forensic investigations

Assessment criteria

The table below gives the assessment criteria for the tasks in the set assignment for this unit. The assessment criteria indicate what is required in these tasks.

This qualification has a compensatory approach. This means that the unit grade awarded is based on the **total** number of achieved criteria for the unit (see Section 6.4). Students do **not** have to achieve **all** criteria for a specific grade to achieve that unit grade (e.g. achieve all Pass criteria to achieve a Pass grade).

Section 7.4 provides full information on how to assess the NEA units and apply the assessment criteria. Students' work must show that all aspects of a criterion have been met in sufficient detail for it to be **successfully achieved** (see Section 7.4.1). If a student's work does not fully meet a criterion, you must not award that criterion.

The command words used in the assessment criteria are defined in Appendix B.

Pass	Merit	Distinction
P1: Identify the aim, scope and scene of the digital forensic investigation.		
P2: Describe the digital evidence required and possible sources for the digital forensic investigation.		
P3: Describe the tools and techniques to be used to handle evidence in the digital forensic investigation.	**M1: Justify** the choice of tools and techniques planned to collect and secure evidence during the digital forensic investigation.	**D1: Discuss** the implications of different factors of digital forensics when completing the digital forensic investigation.
	M2: Explain how the evidence in the digital forensic investigation will be preserved.	
P4: Identify potential issues for the digital forensic investigation.	**M3: Explain** the legal and ethical considerations which will impact the digital forensic investigation.	**D2: Discuss** how digital forensic challenges will impact the digital forensic investigation.
P5: Use tools and techniques to collect digital forensic evidence.	**M4: Explain** how the principles of data storage have been used to collect, recover and preserve the digital forensic evidence.	**D3: Assess** the suitability of the tools and techniques used to collect, recover and preserve digital forensic evidence.
P6: Use tools and techniques to recover digital forensic evidence.		
P7: Use tools and techniques to preserve digital forensic evidence.		
P8: Use tools and techniques to confirm the integrity and accuracy of the digital forensic evidence.	**M5: Discuss** how the evidence found meets the	

Pass	Merit	Distinction
P9: Record the outcomes of the digital forensic investigation in an appropriate format.	needs of the digital forensic investigation.	
P10: Create a report of the digital forensic investigation findings.	**M6: Justify** the conclusions made in the digital forensic investigation findings report.	**D4: Discuss** the accuracy, reliability, and repeatability of the digital forensic investigation.
P11: Explain how the presentation of the digital forensic investigation findings report is suitable for the intended audience.		
P12: Assess the effectiveness of the digital forensic investigation plan.	**M7: Discuss** how the quality of the investigation has been impacted by constraints.	**D5: Justify** potential improvements to the digital forensic investigation.

Assessment guidance

This assessment guidance gives you information relating to the assessment criteria. There might not be additional assessment guidance for each assessment criterion. It is included only where it is needed.

Assessment Criteria	Assessment guidance
P1	• Students **must** use the information given in the scenario to identify the aim, scope and scene of the digital forensic investigation. Any assumptions **must** be stated. This assessment criterion **must** be evidenced in the digital forensic investigation plan.
P2	• Students **must** describe what evidence they are looking for during the investigation and where they could find it. Any assumptions **must** be stated. This assessment criterion **must** be evidenced in the digital forensic investigation plan.
P3	• Students **must** describe which tools and techniques they are going to use to complete their digital forensic investigation. The tools and techniques selected **must** be appropriate for the investigation they intend to complete. This assessment criterion **must** be evidenced in the digital forensic investigation plan.
P4	• This assessment criterion must be evidenced in the digital forensic investigation plan.
M1	• M1 builds on P3. Students **must** justify their choice of tools and techniques they intend to use. The justifications **must** link to the actual investigation students intend to complete. This assessment criterion **must** be evidenced in the digital forensic investigation plan.
M2	• Students' explanations **must** link to the actual investigation students intend to complete. This assessment criterion **must** be evidenced in the digital forensic investigation plan.

M3	• Students **must** explain how the legal and ethical considerations in Topic Area 1.2 impact their investigation. Legal and ethical considerations which are not included in Topic Area 1.2 **could** also be explained.
D1	• Students **must** discuss how the factors in Topic Area 1.1 implicate their investigation.
D2	• Students **must** use content in Topic Area 1.2.3 in their discussions.
Task 2	• During this task students **must** collect and preserve all the evidence detailed in their digital forensic investigation plan. Students **could** also collect and preserve other evidence not on their initial plan depending on how the investigation progresses - they **must not** be penalised for doing this.
P5	• Students **must** start off their investigation by using the tools and techniques planned in Task 1, to collect digital evidence. Students **could** deviate from their plan if they find other tools and techniques are needed. • An individualised teacher observation record (TOR) form **must** be provided for each student as evidence of the digital forensic tools and techniques used to complete the planned digital forensic investigation (Task 2, Topic Area 3). Students **must** also read and sign the TOR form. Each TOR form must describe the digital forensic tools and techniques used by the student. For this task students **must** also provide evidence such as photos or videos showing them collecting digital evidence during their digital forensic investigation.
P6	
P7	
P8	
P9	• Students **must** record the evidence found in one of the formats listed in Topic Area 3.3.
M4	• Students **must** explain how they have used the principles in Topic Area 3.1 during their collection, recovery, and preservation of digital evidence.
M5	• Students **must** relate their discussion back to the digital forensic investigation plan written in Task 1. Where students have deviated from the evidence requirements planned, they **must** justify why.
D3	• Students **must** assess the suitability each tool and technique used during the collection, recovery and preservation of digital evidence. The assessment **must** be based on how successful the tools and techniques were – did they find anything? if nothing was found, why did it fail? Where students have deviated from the tools and techniques planned, in task 1, they **must** justify why.
P10	• Students **must** create a report which shows the findings of their digital forensic investigation. It should follow the report structure given in Topic Area 4.1. This assessment criterion is not looking for detailed explanations or justifications in each report section but for the content to be communicated appropriately for the intended audience.

P11	- Students **must** explain how they have adapted the report presentation considerations listed in Topic Area 4.1 to suit the intended audience for their digital forensic investigation report.
P12	- Students **must** assess how successful their digital forensic investigation plan created in Task 1 was. Students **must** assess which aspects of the investigation were fully planned, and which were not.
M6	- Students **must** justify why they have come to the investigation conclusion, based on the evidence found.
M7	- Students **must** discuss how their digital forensic investigation has been both positively and negatively impacted by constraints. Topic Area 5.2 contains types of constraint which students **must** consider.
D4	- Students **must** discuss the accuracy of what they did in Task 2 and what they found out. - Students **must** also discuss if the investigation was to be completed again, perhaps using different methods, would the same conclusion be reached
D5	- Students **must** justify what they would do differently next time and why.

Synoptic assessment

Some of the knowledge, understanding and skills needed to complete this unit will draw on the learning in Units F193 and F194.

This table details these synoptic links.

Unit F196: Digital forensic investigation		Unit F193: Fundamentals of cyber security	
Topic Area		Topic Area	
1	Fundamentals of digital forensics	2 6	Cyber security vulnerabilities Job roles and responsibilities
2	Plan digital forensic investigations	2	Cyber security vulnerabilities
3	Collect, preserve and analyse digital evidence	2 4	Cyber security vulnerabilities Cyber security mitigations
4	Report digital forensic investigation findings	2 4 5	Cyber security vulnerabilities Cyber security mitigations Policies, procedures, and event handling
5	Check and review digital forensic investigations	2 4 5	Cyber security vulnerabilities Cyber security mitigations Policies, procedures, and event handling

Unit F196: Digital forensic investigation		Unit F194: Fundamentals of networks	
Topic Area		Topic Area	
1	Fundamentals of digital forensics	1 3 4 6	Network types, models, topologies, and services Wired network components Mobile and wireless networks Cloud networks
2	Plan digital forensic investigations	1 3 4 6	Network types, models, topologies, and services Wired network components Mobile and wireless networks Cloud networks
3	Collect, preserve and analyse digital evidence	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks
4	Report digital forensic investigation findings	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks
5	Check and review digital forensic investigations	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks

More information about synoptic assessment in these qualifications can be found in Section 6.2 Synoptic assessment.

5.3.3 Unit F197: Penetration testing and incident response

Unit Aim

Penetration testing is a form of ethical hacking. It is used to attempt to find and exploit vulnerabilities in a computer system. The purpose of this authorised simulated attack is to identify any vulnerabilities in a system's defences which attackers could take advantage of. A test process is followed to simulate an attack using the same methods and tools used during a cyber security incident.

In this unit you will learn the phases of penetration testing strategies, and how to plan and outline the scope of the tests. You will learn how to undertake planned authorised exploits on vulnerable systems using specific methods and tools. You will also learn how to create cyber security incident response plans to be deployed when systems are under attack, how to create playbooks and how to create a maintenance plan to build and upkeep incident response capability.

Unit F197: Penetration testing and incident response	
Topic Area 1: Introduction to penetration testing	
Teaching content	**Exemplification**
1.1 Aims, stages and phases of penetration testing	
□ Aims of penetration testing • Meeting compliance requirements • Establishing a security baseline • Preventing data breaches • Checking security controls • Monitoring application security • Assessing effectiveness of incident detection and response □ Five stages of penetration testing • Reconnaissance/Open Source Intelligence (OSINT) gathering • Scanning • Vulnerability assessment • Exploitation • Analysis and reporting □ Three Phases of penetration testing • Pre-engagement • Rules of Engagement (RoE) • Post-engagement	To include: □ What penetration testing (pen testing) is □ How each aim of penetration testing impacts cyber security □ The purpose and importance of each penetration testing stage □ The purpose and importance of each penetration testing phase □ How penetration testing is used to discover vulnerability to exploitation in target system
1.2 Penetration testing roles	
□ Red team □ Blue team □ Purple team	To include: □ The purpose of the team approach to penetration testing □ The role of each team in penetration testing □ The role of each team during each stage of penetration testing □ The documents created and used by each team Does not include: □ Detailed job descriptions and skills required for each team

1.3 Common system vulnerabilities	
□ Complexity of software □ Design flaws • Coding errors/bugs • Network • Insecure data storage • Misconfiguration issues □ Inadequate logging and monitoring of system □ Insecure in-house developed applications □ Password strength/reuse □ Password theft □ Patch management including unpatched software □ System management □ Unstopped legacy software □ User awareness (lack security awareness and training) □ User error □ Vulnerable third party components	To include: □ The characteristics of each system vulnerability □ How each vulnerability can be potentially exploited by a threat actor □ The likelihood of each vulnerability can be potentially exploited by a threat actor □ The risks different vulnerabilities create during penetration testing

Topic Area 2: Plan penetration testing	
Teaching content	**Exemplification**
2.1 Penetration testing strategies	
□ Penetration testing methodologies • National Institute of Standards and Technology (NIST) • Open Source Security Testing Methodology Manual (OSSTMM) • Open Web Application Security Project (OWASP) • Penetration Testing Methodologies Execution Standard (PTES) □ Penetration testing frameworks • BeEF (Browser Exploitation Framework) • Cobalt Strike • Kali Linux • Metasploit Framework • PowerSploit □ Penetration testing methods • Black box • White box • Grey box □ Types of exploitation activity • Application software penetration • Cloud penetration • Network services penetration • Physical penetration ○ Exploiting door entry systems ○ Lock-picking ○ Personnel or vendor impersonation ○ Tailgating • Social engineering	To include: □ The difference between penetration testing methodologies and penetration testing frameworks □ The use and effectiveness of each penetration testing methodology □ How to select penetration testing methodologies depending on the target □ The features and uses of each penetration testing framework □ How to select penetration testing frameworks when planning penetration testing exploitation activities □ The purpose and characteristics of each penetration testing method □ How each penetration testing method can be used when planning exploitation activities □ The purpose and characteristics of each type of exploitation activity □ How each type of exploitation activity can be used when planning penetration testing

○ Imposter ○ Name-dropping ○ Phishing ○ Tailgating • Unauthorised entry ○ Access control ○ Passwords • Web application • Wireless penetration	
2.2 Impacts of exploitation activities	
□ Data deletion □ Data inaccessibility □ Data manipulation □ Data modification □ Data theft □ Distributed Denial of Service (DDoS) □ Hacking □ Identity theft/impersonation □ Malware attacks	To include: □ The potential consequences of each exploitation activity impact
2.3 Penetration testing scoping plans	
□ Penetration testing planning considerations • Scope • Financial and customer data sources • Remote accessed resources required • Pentest strategies • Testing preparation • Communication plan/protocols ○ Lines of communication ○ Methods of communication (including final report) • Permission to liaise with third parties • Penetration tester skills □ Components of penetration testing scoping plans • Need and purpose • Areas of concern • Pre-engagement and Planning • Intelligence Gathering • Vulnerability Analysis • Reporting • Legislative or compliance requirements • Timeline • Risk identification	To include: □ The features and characteristics of each consideration □ How each consideration makes penetration testing effective □ The components and conventions of penetration testing scoping plans □ The purpose of each component within penetration testing scoping plans □ How each penetration testing scoping plan component contributes towards effective planning □ How to create penetration testing scoping plans Does not include: □ The details of different penetration testing methodologies and associated costings

2.4 Exploitation activities test plan	
Exploitation activity planning considerations □ Scope of the methods and tests • Penetration testing methods • Types of tests to perform • Description of exploitation activities • Information required to test • When to test	To include: □ How to create a plan for testing exploitation activities □ The contents of a plan for testing exploitation activities □ How to construct different types of test □ How to select test data that will test all types of exploitation activities □ The importance of considering expected outcome when planning exploitation activities □ How to select the most appropriate type of testing Does not include: □ Running of the tests or output of the tests as part of the exploitation activities test plan

Topic Area 3: Implement penetration testing scoping plans	
Teaching content	**Exemplification**
3.1 Penetration testing environments	
□ Standard operating systems • GUI operating systems • Command line operating systems □ Specialised operating systems □ Penetration testing labs □ Virtualisation and cloud technology • Virtual machines • Cloud-based machines • Locally hosted machines	To include: □ The features characteristics and use of different environments which can be used in penetration testing Examples of **specialised operating systems** include: □ Kali Linux □ BackBox □ ParrotOS Examples of **penetration testing labs** may include: □ Containerised □ Isolated □ Hybrid Does not include: □ The attack of the live current operating system

3.2 Penetration testing software tools	
□ Address Resolution Protocol (ARP) cache poisoning/spoofing tools □ Network protocol analysers □ Packet sniffers and injectors □ Password cracking tools • Dictionary • Brute force/cryptanalysis • Rainbow table □ Reconnaissance tools	To include: □ The purpose and use of each software tool □ The features and characteristics of each software tool □ How to select and use software tools to complete penetration tests

□ Security assessment tools □ Software frameworks and automation tools □ SQL injection detection □ Vulnerability scanners • Port scanners	Examples of **software tool use** may include: □ Network protocol analysers to monitor http network traffic from a given IP address □ Protocol analysers to capture and analyse packet payloads and contents □ Reconnaissance tools to identify operating systems, hosts, firewalls and services □ Password cracking tools to access protected data/systems □ Automated tools to run repetitive tests on target systems □ Web vulnerability scanners to detect misconfiguration and open ports □ Port scanners find out if targets are currently active

Topic Area 4: Incident response planning	
Teaching content	**Exemplification**
4.1 Cyber security Incident response (CSIR) plan	
□ Content of cyber security incident response (CSIR) plans • Key contacts/team members • Escalation criteria • Incident response stages ○ Preparation/planning ○ Identification and analysis ○ Containment ○ Remediate/eradication ○ Recovery ○ Review/lessons learned • Legal or regulatory requirements □ CSIR plan best practices • Simple checklists • Forms to document and track incidents • Technical guidance on incident response stages	To include: □ What a cyber security incident response (CSIR) plan is □ The purpose of CSIR plans □ The structure, layout, content, and format of CSIR plans □ What makes effective CSIR plans □ How to create CSIR plans

4.2 Incident management	
□ Incident management stages • Detection and identification • Incident triage and classification • Containment and mitigation • Investigation and analysis • Remediation and recovery • Documentation and reporting • Post-incident analysis and lessons learned	To include: □ The features, characteristics and importance of each incident management stage
4.3 Incident playbooks	
□ Content of incident playbook • Define incident type • Goals and objectives • Key contacts and roles • Response procedures • Third party and reporting • Change log	To include: □ The purpose of incident playbooks in incident response planning □ The features and characteristics of incident playbooks □ The structure, layout, content, and format of incident playbooks

Topic Area 5: Develop cyber security incident response capability	
Teaching content	**Exemplification**
5.1 Maintenance plan	
□ Content of maintenance plan • Risks and threats • Current capability baseline • Constraints • Stakeholders and teams for different scenarios • Review and exercise • In-house vs outsourced capability	To include: □ The purpose of a maintenance plan in developing and improving cyber security incident response capability □ The features and characteristics of the maintenance plan □ The structure, layout, content, and format of the maintenance plan
5.2 Employee training	
□ Training types □ Training materials	To include: □ How training can be used to increase employee awareness of different exploits □ The structure, layout content and format of training materials □ How to create training materials which improve employee’s awareness of different exploits and how to avoid them Examples of **training types** may include: □ eLearning □ Instructor-Led Training □ Role play □ Simulation Examples of **training materials** may include: □ Checklists □ Handouts □ Presentations □ Training manuals □ Videos

Topic Area 6: Review penetration testing and incident response capability	
Teaching content	**Exemplification**
6.1 Techniques to review penetration testing and incident response capability	
□ The suitability of: • Planned penetration testing strategies • Planned exploitation activities • Created cyber security incident response (CSIR) plans • Created incident playbooks • Maintenance plans □ The effectiveness of the approaches taken when responding to and managing cyber security incidents □ The effectiveness of recommended improvements to an organisation's cyber security provision	To include: □ How to assess the suitability of planned penetration testing strategies and exploitation activities to test the vulnerabilities of an organisation's IT system □ How to assess the suitability of CSIR plans to contain cyber security incidents □ How to assess the suitability of incident playbooks to prevent the success of cyber security incidents □ How to assess the suitability of maintenance plans to improve an organisation's cyber security provision □ How to assess strengths and weaknesses of the approaches taken when responding to and managing cyber security incidents □ How to assess strengths and weaknesses of recommended improvements to an organisation's cyber security provision

Assessment criteria

The table below gives the assessment criteria for the tasks in the set assignment for this unit. The assessment criteria indicate what is required in these tasks.

This qualification has a compensatory approach. This means that the unit grade awarded is based on the **total** number of achieved criteria for the unit (see Section 6.4). Students do **not** have to achieve **all** criteria for a specific grade to achieve that unit grade (e.g. achieve all Pass criteria to achieve a Pass grade).

Section 7.4 provides full information on how to assess the NEA units and apply the assessment criteria. Students' work must show that all aspects of a criterion have been met in sufficient detail for it to be **successfully achieved** (see Section 7.4.1). If a student's work does not fully meet a criterion, you must not award that criterion.

The command words used in the assessment criteria are defined in Appendix B.

Pass	Merit	Distinction
P1: Use research to **explain** why the data stored on the IT system in the organisation system would be of interest to threat actors.	**M1: Explain** the vulnerabilities of the IT system in the organisation.	**D1: Assess** the potential impacts of cyber security incidents on the organisation.
P2: Describe the planning considerations needed to create the penetration testing scoping plan.	**M2: Justify** which vulnerabilities of the IT system in the organisation the penetration plan will focus on.	**D2: Justify** the choices of the penetration testing strategies included in the penetration testing scoping plan.
P3: Describe the information requirements needed for each planning consideration for the penetration testing scoping plan.		

Pass	Merit	Distinction
P4: Create the penetration testing scoping plan for the IT system in the organisation.	**M3: Explain** the role that the team(s) would play in the planned penetration testing.	
P5: Identify the exploitation activities to be included in the exploitation activities test plan for the IT system in the organisation.	**M4: Explain** the suitability of the planned exploitation activities to test the vulnerabilities of the IT system in the organisation.	**D3: Discuss** the likelihood of the planned exploitation activities being conducted by threat actors.
P6: Create the exploitation activities test plan for the IT system in the organisation.		
P7: Demonstrate three exploitation activities from the exploitation activities test plan.		
P8: Create a cyber security incident response plan which shows how the organisation should respond to **one** cyber security incident.	**M5: Explain** the suitability of the cyber security incident response plan in containing the incident.	**D4: Evaluate** the strengths and weaknesses of your approach taken when responding to and managing cyber security incidents.
P9: Explain how the organisation should manage the cyber security incident in **P8**.		
P10: Create an incident playbook for **one** cyber security incident.	**M6: Explain** the suitability of the incident playbook in preventing the success of the cyber security incident.	
P11: Create a maintenance plan to build and upkeep cyber security incident response capability for the organisation.	**M7: Explain** how the maintenance plan would improve the organisation's cyber security.	**D5: Discuss** the strengths and weaknesses of the organisation's cyber security provision.
P12: Create training materials for **two** different types of exploitation activity from the exploitation activities test plan.		

Assessment guidance

This assessment guidance gives you information relating to the assessment criteria. There might not be additional assessment guidance for each assessment criterion. It is included only where it is needed.

Assessment Criteria	Assessment guidance
P1	• Students **could** research IT systems like the one in the scenario to gain insight into the types of data stored. Students **must** explain why each type of data identified would be of interest to threat actors and the benefits to a threat actor of accessing/stealing it.
P2	• Students **must** contextualise the planning considerations in Topic Area 2.3, so they relate to the IT system in the scenario.

P3	• This is the information required by students to create their penetration testing scoping plan in P4. Topic area 2.3 includes a list of penetration testing planning considerations.
P4	• Students **must** include the components of penetration testing scoping plans listed in Topic Area 2.3 when creating their penetration testing scoping plan.
M1	• Students **must** explain why each vulnerability listed in Topic Area 1.3 is a potential issue for the organisation in the scenario.
M2	• Students **must** justify which vulnerabilities in the IT system they have included in their penetration testing scoping plan and why.
M3	• Students **must** explain the role that the team(s) play in the context of the scenario. The explanation **must** include the actual tasks the team(s) would be doing in the planned penetration testing rather than a generic description of what a team's role is.
D1	• There is no assessment guidance for this criterion.
D2	• Students **must** justify the choices of penetration testing strategies included in their penetration testing scoping plan. Penetration testing strategies which are not included in Topic Area 2.1 **could** also be included.
P5	• Students **must** identify all the exploitation activities that need to be planned so the IT system in the scenario is tested for vulnerabilities. This criterion **could** be evidenced separately or as part of exploitation activities test plan created in P6.
P6	• Students **must** create exploitation activities test plan to test the IT system in the scenario for vulnerabilities. The structure of the exploitation activities test plan is in Topic Area 2.4.
P7	• Students **must** demonstrate **three** exploitation activities from their exploitation activities test plan created in P6, which centres have resources for. This criterion does not have to be completed in the context of the scenario or using an IT system which has the same level of complexity as the organisation's system in the scenario. • A Teacher Observation Record (TOR) form **must** be provided for each student as evidence of demonstrating exploitation activities. Students **must** read and sign the TOR form. The TOR form **must** provide clear evidence that the student has demonstrated **three** exploitation activities from their exploitation activities test plan created in P6. The TOR form **must** include a description of how each exploitation activity was completed by the student including the tools and techniques they used, and the success of the exploitation activity. For other criterions in this task the student must provide suitable evidence in the form of an exploitation activity test plan and written evidence.
M4	• Students **must** take the identified exploitation activities from P5 and look at the suitability of each in identifying and taking advantage of vulnerabilities.

D3	• Students **must** discuss the likelihood of each planned exploitation activity actually happening. Students do not need to specify the type of a threat actor who could conduct the exploitation.
P8	• Students **must** produce a cyber security incident response (CSIR) plan for **one** incident identified in the scenario **or one** from their exploitation activities test plan. The structure of the CSIR plan is in Topic Area 4.1.
P9	• The explanation **must** be for the cyber security incident the student chooses for P8. If students do not achieve P8, it is still possible to achieve this criterion. • Students **must** include in their explanation each of the incident management stages in Topic Area 4.2.
P10	• Students **could** base their incident playbook on the incident from P8, a different incident from the scenario or one they have identified. The content requirements of the incident playbook are in Topic Area 4.3.
M5	• M5 builds on P8. Students **must** explain the suitability of the plan for containing the incident chosen in P8.
M6	• M6 builds on P10. Students **must** explain the suitability of the playbook in preventing the success of the incident chosen in P10.
D4	• There is no assessment guidance for this criterion.
P11	• Students **must** create a maintenance plan for the organisation in the scenario. The content of a maintenance plan is in Topic Area 5.1.
P12	• Students **must** create training materials for **two different** types of exploitation activities included in their exploitation activities test plan created in **Task 2**. If students do not achieve P6, it is still possible to achieve this criterion. • Examples of training materials which **could** be created are in Topic Area 5.2. However, this list is not definitive, and students **could** create any suitable training materials.
M7	• Students **must** include in their explanations why the maintenance will help the organisation in the scenario to be less likely affected by cyber security incidents and exploitations in the future.
D5	• Students **must** discuss the strengths and weaknesses of the organisation's cyber security provision after their cyber security incident response (CSIR) plan, playbook, maintenance plan and training materials created and used.

Synoptic assessment

Some of the knowledge, understanding and skills needed to complete this unit will draw on the learning in Units F193 and F194.

This table details these synoptic links.

Unit F197: Penetration testing and incident response		Unit F193: Fundamentals of cyber security	
Topic Area		Topic Area	
1	Introduction to penetration testing	1 2	The cyber security landscape Cyber security vulnerabilities
2	Plan penetration testing	1 2 4 5	The cyber security landscape Cyber security vulnerabilities Cyber security mitigations Policies, procedures, and event handling
3	Implement penetration testing scoping plans	2 4	Cyber security vulnerabilities Cyber security mitigations
4	Incident response planning	2 3 4 5	Cyber security vulnerabilities Impact of cyber security events Cyber security mitigations Policies, procedures, and event handling
5	Develop cyber security incident response capability	2 3 4 5	Cyber security vulnerabilities Impact of cyber security events Cyber security mitigations Policies, procedures, and event handling
6	Review penetration testing and incident response capability	1 2	The cyber security landscape Cyber security vulnerabilities

Unit F197: Penetration testing and incident response		Unit F194: Fundamentals of networks	
Topic Area		Topic Area	
1	Introduction to penetration testing	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks
2	Plan penetration testing	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks
3	Implement penetration testing scoping plans	1 2 3 4 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Cloud networks
4	Incident response planning	1 3 4 6	Network types, models, topologies, and services Wired network components Mobile and wireless networks Cloud networks

5	Develop cyber security incident response capability	1 3 4 6	Network types, models, topologies, and services Wired network components Mobile and wireless networks Cloud networks
6	Review penetration testing and incident response capability	1 3 4 6	Network types, models, topologies, and services Wired network components Mobile and wireless networks Cloud networks

More information about synoptic assessment in these qualifications can be found in Section 6.2 Synoptic assessment.

5.3.4 Unit F198: Implementing secure local area networks (LANs)

Unit Aim

Local area networks (LANs) are a vital part of the cyber and networking world and the demand for networking capability is enormous and increasing daily. LANs are used for a wide range of purposes within households and organisations and vary in size and complexity. The types of devices connected through LANs range from tiny internet of everything (IoE) sensors to huge rack-based servers.

In this unit you will learn the purpose and components of local area networks (LANs). You will learn about the LAN life-cycle and follow the life-cycle to plan, design, implement, secure and test your own network. You will also learn how to safely complete network installation and configuration tasks and use software utilities to test and diagnose common faults.

Unit F198: Implementing secure local area networks (LANs)	
Topic Area 1: Purpose and components of local area networks (LANs)	
Teaching content	**Exemplification**
1.1 Purpose of LANs	
□ Connect local devices □ Share services and resources	□ To include: □ The advantages and disadvantages to users of being connected to a LAN □ The different shared services and resources which can be provided by LANs □ The advantages and disadvantages for users of being able to use each shared service and resource provided by LANs
1.2 LAN hardware components and transmission media	
1.2.1 End-user devices □ Games controllers □ Internet of everything (IoE) devices □ Mobile devices □ PCs/workstations □ Printers □ Wireless devices □ Voice over internet protocol (VoIP) devices	To include: □ The purpose and use of each end-user device type □ The features and characteristics of each end-user device type □ The transmission media used by each end-user device to connect it to a LAN □ How to compare and recommended end-user devices for use in LANs
1.2.2 Network servers □ Blade □ Rack □ Tower	To include: □ The advantages and disadvantages of each server form factor □ The hardware specifications of network servers □ The purpose and advantages of redundant hardware within network servers □ How to compare and recommend server specifications for use in LANs

1.2.3 Network connection devices □ Bridge • Transparent • Source routing □ Gateway □ Hardware firewalls □ Mobile Wi-Fi (MiFi) boxes □ Network Interface Card (NIC) □ Repeater □ Router □ Brouter (Bridging router) □ Switch • Unmanaged • Fully managed • Smart □ Wireless access points □ Wireless range extenders	To include: □ The purpose and use of each network connection device □ The features and characteristics of each network connection device □ The advantages and disadvantages of Power over Ethernet (PoE) in connection devices □ How to compare and recommended connection devices for use in LANs
1.2.4 Network transmission media □ Cables and connectors • Coaxial • Twisted pair • Optical fibre □ Powerline adapters □ Wireless standards	To include: □ The purpose and use and features of different cables and associated connectors □ The advantages and disadvantages of different cables and associated connectors □ The advantages and disadvantages of using powerline adapters within networking □ The features and characteristics of common wireless standards □ The advantages and disadvantages of common wireless standards □ How to compare and recommend network transmission media for use in LANs
1.2.5 Network organisation □ Data & Server Cabinets □ Patch panels □ Patch/drop cables □ Networking faceplates and modules	To include: □ The importance of secure device storage and cable management in LANs □ The purpose and use of hardware used to store devices and manage cables □ The features and characterises of hardware used to store devices and manage cables □ How to compare and recommend hardware used to store devices and manage cables for use in LANs

1.3 LAN software	
□ Server Operating Systems • Linux • Windows • Unix □ Network application software • Backups • Databases • File management □ LAN device applications • Antivirus software • Internet security applications • Software firewalls	To include: □ The purpose and use of LAN software □ The features and characteristics and functionality of LAN software □ The advantages and disadvantages of LAN software □ How to compare and recommend LAN software for use in LANs

Topic Area 2: Design secure local area networks (LANs)	
Teaching content	**Exemplification**
2.1 LAN design considerations	
□ Types of requirements • Essential • Non-essential • Client • Configuration • End user • Network support user • Security □ Constraints • Budget • Cost • Efficiency • Timescales □ Baselines • Modifications to existing LAN • Expansion of an existing LAN • New LAN	To include: □ The features and characteristics of each LAN requirement □ How each requirement impacts LAN design □ The features and characteristics of each LAN constraint □ How each constraint impacts LAN design □ The role of baselines within LAN design □ How existing LANs can be modified to meet user requirements
2.2 Components of LAN design documentation	
□ Network design proposal • Objectives of the LAN • Hardware component list • Software list • Transmission media • Shared services • Shared resources □ Network diagrams • Logical design ○ Topology ○ Addressing • Physical design • Network map ○ Servers ○ Workstations ○ Routers ○ Other network attached devices □ Hardware device specification □ Security schema	To include: □ The purpose of each LAN design documentation component □ The conventions, layout and format of each LAN design documentation component □ The resources required to produce each LAN design documentation component □ How to create each LAN design documentation component

• Network security o Firewall settings o Media access Control (MAC) o address filtering o Lease times • Wi-Fi security • User security o Groups and memberships o Password policies o Workstation policies o File access rights □ Network configuration • End-user device configuration • Router configuration • Software configuration	

Topic Area 3: Implement and secure local area networks (LANs)	
Teaching content	**Exemplification**
3.1 Safe working practices to implement LANs	
Protective equipment □ Anti-static bags □ Anti-static mats □ Anti-static wristbands Health and safety procedures and routines □ Lone working protocols □ Portable Appliance Testing (PAT) □ Safe use of tools □ Visual safety checks of cables □ Visual safety checks of hardware	To include: □ The purpose and use of protective equipment when implementing LANs □ How to correctly use protective equipment when implementing LANs □ The purpose and use of safety procedures and routines when implementing LANs □ How to follow safety procedures and routines when implementing LANs □ How to complete visual safety checks of cables and hardware components before use Does not include: □ Completing PAT □ Taking on responsibility for formal or informal safety checks on LAN components or other items
3.2 Technical skills to implement LANs	
□ Component connection • Wired connections • Wireless access • Wireless client connections □ Component configuration • Servers • Switches/routers • End-user devices □ Network addressing • Device address • Subnet mask • Default gateway	To include: □ How to connect components including servers, connectivity devices and end user devices to form LANs □ How to setup and configure network hardware including servers and connectivity devices □ How to setup and configure end-user devices for use by users on LANs □ How to setup and configure network addresses

3.3 Techniques to secure LANs	
3.3.1 Securely manage network users □ User accounts and groups □ Folder and file access rights □ User policies • Password policies • End-user device policies	To include: □ How to setup and configure user accounts with layered LAN access □ How to setup and configure policies which control for groups of LAN user □ How to setup and configure folder and files access rights for groups of LAN user
3.3.2 Wireless networking security settings □ Service Set Identifier (SSID) □ Encryption □ Access restriction • MAC address filtering • Restricted guest access	To include: □ How to setup and configure SSIDs for use on wireless networks □ How to setup and configure encryption for use on wireless networks □ How to setup and configure other access restrictions on wireless networks
3.3.3 Secure connection devices □ Device access • Default passwords □ Device hardening • Firmware version □ Security settings • MAC address filtering • Port Forwarding • Remote access • Universal Plug and Play (UPnP) • Wi-Fi Protected Setup (WPS)	To include: □ How to secure access to network connection devices used in LANs Does not include: □ Completing updates of router/modem/ gateway firmware
3.3.4 Firewall settings □ Rules • Incoming/outgoing traffic • Filters • Exceptions • Open ports □ Methods used to inspect traffic	To include: □ The purpose and use of firewall rules □ How to setup and configure firewall rules to secure LANs
3.3.5 End-user devices □ Anti-virus software □ Application updates and patches □ Internet security software □ Operating system updates and patches	To include: □ How to install and configure security measures to protect end-user devices

Topic Area 4: Test local area networks (LANs)	
Teaching content	**Exemplification**
4.1 Techniques to test and troubleshoot LANs	
4.1.1 Techniques to test the functionality of LANs □ Test table content • Test ID • Test type • Test description • Test data • Expected result • Actual result • Remedial action required • Retest result □ Elements test • Performance • Security • Quality of Service (QoS) • Quality of Experience (QoE)	To include: □ The structure, content, and use of test tables □ How to document test results and when/how to retest □ How and why to test iteratively during implementation □ How to plan and complete tests to make sure implemented LANs function as intended □ How to refine/improve implemented LANs so requirements are more closely met Does not include: □ User acceptance testing
4.1.2 Techniques to troubleshoot LAN faults □ Identify LAN faults □ Work out possible causes □ Try one fix at a time □ Finalise the solution □ Check LAN now functions as expected	To include: □ How to identify the possible cause(s) of faults during LAN implementation and testing □ How to correct faults found during LAN implementation and testing Examples of **LAN faults** may include: □ Internet Protocol (IP) address issues □ Domain Name System (DNS) issues □ Wired and wireless connectivity issues □ LAN component or cable failure □ Compatibility issues • Hardware • Software
4.2 Network tools for diagnostics, monitoring and benchmarking	
□ Hardware tools • Cable tester • Protocol analyser □ Software tools • Event & log viewers • Network event logs • Network monitors ○ Benchmarking ○ Device browsers ○ Packet sniffers ○ Performance monitors • Protocol analysers • Terminal • Traffic generators □ Command line/prompt commands	To include: □ The purpose and use of different tools for diagnostic, monitoring, and benchmarking □ How to use tools to diagnose network faults □ How to use tools to measure performance of LANs during testing □ How to use of tools when benchmarking LAN throughput and performance □ How to document measured performance as a benchmark for LANs

	Examples of **command line/prompt commands** may include: □ Ipconfig □ Loopback □ Netstat □ Pathping □ Ping □ Route □ Tracert

Topic Area 5: Review and maintain local area network (LAN) performance and security	
Teaching content	**Exemplification**
5.1 Techniques to review the effectiveness of implemented LANs	
□ Effectiveness of implemented LANs • Functionality • Performance • Security □ Effectiveness of the skills, techniques used when designing, implementing, securing and testing LANs	To include: □ How to assess the strengths and weaknesses of implemented LANs □ How to compare implemented LANs against client briefs or requirements or success criteria (LAN performance, Quality of Service, and Quality of Experience) □ How to assess the effectiveness of techniques used to secure LANs □ How to assess the effectiveness of skills, tools and techniques used to implement LANs
5.2 Improvements and further development to LANs	
□ Improvements • Device choice • Device configuration • Robustness • Security □ Future developments • Additional services and resources • Guest access/bring your own device (BYOD) • Increased capacity • User education • Virtualisation	To include: □ How to assess improvements to implemented LANs □ How to assess future improvements to implemented LANs Does not include: □ Implementing improvements to implemented LANs □ Implementing future developments to implemented LANs

5.3 The maintenance phase	
□ Techniques to maintain performance • Accommodate growth of the LAN • Hardware updates • Maintaining compliance with new standards • Monitoring tools • Proactive LAN component replacement • React to changes in use of the LAN • Software updates □ Technical skills to maintain security • Enhancements to security • Product upgrades • Routine maintenance • Virtual Private Network (VPN) on router/modem/gateway or LAN device	To include: □ The purpose of techniques and technical skills to used maintain the performance and security of LANs □ The strengths and weaknesses of techniques to maintain the performance and security of LANs Does not include: □ Implementation of techniques to maintain network performance and security

Assessment criteria

The table below gives the assessment criteria for the tasks in the set assignment for this unit. The assessment criteria indicate what is required in these tasks.

This qualification has a compensatory approach. This means that the unit grade awarded is based on the **total** number of achieved criteria for the unit (see Section 6.4). Students do **not** have to achieve **all** criteria for a specific grade to achieve that unit grade (e.g. achieve all Pass criteria to achieve a Pass grade).

Section 7.4 provides full information on how to assess the NEA units and apply the assessment criteria. Students' work must show that all aspects of a criterion have been met in sufficient detail for it to be **successfully achieved** (see Section 7.4.1). If a student's work does not fully meet a criterion, you must not award that criterion.

The command words used in the assessment criteria are defined in Appendix B.

Pass	Merit	Distinction
P1: Create a network design proposal to meet the essential requirements of the LAN.	**M1: Explain** the possible ways in which the non-essential requirements of the LAN could be met.	**D1: Justify** the choices made in the network design proposal.
P2: Describe the advantages and disadvantages for users of the shared services and resources proposed for the LAN.		
P3: Create logical and physical designs to meet the client requirements for the LAN.	**M2: Create** design documentation which includes the security schema and network configuration to meet the client requirements for the LAN.	**D2: Explain** the design decisions made for the LAN and how they meet the client requirements.
P4: Create a network map and hardware device specification to meet the client requirements for the LAN.		

Pass	Merit	Distinction
P5: Use technical skills to connect the components of the LAN.	**M3: Use** techniques to configure wireless networking, firewall rules and end-user devices to secure the LAN.	**D3: Use** technical skills and techniques to **implement** a secure LAN which fully meets the client requirements.
P6: Use technical skills to configure the components of the LAN.		
P7: Use techniques to securely manage network users.		
P8: Describe how the functionality of the LAN will be tested.		
P9: Complete testing of the LAN and document test results in an appropriate format.	**M4: Use** techniques to test the performance of the LAN and troubleshoot any faults identified.	**D4: Analyse** the results from performance benchmarking activities on the LAN.
	M5: Use technical skills to configure LAN components to improve performance.	
P10: Explain how the LAN can be maintained.		
P11: Assess the implemented LAN against the scenario requirements and network design documentation.	**M6: Discuss** the effectiveness of the implemented LAN’s functionality, performance and security.	**D5: Discuss** potential improvements, and further development opportunities for the implemented LAN.
P12: Describe how safe working practices have been used when implementing and securing the LAN.	**M7: Assess** the effectiveness of the technical skills and techniques used to implement and secure the LAN	

Assessment guidance

This assessment guidance gives you information relating to the assessment criteria. There might not be additional assessment guidance for each assessment criterion. It is included only where it is needed.

Assessment Criteria	Assessment guidance
P1	• Students **must** identify the objectives required for the LAN in the scenario. • Students **must** identify appropriate specific hardware components to include in the network design proposal, based on their understanding of the essential requirements of the LAN. Depending on the scenario context, hardware components could include specific types of end-user devices, network servers, network connection devices and network organisation. • Students **must** identify appropriate specific software to include in the network design proposal, based on their understanding of the essential requirements of the LAN. Depending on the scenario context, software could include server operating system, network applications, LAN device applications and LAN performance benchmarking tools. • Students **must** identify appropriate specific network transmission media to include in the network design proposal, based on their understanding of the essential requirements of the LAN. • Students are **not** required to list security protocols at this point. • Students **must** identify appropriate shared services and resources to include in the network design proposal, based on their understanding of the essential requirements of the LAN. • The network design proposal could be created in any suitable format.
P2	• Students **must** describe the advantages and disadvantages for users of being able to use each shared service and resource that has been included in the network design proposal.
M1	• Students **must** explain at least **one** way in which each non-essential client requirement could be met, giving clear reasons.
D1	• Students **must** justify the choices made in the network design proposal by providing valid reasons for their choices.

P3 **P4**	• For P3, students **must** create logical and physical designs to meet the client requirements for the LAN outlined in their network design proposal from **Task 1**. • For P4, students **must** create a network map and hardware specification to meet the client requirements for the LAN outlined in their network design proposal from **Task 1**. • The hardware specification **must** provide the specifics of each device on the hardware component list from the network design proposal. • All network design documentation **must** follow common conventions, layouts, and formats. Topic Area 2.2 contains components of LAN design documentation which students **must** consider.
M2	• Students **must** create a security schema that identifies network security, Wi-Fi security and user security to be used on the LAN. • Students **must** create network configuration documentation that identifies the router configuration, network software configuration and end-user device configuration to be used on the LAN. • All network design documentation **must** follow common conventions, layouts and formats. Topic Area 2.2 contains components of LAN design documentation which students **must** consider.
D2	• Students **must** clearly reference specific client requirements (essential and non-essential) when explaining the design decisions that they have made. • Where students have made assumptions about client requirements, such assumptions **must** be clearly stated.
Task 3	• Students **must** provide clear evidence of them using technical skills when implementing and testing the LAN. The form of evidence selected will vary, e.g. photos or videos of the implementation taking place, and will be supported by a Teacher Observation Record. • A Teacher Observation Record (TOR) **must** be provided for each student as evidence of safely connecting and configuring LAN components, and the techniques used troubleshoot faults (Task 3, Topic Areas 3 and 4). Students **must** also read and sign the TOR form. Each TOR form **must** describe how the student safely used tools and techniques when connecting and configuring LAN components and troubleshooting faults. • Before students are provided with network hardware components to connect and configure, they **must** be informed of all relevant health and safety policies and procedures. Teachers **must** intervene if there's a health and safety risk and reflect this in your assessment if the student needed additional help in order to work safely and independently to meet the assessment criteria in this task.
P5	• For P5 the evidence **must** show use of **at least two** technical skills in **connecting** components identified in the network design documentation.

P6	• For P6, the evidence **must** show use of **at least two** technical skills in **configuring** components identified in the network design documentation.
P7	• The evidence **must** show use of **at least three** techniques that securely manage network users.
P8	• For P8 students **must** provide a description of the techniques they **will** use to test the functionality of the LAN. • For P9 students **must** provide evidence that they have **both** completed testing on the functionality **and** documented the test results of the LAN. • Students **could** document their testing in the template for test table provided. If it is not clear from the test table what the testing outcomes are, another evidence format **must** be used (e.g. screen recording or video) and referenced in the test table.
P9	
P10	• Students **must** provide an explanation of ways in which the LAN can be maintained. When writing their explanations students **could** use the content in Topic Area 5.3. • Students **must** give the reasons for, or purposes of, the maintenance that can be carried out on the LAN.
M3	• The evidence **must** show clear use of **at least two** techniques when configuring **each** of wireless networking, firewall rules and end-user devices to secure the LAN.
M4	• The evidence **must** show clear use of **at least three** techniques to test the performance of the LAN. • We do not expect faults to be artificially introduced on the LAN, but when faults are identified, students **must** troubleshoot them.
M5	• Students **must** provide clear evidence that the performance of the LAN has been improved by configuring LAN components. This could be evidenced, for example, through providing LAN performance data before and after changing component configurations. • The evidence **could** come from a range of sources, e.g. diagnostics tools, network monitoring and troubleshooting tools.
D3	• Students must provide clear evidence that the implemented LAN is secure, **and** fully meets the client requirements. • To fully meet the client requirements **all** essential requirements and **at least two** non-essential requirements which form part of their network design documentation must be met.
D4	• Students **must** analyse all the results from performance benchmarking activities on the LAN. • The evidence of the analysis could be done in any appropriate format, e.g. adding comments to the evidence created for P9, M4 and M5, creating a separate written report, etc.
P11	• Students **must** assess the implemented LAN against both the requirements from the scenario and their own network design documentation. The reasons for any differences **must** be justified.

P12	• Students **must** describe how they have used safe working practices when implementing and securing the LAN. Students **could** consider the content in Topic Area 3.1.
M6	• Students **must** include in their discussion the effectiveness of the implemented LANs functionality, performance and security. For students to meet this criterion All **three must** be covered. • When discussing the effectiveness of the implemented LAN students **must** include **both** strengths and weaknesses.
M7	• Students **must** decide if the technical skills and techniques used to implement and secure the LAN were suitable or not. This reasoned judgement **must** be informed by relevant information.
D5	• Students **must** discuss **both** potential improvements to the LAN and further development opportunities of the LAN. These suggestions must relate to the context given in the scenario.

Synoptic assessment

Some of the knowledge, understanding and skills needed to complete this unit will draw on the learning in Units F193 and F194.

This table details these synoptic links.

Unit F198: Implementing secure local area networks (LANs)		Unit F193: Fundamentals of cyber security	
Topic Area		Topic Area	
1	Purpose and components of local area networks (LANs)	2 4	Cyber security vulnerabilities Cyber security mitigations
2	Design secure local area networks (LANs)	1 2 3 4 5	The cyber security landscape Cyber security vulnerabilities Impact of cyber security events Cyber security mitigations Policies, procedures, and event handling
3	Implement and secure local area networks (LANs)	4 5	Cyber security mitigations Policies, procedures, and event handling
4	Test local area networks (LANs)	2 4 5	Cyber security vulnerabilities Cyber security mitigations Policies, procedures, and event handling
5	Review and maintain local area network (LAN) performance and security	1 2 3 4 5	The cyber security landscape Cyber security vulnerabilities Impact of cyber security events Cyber security mitigations Policies, procedures, and event handling

Unit F198: Implementing secure local area networks (LANs)		Unit F194: Fundamentals of networks	
Topic Area		Topic Area	
1	Purpose and components of local area networks (LANs)	1 2 3 4 5	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Network Performance
2	Design secure local area networks (LANs)	1 2 3 4 5	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Network Performance
3	Implement and secure local area networks (LANs)	1 2 3 4 5	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Network Performance
4	Test local area networks (LANs)	1 2 3 4 5	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Network Performance

5	Review and maintain local area network (LAN) performance and security	1	Network types, models, topologies, and services
		2	Network layers, protocols and addressing
		3	Wired network components
		4	Mobile and wireless networks
		5	Network Performance
		6	Cloud networks

More information about synoptic assessment in these qualifications can be found in Section 6.2 Synoptic assessment.

5.3.5 Unit F199: Designing and communicating secure global computing systems

Unit Aim

Many organisations now operate across multiple sites and require their IT systems to operate seamlessly across the globe. The increase in hybrid and remote working has also changed the way users access IT systems and has driven the need to provide a secured online connectivity to work-from-anywhere-anytime. Technologies which interconnect multiple sites are continuously developing to make sure the demands for improved and secured network capacity, reliability, robustness, and resilience are met.

In this unit you will learn about technologies which allow networked computing systems to interconnect across multiple sites and practical applications of using cloud computing and VPN access for working remotely and on the move. You will also learn how to design secure global computing systems which meet client and user requirements and use software simulators to test they function as intended. Communication skills are vital in the digital technologies sector and in this unit, you will also learn how to prepare a "showcase" to demonstrate proposed secure global computing systems to clients.

Unit F199: Designing and communicating secure global computing systems	
Topic Area 1: Fundamentals of secure global computing systems	
Teaching content	**Exemplification**
1.1 Purpose and use of secure global computing	
□ Secure global computing concepts • Easily customised platform • Flexible access for user and organisations to IT assets and data • Highly secured multi-layered access • Integrated solutions to organisations' problems • Organisation-oriented computing systems • Software and hardware solutions designed for global access □ Secure global computing use • Sector use • Organisational use	To include: □ The purpose of secure global computing □ The features and characteristics of secure global computing □ The advantages and disadvantages of secure global computing to organisations □ The risks of secure global computing to organisations □ The typical sectors where secure global computing is used by organisations □ How organisations can use secure global computing to achieve their goals Examples of **sector use** may include: □ Businesses • Banking and finance • Energy • Manufacturing • Technology • Transport □ Non-governmental organisations • Aid and development • Education • Health • International and national • Science and technology collaboration • Sport □ Government organisations • Education • Health • Meteorology • Military

	Examples of **organisational use** may include: □ Communication within organisations □ Data collection/sharing/storage □ Delivery of processes and functions □ Employee recruitment □ Financial scrutiny and accountability □ International collaboration between stakeholders □ Organisational promotion, context and market environment □ Remote working/conferencing □ Shared application and service use
1.2 Secure global computing requirements	
□ Central data storage □ High level of accessibility □ High level of reliability and functionality □ High level of scalability and adaptability □ High level of security □ Platform and software independence	To include: □ The features and characteristics of each secure global computing requirement □ How each requirement impacts the design of secure global computing systems
1.3 Characteristics of cloud computing	
□ Automation □ On-demand self-service □ Pay-As-You-Go □ Resource pooling □ Security □ Ubiquitous access	To include: □ The features and characteristics of cloud computing □ How each cloud computing is used in secure global computing systems □ The advantages and disadvantages of using cloud computing in secure global computing systems
1.4 Technology which enables secure global computing	
□ Core components of secure global computing • Hardware ○ Servers ○ Storage • Software ○ Operating systems ○ Databases ○ Applications • Networking infrastructure ○ Connection devices and media ○ Addressing and Domain Name System/Service (DNS) ○ Protocols ○ Services ○ Telecommunication services and connections • Support infrastructure ○ Backup services available ○ Environmental controls ○ Uninterruptible Power Supply (UPS) • Virtualisation • Orchestration	To include: □ The purpose of each core component of secure global computing □ The features and characteristics of different types of hardware, software, network infrastructure and support infrastructure used in secure global computing □ The advantages and disadvantages of each type of hardware, software, network infrastructure and support structure used in secure global computing □ How virtualisation and orchestration are used in secure global computing □ How to recommend core components for use in secure global computing systems □ The features and characteristics of the security used in secure global computing □ The advantage and disadvantages of the security used in secure global computing □ How to recommend security for use in secure global computing systems □ The features and characteristics of support services used in secure global computing

□ Security of secure global computing • Authentication • Access control • Access rights • Device hardening • Encryption services • Physical security • Virtual Private Network (VPN) □ Support services • Levels of support available	□ The advantage and disadvantages of support services used in secure global computing □ How to recommend support services for use in secure global computing systems □ How secure global computing requirements impact the choice of technology which enables secure global computing

Topic Area 2: Plan and scope secure global computing systems	
Teaching content	**Exemplification**
2.1 Requirements of secure global computing systems	
□ Client requirements • Purpose • Intended outcome • Intended users ○ Types ○ Technical experience ○ Location • Budget □ User requirements • Remote access and evolving work patterns • Availability of applications and data • Accessibility and ease of use • Personalised user experience ○ Role-based interface ○ Accessibility features □ Technical requirements • Hardware • Software • Infrastructure • Capacity • Reliability • Resilience • Robustness • Security • Scalable • Sustainable	To include: □ The features and characteristics of each requirement type □ How each requirement type impacts the planning of secure global computer systems □ How technical requirements verses available infrastructure impact the planning of secure global computing systems □ The components and conventions of requirement specifications □ How to create requirement specifications to document the requirements of secure global computing systems

2.2 Scope secure global computing systems	
□ Outline scope document • Success criteria • Goals • Sub-phases • Tasks • Resources • Budget • Schedule • Legal and ethical considerations	To include: □ The purpose of outline scope document □ The components and conventions of outline scope documents to scope secure global computer systems □ How to use outline scope documents to scope secure global computing systems Does not include: □ Any form of project management planning documentation including workplans and Gantt charts

Topic Area 3: Design secure global computing systems	
Teaching content	**Exemplification**
3.1 Design documentation	
□ Network diagrams • Logical design ○ Platform independent ○ Inputs ○ Outputs ○ Processes ○ Data • Physical design ○ Platform dependent ○ Hardware ○ Software ○ Implementation environment • Security schema	To include: □ The purpose of each design document □ The conventions, layout, and format of each design document □ Resources required to produce each design document □ How to use design documentation to design secure global computing systems

Topic Area 4: Simulate and test secure global computing systems	
Teaching content	**Exemplification**
4.1 Tools to create simulated secure global computing system models	
□ Wide area network (WAN) simulator software □ Simulation software tools • Topology wizards • Scenario builders • Component libraries • Network visualisation • Device configurations • Protocol support • Graphs, logging, and packet capture • Reporting tools • Fault simulation	To include: □ The capabilities of WAN simulation software □ How software tools can be used create simulated secure global computing system models

4.2 Techniques to test secure global computing systems	
□ Test table content • Test ID • Test type • Test description • Test data • Expected result • Actual result • Remedial action required • Retest result □ Elements of secure global computing systems to test • Capacity • Data backup • Device configuration and addressing • Infrastructure design • Performance • Reliability • Robustness and resilience • Security	To include: □ The structure, content, and use of test tables □ How to document test results and when/how to retest □ How to plan and complete tests to make sure secure global computing system simulations function as intended □ How to refine/improve secure global computing systems simulations so requirements are more closely met Does not include: □ User acceptance testing

Topic Area 5: Communicate and review secure global computing systems	
Teaching content	**Exemplification**
5.1 Develop solution showcases to communicate secure global computing systems	
Solution showcases □ Formats □ Design considerations • Colour scheme • Content type • Content depth • Content relevance • Language and vocabulary • Layout • Style	To include: □ The purpose of solution showcases □ The format solution showcases can take and when each is appropriate □ How solution showcase design considerations are adapted for the intended audience □ How to develop solution showcases Examples of **showcase formats** may include: □ Presentation □ Slideshow with audio overlay □ Video
5.2 Techniques to review the effectiveness of secure global computing systems	
□ Meeting of success criteria □ Suitability for client requirements □ Suitability for user requirements □ Technically feasible □ Constraints which limit the effectiveness of secure global computing systems • Budget • Hardware • Legislation • Resources • Skills • Software • Time	To include □ How to assess the strengths and weaknesses of secure global computing systems □ How to compare secure global computing systems against success criteria □ How to compare secure global computing systems against client requirements and success criteria □ How to compare secure global computing systems against user requirements □ How to assess useability of secure global computing systems for different types of user

	□ How to assess if secure global computing systems are technically feasible □ How to assess the impact of constraints on secure global computing systems
5.3 Improvements and further developments	
□ Improvements • Compatibility issues • Performance • Reliability • Robustness and resilience • Security issues • User experience • User personalisation □ Further developments opportunities • Capacity • Develop the security further • Expansion • Greener computing • Implementation • Use of alternative technologies	To include: □ How to recommend improvements to secure global computing systems □ How to identify further development opportunities for secure global computing systems Does not include: □ Implementing improvements □ Implementing further developments

Assessment criteria

The table below gives the assessment criteria for the tasks in the set assignment for this unit. The assessment criteria indicate what is required in these tasks.

This qualification has a compensatory approach. This means that the unit grade awarded is based on the **total** number of achieved criteria for the unit (see Section 6.4). Students do **not** have to achieve **all** criteria for a specific grade to achieve that unit grade (e.g. achieve all Pass criteria to achieve a Pass grade).

Section 7.4 provides full information on how to assess the NEA units and apply the assessment criteria. Students' work must show that all aspects of a criterion have been met in sufficient detail for it to be **successfully achieved** (see Section 7.4.1). If a student's work does not fully meet a criterion, you must not award that criterion.

The command words used in the assessment criteria are defined in Appendix B.

Pass	Merit	Distinction
P1: Describe the client and user requirements of the secure global computing system.	**M1: Create** an outline scope document for the secure global computing solution.	D1: **Discuss** the advantages and disadvantages to the client of implementing the outline scope document.
P2: Identify the success criteria and the goals of the secure global computing system.		
P3: Describe the technical requirements of the secure global computing system.	**M2: Explain** how the secure global computing system will support different user requirements.	

Pass	Merit	Distinction
P4: Create a diagram which shows the logical design for the secure global computing system.	**M3: Explain** the proposed choices of technology included in the design documentation for the secure global computing system.	**D2**: **Discuss** the effectiveness of the security features included in the security schema for the secure global computing system.
P5: Create a diagram which shows the physical design for the secure global computing system.		
P6: Create a security schema for the secure global computing system.		
P7: Describe how the secure global computing system will be tested.		
P8: Create a simulation of the topology for the secure global computing system.	**M4: Use** software tools to simulate a secure global computing system which fully meets the client and user requirements.	**D3: Evaluate** the process used to simulate and test the secure global computing system.
P9: Configure the simulation of the secure global computing system.		
P10: Complete testing of the secure global computing system and document test results in an appropriate format.	**M5: Analyse** the test results documenting any required remedial action.	
P11: Create a showcase which communicates the secure global computing system.	**M6: Explain** how the design of the showcase is appropriate for the audience.	
P12: Analyse the strengths and weaknesses of the secure global computing system.	**M7: Assess** the suitability of the secure global computing system for meeting the client and user requirements.	**D4: Discuss** improvements and further development opportunities for the secure global computing system.
		D5: Assess the technical feasibility of the secure global computing system.

Assessment guidance

This assessment guidance gives you information relating to the assessment criteria. There might not be additional assessment guidance for each assessment criterion. It is included only where it is needed.

Assessment Criteria	Assessment guidance
P1	• Students **must** describe **both** the client requirements **and** the user requirements of the secure global computing system.
P2	• Students **must** identify **both** the success criteria **and** the goals of the secure global computing system.
P3	• Students **must** describe **at least five** technical requirements relevant to the secure global computing system. • Where students make assumptions about technical requirements, such assumptions must be clearly stated.
M1	• Students **must** create an outline scope document for the secure global computing solution. • The outline scope document **must** include all components relevant to the secure global computing system from the scenario. • The outline scope **could** be created in any suitable format and must follow conventions to scope a secure global computing system.
M2	• Students' explanations **must** include **at least three** different user requirements. • They must explain **at least one** way in which the secure global computing system could support **each** of the different user requirements.
D1	• Students **must** discuss **both** the advantages **and** disadvantages **to the client** of implementing the outline scope document. • This could include qualitative judgements about the impact **on the client** of implementing the scope document.
P4	• For P4, students **must** create a diagram which shows the logical design of the secure global computing system. • For P5, students **must** create a diagram which shows the physical design of the secure global computing system. • All network diagrams must follow common conventions, layout and formats. Topic Area 2.2 contains design documentation which students **must** consider.
P5	
P6	• Students **must** create a security schema for the secure global computing system. • The security schema **must** include **all relevant** security technology that could enable the secure global computing system **to be secured**, e.g. authentication, access control, access rights, device hardening.
P7	• Students **must** describe how they intend to test the secure global computing including the elements they intend to test. The description of how the secure global computing system will be tested **could** include the content in Topic Area 4.2.

M3	• Students **must** explain the reasons for their choices of technology included in the design documentation for the secure global computing system. • Students **must** provide an explanation that covers **all** choices made about the technology which enables the secure global computing system, e.g. hardware, software, infrastructure, security and support services.
D2	• Students **must** discuss the effectiveness of **all** security features included in the security schema for the secure global computing system. • Students **could** consider the characteristics, advantages and disadvantages of the security features included in their security schema. • The analysis produced by students **must** relate to the context given in the scenario.
P8	• Students **must** use software to create a network simulation of the topology of the secure global computing system designed in Task 2.
P9	• Students **must** provide clear evidence that the simulation of the secure global computing system **has been** configured.
P10	• Students **must** provide clear evidence that they have completed testing of the secure global computing system. • Students **could** document their testing in the template for test table provided. If it is not clear from the test table what the testing outcomes are, another evidence format **must** be used (e.g. screen recording or video) and referenced in the test table.
M4	• Students **must** provide clear evidence that they have used software tools to simulate a secure global computing system that fully meets the client and user requirements. • The secure global computing system will fully meet the client and user requirements when all related success criteria and goals have been shown to be met.
M5	• Students **must** provide clear evidence that they have analysed all test results. • Students **must** also document any required remedial action identified during the analysis. • We do **not** expect faults to be artificially introduced to the simulation of the secure global computing system, but when issues occur, required remedial action identified **must** be documented.
D3	• Students **must** evaluate the processes they followed to simulate and test the secure global computing system. Students **could** evaluate the individual tools and techniques they have used during the process.

P11	• Students **must** create a showcase which communicates the secure global computing system. • The showcase **must** include content that is appropriate for the audience detailed in the scenario. • The showcase **could** be created in any suitable format.
P12	• Students **must** analyse the strengths and weaknesses of the secure global computing system in relation to the requirements identified in Task 1.
M6	• Students **must** explain how the design of the showcase is appropriate for the audience. • When explaining the appropriateness of the design of the showcase, students must make clear reference to the audience and context from the scenario.
M7	• Students **must** provide clear evidence that they have assessed the suitability of the secure global computing system for meeting the client and user requirements. • When assessing the suitability of the secure global computing system, students could also consider the success criteria and goals included in the outline scope document, where these were derived from the client and user requirements.
D4	• Students **must** discuss **at least three** improvements that could be made to the secure global computing system. Students **must** present, analyse and evaluate relevant points to make a reasoned judgement about the improvements, related to the context of the scenario. • Students **must** also discuss **at least two** further development opportunities for the secure global computing system. Students **must** present, analyse and evaluate relevant points to make a reasoned judgement about the further development opportunities, related to the context of the scenario.
D5	• Students **must** assess the technical feasibility of the secure global computing system. • Students **must** decide whether the secure global computing system is technically feasible. This reasoned judgement must be informed by relevant information.

Synoptic assessment

Some of the knowledge, understanding and skills needed to complete this unit will draw on the learning in Units F193 and F194.

This table details these synoptic links.

Unit F199: Designing and communicating secure global computing systems		Unit F193: Fundamentals of cyber security	
Topic Area		Topic Area	
1	Fundamentals of secure global computing systems	1 2 4	The cyber security landscape Cyber security vulnerabilities Cyber security mitigations
2	Plan and scope secure global computing systems	1 2 3 4 5	The cyber security landscape Cyber security vulnerabilities Impact of cyber security events Cyber security mitigations Policies, procedures, and event handling
3	Design secure global computing systems	1 2 3 4	The cyber security landscape Cyber security vulnerabilities Impact of cyber security events Cyber security mitigations
4	Simulate and test secure global computing systems	1 2 3 4	The cyber security landscape Cyber security vulnerabilities Impact of cyber security events Cyber security mitigations
5	Communicate and review secure global computing systems	1 2 3 4 5	The cyber security landscape Cyber security vulnerabilities Impact of cyber security events Cyber security mitigations Policies, procedures, and event handling

Unit F199: Designing and communicating secure global computing systems		Unit F194: Fundamentals of networks	
Topic Area		Topic Area	
1	Fundamentals of secure global computing systems	1 5 6	Network types, models, topologies, and services Network performance Cloud networks
2	Plan and scope secure global computing systems	1 3 4 5 6	Network types, models, topologies, and services Wired network components Mobile and wireless networks Network performance Cloud networks
3	Design secure global computing systems	1 2 3 4 5 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Network Performance Cloud networks

4	Simulate and test secure global computing systems	1 2 3 4 5	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Network Performance
5	Communicate and review secure global computing systems	1 2 3 4 5 6	Network types, models, topologies, and services Network layers, protocols and addressing Wired network components Mobile and wireless networks Network Performance Cloud networks

More information about synoptic assessment in these qualifications can be found in Section 6.2 Synoptic assessment.

6 Assessment and grading

6.1 Overview of the assessment

Entry code	H037
Qualification title	OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate)
GLH	150*
Reference	TBC
Total Units	Has two units: • Mandatory units F193 and F195

Entry code	H137
Qualification title	OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate)
GLH	360*
Reference	TBC
Total Units	Has five units: • Mandatory units F193, F194 and F195 • and two other units from F196, F197, F198 and F199.

*the GLH includes assessment time for each unit

Unit F193: **Fundamentals of cyber security**

75 GLH

1 hour 15 minute written exam

60 marks (60 UMS)

Set and marked by us

Calculators are not required in this exam

The exam will always **have**:

- A short scenario which will develop through the paper
- Forced choice/controlled response questions
- Short answer, closed response questions
- Extended constructed response questions with points-based marks schemes
- Extended constructed response questions with levels of response marks schemes
- One six mark and one nine mark extended constructed response question with a levels of response marks scheme

Unit F194: Fundamentals of networks

75 GLH

1 hour 15 minute written exam

60 marks (60 UMS)

Set and marked by us

Calculators may be used in this exam

The exam will **always** have:

- A short scenario which will develop through the paper
- Forced choice/controlled response questions
- Short answer, closed response questions
- Extended constructed response questions with points-based marks schemes
- Extended constructed response questions with levels of response marks scheme
- One six mark and one nine mark extended constructed response question with a levels of response marks scheme

The exam **may** have:

- Short answer questions with calculation/working

Unit F195: Preventing cyberattacks
75 GLH OCR-set assignment Centre-assessed and moderated by us This set assignment has four practical tasks. It should take 15 GLH to complete

Unit F196: Digital forensic investigation
70 GLH OCR-set assignment Centre-assessed and moderated by us This set assignment has three practical tasks. It should take 15 GLH to complete.

Unit F197: Penetration testing and incident response
70 GLH OCR-set assignment Centre-assessed and moderated by us This set assignment has four practical tasks. It should take 15 GLH to complete.

Unit F198: Implementing secure local area networks (LANs)
70 GLH OCR-set assignment Centre-assessed and moderated by us This set assignment has four practical tasks. It should take 15 GLH to complete.

Unit F199: Designing and communicating secure global computing systems
70 GLH OCR-set assignment Centre-assessed and moderated by us This set assignment has four practical tasks. It should take 15 GLH to complete.

OCR-set assignments for NEA units are on our secure website, Teach Cambridge. Each NEA assignment is live for two years. The intended cohort is shown on the front cover. It is important you use the correct NEA set assignment for each cohort, as starting a new cohort of Year 12 students on an NEA set assignment that has already been live for one year will mean that these students will only have one year to work on the assignment.

6.2 Synoptic assessment

Synoptic assessment is a built-in feature of these qualifications. It means that students need to use an appropriate selection of their knowledge, understanding and skills developed across each qualification in an integrated way and apply them to a key task or tasks.

This helps students to build a holistic understanding of the subject and the connections between different elements of learning, so they can go on to apply what they learn from these qualifications to new and different situations and contexts.

The externally assessed units allow students to gain underpinning knowledge and understanding relevant to cyber security and digital networking The NEA units draw on and strengthen this learning by assessing it in an applied and practical way.

It is important to be aware of the synoptic links between the units so that teaching, learning and assessment can be planned accordingly. Then students can apply their learning in ways which show they are able to make connections across the qualification. Section 5.3 shows the synoptic links for each unit.

6.3 Transferable skills

These qualifications give students the opportunity to gain broad, transferable skills and experiences that they can apply in future study, employment and life.

Higher Education Institutions (HEIs) have told us that developing some of these skills helps students to transition into higher education.

These skills include:

- Communication
- Creativity
- Critical thinking
- Independent learning
- Presentation skills
- Problem solving
- Reflection
- Resilience
- Risk taking
- Self-directed study
- Time management
- Writing for different purposes

6.4 Grading and awarding grades

Externally assessed units

We mark all the externally assessed units.

Each external assessment is marked according to a mark scheme, and the mark achieved will determine the unit grade awarded (Pass, Merit or Distinction). We determine grade boundaries for each of the external assessments in each assessment series.

If a student doesn’t achieve the mark required for a Pass grade, we issue an unclassified result for that unit. The marks achieved in the external assessment will contribute towards the student’s overall qualification grade, even if a Pass is not achieved in the unit assessment.

NEA units

NEA units are assessed by the teacher and externally moderated by us.

Each unit has specified Pass, Merit and Distinction assessment criteria. The assessment criteria for each unit are provided with the unit content in Section 5.3 of this specification. Teachers must judge whether students have met the criteria or not.

A unit grade can be awarded at Pass, Merit or Distinction. The number of assessment criteria needed to achieve each grade has been built into each assignment. These are referred to as design thresholds. The table below shows the design thresholds for each grade outcome for the NEA assessments in these qualifications. The unit grade awarded is based on the **total** number of achieved criteria for the unit. The total number of achieved criteria for each unit can come from achievement of any of the criteria (Pass, Merit or Distinction). This is **not** a ‘hurdles-based’ approach, so students do **not** have to achieve **all** criteria for a specific grade to achieve that grade (e.g. all Pass criteria to achieve a Pass).

The number of assessment criteria achieved for an NEA unit will be classed as the raw mark. Teachers will assess students' work and identify the number of criteria (raw marks) achieved for each NEA unit. Our moderators will moderate samples of work from each centre. This moderation process may result in the number of assessment criteria (raw marks) achieved being changed. The final raw mark achieved after moderation has taken place will be converted into a mark on the Uniform Mark Scale (UMS) and will contribute towards the student's overall qualification grade. (More information about UMS is in the section Calculating the qualification grade.)

To make sure we can keep outcomes fair and comparable over time, we will review the performance of the qualifications through their lifetime. The review process might lead to changes in these design thresholds if any unexpected outcomes or significant changes are identified.

Unit size (GLH)	**70**	**75**
Number of pass criteria	12	12
Number of merit criteria	7	7
Number of distinction criteria	5	5
Total number of criteria needed for a unit pass	10	10
Total number of criteria needed for a unit merit	15	15
Total number of criteria needed for a unit distinction	20	20
Total number of criteria available for the unit	24	24

If a student doesn't achieve enough criteria to achieve a unit Pass, we will issue an unclassified result for that unit. The number of criteria achieved will be converted into a mark on the Uniform Mark Scale (UMS) and will contribute towards the student's overall qualification grade, even if a Pass is not achieved in the unit assessment. More information about this is in the section below (Calculating the qualification grades).

Qualifications

The overall qualification grades are:

Certificate and Extended Certificate

- Distinction* (D*)
- Distinction (D)
- Merit (M)
- Pass (P)
- Unclassified (U)

Calculating the qualification grades

When we work out students' overall grades, we need to be able to compare performance on the same unit in different assessments over time and between different units. We use a Uniform Mark Scale (UMS) to do this.

A student's uniform mark for each externally assessed unit is calculated from the student's raw mark on that unit. A student's uniform mark for each NEA unit is calculated from the number of criteria the student achieves for that unit. The raw mark or number of criteria achieved are converted to the equivalent mark on the uniform mark scale. Marks between grade boundaries are converted on a pro rata basis.

When unit results are issued, the student's unit grade and uniform mark are given. The uniform mark is shown out of the maximum uniform mark for the unit (for example, 48/60).

The student's uniform marks for each unit will be aggregated to give a total uniform mark for the qualification. The student's overall grade will be determined by the total uniform mark.

The tables below show:

- the maximum raw marks or number of criteria, and uniform marks for each unit in the qualifications
- the uniform mark boundaries for each of the assessments in each qualification
- the minimum total mark for each overall grade in the qualifications.

Certificate Qualification:

Unit	Maximum raw mark/number of criteria	Maximum uniform mark (UMS)	Distinction* (UMS)	Distinction (UMS)	Merit (UMS)	Pass (UMS)
F193	60	60	-	48	36	24
F195	24	60	-	48	36	24
Qualification Totals	84	120	108	96	72	48

Extended Certificate Qualification:

Unit	Maximum raw mark/number of criteria	Maximum uniform mark (UMS)	Distinction* (UMS)	Distinction (UMS)	Merit (UMS)	Pass (UMS)
F193	60	60	-	48	36	24
F194	60	60	-	48	36	24
F195	24	60	-	48	36	24
F196	24	60	-	48	36	24
F197	24	60	-	48	36	24
F198	24	60	-	48	36	24
F199	24	60	-	48	36	24
Qualification Totals	192	300	270	240	180	120

You can find a marks calculator on the qualification page of our website to help you convert raw marks/number of achieved criteria into uniform marks.

6.5 Performance descriptors

Performance descriptors indicate likely levels of attainment by representative students performing at the Pass, Merit and Distinction grade boundaries at Level 3.

The descriptors must be interpreted in relation to the content in the units and the qualification as a whole. They are not designed to define that content. The grade achieved will depend on how far the student has met the assessment criteria overall. Shortcomings in some parts of the assessment might be balanced by better performance in others.

Level 3 Pass

At Pass, students show adequate knowledge and understanding of the basic elements of much of the content being assessed. They can develop and apply their knowledge and understanding to some basic and familiar contexts, situations and problems.

Responses to higher order tasks involving detailed discussion, evaluation and analysis are often limited.

Many of the most fundamental skills and processes relevant to the subject are executed effectively but lack refinement, producing functional outcomes. Demonstration and application of more advanced skills and processes might be attempted but not always executed successfully.

Level 3 Merit

At Merit, students show good knowledge and understanding of many elements of the content being assessed. They can sometimes develop and apply their understanding to different contexts, situations and problems, including some which are more complex or less familiar.

Responses to higher order tasks involving detailed discussion, evaluation and analysis are likely to be mixed, with some good examples at times and others which are less accomplished.

Skills and processes relevant to the subject, including more advanced ones, are developed in terms of range and quality. They generally lead to outcomes which are of good quality, as well as being functional.

Level 3 Distinction

At Distinction, students show thorough knowledge and understanding of most elements of the content being assessed. They can consistently develop and apply their understanding to different contexts, situations and problems, including those which are more complex or less familiar.

Responses to higher order tasks involving detailed discussion, evaluation and analysis are successful in most cases.

Most skills and processes relevant to the subject, including more advanced ones, are well developed and consistently executed, leading to high quality outcomes.

7 Non examined assessment (NEA) units

This section gives guidance on completing the NEA units. In the NEA units, students build a portfolio of evidence to meet the assessment criteria for the unit.

Assessment for these qualifications **must** adhere to JCQ's Instructions for Conducting Coursework. Do **not** use JCQ's Instructions for Conducting Non-examination Assessments – these are only relevant to GCE and GCSE specifications.

The NEA units are centre-assessed and externally moderated by us.

You **must** read and understand all the rules and guidance in this section **before** your students start the set assignments.

If you have any questions, please contact us for help and support.

7.1 Preparing for NEA unit delivery and assessment

7.1.1 Centre and teacher/assessor responsibilities

We assume the teacher is the assessor for the NEA units.

Before you apply to us for approval to offer these qualifications you must be confident your centre can fulfil all the responsibilities described below. Once you're approved, you can offer any of our general qualifications, Cambridge Nationals or Cambridge Advanced Nationals **without** having to seek approval for individual qualifications.

Here's a summary of the responsibilities that your centre and teachers must be able to fulfil. It is the responsibility of the head of centre[1] to make sure our requirements are met. The head of centre must ensure that:

- there are enough trained or qualified people to teach and assess the expected number of students you have in your cohorts.
- teaching staff have the relevant level of subject knowledge and skills to deliver and assess these qualifications.
- teaching staff will fully cover the knowledge, understanding and skills requirements in teaching and learning activities.
- allowed combinations of units are considered at the start of the course to be confident that all students can access a valid route through the qualifications.
- all necessary resources are available for teaching staff and students during teaching and assessment activities. This gives students every opportunity to meet the requirements of the qualification and reach the highest grade possible.
- there is a system of internal standardisation in place so that all assessment decisions for centre-assessed assignments are consistent, fair, valid and reliable (see Section 7.4.3).
- there is enough time for effective teaching and learning, assessment and internal standardisation.
- robust processes are in place to make sure that students' work is individual and confirmed as authentic (see Section 7.2.1).

[1] This is the most senior officer in the organisation, directly responsible for the delivery of OCR qualifications, For example, the headteacher or principal of a school/college. The head of centre accepts full responsibility for the correct administration and conduct of OCR exams.

- OCR-set assignments are used for students' summative assessments. You must make sure that students use the assignment that is live for the period during which they are taking their summative assessment.
- OCR-set assignments are **not** used for practice. This includes both assignments that are currently live or live assignments that have expired. Sample assessment material for each of the NEA units is available on our website. This sample assessment material can be used for practice purposes.
- students understand what they need to do to achieve the criteria.
- students understand what it means when we say work must be authentic and individual and they (and you) follow our requirements to make sure their work is their own.
- students know they must not reference another individual's personal details in any evidence produced for summative assessment, in accordance with the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR). It is the student's responsibility to make sure evidence that includes another individual's personal details is anonymised.
- outcomes submitted to us are correct and are accurately recorded and adhere to the published deadlines.
- assessment of set assignments adheres to the JCQ Instructions for Conducting Coursework and JCQ AI Use in Assessments: Protecting the Integrity of Qualifications.
- a declaration is made at the point you're submitting any work to us for assessment that confirms:
    - all assessment is conducted according to the specified regulations identified in the Administration area of our website.
    - students' work is authentic.
    - marks have been transcribed accurately.

(Failing to meet the assessment requirements might be considered as malpractice.)

- centre records and students' work are kept according to these requirements:
    - students' work **must** be kept until **after** the unit has been awarded and any review of results or appeals processed. We cannot consider any review if the work has not been kept.
    - internal standardisation and assessment records must be kept securely for a minimum of three years after the date we've issued a certificate for a qualification.
- all cases of suspected malpractice involving teachers or students are reported (see Section 7.3.1).

7.2 Requirements and guidance for delivering and marking the OCR-set assignments

The assignments are:

- set by us.
- taken under supervised conditions (unless we specify otherwise in the assessment guidance).
- assessed by the teacher.
- moderated by us.

You can find the set assignments on our secure website, Teach Cambridge. The set assignments give an approximate time that it will take to complete all the tasks. These timings are for guidance only, but should be used by you, the teacher, to give students an indication of how long to spend on each task. You can decide how the time should be allocated between each task or part task. Students can complete the tasks and produce the evidence across several sessions. Students' evidence (either hard copy or digital) must be kept securely by the teacher and access to assessment responses must be controlled. Students aren't permitted to access their work in between the assessment sessions.

We will publish a new set assignment each year and they will be live for two years. Each new set assignment will be released on 1 June. for teacher planning. You must not start delivery of live assignments with students until the live assessment dates, which are shown on the front cover. We strongly recommend you use the set assignment released in the same calendar year as the new cohort starts to ensure they have two years for that assignment. You may be disadvantaging students if you allow new cohorts to use assignments which have already been live for a year. This is because the assignments for each unit are designed for students to access throughout their two years of study. This enables resubmission opportunities across academic years if needed. Students are allowed one resubmission of work based on the same live assignment. Section 7.4.6 provides more information about resubmissions.

You must:

- only download set-assignments from our secure website, Teach Cambridge, and use a set assignment that is live for assessment for all summative assessment of students.
- have made unit entries before submitting NEA work for moderation.
- not share the set assignments with anyone from outside of your centre. These must only be shared with appropriate centre staff and students taking the assessments.
- (More information about maintaining the integrity of assessment materials is in the JCQ document General Regulations for Approved Centres General and Vocational qualifications.)
- make sure students know that they must not share assessment material or their own work with others, including posting or sharing on social media.
- (More information is in the JCQ guidance Information for candidates Using social media and examinations/assessments.)

Appendix A of this specification gives guidance for creating electronic evidence for the NEA units. Read Appendix A in conjunction with the unit content and assessment criteria grids to help you plan the delivery of each unit.

The rest of this section is about how to manage the delivery and marking of the set assignments so that assessment is valid and reliable. Please note that failing to meet these requirements might be considered as malpractice.

Here is a summary of what you need to do.

You **must**:

- have covered the knowledge, understanding and skills with your students and be sure they are ready for assessment **before** you start the summative assessment. This may include students practising applying their learning and receiving feedback from teachers in preparing to take the assessment.
- use the correct live OCR-set assignment for summative assessment of the students. The dates for which set assignments are live for summative assessment are shown on the front cover. These assignments are available on Teach Cambridge.
- give students the Student Guide before they start the assessment.

- familiarise yourself with the assessment guidance relating to the tasks. The assessment guidance for each unit is in Section 5 after the assessment criteria grids and with the student tasks in the assignments.

- make sure students are clear about the tasks they must complete and the assessment criteria they are attempting to meet.

- give students a reasonable amount of time to complete the assignments and be fair and consistent to all students. The estimated time we think each assignment should take is stated in the set assignments. In that time students can work on the tasks under the specified conditions until the date that you collect the work for centre assessment.

- tell the students the resources they can use in the assignment before they start the assessment tasks.

- only give students our templates. Where we think a template is useful for a task, we have provided it in the assignment. You must **not** give students any other templates to use when completing their live assignments. If they choose to use a different template from a book, a website or course notes (for example, to create a plan) they **must** make sure the source is referenced and that the template is not pre-populated with responses for which the students may gain marks.

- monitor students' progress to make sure work is capable of being assessed against the assessment criteria, on track for being completed in good time and is the student's own work:

    - NEA work must be completed in the centre under teacher supervision. Supervision is not invigilation. A supervised classroom does not require exam conditions in that classroom This would typically be in normal curriculum time:

        - work must be completed with enough supervision to make sure that it can be authenticated as the student's own work. The supervising teacher must be the teacher who will authenticate the students' work. You must be familiar with the requirements of the JCQ document AI Use in Assessments: Protecting the Integrity of Qualifications before assessment starts.

        - there may be exceptions to the requirement for supervised conditions if there is work to complete to support the assignment tasks (e.g. research). The assignment and assessment guidance will specify if there are exceptions.

          Where students are allowed to complete work outside of supervised conditions (e.g. research that may be allowed between supervised sessions) you **must** make sure that they only bring notes relating to the work they are allowed to complete unsupervised into the supervised sessions (e.g. notes relating to the research they have done) and to make sure any work they have done is independent. They must not use unsupervised time as an opportunity to:
            - Create drafts of work for their tasks.
            - Gather information to use in other aspects of their tasks.

        - if you provide any material to prepare students for the set assignment, you must adhere to the rules on using referencing and on acceptable levels of guidance to students. This is in Section 7.2.3 and 7.3.

        - students must produce their work independently (see Sections 7.2.1 and 7.3).

        - you must make sure students know to keep their work and passwords secure and know that they must not share completed work with other students, use any aspect of another student's work or share their passwords.

- complete the **Teacher Observation Record** that is with the assignments for tasks that state it is needed. This must be submitted with the students' evidence. You **must** follow the guidance with the form given when completing it.
- use the assessment criteria to assess students' work.
- before submitting a final outcome to us, you can mark students' completed work and allow them to repeat any part of the assignment, reworking their original evidence. We call this a reattempt. Students must have completed the whole assignment before you mark their work. Any feedback you give to students on the marked work, must:
  - be factual: telling the student what you have observed, not what to do to improve their work.
  - be recorded.
  - be available to the moderator.

(See Section 7.3 on Feedback and Section 7.4.4 on reattempting work.)

You **must not**:

- create your own assignments for students to use for practice or live assessment.
- change any part of the OCR-set assignments (scenarios or tasks).
- mark students' work in stages, providing feedback at each stage. This would be iterative assessment which is not allowed.
- accept multiple reattempts of work where small changes have been made in response to feedback. Marking and feedback must not be an iterative process
- allow teachers or students to add, amend or remove any work **after** submission for moderation.
- give detailed advice and suggestions to individuals or the whole class on how work may be improved to meet the assessment criteria. This includes giving access to student work as an exemplar.
- allow students access to their assignment work between teacher supervised sessions. (There may be exceptions where students are allowed to complete work independently (e.g. research). Any exceptions will be stated in the assignments.)
- practise the live OCR-set assignment tasks with the students. We provide Sample Assignments for you to use for practice purposes.

7.2.1 Ways to authenticate work

All NEA work must be completed under teacher supervision (unless the assessment guidance for a specific task or sub-task advises otherwise). In addition, you must complete enough checks to be confident that the work you mark is the student's own and was produced independently.

You should discuss work in progress with students, including asking them questions such as what they are planning/doing and why This will make sure that work is being completed in a planned and timely way and will give you opportunities to check the authenticity of the work. This is not an opportunity to offer additional guidance to students.

You **must**:

- have read and understood the JCQ document AI Use in Assessments: Protecting the Integrity of Qualifications.

- make sure students and other teachers understand what constitutes plagiarism and other forms of malpractice (e.g. collusion and copying).
- not accept plagiarised work as evidence.
- use questioning as appropriate to confirm authenticity.
- make sure students and teachers fill in authentication statements.

7.2.2 Group work

Group work is not allowed for the NEA assignments in these qualifications.

7.2.3 Plagiarism

Students must use their own words when they produce final written pieces of work to show they have genuinely applied their knowledge and understanding. When students use their own words, ideas and opinions, it reduces the possibility of their work being identified as plagiarised. Plagiarism is:

- the submission of someone else's work as your own
- failure to acknowledge a source correctly, including any use of written material, the internet or Artificial Intelligence (AI).

You might find the following JCQ documents helpful:

- Plagiarism in Assessments
- AI Use in Assessments: Protecting the Integrity of Qualifications

Due to increasing advancements in AI technology, we strongly recommend that you are familiar with the likely outputs from AI tools. This could include using AI tools to produce responses to some of the assignment tasks, so that you can identify typical formats and wording that these may produce. This may help you identify any cases of potential plagiarism from students using AI tools to generate written responses.

Plagiarism makes up a large percentage of cases of suspected malpractice reported to us by our moderators. You must **not** accept plagiarised work as evidence.

Plagiarism often happens innocently when students do not know that they must reference or acknowledge their sources or aren't sure how to do this. It's important to make sure your students understand:

- the meaning of plagiarism and what penalties may be applied.
- that they can refer to research, quotations or evidence produced by somebody else, but they must list and reference their sources and clearly mark quotations.
- quoting someone else's work, even when it's properly sourced and referenced, doesn't evidence understanding. The student must 'do' something with that information to show they understand it. For example, if a student has to analyse data from an experiment, quoting data doesn't show that they understand what it means. The student must interpret the data and, by relating it to their assignment, say what they think it means. The work must clearly show how the student is using the material they have referenced to inform their thoughts, ideas or conclusions.

We have The OCR Guide to Referencing on our website. We have also produced a poster about referencing and plagiarism which may be useful to share with your students.

Teach your students how to reference and explain why it's important to do it. At Key Stage 5 they must:

- use quote marks to show the beginning and end of the copied work.
- list the html address for website text and the date they downloaded information from the website.
- show the name of the AI source used and the date the content was generated for computer-generated content (such as an AI Chatbot).
- for other publications, list:
    - the name of the author.
    - the name of the resource/book/printed article.
    - the year in which it was published.
    - the page number.

Teach your students to:

- always reference material copied from the internet or other sources. This also applies to infographics (graphical information providing data or knowledge).
- always identify information they have copied from teaching handouts and presentations for the unit, using quote marks and stating the text is from class handouts.

Identifying copied/plagiarised work

Inconsistencies throughout a student's work are often indicators of plagiarism. For example:

- different tones of voice, sentence structure and formality across pieces of work.
- use of American expressions, spellings and contexts (such as American laws and guidelines).
- dated expressions and references to past events as being current.
- sections of text in a document where the font or format is inconsistent with other sections.

What to do if you think a student has plagiarised

If you identify plagiarised work during assessment or internal standardisation, you must:

- consider the plagiarism when judging the number of assessment criteria achieved. (You must not award assessment criteria where the work is plagiarised.)
- record that there is plagiarism in the work on the Unit Recording Sheet (URS) and that you have adjusted the number of assessment criteria achieved to take account of the plagiarism.
    - if the work is requested as part of the moderation sample, it must be provided to our moderator with the other work requested.

If plagiarism is identified during ongoing monitoring of students' work, you can address this in your centre (for example, by instructing the student(s) involved to re-do the affected tasks).

If plagiarism is identified when the work has been submitted to you as final for marking, you must:

- report the student(s) for plagiarism in line with the JCQ document Suspected Malpractice Policies and Procedures
    - fill in the **JCQ form M1**.

In line with JCQ's policies and procedures on suspected malpractice, the penalties applied for plagiarism will usually result in the work not being allowed (disqualification) or the mark being significantly reduced.

7.3 Feedback

Feedback to students on work in progress towards summative assessment

You can discuss work in progress towards summative assessment with students to make sure it's being done in a planned and timely way. It also provides an opportunity to check the authenticity of the work. You must intervene if there's a health and safety risk (and reflect this in your assessment if the student's ability to operate safely and independently is part of the criteria).

Generic guidance to the whole class is also allowed. This could include reminding students to check they have provided evidence to cover all key aspects of the task. Individual students can be prompted to double check for gaps in evidence providing that specific gaps are not pointed out to them.

You can give general feedback and support if one or more students are struggling to get started on an aspect of the assignment or following a break between sessions working on the assignment. For example, if a student is seeking more guidance that suggests they are not able to apply knowledge, skills and understanding to complete their evidence, you can remind them that they had a lesson which covered the topic. The student would then need to review their own notes to find this information and apply it as needed.

If a student needs additional help to get started on an initial task that is critical to accessing the rest of the assessment, you can provide this help if you feel it is necessary, but you must not award the student with any assessment criteria directly associated with the part(s) of the task for which they received help. This **must** be recorded on the student's work and/or Unit Recording Sheet (URS) for our moderator to see. More information about how to record additional help given in these circumstances is in Section 7.4.1.

With the exception of the specific feedback allowed to help students start a critical task, mentioned above, feedback must not provide specific advice and guidance that would be construed as coaching. This would compromise the student's ability to independently perform the task(s) they are doing and constitutes malpractice. Our moderators use a number of measures to assure themselves the work is the student's own.

Assessing completed work

When students have completed their work on an assignment, you must assess it and give feedback to them on the completed work they submitted to you for assessment. (Section 7.4.1 has more information about how to assess NEA work.) Assessment should not be an iterative process. This means you must not assess work and give feedback on it in stages. You must only assess the work when the assignment is complete.

Feedback **must**:

- be supportive, encouraging and positive.
- tell the student what has been noticed, not what you think (for example, if you have observed the student completing a task, you can describe what happened, what was produced and what was demonstrated).

Feedback **can**:

- identify what task and part of the task could be improved, but not say how to improve it. You could show the student work from a **different** unit that demonstrates higher achievement, but you must not detail to the student how they could achieve that in their work. If you are using another student's work from a different unit as an example, you must anonymise this work and make sure that the potential to plagiarise from this work is minimised. You could remind students that they had a lesson on a specific topic and that they could review their notes, but you must not tell them how they could apply the teaching to improve their work.

- comment on what has been achieved, for example 'the evidence meets the P2 and M2 criteria'.
- identify that the student hasn't met a command word or assessment criteria requirement. For example, 'This is a description, not an evaluation'.
- use text from the specification, assignment or assessment criteria in general guidance to clarify what is needed in the work. For example, 'P2 requires you to use a risk matrix to define the severity level of all risks identified in P1'.

Feedback **must not**:

- point out specific gaps. For example, you must not prompt the student to include specific detail in their work, such as 'The justifications for D3 don't justify how each cyber security prevention policy and measure designed relate to the three pillars of information security. Some justifications don't mention process, and all don't mention technology.'
- be so detailed that it leads students to the answer. For example, you must not give:
    - model answers.
    - step-by-step guidance on what to do to complete or improve work.
    - headings or prompts that include examples which give all or part of what students have to write about or produce.
- talk the student through how to achieve or complete the task.
- give detail on where to find information/evidence.

In other words, feedback must help the student to take the initiative in making changes. It must not direct or tell the student what to do to complete or improve their work in a way that means they do not need to think how to apply their learning. Students need to recall or apply their learning. You must not do the work for them.

Students can reattempt their work on an assignment after you have marked it and provided feedback. This **must** happen before the work is submitted to us for moderation. Neither you nor the student can add, amend or remove any work after the final mark has been submitted for moderation.

Sections 7.4.4 and 7.4.6 give more guidance for students who wish to reattempt or resubmit their work following feedback.

What improper assistance might look like

When we see anything that suggests the teacher has led students to the answer, we become concerned because it suggests students have not worked independently to produce their assignment work. The following are examples of what might indicate improper assistance by the teacher:

- prompts that instruct students to include specific detail in their work, such as, 'You need to include the aims of the activity. Who is it aimed at? What is the purpose of the activity? How will it benefit the specific group/individual?'
- headings or templates that include examples which give all or part of what students have to write about or produce, such as sources of support.

Our moderators will report suspected malpractice when they cannot see differences in content between students' work in the sample they are moderating. An exception is when students have only used and referenced technical facts and definitions. If our moderator is in any doubt, they will report suspected malpractice. The decision to investigate or not is made by us, not the moderators.

7.3.1 Reporting suspected malpractice

It is the responsibility of the head of centre to report all cases of suspected malpractice involving teachers or students.

A JCQ Report of Suspected Malpractice form (JCQ/M1 for student suspected malpractice or JCQ/M2 for staff suspected malpractice) is available to download from the JCQ website. The form must be completed as soon as possible and emailed to us at compliance@ocr.org.uk.

When we ask centres to gather evidence to assist in any malpractice investigation, heads of centres must act promptly and report the outcomes to us.

The JCQ document Suspected Malpractice Policies and Procedures has more information about reporting and investigating suspected malpractice, and the possible sanctions and penalties which could be imposed. You can also find out more on our website.

7.3.2 Student and centre declarations

Both students and teachers must declare that the work is the student's own:

- **each student** must sign a declaration before submitting their work to their teacher. A **candidate authentication statement** can be used and is available to download from our website. You must keep these statements in the centre until all reviews of results, malpractice and appeal issues have been resolved.

- **teachers** must declare the work submitted for centre assessment is the students' own work by completing a centre authentication form (CCS160) for each cohort of students for each unit. You must keep centre authentication forms in the centre until all post-results issues have been resolved

7.3.3 Generating evidence

The set assignments will tell the students what they need to do to meet the assessment criteria for the NEA units. It is your responsibility to make sure that the methods of generating evidence for the assignments are:

- valid
- safe and manageable
- suitable to the needs of the student.

Valid

The evidence presented must be valid. For example, it would not be appropriate to present an organisation's equal opportunities policy as evidence towards a student's understanding of how the equal opportunities policy operates in an organisation. It would be more appropriate for the student to incorporate the policy in a report describing the different approaches to equal opportunities.

Safe and manageable

You must make sure that methods of generating evidence and approaches taken:

- are safe and manageable
- do not put unnecessary demands on the student.

- are appropriate and in line with ethical standards and your centre's safeguarding responsibilities.

Suitable to the needs of the student

We are committed to ensuring that achievement of these qualifications is free from unnecessary barriers.

Observation and questioning

The primary evidence for assessment is the work submitted by the student, however the following assessment methods might be suitable for you to use for some aspects of these qualifications, where identified:

- **observation** of a student doing something
- **questioning** of the student or witness.

Observation

You and the student should plan observations together, but it is your responsibility to record the observation properly (for example observing a student undertaking a practical task). More information is in the Teacher Observation Records section.

Questioning

Questioning the student is normally an ongoing part of the formative assessment process and may, in some circumstances, provide evidence to support achievement of the criteria.

Questioning is often used to:

- test a student's understanding of work which has been completed outside of the classroom (where this may be permitted)
- check if a student understands the work they have completed
- collect information on the type and purpose of the processes a student has gone through.

If questioning is used as evidence towards achievement of specific topic areas, it is important that you record enough information about what they asked and how the student replied, to allow the assessment decision to be moderated.

7.3.4 Teacher Observation Records

You **must** complete the Teacher Observation Record form in the OCR-set assignment for:

Unit F196 - a Teacher Observation Record (TOR) form **must** be provided for each student as evidence of the digital forensic tools and techniques used to complete the planned digital forensic investigation (Task 2, Topic Area 3). Students **must** also read and sign the TOR form. Each TOR form **must** describe the digital forensic tools and techniques used by the student. For this task students **must** also provide evidence such as photos or videos showing them collecting digital evidence during their digital forensic investigation.

Unit F197 - a Teacher Observation Record (TOR) form **must** be provided for each student as evidence of demonstrating exploitation activities (Task 3, Topic Area 3). Students **must** also read and sign the TOR form. The TOR form **must** provide clear evidence that the student has demonstrated **three** exploitation activities from their exploitation activities test plan (P5). The TOR form **must** include a description of how each exploitation activity was completed by the student including the tools and techniques they used, and the success of the exploitation activity. For other criteria in this task the student **must** provide suitable evidence in the form of an exploitation activity test plan and written evidence.

Unit F198 - a Teacher Observation Record (TOR) form **must** be provided for each student as evidence of safely connecting and configuring LAN components, and the techniques used troubleshoot faults (Task 3, Topic Areas 3 and 4). Students **must** also read and sign the TOR form. Each TOR form **must** describe how the student safely used tools and techniques when connecting and configuring LAN components and troubleshooting faults. You **must** intervene if there's a health and safety risk and reflect this in your assessment if the student needed additional help in order to work safely and independently to meet the assessment criteria in this task. For this task students **must** also provide evidence such as photos or videos showing them connecting and configuring LAN components and troubleshooting faults.

Teacher observation **cannot** be used as evidence of achievement for a whole unit. Most evidence **must** be produced directly by the student. Teacher observation **must only** be used where specified as an evidence requirement.

Teacher Observation Records must be individual to each student and suitably detailed to help moderators to determine if the assessment criteria have been met. You must follow the guidance provided in the 'guidance notes' section of the form so that the evidence captured and submitted is appropriate. Both you and the student must sign and date the form to show that you both agree its contents. Electronic signatures are acceptable. The signed form must form part of the students' evidence and be submitted with work requested for moderation.

Where the guidance has not been followed, the reliability of the form as evidence may be called into question. If doubt about the validity of the Teacher Observation Record form exists, it cannot be used as assessment evidence and marks based on it cannot be awarded. Our moderators will be instructed to adjust centre marks accordingly.

7.3.5 Presentation of the final piece of work

Students must submit their evidence in the format specified in the tasks where specific formats are given. Written work can be digital (e.g. word processed) or hand-written and tables and graphs (if relevant) can be produced using appropriate ICT.

Any sourced material must be suitably acknowledged. Quotations must be clearly marked and a reference provided.

A completed Unit Recording Sheet (URS) must be attached to work submitted for moderation.

The URS can be downloaded from the qualification webpage or Teach Cambridge. Centres **must** show on the URS where specific evidence can be found. The URS tells you how to do this.

Work submitted digitally for moderation **must** be in a suitable file format and structure. Appendix A gives more guidance about submitting work in digital format.

7.4 Assessing NEA units

All NEA units are assessed by teachers and externally moderated by our moderators. Assessment of the set assignments must adhere to JCQ's Instructions for Conducting Coursework.

The centre is responsible for appointing someone to act as the internal assessor. This would usually be the teacher who has delivered the programme but could be another person from the centre. The assessment criteria must be used to assess the student's work. These specify the levels of skills, knowledge and understanding that the student needs to demonstrate.

7.4.1 Applying the assessment criteria

When students have completed the assignment, they must submit their work to you to be assessed.

You must assess the tasks using the assessment criteria and any additional assessment guidance provided. Each criterion states what the student needs to do to achieve that criterion (e.g. Create an appropriate risk assessment for the organisation). The command word and assessment guidance provide additional detail about breadth and depth where it is needed.

You must judge whether each assessment criterion has been **successfully achieved** based on the evidence that a student has produced. For the criterion to be achieved, the evidence must show that all aspects have been met in sufficient detail.

When making a judgement about whether a criterion has been **successfully achieved**, you must consider:

- the requirements of the specific NEA task that the student is completing
- the criterion wording, including the command word used and its definition
- any assessment guidance for the criterion
- the unit content that is being assessed.

You must annotate the work to show where evidence meets each criterion (see Section 7.4.2). You can then award the criterion on the Unit Recording Sheet (URS). Assessment should be positive, rewarding achievement rather than penalising failure or omissions.

The number of criteria needed for each unit grade (Pass, Merit or Distinction) is provided in Section 6.4.

You must complete a Unit Recording Sheet (URS) for each unit a student completes. On the URS you must identify:

- whether the student has met each criterion or not (by adding a tick (✓) or X in the column titled **Assessment criteria achieved**)
    - you should also indicate where the evidence can be found if a '✓' is identified.
    - a X indicates that there is insufficient evidence to fully meet the criterion or it was not attempted.
- the total number of criteria achieved by the student for the unit. The total number of criteria achieved is their 'raw mark'

You must be convinced, from the evidence presented, that students have worked independently to the required standard.

If you have given additional, more specific support or guidance to an individual student to get them started on a task, because they could not start a task or part of a task that was **critical to them accessing the rest of the task or assignment** (see Section 7.3), this **must** also be recorded on the student's work and/or Unit Recording Sheet (URS) for our moderator to see. In this situation, the student should **not** be awarded the assessment criteria for the work for which they received help, and the number of criteria achieved must be adjusted appropriately. Recording this on the student's work and/or URS will help our moderator to understand why the assessment criteria have not been awarded.

Your centre must internally standardise the assessment decisions for the cohort **before** you give feedback to students (see Section 7.4.3). When you are confident the internal assessment standardisation and appeals process is complete, you can submit work for moderation at the relevant time. You **must not** add, amend or remove any work after it has been submitted to us for final moderation. Work **must** be kept securely until the end of the review of results process.

7.4.2 Annotating students' work

Each piece of NEA work must show how you are satisfied the assessment criteria have been met.

Comments on students' work and the Unit Recording Sheet (URS) provide a means of communication about assessment decisions made, between teachers during internal standardisation, and with our moderators if the work is part of the moderation sample. (Comments or annotations must not be used as a method of communication with our moderator for any other reason.)

7.4.3 Internal standardisation

It is important that all teachers are assessing work to common standards. For each unit, centres must make sure that internal standardisation of outcomes across teachers and teaching groups takes place using an appropriate procedure.

This can be done in a number of ways. In the first year, reference material and our training meetings will provide a basis for your centre's own standardisation. In following years, this, and/or your own centre's archive material, can be used. We advise you to hold preliminary meetings of staff involved to compare standards through cross-marking a small sample of work. After you have completed most of the assessment, a further meeting at which work is exchanged and discussed will help you make final adjustments.

If you are the only teacher in your centre assessing these qualifications, we still advise you to make sure your assessment decisions are internally standardised by someone else in your centre. Alternatively, this could be a teacher that may be delivering in another local centre or as part of your Multi Academy Trust (MAT) if relevant. Ideally this person will have experience of these types of qualifications, for example someone who:

- is delivering a similar qualification in another subject.
- has relevant subject knowledge.

You must keep evidence of internal standardisation in the centre for our moderators to see.

We have a guide to how internal standardisation can be approached on our website.

7.4.4 Reattempting work to improve the grade before submitting marks to us

As described in Section 7.2, **before** submitting a final outcome to us for external moderation, you can allow students to repeat any element of the assignment and rework their original evidence. We refer to this as a reattempt. A reattempt allows the student to reflect on **internal** feedback, and to improve their work. A reattempt is **not** an iterative process where students make small modifications through ongoing feedback to eventually achieve the desired outcome.

Any feedback **must** be noted by the teacher and a record of this kept in centre. We have provided a feedback form for this purpose, which can be found on our website and Teach Cambridge. We recommend that you use the feedback form we provide or create your own recording form.

To summarise, a reattempt is a process that is internal to the centre. This allows students to rework their evidence:

- after it has been marked by you as a complete assignment.
- before it is submitted to us as the final work.

A reattempt **must** be done before submission for external moderation. When a student submits the work to you as final for external moderation, they **must not** complete any further work on any aspect of it.

7.4.5 Submitting outcomes

When you have assessed the work and it has been internally standardised, outcomes can be submitted to us. For the purpose of submission, outcomes will be considered as 'marks'. You will submit the total number of criteria achieved for units as marks. You must have made entries before you can submit marks. You can find the key dates and timetables on our website.

There should be clear evidence that work has been attempted and some work produced. If a student does not submit any work for an NEA unit, the student should be identified as being absent from that unit.

If a student completes any work at all for an NEA unit, you must assess the work using the assessment criteria and award the appropriate number of criteria. This might be zero.

7.4.6 Resubmitting moderated work to us to improve the grade

We use the term 'resubmission' when referring to student work that has previously been submitted to us for moderation. Following moderation, if you and the student feel they have not performed at their best during the assessment, the student can, with your agreement, improve their work and resubmit it to you again for assessment and to us for external moderation. You must be sure it is in the student's best interests to resubmit the work for assessment. There is one resubmission opportunity per NEA assignment. If you have submitted the same assignment twice for a student, they will need to use the next live assignment for any further reattempt and resubmission.

Students can only resubmit work using the **same** assignment if the assignment is still live. The live assessment dates and intended cohort will be shown on the front cover of the assignment. We will not accept work based on an assignment that is no longer live. If the assignment is no longer live, students will need to produce work using the new live assignment for the unit for the resubmission.

If students are resubmitting using a new live assignment, they can use the evidence they produced for the previous assignment, but they will need to make any changes that are necessary so that the work meets the requirements of the new scenario and task.

Students can also build on the work to improve it. All work for a resubmission must be completed under the required teacher supervised conditions and marked against the assessment criteria and assessment guidance. You must not over direct students on how to adapt/improve work to meet the requirements of the new assignment. You must adhere to all requirements relating to giving and recording feedback from Section 7.3 and Section 7.4.4.

To summarise, a resubmission is the reworking and submitting of assignment evidence and marks to us, following previous external moderation by us.

7.5 Moderating NEA units

The purpose of external moderation is to make sure that the standard of assessment is the same for all centres and that internal standardisation has taken place.

The administration pages of our website give full details about how to submit work for moderation.

This includes the deadline dates for entries and submission of marks. For moderation to happen, you must submit your marks by the deadline.

7.5.1 Sample requests

Once you have submitted your marks, we will tell you which work will be sampled as part of the moderation process. Samples will include work from across the range of students' attainment.

Students’ work must be securely kept until after the unit has been awarded and any review of results and appeals windows are closed.

Centres will receive the final outcomes of moderation when the provisional results are issued. Results reports will be available for you to access. More information about the reports that are available is on our administration pages.

We need sample work to help us monitor standards. We might ask some centres to release work for this purpose. We will let you know as early as possible if we need this from you. We always appreciate your co-operation.

8 Administration

This section gives an overview of the processes involved in administering these qualifications. More information about the processes and deadlines involved at each stage is on our administration pages.

8.1 Assessment availability

There are two assessment opportunities available each year for the externally assessed units: one in January and one in June. Students can be entered for different units in different assessment series.

All students must take the exams at a set time on the same day in a series.

NEA assignments can be taken by students at any time during the live period shown on the front cover. It is important you use the set assignment that is released in the same calendar year as the new cohort starts to ensure that students have two years to use the assignment.

There are two windows each year to submit NEA outcomes.

You must make unit entries for students before you can submit outcomes for a visit. All dates relating to NEA moderation are on our administration pages.

Qualification certification is available at each results release date.

8.2 Collecting evidence of student performance to ensure resilience in the qualifications system

Regulators have published guidance on collecting evidence of student performance as part of long-term contingency arrangements to improve the resilience of the qualifications system. You should review and consider this guidance when delivering this qualification to students at your centre.

For more detailed information on collecting evidence of student performance please visit our website.

8.3 Equality Act information relating to Cambridge Advanced Nationals

The Cambridge Advanced Nationals require assessment of a broad range of skills and, as such, prepare students for further study and higher-level courses.

The Cambridge Advanced National qualifications have been reviewed to check if any of the competences required present a potential barrier to disabled students. If this was the case, the situation was reviewed again to make sure that such competences were included only where essential to the subject.

8.4 Accessibility

There can be adjustments to standard assessment arrangements based on the individual needs of students. It is important that you identify as early as possible if students have disabilities or particular difficulties that will put them at a disadvantage in the assessment situation and that you choose a qualification or adjustment that allows them to demonstrate attainment.

If a student requires access arrangements that need approval from us, you must use Access arrangements (online) to gain approval. You must select the appropriate qualification type(s) when you apply. Approval for GCSE or GCE applications alone does not extend to other qualification types. You can select more than one qualification type when you make an application. For guidance or support please contact our Special Requirements Team.

The responsibility for providing adjustments to assessment is shared between your centre and us. Please read the JCQ document Access Arrangements and Reasonable Adjustments.

If you have students who need a post-exam adjustment to reflect temporary illness, indisposition or injury when they took the assessment, please read the JCQ document A guide to the special consideration process.

If you think any aspect of these qualifications unfairly restricts access and progression, please email Support@ocr.org.uk or call our Customer Support Centre on **01223 553998**.

The following access arrangements are allowed for this specification:

Access arrangement	Type of assessment
Reader/computer reader	All assessments
Scribes/speech recognition technology	All assessments
Practical assistants	All assessments
Word processors	All assessments
Communication professional	All assessments
Language modifier	All assessments
Modified question paper	Timetabled exams
Extra time	All assessments with time limits

8.5 Requirements for making an entry

We provide information on key dates, timetables and how to submit marks on our website.

Your centre must be registered with us as an approved centre before you enrol students and can make entries. Centre approval should be in place well in advance of making your first entries. Details on how to register with us are on our website.

8.5.1 Making estimated unit entries

Estimated entries are not needed for Cambridge Advanced National qualifications.

8.5.2 Making final unit entries

When you make an entry, you need to know the unit entry codes including the option code where required. Students submitting work must be entered for the appropriate unit entry code from the table below.

The short title for these Cambridge Advanced Nationals is CAN AAQ. This is the title that will be displayed on Interchange, and some of our administrative documents.

Individual unit entries should be made for each series in which you intend to submit or resubmit an NEA unit or sit an externally assessed examination.

Make a certification entry using the overall qualification code (see Section 8.6) in the final series only.

Unit entry code	Component code	Assessment method	Unit titles
F193	01	Written paper	Fundamentals of cyber security
F194	01	Written paper	Fundamentals of networks
F195	01	Moderated	Preventing cyberattacks
F196	01	Moderated	Digital forensic investigation
F197	01	Moderated	Penetration testing and incident response
F198	01	Moderated	Implementing secure local area networks (LANs)
F199	01	Moderated	Designing and communicating secure global computing systems

8.6 Certification rules

You must enter students for qualification certification separately from unit assessment(s). If a certification entry is **not** made, no overall grade can be awarded. These are the qualifications that students should be entered for:

- OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Certificate) - certification code H037.
- OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate) - certification code H137.

8.7 Unit and qualification resits

Students can resit the assessment for each unit and the best result will be used to calculate the certification result. Students may resit each external assessment twice before certification.

Resit opportunities must be fair to all students and **not** give some students an unfair advantage over other students. For example, the student must not have direct guidance and support from the teacher in producing further evidence for NEA units. When resitting an NEA unit, students must submit new, amended or enhanced work, as detailed in the JCQ Instructions for Conducting Coursework.

When you arrange resit opportunities, you must make sure that you do not adversely affect other assessments being taken.

Arranging a resit opportunity is at the centre’s discretion. Summative assessment series must not be used as a diagnostic tool and resits should only be planned if the student has taken full advantage of the first assessment opportunity and any formative assessment process.

8.8 Post-results services

A number of post-results services are available:

- Reviews of results - if you think there might be something wrong with a student's results, you may submit a review of marking or moderation.
- Missing and incomplete results - if an individual subject result for a student is missing, or the student has been omitted entirely from the results supplied you should use this service.
- Access to scripts - you can ask for access to marked scripts.
- Late certification - following the release of unit results, if you have not previously made a certification entry, you can make a late request, which is known as a late certification. This is a free service.

Please refer to the JCQ Post-Results Services booklet and our Administration page for more guidance about action on the release of results.

For each NEA unit, a review of moderation can only be requested for the cohort. It cannot be requested for individual students.

Appendix A: Guidance for the production of electronic evidence

Structure for evidence

The NEA units in these qualifications are units F195–F199. For each student, all the tasks together will form a portfolio of evidence, stored electronically. Evidence for each unit must be stored separately.

An NEA portfolio is a collection of folders and files containing the student's evidence. Folders should be organised in a structured way so that the evidence can be accessed easily by a teacher or OCR moderator. This structure is commonly known as a folder tree. It would be helpful if the location of particular evidence is made clear by naming each file and folder appropriately and by use of an index called 'Home Page'.

There should be a top-level folder detailing the student's centre number, OCR candidate number, surname and forename, together with the unit code (F195–F199), so that the portfolio is clearly identified as the work of one student.

Each student's portfolio should be stored in a secure area on the centre's network. Before submitting the portfolio to us, the centre should add a folder to the folder tree containing the internal assessment and summary forms.

Data formats for evidence

It is necessary to save students' work using an appropriate file format to minimise software and hardware capability issues.

Students must use formats appropriate:

- to their evidence
- for viewing for assessment and moderation.

Formats must be open file formats or proprietary formats for which a downloadable reader or player is available. If a downloadable reader or player is not, the file format is **not** acceptable.

Evidence submitted is likely to be in the form of word-processed documents, presentation documents, digital photos and digital video.

All files submitted electronically must be in the formats listed on the following page. Where new formats become available that might be acceptable, we will give more guidance. It is the centre's responsibility to make sure that the electronic portfolios submitted for moderation are accessible to our moderator and fully represent the evidence available for each student.

Standard file formats acceptable as evidence for the Cambridge Advanced Nationals are listed here.

File type	File format	Max file size*
Audio	.3g2 .3ga .aac .aiff .amr .m4a .m4b .m4p .mp3 .wav	25GB
Compression	.zip .zipx .rar .tar .tar .gz .tgz .7z .zipx .zz	25GB
Data	.xls .xlsx .mdb .accdb .xlsb	25GB
Document	.odt .pdf .rtf .txt .doc .docx .dotx .	25GB
Image	.jpg .png .jpeg .tif .jfif .gif .heic .psd .dox .pcx .bmp .wmf	25GB
Presentation	.ppt .pptx .pdf .gslides .pptm .odp .ink .potx .pub	25GB
Video	.3g2 .3gp .avi .flv .m4v .mkv .mov .mp4 .mp4v .wmp .wmv	25GB
Web	.wlmp .mts .mov-1 .mp4-1 .xspf .mod .mpg	25GB

If you are using **.pages** as a file type, please convert this to a .pdf prior to submission.

*max file size is applicable when using our Submit for Assessment service.

Submit for Assessment is our secure web-based submission service. You can access Submit for Assessment on any laptop or desktop computer running Windows or macOS and a compatible browser. It supports the upload of files in the formats listed in the table above as long as they do not exceed the maximum file size. Other file formats and folder structures can be uploaded within a compressed file format.

When you view some types of files in our Submit for Assessment service, they will be streamed in your browser. It would help our moderator or examiner if you could upload files in the format shown in the table below:

File type	File format	Chrome	Firefox
Audio	.mp3	Yes	Yes
Audio	.m4a	Yes	Yes
Audio	.aac	No	Yes
Document	.txt	Yes	Yes
Image	.png	Yes	Yes
Image	.jpg	Yes	Yes
Image	.jpeg	Yes	Yes
Image	.gif	Yes	Yes
Presentation	.pdf	Yes	Yes
Video	.mp4	Yes	Yes
Video	.mov	No	Yes
Video	.3gp	Yes	No
Video	.m4v	Yes	Yes
Web	.html	Yes	Yes
Web	.htm	Yes	Yes

Appendix B: Command Words

External assessment

The table below shows the command words that will be used in exam questions. This shows what we mean by the command word and how students should approach the question and understand its demand. Remember that the rest of the wording in the question is also important.

Command Word	Meaning
Analyse	• Separate or break down information into parts and identify their characteristics or elements • Explain the different elements of a topic or argument and make reasoned comments • Explain the impacts of actions using a logical chain of reasoning
Annotate	• Add information, for example, to a table, diagram or graph
Calculate	• Work out the numerical value. Show your working unless otherwise stated
Choose	• Select an answer from options given
Compare	• Give an account of the similarities and differences between two or more items or situations
Complete	• Add information, for example, to a table, diagram or graph to finish it
Describe	• Give an account that includes the relevant characteristics, qualities or events
Discuss (how/whether/etc)	• Present, analyse and evaluate relevant points (for example, for/against an argument) to make a reasoned judgement
Draw	• Produce a picture or diagram
Explain	• Give reasons for and/or causes of something • Make something clear by describing and/or giving information
Give examples	• Give relevant examples in the context of the question
Identify	• Name or provide factors or features from stimulus
Label	• Add information, for example, to a table, diagram or graph until it is final
Outline	• Give a short account or summary
State	• Give factors or features • Give short, factual answers

Non examined assessment (NEA)

The table shows the command words that will be used in the NEA assignments and/or assessment criteria.

Command Word	Meaning
Adapt	• Change to make suitable for a new use or purpose
Analyse	• Separate or break down information into parts and identify their characteristics or elements • Explain the different elements of a topic or argument and make reasoned comments • Explain the impacts of actions using a logical chain of reasoning
Assess	• Offer a reasoned judgement of the standard or quality of situations or skills. The reasoned judgement is informed by relevant facts
Calculate	• Work out the numerical value. Show your working unless otherwise stated
Classify	• Arrange in categories according to shared qualities or characteristics
Compare	• Give an account of the similarities and differences between two or more items, situations or actions
Conclude	• Judge or decide something
Describe	• Give an account that includes the relevant characteristics, qualities or events
Discuss (how/whether/etc)	• Present, analyse and evaluate relevant points (for example, for/against an argument) to make a reasoned judgement
Evaluate	• Make a reasoned qualitative judgement considering different factors and using available knowledge/experience
Examine	• To look at, inspect, or scrutinise carefully, or in detail
Explain	• Give reasons for and/or causes of something • Make something clear by describing and/or giving information
Interpret	• Translate information into recognisable form • Convey one's understanding to others, e.g. in a performance
Investigate	• Inquire into (a situation or problem)
Justify	• Give valid reasons for offering an opinion or reaching a conclusion
Research	• Do detailed study in order to discover (new) information or reach a (new) understanding
Summarise	• Express the most important facts or ideas about something in a short and clear form

We might also use other command words but these will be:

- commonly used words whose meaning will be made clear from the context in which they are used (e.g. create, improve, plan)
- subject specific words drawn from the unit content.

Contact the team at:

☎ 01223 553998

ocr.org.uk

To stay up to date with all the relevant news about our qualifications,
register for email updates at ocr.org.uk/updates

Visit our Online Support Centre at support.ocr.org.uk

CAMBRIDGE
UNIVERSITY PRESS & ASSESSMENT

OCR is part of Cambridge University Press & Assessment, a department of the University of Cambridge.

OCR is a Company Limited by Guarantee and an exempt charity. Registered in England. Registered office: The Triangle Building, Shaftesbury Road, Cambridge, CB2 8EA. Registered company number: 3484466.

We operate academic and vocational qualifications regulated by Ofqual, Qualifications Wales and CCEA as listed in their qualifications registers.

We are committed to providing a fully accessible experience across all our products, platforms, and websites. Find out more about our accessibility standards.

We update our publications regularly so please check you have the most up-to-date version.

We cannot be held responsible for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication and do not guarantee that any content on such websites is, or will remain, accurate or appropriate.

When we update our specifications, you'll see a new version number and a summary of the changes. While we do our best to reflect these changes in all associated resources on Teach Cambridge, if you notice any discrepancies, please refer to the latest specification on our website and let us know.

Our resources do not represent any teaching method we expect you to use. We cannot be held responsible for any errors or omissions in our resources.