Institute for Apprenticeships & Technical Education

Higher technical qualification submission form

Awarding body information

Awarding body information

What is the name of the awarding body?
New College Durham

Is the awarding body a higher education provider?
Yes

Is the awarding body on the Office for Students register?
Yes

Qualification information

Qualification information

You can only submit one qualification for each form. If you are submitting multiple qualifications you must start a new form for each qualification. Please include the name of the qualification as it appears on Ofqual register or UCAS. Include the size of the qualification. e.g. award, certificate, diploma

What is the name of the qualification?
FdSc.Cyber Security

Is the qualification on the Ofqual register?
No

If the qualification is not regulated by Ofqual, the organisation owning the qualification must be OfS regulated. This is typically the case of qualifications from Higher Education Providers. For organisations which are Ofqual regulated, the specific qualification must be on the Ofqual register for the application to be progressed. The form will not prevent continuing if this is not completed, but your application cannot be progressed by the approval managers following submission if the awarding organisation is regulated by Ofqual but the qualification is not.

What is the level of the qualification?
Level 5

Route and occupational standards

Route and occupational standards

Awarding bodies must demonstrate that a qualification will enable a person to demonstrate that they have attained as many of the knowledge, skills and behaviours set out in the standard as may be reasonably expected by undertaking a course of education.

Please note:

- Qualifications will only be considered for approval against occupational standards approved by the Institute.

If qualifications have optional units or pathways, we will only approve qualifications where every possible combination of units/ pathways ensures that a learner achieves competence in at least one occupation for which there is a standard. Qualifications with optional units that do not ensure this should be redesigned or remove optional units that do not align to occupations.
Awarding bodies must fill out all sections of this form. They must also submit supporting documentation to provide evidence of the following:

- The content of the qualification (for example, the specification of content)
- Evidence of employer engagement in the development and validation of the qualification (for example this could be within the qualification design and validation documentation that was used through the development of the qualification which evidences where and how employers were involved)

Which route does the qualification fall under?
Digital

Which occupational standards are aligned to the qualification?
Cyber-secruity technologist/Level: 4

Attach documents

Please attach the following documents:

- The content of the qualification (for example, the specification of content)
- Evidence of employer engagement in the development and validation of the qualification (for example this could be within the qualification design and validation documentation that was used through the development of the qualification which evidences where and how employers were involved)

Upload
FdSc Computing with Networking . FdSc Cyber Security modifications.pdf

Employer Engagement - Cyber Security.docx

Cyber-security technologist

Cyber-security technologist

Knowledge, skills and behaviours coverage within the qualification

Please identify which knowledge, skill and behaviour statements from the occupational standard are covered within the qualification.

Where knowledge, skill and behaviour statements are covered, please provide a reference to the qualification content. This should be a unit or module reference along with associated page/paragraph/line numbers (as appropriate) in the attached specification. Please be as specific as possible which content in the qualification aligns to the statement in the standard.

Where knowledge, skill or behaviour statements are partially covered or not covered, you will be asked to provide a rationale for the exclusion of this content from the qualification. The employer engagement evidence provided should support this rationale.

The following questions assess how knowledge, skill and behaviour statements from the occupational standards are covered within the qualification.

This page has automatically generated an item for each knowledge, skill and behaviour statement (KSB) contained within the chosen standard. So please do not remove or add any further KSBs, as it requires the exact number.

KSBgenerator

KSB

KSB 1

K1 Principles of networks: OSI and TCP/IP models, data, protocols and how they relate to each other; the main routing protocols; the main factors affecting network performance including typical failure modes in protocols and approaches to error control; virtual networking.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Introduction to Networking (See Modifications June 2020 Document page 5-6), Switching, Routing and Wireless Essentials (See Modifications June 2020 Document page 13-15).

KSB 2

K2 The concepts, main functions and features of at least three Operating Systems (OS) and their security functions and associated security features.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD1 page 60-61 Validation Document LOs 2, 3 and 4; CST Apprentices are required to include at least 3 Operating Systems and their security functions and associated security features for assessment in this module

KSB 3

K3 Cyber security concepts and why cyber security matters to business and society; Security assurance concepts and how assurance may be achieved in practice including penetration testing and extrinsic assurance methods.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Cyber Security Fundamentals Page 72-73 Validation Document, Concepts and Future Trends, page 94-96 Validation Document

KSB 4

K4 The main types of common attack techniques; also the role of human behaviour, including the significance of the 'insider threat'. Including: - how attack techniques combine with motive and opportunity to become a threat. - techniques and strategies to defend against attack techniques and mitigate hazards.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Concepts and Future Trends, page 94-95 Validation Document, Security Technology and Applied Cryptography page 102-104

KSB 5

K5 The significance of identified trends in cyber security threats and understand the value and risk of this analysis. How to deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Fundamentals of Security Programming page 79-81 Validation Document, Concepts and Future Trends, page 94-96 Validation Document

KSB 6

K6 Lifecycle and service management practices to an established standard to a foundation level for example Information Technology Infrastructure Library (ITIL) foundation level.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD1 page 60-61 and Work Related Learning 1 page 64-66 Validation Document, CST Apprentices are required to demonstrate life cycle and service management practices to their employer's quality standard in their evidence for assessment in these modules

KSB 7

K7 Cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Security Technology and Applied Cryptography, page 102-104, Cyber Security Operations page 27-29 Modifications June 2020 Document

KSB 8

K8 Understands the main features, applicability and how to apply the significant law, regulations and standards relevant specifically to cyber security. To include: laws, regulations & standards relating to personal data and privacy (e.g. Data Protection Act 2018 implementing General Data Protection Regulation); use of digital systems (e.g. Computer Misuse Act 1990); regulatory standards for cyber security, intelligence collection and law enforcement (e.g. Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000; standards for good practice in cyber security (e.g. ISO 27001, CyberEssentials, NIST) and any updates or additions.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 1 (Legislation, regulations and ethical standards), page 64-66 Validation Document

KSB 9

K9 Ethical principles and codes good practice of at least one significant cyber security professional body and the ethical responsibilities of a cyber security professional.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 1 (Legislation, regulations and ethical standards), page 64-66 Validation Document

KSB 10

K10 How to analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD2 (Security Case Development) page 83-85 Validation Document

KSB 11

K11 Horizon scanning including use of recognised sources of threat intelligence and vulnerabilities.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD2 (Security Case Development) page 83-85 Validation Document

KSB 12

K12 Common security architectures and methodologies; be aware of reputable security architectures that incorporates hardware and software components, and sources of architecture patterns and guidance. How cyber security technology components are typically deployed in digital systems to provide security functionality including: hardware and software to implement security controls.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Cyber Security Fundamentals page 72-74 Validation Document, PPD2 (Security Case Development) page 85-87 Validation Document

KSB 13

K13 The basic terminology and concepts of cryptography; common cryptography techniques in use; the importance of effective key management and the main techniques used; legal, regulatory and export issues specific to use of cryptography.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Security Technology and Applied Cryptography page102-104 Validation Document, PPD2 (Security Case Development) page 83-85 Validation Document

KSB 14

K14 Risk assessment and audit methodologies and approaches to risk treatment; approaches to identifying the vulnerabilities in organisations and security management systems; the threat intelligence lifecycle; the role of the risk owner in contrast with other stakeholders.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) Page 86-88 Validation Document

KSB 15

K15 Principles of security management systems, including governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 1 (Legislation, regulations and ethical standards) page 64-66 Validation Document, Cyber Security Fundamentals page 72-74 Validation Document

KSB 16

K16 Function and features of significant digital system components; typical architectures; common vulnerabilities in digital systems; principles and common practice in digital system security.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Cyber Security Fundamentals page 72-74 and Security Technology and Applied Cryptography page 102-104 Validation Document, Introduction to Networks page 5-7 and Switching, Routing and Wireless Essentials page 13-15 Modification Document

KSB 17

K17 Programming or scripting languages.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Fundamentals of Security Programming page 79-81 Validation Document

KSB 18

S1 Discover vulnerabilities in a system by using a mix of research and practical exploration).

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Fundamentals of Security Programming page 79-81 and Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document, Cyber Security Operations page 27-29 Modification Document

KSB 19

S2 Analyse and evaluate security threats and hazards to a system or service or processes. Use relevant external source of threat intelligence or advice (e.g. National Cyber Security Centre) Combine different sources to create an enriched view of cyber threats and hazards.

Is the statement covered within the qualification?

Fully covered

Where within the qualification is the statement covered?
Cyber Security Fundamentals page 72-74 Validation Document, Cyber Security Operations page 27-29 Modification Document

KSB 20

S3 Research and investigate common attack techniques and relate these to normal and observed digital system behaviour and recommend how to defend against them. Interpret and demonstrate use of external source of vulnerabilities (e.g. OWASP, intelligence sharing initiatives, open source).

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development), page 83-85 Validation Document, Cyber Security Operations page 27-29 Modification Document

KSB 21

S4 Undertake security risk assessments for simple systems without direct supervision and propose basic remediation advice in the context of the employer.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development), page 83-85 and Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document,

KSB 22

S5 Source and analyse security cases and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development), page 83-85 Validation Document

KSB 23

S6 Analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development), page 83-85 and Work Related Learning 2 (Risk Assessment) page

86-88 Validation Document

KSB 24

S7 Identify and follow organisational policies and standards for information and cyber security and operate according to service level agreements or other defined performance targets.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document, Concepts and Future Trends page 94-96 Validation Document

KSB 25

S8 Configure, deploy and use computer, digital network and cyber security technology.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document, Security Technology and Applied Cryptography page 102-104 Validation Document

KSB 26

S9 Recommend improvements to the cyber security posture of an employer or customer based on research into future potential cyber threats and considering threat trends.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document, Security Technology and Applied Cryptography page 102-104 Validation Document

KSB 27

S10 Design, build, test and troubleshoot a network incorporating more than one subnet with static and dynamic routes, to a given design requirement without supervision. Provide evidence that the system meets the design requirement.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Introduction to Networks page 5-7 Modification Document, Enterprise Networking, Security and Automation page 20-22 Modification Document

KSB 28

S11 Analyse security requirements (functional and non-functional security requirements that may be presented in a security case) against other design requirements (e.g. usability, cost, size,

weight, power, heat, supportability etc.), given for a given system or product. Identify conflicting requirements and propose, with reasoning, resolution through appropriate trade-offs.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development), page 83-85 Validation Document

KSB 29

S12 Design and build, systems in accordance with a security case within broad but generally well-defined parameters. This should include selection and configuration of typical security hardware and software components. Provide evidence that the system has properly implemented the security controls required by the security case.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development), page 83-85 Validation Document, Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document

KSB 30

S13 Write program code or scripts to meet a given design requirement in accordance with employers' coding standards.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Fundamentals of Security Programming page 79-81 Validation Document, Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document

KSB 31

S14 Design systems employing encryption to meet defined security objectives. Develop and implement a plan for managing the associated encryption keys for the given scenario or system.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Security Technology and Applied Cryptography page 102-104 Validation Document

KSB 32

S15 Use tools, techniques and processes to actively prevent breaches to digital system security.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?

Security Technology and Applied Cryptography page 102-104 Validation Document

KSB 33

S16 Conduct cyber-risk assessments against an externally (market) recognised cyber security standard using a recognised risk assessment methodology.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document

KSB 34

S17 Identify cyber security threats relevant to a defined context.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development) page 83-85 Validation Document, Security Technology and Applied Cryptography page 102-104 Validation Document

KSB 35

S18 Develop information security policies or processes to address a set of identified risks, for example from security audit recommendations.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development) page 83-85 Validation Document

KSB 36

S19 Develop information security policies within a defined scope to take account of legislation and regulation relevant to cyber security.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development) page 83-85 Validation Document

KSB 37

S20 Take an active part in a security audits against recognised cyber security standards, undertake gap analysis and make recommendations for remediation.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
PPD 2 (Security Case Development) page 83-85 Validation Document, PPD 2 (Security Case Development) page 83-85 Validation Document

KSB 38

S21 Develop plans for incident response for approval within defined governance arrangements for incident response.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Concepts and Future Trends page 94-96 Validation Document, Security Technology and Applied Cryptography page 102-104 Validation Document, Cyber Security Operations page 27-29 Modification Document

KSB 39

S22 Develop plans for local business continuity for approval within defined governance arrangements for business continuity.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document

KSB 40

S23 Assess security culture using a recognised approach.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 1 (Legislation, regulations and ethical standards) page 64-66 Validation Document, Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document

KSB 41

S24 Design and implement a simple ‘security awareness’ campaign to address a specific aspect of a security culture.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 1 (Legislation, regulations and ethical standards) page 64-66 Validation Document, Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document

KSB 42

S25 Integrate and correlate information from various sources (including log files from different sources, digital system monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compare to known threat and vulnerability data to form a judgement based on evidence with reasoning that the anomaly represents a digital system security breach.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Concepts and Future Trends page 94-96 Validation Document, Security Technology and Applied Cryptography page 102-104 Validation Document

KSB 43

S26 Recognise anomalies in observed digital system data structures (including by inspection of network packet data structures) and digital system behaviours (including by inspection of protocol behaviours) and by inspection of log files and by investigation of alerts raised by automated tools including SIEM tools.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Security Technology and Applied Cryptography page 102-104 Validation Document, Cyber Security Operations page 27-29 Modifications Document

KSB 44

S27 Accurately, objectively and concisely record and report the appropriate cyber security information, including in written reports within a structure or template provided.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Cyber Security Fundamentals page 72-74 Validation Document, Security Technology and Applied Cryptography page 102-104 Validation Document

KSB 45

S28 Configure digital system monitoring and analysis tools (e.g. SIEM tools), taking account of threat & vulnerability intelligence, indicators of compromise.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Cyber Security Fundamentals page 72-74 Validation Document, Cyber Security Operations page 27-29 Modifications Document

KSB 46

S29 Undertake root cause analysis of events and make recommendations to reduce false positives and false negatives.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document, Security Technology and Applied Cryptography page 102-104 Validation Document

KSB 47

S30 Manage local response to non-major incidents in accordance with a defined procedure.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Concepts and Future Trends page 94-96 Validation Document, Security Technology and Applied Cryptography page 102-104 Validation Document

KSB 48

B1 Logical - Applies logical thinking, for example, uses clear and valid reasoning when making decisions related to undertaking the work instructions.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) page 86-88 Validation Document and all modules

KSB 49

B2 Analytical - working with data effectively to see patterns, trends and draw meaningful conclusions.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Concepts and Future Trends page 94-96 Validation Document and all modules

KSB 50

B3 Works independently and takes responsibility. For example, works diligently regardless of how much they are being supervised, and stays motivated and committed when facing challenges.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?

Personal and Professional Development 1 page 60-62 Validation Document and all modules

KSB 51

B4 Shows initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Personal and Professional Development 1 page 60-62 Validation Document and all modules

KSB 52

B5 Thorough & organised. For example uses their time effectively to complete work to schedule and takes responsibility for managing their own work load and time.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Personal and Professional Development 1 page 60-62 Validation Document and all modules

KSB 53

B6 Works effectively with a wide range of people in different roles, internally and externally, with a regard to inclusion & diversity policy.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) page 86-88 and all modules

KSB 54

B7 Communicates effectively in a wide variety of situations for example contributing effectively to meetings and presenting complex information to technical and non-technical audiences.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Work Related Learning 2 (Risk Assessment) page 86-88 and all modules

KSB 55

B8 Maintains a productive, professional and secure working environment.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?

Personal and Professional Development 1 page 60-62 Validation Document and all modules

KSB 56

B9 Creative - taking a variety of perspectives, taking account of unpredictable adversary and threat behaviours and approaches, bring novel and unexpected solutions to address cyber security challenges.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Concepts and Future Trends page 94-96 Validation Document

KSB 57

B10 Problem Solving - Identifies issues quickly, solves complex problems and applies appropriate solutions. Dedicated to finding the true root cause of any problem and find solutions that prevent recurrence.

Is the statement covered within the qualification?
Fully covered

Where within the qualification is the statement covered?
Fundamentals of Security Programming page 79-81 Validation Document, Security Technology and Applied Cryptography page 102-104 Validation Document

Additional occupationally relevant content

Additional occupationally relevant content

Item 1

As well as the content aligned to the knowledge, skills and behaviours in the occupational standard, the qualification can include additional occupationally relevant content which is deemed of value to employers. Awarding bodies are asked to justify any content that does not directly align to the occupational standard, using evidence from employers.

Content should be identified at a unit or modular level and each item should be added separately by using the Add Item button. If the qualification does not include any additional content, please leave this section blank.

Unit or module containing additional content
Personal and Professional Development 1

Please give a short description of the additional content
This module includes opportunities for apprentices to demonstrate a comprehensive range of knowledge, skills and behaviours specific to their job role

Where within the qualification is the additional content covered?
Page 60-62

Please provide an explanation of how the content is relevant to the occupation, including evidence from employers that supports its inclusion in the qualification.

Apprentices will identify any KSBs not specifically included in modules and undertake independent learning to develop competence in these areas ready for assessment.

Item 2

As well as the content aligned to the knowledge, skills and behaviours in the occupational standard, the qualification can include additional occupationally relevant content which is deemed of value to employers. Awarding bodies are asked to justify any content that does not directly align to the occupational standard, using evidence from employers.

Content should be identified at a unit or modular level and each item should be added separately by using the Add Item button. If the qualification does not include any additional content, please leave this section blank.

Unit or module containing additional content
Work Related Learning 2 (Risk Assessment)

Please give a short description of the additional content
This module includes opportunities for apprentices to demonstrate a comprehensive range of knowledge, skills and behaviours specific to their job role

Where within the qualification is the additional content covered?
Page 86-88 Validation Document

Please provide an explanation of how the content is relevant to the occupation, including evidence from employers that supports its inclusion in the qualification.
This module includes opportunities for apprentices to demonstrate a comprehensive range of knowledge, skills and behaviours as detailed in the standard and specific to the employer business needs by contributing to the completion of a project.

Please attach any additional, relevant employer engagement evidence for the inclusion of additional content.
Employer Engagement - Cyber Security.docx

Assessment methods

Assessment methods

Please confirm that the assessment covers all of the content relevant to the knowledge, skills and behaviours in the occupational standard.
Yes

Please outline the methods used to assess the content and provide a rationale for why these methods are valid for the qualification.
Personal Professional Development 1: Assessed by a Personal Development Project enables apprentices to identify personal KSB gaps, source appropriate CPD and engage in Independent Learning demonstrating effective implementation of a personal development plan and ensuring an ability to show current and future employers the ability to independently learn and apply new knowledge and skills as required in the computing sector

Work Related Learning 1 (Legislation, regulations and ethical standards): Assessed with a Research Project ensuring the ability to maintain currency in legislation, regulations and ethical standards which is appropriate as standards and regulations change and apprentices must be able to keep up to date. Also assessed with an Interview/presentation to ensure apprentices are able to relate the key concepts and benefits appropriate to their job role, the apprenticeship standard and ISO standards

Introduction to Networks: this module incorporates Cisco CCNA v7 exams and is assessed by a Practical Skills Exam and Report and Cisco Online Exams.

Cyber Security Fundamentals: this module incorporates Cisco exams and is assessed by a Practical Skills Exam and Report and Cisco Online Exams. The assessments aim is to ensure deep knowledge and understanding and the ability to appropriately apply skills.

Switching, Routing and Wireless Essentials: this module incorporates Cisco exams and is assessed by a Practical Skills Exam and Report and Cisco Online Exams. The assessments aim is to ensure deep knowledge and understanding and the ability to appropriately apply skills.

Fundamentals of Security Programming: assessment is by a formal report followed by the design and production of a programme which is evaluated by the apprentice in an assessed presentation. The learning outcomes allow flexibility for the assessment to be contextualised to the job role where appropriate.

Personal Professional Development 2 (Security Case Development): Apprentices will submit a Security Case Project and deliver a Presentation to demonstrate all of the learning outcomes which are contextualised to their job role and apprenticeship standard.

Work Related Learning 2 (Risk Assessment): Assessed by Report, Product and Interview/Presentation covering all of the module outcomes and ensuring the flexibility to contextualise the assessment against the apprentice job role and the standard. Apprentices will engage in a project in their workplace approved by the module tutor and apprentice skills coordinator to provide the evidence for this module.

Enterprise Networking, Security and Automation: this module incorporates Cisco exams and is assessed by a Practical Skills Exam and Report and Cisco Online Exams. The assessments aim is to ensure deep knowledge and understanding and the ability to appropriately apply skills.

Concepts and Future Trends: Assessed by a report before formally delivering a presentation. Appropriate as these are activities that will need to be carried out regularly in the work place to keep up with this rapidly changing sector.

Cybersecurity Operations: this module incorporates Cisco exams and is assessed by a Practical Skills Exam and Report and Cisco Online Exams. The assessments aim is to ensure deep knowledge and understanding and the ability to appropriately apply skills.

Security Technology & Applied Cryptography: Assessed by Presentation and Report. This is appropriate to ensure cyber security technologists are able to articulate complex issues to a professional standard and appropriately to the target audience.

The range of assessment methods are appropriate to the modules and have been developed to prepare apprentices to become work ready and allow for contextualisation to the apprentice's job role and their apprenticeship standard where appropriate. The vast majority of learning is made up of hands on practical activities conducted in the Cisco lab which includes cisco cabinets enabling students to design, build and test networks and the cyber security lab which includes an isolated network to allow students to carry out security checks, ethical hacking and penetration testing activities is a safe way. All modules are developed to enable contextualisation to ensure apprentices are able to be assessed for all of the KSBs detailed in the apprenticeship standard.

Employer engagement

Employer engagement

Please describe how employers and industry practitioners were consulted throughout the development of the qualification, including:

- the process of identifying and recruiting relevant employers
- how employers were involved in the development, review and validation of the qualification materials.

Please describe how employers and industry practitioners were consulted throughout the development of the qualification.
All Foundation Degrees are designed in collaboration with employers from the computing & digital sector with an interest in the specific course knowledge skills and behaviours. Additionally, it is an essential requirement of validation that an employer with expertise in the subject as well as a subject specialist academic is a member of the validation panel.

Focus Groups
All foundation degrees in computing have been mapped to the associated standard and so already have a significant employer contribution. When designing a Foundation Degree, a focus group is established to encourage employers to consider the knowledge skills and behaviours they value from students who achieve.

Discussions among the employers help to ensure that in addition to relevant and valid modules, learning outcomes are sufficiently clear to ensure the standards are met and sufficiently vague to allow the content within the modules to be contextualised to a higher apprentice job role. This ensures that the higher apprentice has the opportunity to cover the knowledge skills and behaviours required by the standard between the foundation degree and work based learning.

In developing the FdSc Cyber Security Foundation Degree, employers from the following organisations contributed to the design in preparation for validation and/or have provided positive support throughout delivery of the course:

- Leighton Group
- British Airways
- Opta
- NVIDIA
- British Telecom
- Durham County Council
- Waterstons
- Durham Police

The Validation of all Foundation Degrees at New College Durham requires that all validation documents are scrutinised by an employer from the associated sector and an academic who specialises in the subject. Both the employer and the academic sit on the Validation Panel and interrogate the curriculum team regarding subject content, assessment methods, employer engagement activities, relevance to apprenticeship standards where appropriate and academic standards in relation to the UK Quality Code and QAA. Validation is only approved when the panel is fully satisfied that the Foundation Degree content, assessment methods, occupational relevance and academic standards are assured.

Please refer to:
-Stage 2, item (ii), page 2
-Stage 1, paragraph 2, page 5
-Questions for the panel to consider, item (iv) page 6
-Stage 2, paragraphs 2 and 3, page 7
-Documentation required Notes, item (ii) page 9
-Stage 4, paragraph 2 page 13
of the attached Validation Process Document

Please attach evidence of employer validation of the qualification.
Validation Process Document.pdf