CAMBRIDGE
OCR

Cambridge Advanced Nationals (AAQs)

Cyber Security and Networks (H037/H137)

First Teaching September 2026

Vinay Thawait/Neil Hateley | 21 Jan 2026

Subject Advisors - Computer Science, IT and iMedia

© Cambridge OCR 2025

Troubleshooting

- If you are having difficulties with your audio, please check your audio settings within Teams by clicking the “More” button (three dots) then “Audio settings” and ensure your speaker is set to the correct output. If this does not resolve your problems, please try leaving and rejoining the session.
- If you are still having problems, please let us know in the chat window or email teacher_networks@ocr.org.uk.
- Cameras and microphones are disabled for attendees by default.
- Please submit any comments and questions in the chat window. You can access this by clicking the following icon at the top of your screen:

- Today’s session will be recorded. Please be aware that your screen name may appear in the recording.

Today's session

- An introduction
- OCR Level 3 Cambridge Advanced National (AAQ) in **Cyber Security and Networks**
- What teaching content and assessment looks like
- OCR's full compensation marking model
  - How it will benefits teachers and students
- Support provision
- Q&A with the subject advisor
- The next steps?

Introductions

Your Subject Advisors

Vinay Thawait

Computer Science, IT and iMedia

Caredig Cattanach-Chell

Computer Science, IT and iMedia

Neil Hateley

Computer Science, IT and iMedia

Connor Toms

Computer Science, IT and iMedia

Contact us: support@ocr.org.uk | 01223 553 998

What are Alternative Academic Qualifications?

What are Alternative Academic Qualifications (AAQs)?

- Designed for students aged 16 to 19 years, Alternative Academic Qualifications (AAQs) are Level 3 academic qualifications that can be combined with A Levels as part of a post-16 mixed-study programme.
- They are designed to help students learn the wider transferable skills, knowledge and understanding desired by HEIs.

Cambridge Advanced Nationals, our AAQs, **encourage students** to:

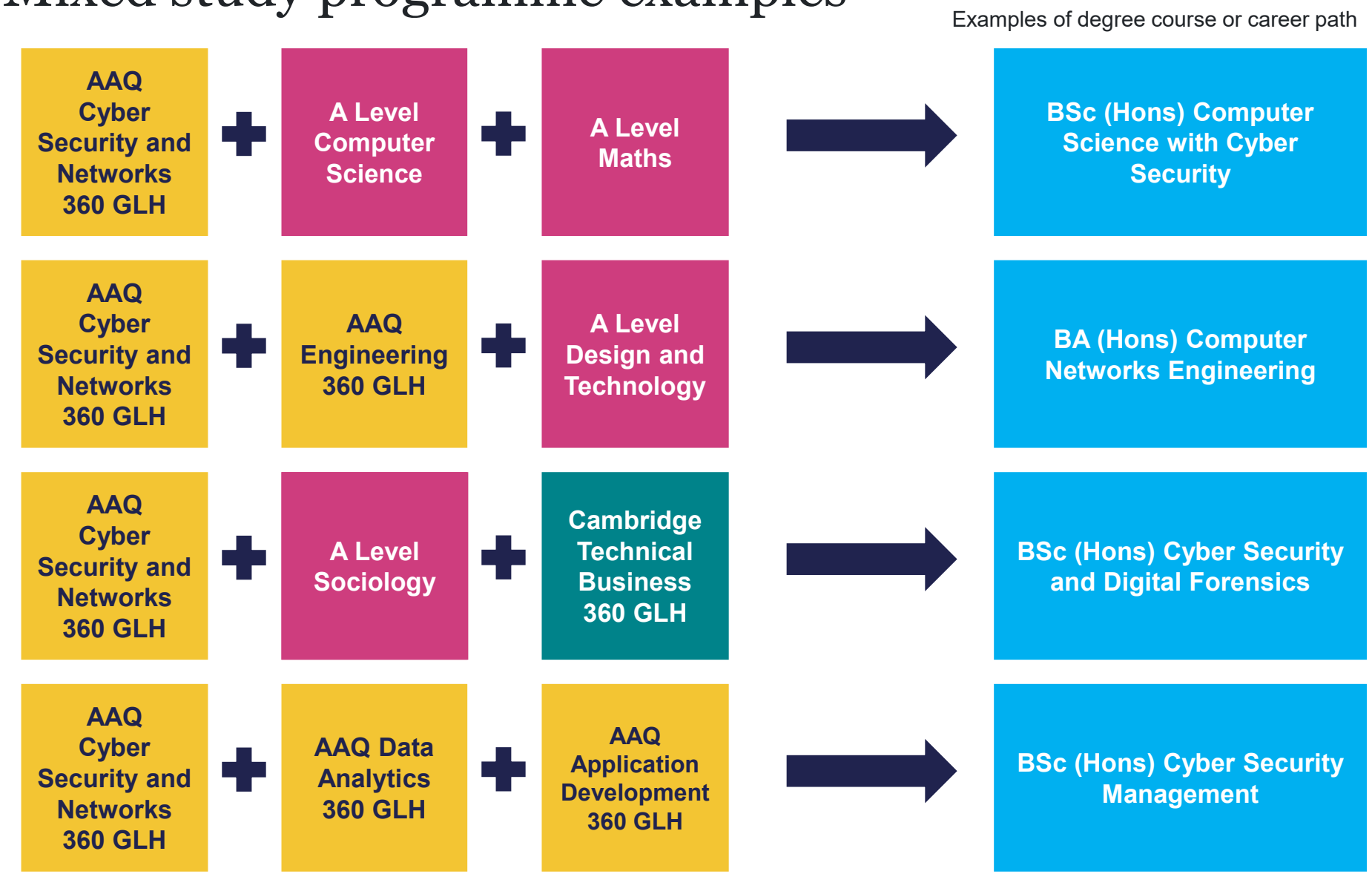
- develop key knowledge, understanding and skills, relevant to the subject
- think creatively, innovatively, analytically, logically and critically
- develop valuable communication skills that are important in all aspects of further study and life
- develop transferable learning and skills, such as evaluation, planning, presentation and research skills
- develop independence and confidence in applying the knowledge and skills

CAMBRIDGE OCR

Where do AAQs fit into a post-16 mixed programme of study?

- Students who want to progress onto further or higher education, but don't want to study only A Levels (or a T Level programme), can choose a mixed study programme.
- Cambridge Advanced Nationals (AAQs) are designed to complement existing A Level study programmes and provide flexibility for students, allowing them to choose a programme that best aligns with their abilities and goals.
- Cambridge Advanced Nationals are currently available as a **Certificate** or **Extended Certificate**.
  - The Certificate (150 or 180 GLH) is equivalent to **one AS Level**
  - The Extended Certificate (360 GLH) is equivalent to **one A Level**.
- These can be taken alongside complimentary A Levels to create a mixed study programme.
- Here are some examples:

Mixed study programme examples



Mixed study programme examples

Why Choose OCR - Unique Features

Why choose Cambridge Advanced Nationals?

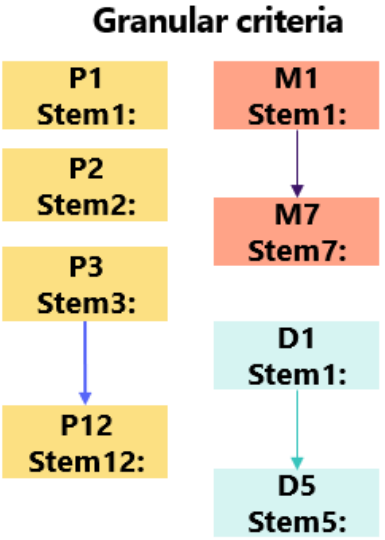
Full compensation grading: Students are always rewarded for their demonstrated abilities - every single mark your students earn will directly contribute to their final grade. No mark will go to waste.

Every mark matters: Gone are the days of hurdle elements in units. If a student meets all but one Pass criterion and some Merit criteria, they won't face failure. Our approach compensates for performance at both the unit and qualification levels, ensuring fairness and encouragement for every student.

Features teachers love and more: Cambridge Advanced Nationals incorporate the popular features from our Cambridge Technicals, including **visiting moderation**, a blend of examination and coursework units, and we're keeping the well-recognised Pass, Merit, Distinction grade scale. Plus, you'll continue to benefit from our range of comprehensive support and resources.

Pathways to university: Designed in **collaboration with teachers and universities**, Cambridge Advanced Nationals equip students with a well-rounded skill set for today's undergraduate studies as part of a Level 3 programme of study.

Complementary practical application: Designed to be taken alongside A Levels, Cambridge Advanced Nationals seamlessly complement a mixed study programme while maintaining a strong focus on the practical application of skills and knowledge - a valuable supplement to A Levels, preparing students for progression to university.



How are Cambridge Advanced Nationals assessed

- Cambridge Advanced Nationals are **assessed holistically** and have **a simple and intuitive assessment model**, comprising:
- externally assessed units, which focus on subject knowledge and understanding
- applied or practical non-exam assessment units (NEA)
- optional NEA units to provide flexibility

Qualification	Size	External assessment (Exam)	Non-exam assessment (NEA)
Certificate	150 GLH	50%	50%
Extended Certificate	360 GLH	40%	60%

Key points to know

Set assignments for each new year 12 cohort for all NEA units, i.e. with a 2-year life-span

Compensation-based NEA assessment model

Opportunity for students to improve and resubmit work

(more on our moderation approach later)

Practical and technical skills aligned to cyber security and networks progression routes

2 resits per exam available in a January or June series, i.e. 3 attempts per paper – best mark is used for certification

Strong focus on accessibility –mixture of question items, consistency each year – **maximum 1 hour 15 per exam paper**

Clear and granular assessment criteria with assessment guidance:

One criteria, one mark

Certificate option available – unique from other board's AAQ proposals

Unique features of Cyber Security and Networks AAQ

- The only AAQ with a **distinct focus** on cyber security and networks
- Enables students to get **hands on** with the practical elements of cyber security and networks
- **Engaging content** that will appeal to students:
  - digital forensic investigations,
  - exploitations of vulnerable systems,
  - designing and implementing secure local area networks (LANs) based on client and user requirements
- **Optional units** with a cyber security or networks focus
- Prepares young people for **progression into higher education**:
  - Computer Networks and Cyber Security
  - Computer Networks Engineering
  - Cyber Security and Digital Forensics
  - Ethical Hacking and Cyber Security
  - Computer Science with Cyber Security
- Units are either 70 or 75 GLH, allowing for straightforward planning and timetabling.

Teacher feedback

Looks like an excellent pathway for a growing industry specialism.

This looks super interesting and exciting in a constantly shifting sector.

The topics sound interesting and engaging for learners.

This I love, this encompasses everything I am able to understand and teach

An exciting pathway, one that is easy to market and has critical skills that are needed in industry and commerce today. I see direct links to University progression

Specification content overview

Cyber Security and Networks

Cambridge Advanced Nationals (AAQ) in Cyber Security and Networks

Extended Certificate – H137 (360GLH*)

- Two mandatory externally assessed units
- One mandatory NEA unit
- Two optional NEA units (from four)

Certificate – H037 (150GLH*)

- One mandatory externally assessed units
- One mandatory NEA unit

Unit number and title		How is it assessed?	Mandatory or optional
F193**	**Fundamentals of cyber security****	Examined	Mandatory
F194	Fundamentals of networks	Examined	Mandatory
F195**	**Preventing cyberattacks****	Non-Examined	Mandatory
F196	Digital forensic investigation	Non-Examined	Optional
F197	Penetration testing and incident response	Non-Examined	Optional
F198	Implementing secure local area networks (LANs)	Non-Examined	Optional
F199	Designing and communicating secure global computing systems	Non-Examined	Optional

***The GLH includes assessment time for each unit**

****F193 and F195 form the 150GLH Certificate**

CAMBRIDGE OCR

Unit F193: Fundamentals of cyber security

Mandatory EA

Topic Areas

1. **The cyber security landscape**
   - 1.1 Importance and key concepts of cyber security
   - 1.2 Types of cyber security incidents
   - 1.3 Targets of cyber security incidents
   - 1.4 Actors and motivations
2. **Cyber security vulnerabilities**
   - 2.1 Vulnerability vectors
   - 2.2 Physical vulnerabilities
   - 2.3 System vulnerabilities
3. **Impact of cyber security events**
   - 3.1 Disruption
   - 3.2 Loss
   - 3.3 Safety
4. **Cyber security mitigations**
   - 4.1 Endpoint mitigation measures
   - 4.2 Detection measures
   - 4.3 Intelligence assessment
5. **Policies, procedures and event handling**
   - 5.1 Policies and procedures
   - 5.2 Event handling
   - 5.3 Legislation, regulations and standards
6. **Job roles and responsibilities**
   - 6.1 General cyber security roles
   - 6.2 Communication skills

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

CAMBRIDGE OCR

Unit F193: Fundamentals of cyber security

Mandatory EA

Topic Areas

1. **The cyber security landscape**
   - 1.1 Importance and key concepts of cyber security
   - 1.2 Types of cyber security incidents
   - 1.3 Targets of cyber security incidents
   - 1.4 Actors and motivations
2. **Cyber security vulnerabilities**
   - 2.1 Vulnerability vectors
   - 2.2 Physical vulnerabilities
   - 2.3 System vulnerabilities
3. **Impact of cyber security events**
   - 3.1 Disruption
   - 3.2 Loss
   - 3.3 Safety
4. **Cyber security mitigations**
   - 4.1 Endpoint mitigation measures
   - 4.2 Detection measures
   - 4.3 Intelligence assessment
5. **Policies, procedures and event handling**
   - 5.1 Policies and procedures
   - 5.2 Event handling
   - 5.3 Legislation, regulations and standards
6. **Job roles and responsibilities**
   - 6.1 General cyber security roles
   - 6.2 Communication skills

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

CAMBRIDGE OCR

Unit F194: Fundamentals of networks

Mandatory EA

Topic Areas

1. **Network types, models, topologies and services**
   - 1.1 Network types
   - 1.2 Network models
   - 1.3 Network topologies
   - 1.4 Network Services
2. **Network layers, protocols and addressing**
   - 2.1 Network layers
   - 2.2 Network protocols
   - 2.3 Network Addressing
3. **Wired network components**
   - 3.1 Communications media
   - 3.2 Network connection devices
   - 3.3 Host devices
4. **Mobile and wireless networks**
   - 4.1 Transmission media
   - 4.2 Connectivity
   - 4.3 Concepts of mobile and wireless networks
   - 4.4 Networking standards
5. **Network Performance**
   - 5.1 Network performance indicators
   - 5.2 Network data transfer rate measurement
   - 5.3 Factors affecting network performance
6. **Cloud networks**
   - 6.1 Cloud environments
   - 6.2 Network virtualisation

Unit F194: Fundamentals of networks

70 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

DRAFT

CAMBRIDGE OCR

Unit F194: Fundamentals of networks

Mandatory EA

Topic Areas

1. **Network types, models, topologies and services**
   - 1.1 Network types
   - 1.2 Network models
   - 1.3 Network topologies
   - 1.4 Network Services
2. **Network layers, protocols and addressing**
   - 2.1 Network layers
   - 2.2 Network protocols
   - 2.3 Network Addressing
3. **Wired network components**
   - 3.1 Communications media
   - 3.2 Network connection devices
   - 3.3 Host devices
4. **Mobile and wireless networks**
   - 4.1 Transmission media
   - 4.2 Connectivity
   - 4.3 Concepts of mobile and wireless networks
   - 4.4 Networking standards
5. **Network Performance**
   - 5.1 Network performance indicators
   - 5.2 Network data transfer rate measurement
   - 5.3 Factors affecting network performance
6. **Cloud networks**
   - 6.1 Cloud environments
   - 6.2 Network virtualisation

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

CAMBRIDGE
OCR

Unit 195: Preventing Cyberattacks

Mandatory NEA

Topic Areas

1. **Cyber security aims and threats**
   - 1.1 Concepts of cyber security
   - 1.2 Threats against cyber security and countermeasures
2. **Identify risks to networks and data**
   - 2.1 Risks to digital networks and data
   - 2.2 Tools and techniques to identify and record risks
3. **Audit and improve cyberattack prevention measures**
   - 3.1 Tools and techniques to audit and improve cyberattack prevention measures
   - 3.2 Methods of network access control
   - 3.3 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
4. **Design access control policies**
   - 4.1 Access control
   - 4.2 Access control policies
5. **Design written user policies**
   - 5.1 Policy writing considerations
   - 5.2 Written user policies
6. **Review designed cyberattack prevention measures**
   - 6.1 Techniques to review the success of designed cyberattack prevention measures

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

Assessment

- Students will be given a scenario which they will use to create a risk assessment using tools and techniques they have learned.
- They will audit the cyberattack prevention measures and identify gaps;
- They will design cyber security prevention measures
- Evaluate the effectiveness of the measures they design.

CAMBRIDGE OCR

Unit 195: Preventing Cyberattacks

Mandatory NEA

Topic Areas

1. **Cyber security aims and threats**
   - 1.1 Concepts of cyber security
   - 1.2 Threats against cyber security and countermeasures
2. **Identify risks to networks and data**
   - 2.1 Risks to digital networks and data
   - 2.2 Tools and techniques to identify and record risks
3. **Audit and improve cyberattack prevention measures**
   - 3.1 Tools and techniques to audit and improve cyberattack prevention measures
   - 3.2 Methods of network access control
   - 3.3 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
4. **Design access control policies**
   - 4.1 Access control
   - 4.2 Access control policies
5. **Design written user policies**
   - 5.1 Policy writing considerations
   - 5.2 Written user policies
6. **Review designed cyberattack prevention measures**
   - 6.1 Techniques to review the success of designed cyberattack prevention measures

Tasks for students and assessment criteria

Unit F195: Preventing cyberattacks

Scenario title: Progress Health Services (PHS)

Valid for assessment from September 20XX to 20XX.
For use by students beginning the qualification in September 20XX.

Scenario

PHS delivers bespoke training courses aimed at health in the workplace. The training courses can be delivered either onsite at PHS or at the offices of the business or school who have requested the training course. Awareness of mental health in the workplace and how employers should support this has increased throughout the country in recent years. This has led to a higher number of requests for PHS to deliver training. As a result, management at PHS have been discussing the possibility of creating online courses as well as their existing face-to-face courses.

PHS management is also aware of some of the cyber threats which have been widely reported in the news. They have been informed of the National Cyber Security Centre certification in Cyber Essentials, which can be used to assure customers that they have met a specific level of cyber security resilience. You have been hired by PHS who are considering applying for the Cyber Essentials certification.

Before applying for the Cyber Essentials certification, better prepared for the certification process. You will cyber security practices and create cyber security pol implemented.

Task 1

Creating a risk assessment

Topic Areas 1 and 2 are assessed in this task

The task is:

Create a risk assessment for the organisation.

- You will use appropriate tools and techniques to create the risk assessment for Progress Health Services (PHS) which identifies cyber security risks.
- You will also define the level of severity of each risk and identify the assumptions made.

Your evidence **must** include:

- A risk assessment.
- Written evidence.

CAMBRIDGE OCR

Unit 195: Preventing Cyberattacks

Mandatory NEA

Topic Areas

1. **Cyber security aims and threats**
   - 1.1 Concepts of cyber security
   - 1.2 Threats against cyber security and countermeasures
2. **Identify risks to networks and data**
   - 2.1 Risks to digital networks and data
   - 2.2 Tools and techniques to identify and record risks
3. **Audit and improve cyberattack prevention measures**
   - 3.1 Tools and techniques to audit and improve cyberattack prevention measures
   - 3.2 Methods of network access control
   - 3.3 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
4. **Design access control policies**
   - 4.1 Access control
   - 4.2 Access control policies
5. **Design written user policies**
   - 5.1 Policy writing considerations
   - 5.2 Written user policies
6. **Review designed cyberattack prevention measures**
   - 6.1 Techniques to review the success of designed cyberattack prevention measures

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.	

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.

Unit 196: Digital Forensic Investigation

Optional NEA

Topic Areas

1. **Fundamentals of digital forensics**
   - 1.1 Applications of digital forensics
   - 1.2 Digital forensic investigation considerations and challenges
2. **Plan digital forensic investigations**
   - 2.1 Techniques to plan digital forensic investigations
   - 2.2 Crime scenes and digital evidence
   - 2.3 Techniques to handle evidence
3. **Collect, preserve and analyse digital evidence**
   - 3.1 Principles of data storage
   - 3.2 Tools to collect and preserve digital forensic evidence
   - 3.3 Techniques to record investigation outcomes
   - 3.4 Digital forensic investigation evidence integrity and accuracy
   - 3.5 Stages of evidence analysis
4. **Report digital forensic investigation findings**
   - 4.1 Digital forensic investigation findings report
5. **Review digital forensic investigations**
   - 5.1 Techniques to review digital forensic investigations
   - 5.2 Digital forensic investigation constraints

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

Assessment

- Students will plan and carry out a digital forensic investigation for the scenario they are given.
- They will use digital forensic tools and techniques and check that the evidence found meets the needs of the investigation.
- They will also generate a report of the investigation.

CAMBRIDGE OCR

Unit 197: Penetration testing and incident response

Optional NEA

Topic Areas

1. **Introduction to penetration testing**
   - 1.1 Aims, stages and phases of penetration testing
   - 1.2 Penetration testing roles
   - 1.3 Common system vulnerabilities
2. **Plan penetration testing**
   - 2.1 Penetration testing strategies
   - 2.2 Impacts of exploitation activities
   - 2.3 Penetration testing scoping plans
   - 2.4 Exploitation activities test plan
3. **Implement penetration testing scoping plans**
   - 3.1 Penetration testing environments
   - 3.2 Penetration testing software tools
4. **Incident response planning**
   - 4.1 Cyber security Incident response (CSIR) plan
   - 4.2 Incident management
   - 4.3 Incident playbooks
5. **Develop cyber security incident response capability**
   - 5.1 Maintenance plan
   - 5.2 Employee training
6. **Review penetration testing and incident response capability**
   - 6.1 Techniques to review penetration testing and incident response capability

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

Assessment

- Students will explore the vulnerabilities and impacts of cyber security incidents
- Create a penetration test scoping plan for the scenario they are given.
- They will identify and demonstrate the exploitation activities that could be used.
- They will also create a cyber security incident response plan, explain the management of the incident and create an incident response playbook
- Create a maintenance plan including training materials.

CAMBRIDGE OCR

Unit 197: Penetration testing and incident response

Optional NEA

Topic Areas

1. **Introduction to penetration testing**
   - 1.1 Aims, stages and phases of penetration testing
   - 1.2 Penetration testing roles
   - 1.3 Common system vulnerabilities
2. **Plan penetration testing**
   - 2.1 Penetration testing strategies
   - 2.2 Impacts of exploitation activities
   - 2.3 Penetration testing scoping plans
   - 2.4 Exploitation activities test plan
3. **Implement penetration testing scoping plans**
   - 3.1 Penetration testing environments
   - 3.2 Penetration testing software tools
4. **Incident response planning**
   - 4.1 Cyber security Incident response (CSIR) plan
   - 4.2 Incident management
   - 4.3 Incident playbooks
5. **Develop cyber security incident response capability**
   - 5.1 Maintenance plan
   - 5.2 Employee training
6. **Review penetration testing and incident response capability**
   - 6.1 Techniques to review penetration testing and incident response capability

Task 2
Planning exploitation activities

Topic Areas 1, 2, 3 and 6 are assessed in this task

The task is:

Create the exploitation activities test plan for Credit General.

- Identify exploitation activities that could be used to target the IT system in the organisation.
- Create the exploitation activities test plan.
- Demonstrate exploitation activities.

Your evidence **must** include:

- An exploitation activity test plan
- Written evidence.
- A Teacher Observation Record (TOR) form signed by you and your teacher.

Examples of browser-based cyber security training platforms include:

https://tryhackme.com/

https://www.hackthebox.com/

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.

CAMBRIDGE OCR

Unit 198: Implementing secure local area networks (LANs)

Optional NEA

Topic Areas

1. **Purpose and components of local area networks (LANs)**
   - 1.1 Purpose of LANs
   - 1.2 LAN hardware components and transmission media
   - 1.3 LAN software
2. **Design secure local area networks (LANs)**
   - 2.1 LAN design considerations
   - 2.2 Components of LAN design documentation
3. **Implement and secure local area networks (LANs)**
   - 3.1 Safe working practices to implement LANs
   - 3.2 Technical skills to implement LANs
   - 3.3 Techniques to secure LANs
4. **Test local area networks (LANs)**
   - 4.1 Techniques to test and troubleshoot LANs
   - 4.2 Network tools for diagnostics, monitoring and benchmarking
5. **Review and maintain local area network (LAN) performance and security**
   - 5.1 Techniques to review the effectiveness of implemented LANs
   - 5.2 Improvements and further development to LANs
   - 5.3 The maintenance phase

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

Assessment

- Students will use client requirements from a provided scenario to create a network design proposal.
- They will create documentation for the design following common conventions, layouts and formats.
- They will implement the LAN they design and test its functionality
- They will review their practices, skills and techniques and discuss potential improvements.

CAMBRIDGE OCR

Unit 199: Implementing secure local area networks (LANs)

Optional NEA

Topic Areas

1. **Fundamentals of secure global computing systems**
   - 1.1 Purpose and use of secure global computing
   - 1.2 Secure global computing requirements
   - 1.3 Characteristics of cloud computing
   - 1.4 Technology which enables secure global computing
2. **Plan and scope secure global computing systems**
   - 2.1 Requirements of secure global computing systems
   - 2.2 Scope secure global computing systems
3. **Design secure global computing systems**
   - 3.1 Design documentation
4. **Simulate and test secure global computing systems**
   - 4.1 Tools to create simulated secure global computing system models
   - 4.2 Techniques to test secure global computing systems
5. **Communicate and review secure global computing systems**
   - 5.1 Develop solution showcases to communicate secure global computing systems
   - 5.2 Techniques to review the effectiveness of secure global computing systems
   - 5.3 Improvements and further developments

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

Assessment

- Students will be given a scenario
- They will scope the requirements for a secure global computing system.
- They will design the system using design documentation and describe how the system will be tested.
- They will create a simulation of the system and test that it functions as intended.
- Students will then showcase their solution.

CAMBRIDGE
OCR

Assessment Overview

Full Compensation NEA Marking Model

© Cambridge OCR 2025

Cyber Security and Networks

Assessment Overview – H137 and H037

Extended certificate H137

- F193 Exam 1 hour 15 minutes – M (75 GLH) 60 marks
- F194 Exam 1 hour 15 minutes – M (70 GLH) 60 marks
- F195 NEA 15 GLH – M (75 GLH)
- F196 NEA 15 GLH – O (70GLH)
- F197 NEA 15 GLH – O (70GLH)
- F198 NEA 15 GLH – O (70GLH)
- F199 NEA 15 GLH – O (70GLH)

4.1.4 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.

Certificate H037

- F193 Exam 1 hour 15 minutes – M (75 GLH) 60 marks
- F195 NEA 15 GLH – M (75GLH)

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.

Cyber Security and Networks

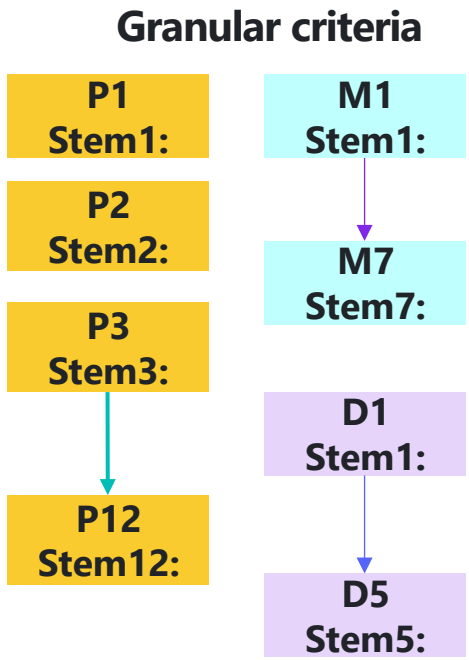
Assessment Overview – H137, H037

The table below shows **the design thresholds** for each grade outcome for the **NEA assessments** in these qualifications.

Unit size (GLH)	70	75
Total number of criteria	24	24
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

- Made criteria much more specific and granular
- Support teachers in identifying the evidence required to meet each criterion
- Rewards students for the evidence they were able to produce.

It does not increase teaching and learning time, or assessment volume.



Compensation at unit level assessment

Hurdles based model

P1	M1	D1
P2	M2	D2
P3	M3	
P4		

In the hurdles-based model above, the student would fail to achieve a pass grade for the unit.

New Compensation based model

P1	M1	D1
P2	M2	D2
P3	M3	
P4		

Using our new compensation-based model, the same student would still achieve a result for the unit.

Boundaries* for each unit can be found in the specification. The example above is simplified for illustration.

Compensation at qualification level

Every criterion that a student achieves will count towards their final qualification outcome.

Hurdles based model

P1	M1	D1
P2	M2	D2
P3	M3	
P4		

In the hurdles-based model above, M1, M2 and D1 would not count towards the final qualification grade and the student would have achieved a Pass at unit level.

Compensation based model

P1	M1	D1
P2	M2	D2
P3	M3	
P4		

Using our new compensation-based model, M1, M2 and D1 all count towards the final qualification grade, even if a student had not achieved a Merit or Distinction at unit level.

Boundaries* for each unit can be found in the specification. The example above is simplified for illustration.

Expanded unit level example

(Cyber security and Networks Unit F195)

75GLH unit (F195): **24 Criteria** (12 Pass, 7 Merit, 5 Distinction)

Pass: 10 **Merit: 15** **Distinction: 20**

Pass	Merit	Distinction
P1: Create a risk assessment appropriate for the organisation. (PO4)	**M1: Explain** how the risks identified could impact the network and data security of the organisation. (PO2)	**D1: Evaluate** the tools and techniques used to identify risks and their level of severity. (PO3)
P2: Use a risk matrix to define the severity level of each risk identified. (PO4)		
P3: Identify three assumptions made when defining the severity of the risks. (PO2)	**M2: Justify** the assumptions identified when defining the severity of the risks. (PO3)	

Pass	Merit	Distinction
P4: Complete an audit of the existing cyberattack prevention measures used. (PO4)	**M3: Assess** the strengths and weaknesses of the existing cyberattack policies, procedures and methods identified in the audit. (PO3)	**D2: Discuss** how each improvement to the organisation's cyber security policies, procedures and methods will enhance their cyber security. (PO3)
P5: Identify the gaps in the existing cyberattack policies, procedures and methods used. (PO2)	**M4: Describe** improvements to each of the existing cyberattack policies, procedures and methods used. (PO2)	

Pass	Merit	Distinction
P6: Design access control policies for external access to systems/networks. (PO4)	**M5: Design** cyber security prevention measures which make use of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). (PO4)	**D3: Justify** how each cyber security prevention policy and measure designed relate to the concepts of cyber security. (PO3)
P7: Design access control policies for internal access to systems/networks. (PO4)		
P8: Design access control policies for access rights of different user groups. (PO4)		
P9: Design written user policies which outline how technology should be used in the organisation. (PO4)		

Pass	Merit	Distinction
P10: Describe the purpose of each policy and measure designed. (PO2)	**M6: Explain** how each policy and measure designed could be implemented. (PO2)	**D4: Discuss** the impact of implementing each policy and measure designed on the users of the organisation's system. (PO3)
P11: Explain how each policy and measure designed prevents exposure to cyber security threats. (PO2)	**M7: Analyse** the advantages and disadvantages of each policy and measure designed. (PO3)	**D5: Evaluate** the effectiveness of each policy and measure designed in reducing the cyber security risks identified. (PO3)
P12: Explain how each policy and measure designed reduces the likelihood and severity of cyber security risk. (PO2)		

Expanded unit level example at Pass grade

(Cyber security and Networks Unit F195)

75GLH unit (F195): **24 Criteria** (12 Pass, 7 Merit, 5 Distinction)

Pass: 10 **Merit: 15** **Distinction: 20**

Pass	Merit	Distinction
P1: Create a risk assessment appropriate for the organisation. (PO4)	**M1: Explain** how the risks identified could impact the network and data security of the organisation. (PO2)	**D1: Evaluate** the tools and techniques used to identify risks and their level of severity. (PO3)
P2: Use a risk matrix to define the severity level of each risk identified. (PO4)		
P3: Identify three assumptions made when defining the severity of the risks. (PO2)	**M2: Justify** the assumptions identified when defining the severity of the risks. (PO3)	

Pass	Merit	Distinction
P4: Complete an audit of the existing cyberattack prevention measures used. (PO4)	**M3: Assess** the strengths and weaknesses of the existing cyberattack policies, procedures and methods identified in the audit. (PO3)	**D2: Discuss** how each improvement to the organisation's cyber security policies, procedures and methods will enhance their cyber security. (PO3)
P5: Identify the gaps in the existing cyberattack policies, procedures and methods used. (PO2)	**M4: Describe** improvements to each of the existing cyberattack policies, procedures and methods used. (PO2)	

Pass	Merit	Distinction
P6: Design access control policies for external access to systems/networks. (PO4)	**M5: Design** cyber security prevention measures which make use of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). (PO4)	**D3: Justify** how each cyber security prevention policy and measure designed relate to the concepts of cyber security. (PO3)
P7: Design access control policies for internal access to systems/networks. (PO4)		
P8: Design access control policies for access rights of different user groups. (PO4)		
P9: Design written user policies which outline how technology should be used in the organisation. (PO4)		

Pass	Merit	Distinction
P10: Describe the purpose of each policy and measure designed. (PO2)	**M6: Explain** how each policy and measure designed could be implemented. (PO2)	**D4: Discuss** the impact of implementing each policy and measure designed on the users of the organisation's system. (PO3)
P11: Explain how each policy and measure designed prevents exposure to cyber security threats. (PO2)	**M7: Analyse** the advantages and disadvantages of each policy and measure designed. (PO3)	**D5: Evaluate** the effectiveness of each policy and measure designed in reducing the cyber security risks identified. (PO3)
P12: Explain how each policy and measure designed reduces the likelihood and severity of cyber security risk. (PO2)		

Score 11

SAMPLE

Expanded unit level example at Merit grade

(Cyber security and Networks Unit F195)

75GLH unit (F195): **24 Criteria** (12 Pass, 7 Merit, 5 Distinction)

Pass: 10 **Merit: 15** **Distinction: 20**

Pass	Merit	Distinction
P1: Create a risk assessment appropriate for the organisation. (PO4)	**M1: Explain** how the risks identified could impact the network and data security of the organisation. (PO2)	**D1: Evaluate** the tools and techniques used to identify risks and their level of severity. (PO3)
P2: Use a risk matrix to define the severity level of each risk identified. (PO4)		
P3: Identify three assumptions made when defining the severity of the risks. (PO2)	**M2: Justify** the assumptions identified when defining the severity of the risks. (PO3)	

Pass	Merit	Distinction
P4: Complete an audit of the existing cyberattack prevention measures used. (PO4)	**M3: Assess** the strengths and weaknesses of the existing cyberattack policies, procedures and methods identified in the audit. (PO3)	**D2: Discuss** how each improvement to the organisation's cyber security policies, procedures and methods will enhance their cyber security. (PO3)
P5: Identify the gaps in the existing cyberattack policies, procedures and methods used. (PO2)	**M4: Describe** improvements to each of the existing cyberattack policies, procedures and methods used. (PO2)	

Pass	Merit	Distinction
P6: Design access control policies for external access to systems/networks. (PO4)	**M5: Design** cyber security prevention measures which make use of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). (PO4)	**D3: Justify** how each cyber security prevention policy and measure designed relate to the concepts of cyber security. (PO3)
P7: Design access control policies for internal access to systems/networks. (PO4)		
P8: Design access control policies for access rights of different user groups. (PO4)		
P9: Design written user policies which outline how technology should be used in the organisation. (PO4)		

Pass	Merit	Distinction
P10: Describe the purpose of each policy and measure designed. (PO2)	**M6: Explain** how each policy and measure designed could be implemented. (PO2)	**D4: Discuss** the impact of implementing each policy and measure designed on the users of the organisation's system. (PO3)
P11: Explain how each policy and measure designed prevents exposure to cyber security threats. (PO2)	**M7: Analyse** the advantages and disadvantages of each policy and measure designed. (PO3)	**D5: Evaluate** the effectiveness of each policy and measure designed in reducing the cyber security risks identified. (PO3)
P12: Explain how each policy and measure designed reduces the likelihood and severity of cyber security risk. (PO2)		

Score 16

SAMPLE

Calculating the overall qualification grade

Calculating the overall grade requires grades for all the units a student has completed.

- The Extended Certificate has 5 units in total. To calculate the overall grade out of a maximum UMS score of 300 marks, we need to apply UMS scaling to the student grades in each of the NEA units, the examined units are marked out of 60 and do not need to be scaled.

The tables on the right 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.

Design Specification
60/24 = 2.5
UMS = <Raw mark> x 2.5

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

Calculating the overall qualification grade

Whilst **the actual UMS calculations will be determined at the first awarding meeting for this qualification**, at this stage the best we can work with is **the design specification** which is as follows:

Raw	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
UMS	60	58	55	53	50	48	45	43	40	38	35	33	30	28	25	23	20	18	15	13	10	8	5	3	0

The table above is using the formula UMS = <Raw mark> x 2.5

- Students will probably generate a spikey profile, rather than the same grade for every unit, which will slightly complicate the process, but this would allow student to aim for a specific number of criteria equivalent to a projected grade.
    - **Pass= 10**
    - **Merit = 15**
    - **Distinction = 20**
    - **Distinction * = 22 which is only awarded at qualification level**
- **To calculate the awarded grade, all the UMS marks from the 5 units are added together to provide a total UMS mark for the whole qualification grade.**
- **Every UMS mark counts towards the final grade, including those from units at U grade with less than 10 marks.**
- A student's uniform mark for each externally assessed unit is calculated from the student's raw mark on that unit.

Calculating the overall qualification grade example Pass

CAMBRIDGE OCR

Raw	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
UMS	60	58	55	53	50	48	45	43	40	38	35	33	30	28	25	23	20	18	15	13	10	8	5	3	0

Total number of criteria: 24 (12 Pass, 7 Merit and 5 Distinction)

- **Pass= 10; Merit = 15; Distinction = 20**
- **Distinction * = 22 which is only awarded at qualification level**

Units	Mandatory / Optional Exam / Internal	Available Exam marks	Available NEA marks	Achieved Raw marks	Converted UMS mark	Unit Level Grade	Overall Qualification Grade
F193 Fundamentals of cyber security	(M) - E	60 (60 UMS)		25	25	P	
F194 Fundamentals of networks	(M) - E	60 (60 UMS)		35	35	P	
F195 Preventing cyberattacks	(M) - I		24	15	38	M	
F196 Digital forensic investigation	(O) - I		24	9	23	U	
F199 Designing and communicating secure global computing system	(O) – I		24	11	28	P	
				Total UMS Marks	**149**		**Pass**

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

NEA Moderation and Examination

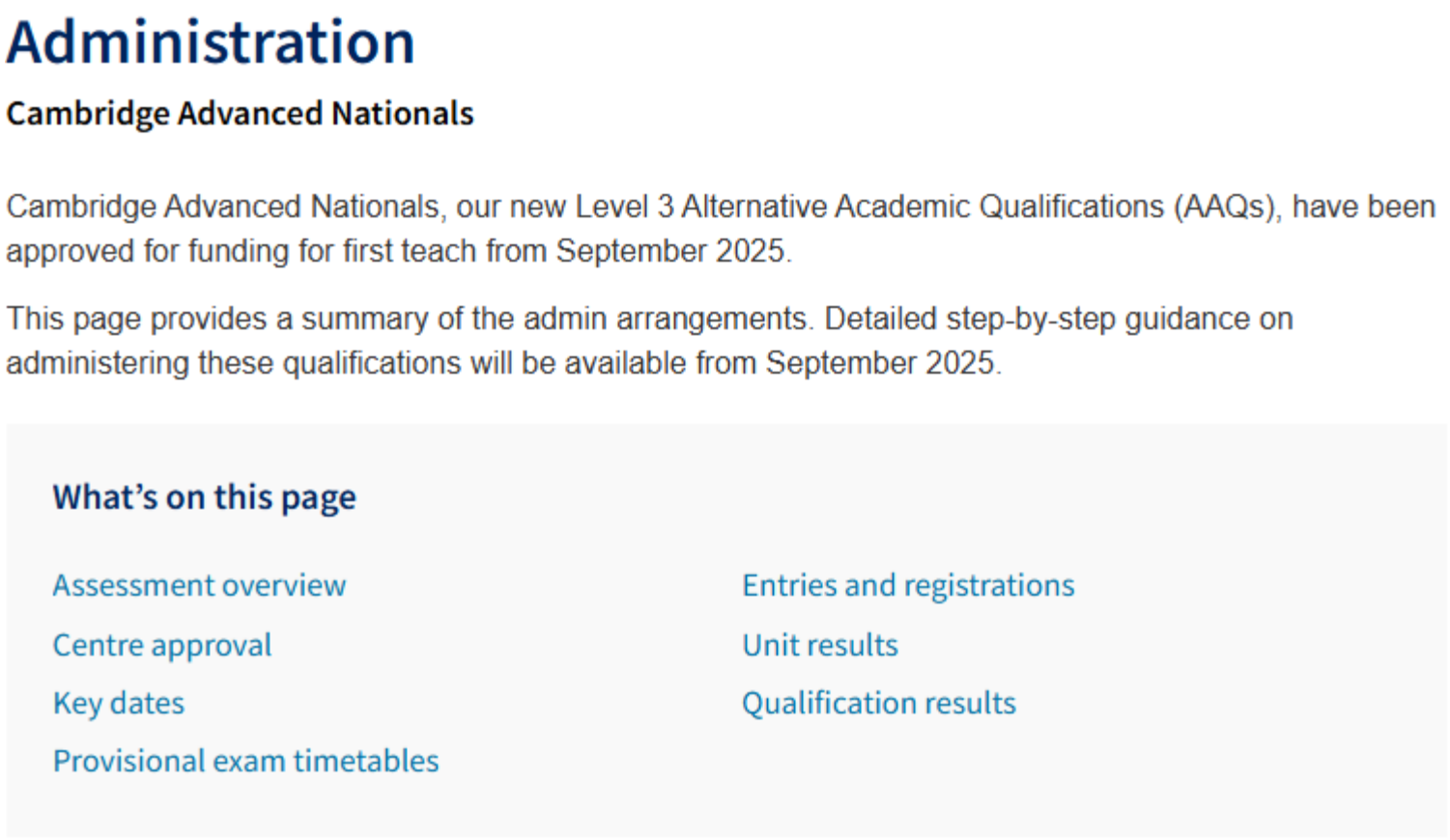
Admin

FAQ on Entries and Registration

FAQ on Registration and Entries for AAQs

- Cambridge Advanced Nationals FAQ page

Administration for AAQs



Administration

Cambridge Advanced Nationals

Cambridge Advanced Nationals, our new Level 3 Alternative Academic Qualifications (AAQs), have been approved for funding for first teach from September 2025.

This page provides a summary of the admin arrangements. Detailed step-by-step guidance on administering these qualifications will be available from September 2025.

What's on this page

Assessment overview
Centre approval
Key dates
Provisional exam timetables
Entries and registrations
Unit results
Qualification results

- Cambridge Advanced Nationals Administration page

OCR NEA Moderation

- Two windows, spring and summer, each year to submit NEA outcomes
- NEA assignment will be released on Teach Cambridge on **1 June** for **'teacher planning'** and to use in the following academic year
- NEA assignments are live for 2 years and will be shown on the front cover alongside the intended cohort
- NEA work must be completed in the centre under **teacher supervision in normal curriculum time** (spec point 6.2)
- **Do not allow students access to their assignment work between teacher supervised sessions**
- Request a moderation visit or a virtual moderation by an OCR assessor
- You must make unit entries for students before submitting outcomes to request a visit
  - Reviewing internally standardised candidate's work sample
  - Usually 6 candidates per unit
  - Constructive feedback from our moderator
- Students can improve their work and submit it to you again for an internal assessment, before submitting marks to OCR
- **One re-submission opportunity per NEA assignment - the same live assignment**

Examination

- **January and June Series**
- Students can resit the examined unit **twice** before they complete the qualification

Interested in joining our Moderation/Exam marking team?

We've several vacancies for Cambridge Advanced Nationals.

Find out more and apply here: https://teach.ocr.org.uk/cambridge-advanced-nationals-assessor-recruitment

Reminder! You should initially use the live set assignment released in the same calendar year as the new cohort starts to ensure they have two years for that assignment.

Registration and Entries for AAQs

CAMBRIDGE OCR

Deadline for Examined unit entries

Series	Entries deadline
January	21 October
June	21 February

Deadline for NEA unit entries

From 2026/27 **Provisional**

Moderation window	Series	Entries deadline
Window 1 (Winter)	February	21 November
Window 2 (Summer)	June	21 February

2026/27 Moderation Windows

- Window 1 (Winter): **30 November 2026 to 26 February 2027**
- Window 2 (Summer): **8 March to 4 June 2027**

2026/27 visit arrangement request deadline
Window 1: February Series - 21st November
Window 2: June Series - 21st February

My Cambridge

- Cambridge Advanced Nationals Registration and Entries

UCAS Tariff Points and Higher Education Support

- Cambridge Advanced Nationals are worth UCAS Tariff points
- Our qualifications are on the UCAS Tariff points calculator.

Certificate		Extended Certificate	
Distinction*	28 points	Distinction*	56 points
Distinction	24 points	Distinction	48 points
Merit	16 points	Merit	32 points
Pass	8 points	Pass	16 points

- We have letters of support from a wide range of universities, including Russell Group universities.

https://www.ocr.org.uk/qualifications/alternative-academic-qualifications/ucas-tariff-points/

What support will be available for centres?

CAMBRIDGE OCR

Cyber Security and Networks - Teacher and Student Resources

Teaching & Learning	Assessment	Training
• Textbook • Switching Guide • Mapping Guide • Getting Started Guide • Curriculum Planner • Scheme of Work • E-Learning course	• Annotated Sample Assessment Materials • Assessment Story • Practice Papers • Candidate Style Answers (EA) • Candidate Style Work (NEA) • NEA Guide • Student Guide	• Choosing AAQs • Understanding the compensation model • Starting to Teach • Ask the SA • Ask the Moderator • Preparing for the Exam • Preparing for the NEA • Exploring the exam (*after live examination series*) • Exploring the NEA (*after live examination series)* • Enhance your teaching

https://teachcambridge.org/ https://www.ocr.org.uk/qualifications/professional-development/events/

Scheme of Work

Area of study: 1.1 Programs and applications

Lessons

Lesson number	Specification coverage	GLH	Lesson aims and outcomes	Lesson ideas, key words and activities	Useful resources	Student independent learning – ideas and useful resources
1	1.1 Programs	1	By the end of the lesson students should: • know what a 'program' is • know the characteristics of a program • understand the purpose of a program.	**Starter** Think pair share: ask students to think about different types of software they use daily (e.g., games, word processors, web browsers) and write them on the board. **Main task** Teach students what a **program** is, the characteristics and the purposes of certain programs. Explain to students that a program does not necessarily have an end user or a purpose commercially, but maybe a script or file a programmer may construct. Give students a range of different scenarios, get them to categorise if they are a **program** or not. Group Work: divide students into small groups and assign each group a type of program (e.g., utility, game, educational software). Each group should identify the characteristics and purpose of their assigned program type and present their findings to the class.	Application vs. Program (What's the Difference?) - Rapid Blog Is There any Difference between a "Program" and an "Application"? How to Create and Run a Batch File in Windows 10 and 11	Students should use Cornell note taking to create structured notes to reflect on the lesson. Create a glossary of definitions to add to, using flash cards or paper.

Subject knowledge support for this area of study

Subject knowledge enhancement	Details
Underlying knowledge and understanding	Students should have a basic understanding of the concept of applications and algorithms, as well as types of devices used.
Common misconceptions	Programs can be created for different reasons: to solve problems, automate tasks, or for entertainment. Highlight that not all programs are designed for end-users; some are tools for developers (e.g., scripts, libraries).
Key concepts	**Program:** a program is a set of instructions that a computer follows to perform a specific task. It can be as simple as a script that adds two numbers or as complex as an operating system. Programs are the building blocks of software and can run independently or as part of a larger system. **Application:** an application (or app) is a type of program designed for end-users to perform specific tasks. Applications are typically more user-friendly and are built to help users complete activities like word processing, browsing the internet, or playing games. Essentially, all applications are programs, but not all programs are applications. **Characteristics of a program:** • set of instructions: a program consists of a sequence of instructions that a computer follows to perform a specific task • execution: programs are executed by the computer's CPU • purpose: programs can be created for various purposes, such as solving problems, automating tasks, or performing calculations • independence: programs can run independently or as part of a larger system • flexibility: programs can be simple (like a script) or complex (like an operating system). **Characteristics of an application:** • user-focused: applications are designed with end-users in mind, providing a user-friendly interface • specific tasks: applications are created to help users perform specific tasks, such as word processing, browsing the internet, or playing games • integration: applications often integrate multiple programs to provide a cohesive user experience • installation: applications usually come with an easy installation process and can be easily uninstalled

 © OCR 2025

Subject knowledge enhancement	Details
	IoT devices: internet of things devices, such as smart sensors and connected appliances, run specialized software to communicate and perform tasks.
Subject knowledge enhancement for teachers (further reading)	Read: Application vs. Program (What's the Difference?) - Rapid Blog Watch: What is Software Listen: Software Engineering Daily | Podcast on Spotify Refer to the OCR endorsed textbook.

Benefits to teachers

- Access to on-demand and live training throughout the year
- Access to teaching materials and assessment support
- All the benefits of our collaborative and constructive moderation processes
- Deliver exciting, relevant and up-to-date content that students will enjoy

Benefits to students

- Reliable assessments – papers that are accessible and ramp-up, every question can be attempted
- Minimum time sat in exam halls
- Chances to resit papers in January and June
- Resubmit coursework in the next appropriate window
- No more hurdles – every single mark counts towards their final grade
- Content is relevant, up-to-date, and career-orientated

Support for all OCR teachers

Free ***My Cambridge*** login for all teachers (and technicians) via your exams officer that gives you access to:

- **Teach Cambridge**: teaching resources, schemes of work, assessment materials and set assignments
- **Professional development**: discover and book our comprehensive programme
- **OCR Train**: our on-demand training and standardisation platform
- **Interchange**: request your moderation visits during the two windows
- **Active Results**: compare your school's results against national averages and drill down into item-level and candidate-level analysis
- **Access to Scripts**: see candidate papers after results day
- **Submit for Assessment**: digital upload of candidate work for moderation
- **ExamBuilder**: create assessments from our large bank of question from the Cambridge Technical course, as well as access to all A level and GCSE questions

Further support and next steps

Updates

- DfE funding available for all AAQs offered by OCR – Qualifications approved for funding
- Discount codes could be available by Spring term 2026
- UCAS Tariff Points available – calculate it here
- Specification – **please download to review and plan for Sept 2026**
- New JCQ instructions for conducting NEA (VTQs) 2025-26

JCQ Joint Council for Qualifications CIC

Instructions for conducting non-examination assessments (Vocational and Technical Qualifications)

1 September 2025 to 31 August 2026

Certificate		Extended Certificate	
Distinction*	28 points	Distinction*	56 points
Distinction	24 points	Distinction	48 points
Merit	16 points	Merit	32 points
Pass	8 points	Pass	16 points

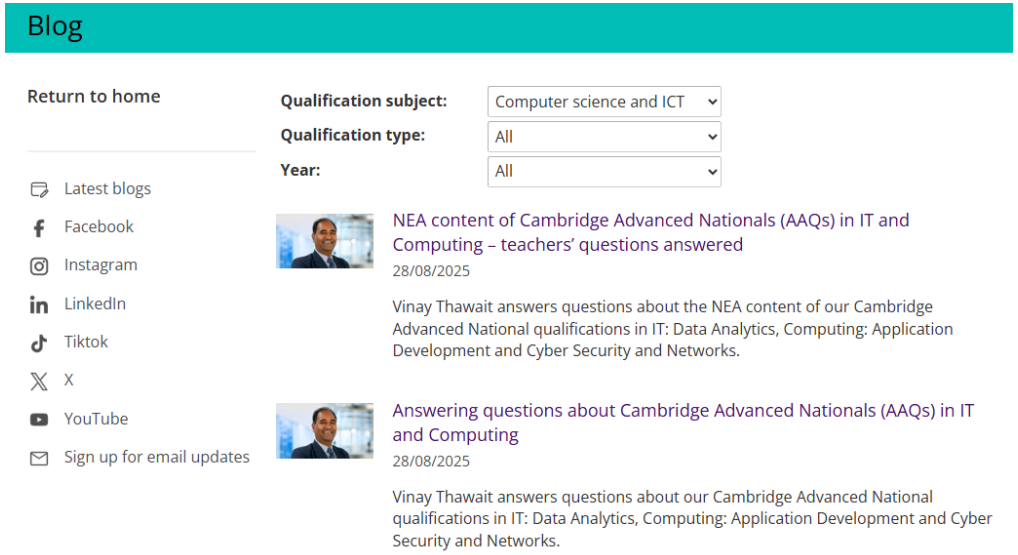
Options Evening Pack

- The pack can be downloaded using the link
- Each Download file comprises:
  - Cambridge Advanced Nationals Explained brochure
  - Course summary factsheet
  - Careers poster
  - PowerPoint presentation you can download and tailor to your needs.

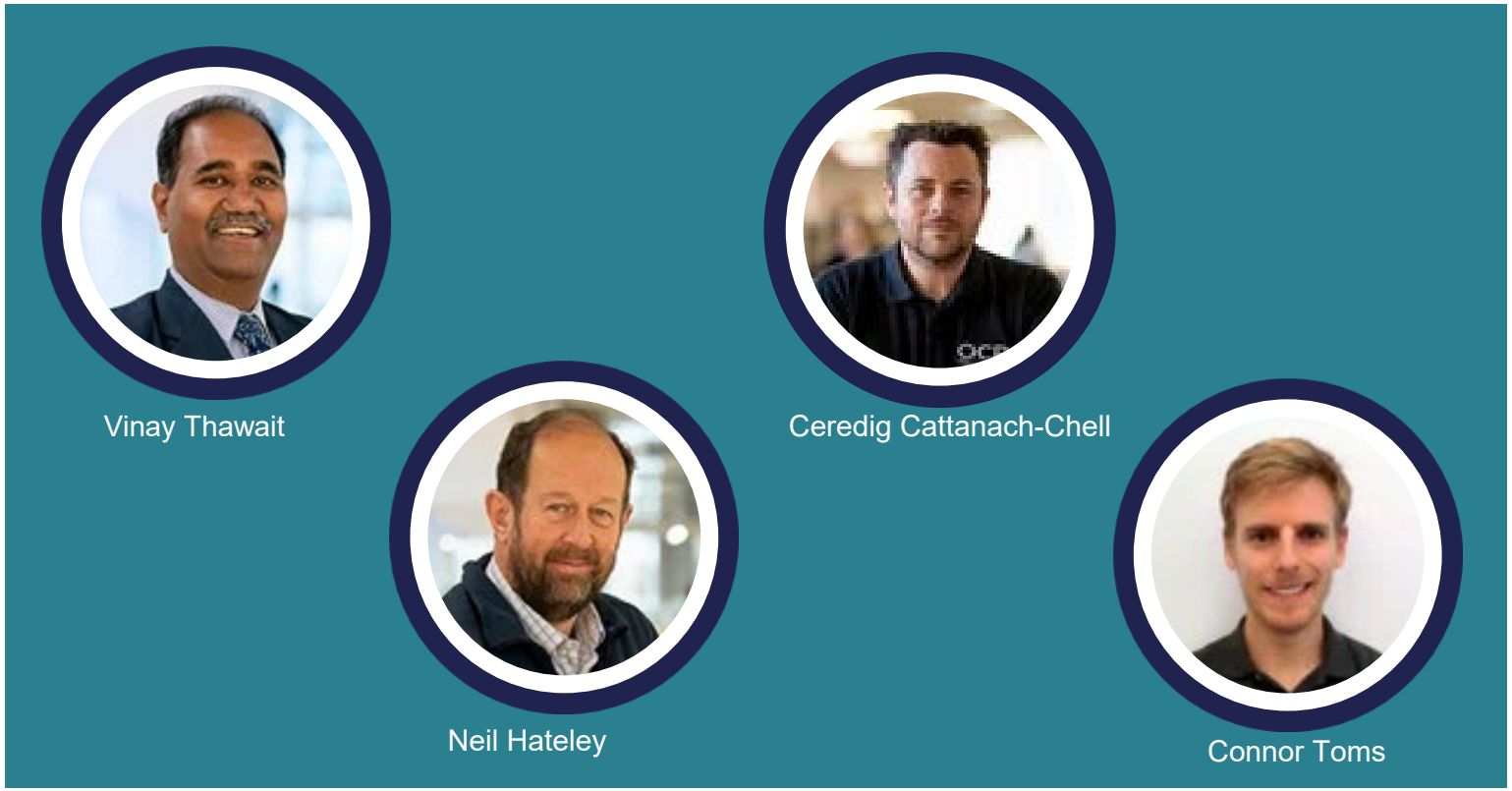
https://teach.ocr.org.uk/cambridge-advanced-nationals-options-evening-toolkit-download

Blogs

- V Levels vs AAQs in IT, Computing and Cyber Security
- Cambridge Advanced Nationals (AAQs) FAQ
- Other blogs related to AAQs



Support from the Computing Subject Advisor Team



@OCR_ICT support@ocr.org.uk 01223 553998

https://teach.ocr.org.uk/meet-the-subject-team-computing

- Support with delivery and assessment preparation
- One-to-one MS Teams meetings
- Regular subject briefings – teacher networks
- Support with becoming OCR's AAQ and Computing Ambassador School
- Attendance and talks at conferences
- Supporting CAS Hub meetings
- MAT Computing Teachers' meetings
- Other relevant support with computing qualifications

Next steps

- Complete our Expression of Interest Form
- Visit the new Cambridge Advanced Nationals landing page and download our specifications, sample assessment materials, switching guides and more
- Book onto one of our free professional development courses
- Watch our full compensation marking video and download the Cambridge Advanced Nationals summary brochure
- Sign up for email updates (be sure to select “Cambridge Advanced Nationals” and/or your subject areas)
- Join the OCR Facebook group for teacher support
- Cambridge Advanced Nationals FAQ page
- Cambridge Advanced Nationals Administration page
- Cambridge Advanced Nationals Moderation
- If you have any questions or need support with planning, then let the Partnership team know partnerships@cambridge.org

CAMBRIDGE
OCR

Thank You

© Cambridge OCR 2025