NCFE Level 5 Diploma: Cloud Systems and Secure Networking
QN: 610/5971/7

Qualification Specification

HIGHER TECHNICAL QUALIFICATION

Version 1.0 May 2026

Visit ncfe.org.uk **Call** 0191 239 8000

Qualification summary

Qualification title	**NCFE Level 5 Diploma: Cloud Systems and Secure Networking**
Ofqual qualification number (QN)	610/5971/7
Guided learning hours (GLH)	540
Total qualification time (TQT)	1200
Credit value	120
Minimum age	18
Qualification purpose	This qualification is designed for learners who want to upskill or retrain within the digital sector. It is also suitable for learners who want to further their studies in the digital sector. This higher technical qualification (HTQ) will give learners the skills, knowledge and behaviours to meet specific employer needs and industry requirements.
Grading	Pass/merit/distinction
Assessment method	Internally assessed and externally quality assured portfolio of evidence, including task-based assessments.
Work/industry placement experience	Work/industry placement experience is not required.
Apprenticeship/ Occupational standards	Network engineer (OCC0127) This HTQ content has been aligned with the Network Engineer occupational standard. This HTQ is designed to be delivered as a stand-alone qualification which is an alternative to an apprenticeship. It does not form part of an apprenticeship.
Regulation information	This is a regulated qualification. The regulated number for this qualification is 610/5971/7.
Funding	This qualification may be eligible for funding. For further guidance on funding, please contact your local funding provider.

Contents

Section 1: introduction

Centres must ensure they are using the most recent version of the Qualification Specification on the NCFE website.

A higher technical qualification (HTQ) is a prestigious, kite-marked qualification aimed at meeting employers' needs and increasing learner engagement in level 4 or 5 technical education. This HTQ content has been aligned with the Network Engineer apprenticeship standard.

This qualification aims to:

- provide the knowledge, skills and behaviours that are needed to enter occupations across the country
- be understood and recognised as high quality by employers and so have national labour market currency
- give learners confidence that those qualifications are recognised by employers and are perceived to be a credible, prestigious and distinct pathway.

Aims and objectives

This qualification aims to:

- focus on the study of cloud systems and secure networking within the digital sector
- offer breadth and depth of study, incorporating a key core of knowledge
- provide opportunities to acquire a number of practical and technical skills.

The objectives of this qualification are to provide learners with knowledge, skills and behaviours related to the following areas:

- cloud networking protocols, services and topologies
- cyber security threats and risk management
- network performance, optimisation, and maintenance
- change management and business continuity in network infrastructure
- security compliance and legislation
- secure system administration.

Support Handbook

This Qualification Specification must be used alongside the mandatory Support Handbook, which can be found on the NCFE website. This contains additional supporting information to help with planning, delivery and assessment.

This Qualification Specification contains all the qualification-specific information you will need that is not covered in the Support Handbook.

Guidance for entry and registration

This qualification is designed for learners who want to advance their career in secure network infrastructure.

It may also be useful to those with suitable industry experience, or for learners studying qualifications in the following sectors/areas:

- cloud computing
- cyber security
- networking
- software development
- data and analytics.

Registration is at the discretion of the centre in accordance with equality legislation and should be made on the NCFE Portal.

There are no specific prior skills/knowledge a learner must have for this qualification. However, learners may find it helpful if they have already achieved a level 4 qualification.

Centres are responsible for ensuring that all learners are capable of achieving the units and/or learning outcomes (LOs) and complying with the relevant literacy, numeracy, and health and safety requirements.

Learners registered on this qualification should not undertake another qualification at the same level, or with the same/a similar title, as duplication of learning may affect funding eligibility.

Achieving this qualification

To be awarded this qualification, learners are required to successfully achieve **120 credits overall, which is a minimum of a pass** in each of the **6** graded mandatory units.

Please refer to the list of units in appendix A or the unit summaries in section 2 for further information.

To achieve this qualification, learners must successfully demonstrate their achievement of all LOs of the units as detailed in this Qualification Specification. A partial certificate may be requested for learners who do not achieve the full qualification but have achieved at least one whole unit; partial achievement certificate fees can be found in the Fees and Pricing document on the NCFE website.

Progression

Learners who achieve this qualification could progress to the following:

- employment:
  - cloud engineer
  - cloud solutions architect
  - cyber security analyst
  - network engineer
  - security architect
- further education:
  - related apprenticeships
- higher education:
  - cloud computing degree
  - networking degree
  - cyber security degree
  - degree apprenticeship.

Resource requirements

There are no mandatory resource requirements for this qualification, but centres must ensure learners have access to suitable resources to enable them to cover all the appropriate LOs.

Realistic work environment (RWE) recommendation

The assessment of competence-based criteria should ideally be conducted within the workplace. However, in instances where this is not feasible, learners can be assessed in a realistic work environment (RWE) designed to replicate real work settings.

It is essential for organisations utilising an RWE to ensure it accurately reflects current and authentic work environments. By doing so, employers can be confident that competence demonstrated by a learner in an RWE will be translated into successful performance in employment.

In establishing an RWE, the following factors should be considered.

The work situation being represented is relevant to the competence requirements being assessed:

- The work situation should closely resemble the relevant setting.
- Equipment and resources that replicate the work situation must be current and available for use to ensure that assessment requirements can be met.
- Time constraints, resource access and information availability should mirror real conditions.

The learner's work activities reflect those found in the work environment being represented, for example:

- interaction with colleagues and others should reflect expected communication approaches
- tasks performed must be completed to an acceptable timescale
- learners must be able to achieve a realistic volume of work as would be expected in the work situation being represented
- learners operate professionally with clear understanding of their work activities and responsibilities
- feedback from colleagues and others (for example, customers, service users) is maintained and acted upon
- account must be taken of any legislation, regulations or standard procedures that would be followed in the workplace

How the qualification is assessed

Assessment is the process of measuring a learner's skill, knowledge and understanding against the standards set in a qualification.

This qualification is internally assessed and externally quality assured.

The assessment consists of one component:

- an internally assessed portfolio of evidence, which is assessed by centre staff and externally quality assured by NCFE (internal quality assurance must still be completed by the centre as usual).

Learners must be successful in this component to gain the Level 5 Diploma: Cloud Systems and Secure Networking.

Learners who are not successful can resubmit work within the registration period; however, a charge may apply in cases where additional external quality assurance visits are required.

All the evidence generated by the learner will be assessed against the standards expected of a level 5 learner for each LO.

Unless otherwise stated in this specification, all learners taking this qualification must be assessed in English and all assessment evidence presented for external quality assurance must be in English.

Internal assessment

We have created three sample assessments for the internally assessed units, which include a holistic, unit, and partial assessment. These can be found within three separate sample assessment materials documents on the NCFE website. These tasks are not mandatory. You can contextualise these tasks to suit the needs of your learners to help them build up their portfolio of evidence. The tasks have been designed to cover some of the LOs from 4 units and provide opportunities for stretch and challenge. For further information about contextualising the tasks, please contact the Provider Development team.

Each learner must create a portfolio of evidence generated from appropriate assessment tasks to demonstrate achievement of all the LOs associated with each unit. The assessment tasks should allow the learner to respond to a real-life situation that they may face when in employment. On completion of each unit, learners must declare that the work produced is their own and the assessor must countersign this.

If a centre needs to create their own internal assessment tasks, there are four essential elements in the production of successful centre-based assessment tasks; these are:

- ensuring the assessment tasks are meaningful with clear, assessable outcomes
- appropriate coverage of the content, LOs or assessment criteria (AC)
- having a valid and engaging context or scenario
- including sufficient opportunities for stretch and challenge for higher attainers.

External quality assurance

Summatively assessed and internally quality assured grades for completed units must be submitted via the NCFE Portal, prior to an external quality assurance review taking place. Following the external quality assurance review, the unit grades will either be accepted and banked by your external quality assurer (EQA) or, if they disagree with the grades, they will be rejected. More detailed guidance on this process and what to do if your grades are rejected can be found in the Support Handbook and on the NCFE website.

Enquiries about results

All enquiries relating to learners' results must be submitted in line with our Enquiries about Results and Assessment Decisions Policy, which is available on the NCFE website.

Not yet achieved grade

A result that does not achieve a pass grade will be graded as a not yet achieved grade. Learners may have the opportunity to resit.

Grading information

Each unit of the qualification is graded using a structure of not yet achieved, pass, merit, distinction.

Grading internally assessed units

The grading criteria for each unit have been included in the Qualification Specification. Grading criteria have been written for each LO in a unit. Assessors must be confident that, as a minimum, all LOs have been evidenced and met by the learner. Assessors must make a judgement on the evidence produced by the learner to determine the grading decision for the unit.

Once assessors are confident that all the pass criteria have been met, they can move on to decide if the merit criteria have been met. If the assessor is confident that all the merit criteria have been met, they can decide if the distinction criteria have been met. As the grading criteria build up from the previous grade's criteria, the evidence must meet 100% of the grade's criteria to be awarded that grade for the unit.

If the learner has insufficient evidence to meet the pass criteria, a grade of not yet achieved must be awarded for the unit.

Centres must then submit each unit grade via the NCFE Portal. The grades submitted will be checked and confirmed through the external quality assurance process. This is known as 'banking' units. Once a learner's grade has been banked, they are permitted one opportunity to revise and redraft their work; more detail on this process can be found in the Support Handbook.

The internal assessment component is based on performance of open-ended tasks that are assessed holistically against the grading criteria to achieve a grade. Each unit of the qualification is internally assessed and will be allocated a weighting based on the guided learning hours (GLH) and a score based on the holistic grade.

All of the assessment points need to be evidenced in the learner's portfolio, but the grade awarded is based on the standard of work for the LO as a whole. This allows for increased professional judgement on the part of the assessor in terms of the learner's overall level of performance against the LOs.

Awarding the final grade

To achieve the qualification, learners must have achieved a pass in all units.

The calculation of the overall qualification grade is based on the learner's overall performance across all of the units. Learners are awarded their grade based on the points allocated for each grade, across all units. The table below shows the amount of points awarded for each credit, per unit:

Grade	Points per credit
Pass	1
Merit	3
Distinction	5

This means that if a learner gains a pass in a unit of 20 credits, they would receive 20 points.

If they then gained a merit in a unit of 20 credits, they would receive 60 points.

If they then gained a distinction in their remaining units, totalling 80 credits, they would receive 400 points.

This would give a total of 480 points, which would then be used to calculate the overall grade, using the table below.

The table below shows the overall total points required for each grade boundary:

Grade	Points score
Not yet achieved	0 to 119
Pass	120 to 239
Merit	240 to 479
Distinction	480+

The final grade for the qualification is based on a structure of not yet achieved, pass, merit, distinction and will be issued to the centre by NCFE upon the centre claiming the learner's certificate on the NCFE Portal.

For further information on assessment, please refer to the User Guide to the External Quality Assurance Report, which can be found on the NCFE website.

NCFE does not anticipate any changes to our aggregation methods or any overall grade thresholds; however, there may be exceptional circumstances in which it is necessary to do so to secure the maintenance of standards over time. Therefore, overall grade thresholds published within this Qualification Specification may be subject to change.

Records of grades achieved for the NCFE Level 5 Diploma: Cloud Systems and Secure Networking (610/5971/7)

Grades achieved			Distinction		Merit		Pass		Points/ grade
Regulated unit number	**Unit title**	**Credits per unit**	**Points per credit**	**Points**	**Points per credit**	**Points**	**Points per credit**	**Points**	
R/651/6926	Cloud networking protocols, services and topologies	30	5	150	3	90	1	30	
T/651/6927	Cyber security threats and risk management	20	5	100	3	60	1	20	
Y/651/6928	Network performance, optimisation, and maintenance	20	5	100	3	60	1	20	
A/651/6929	Change management and business continuity in network infrastructure	20	5	100	3	60	1	20	
H/651/6930	Security compliance and legislation	15	5	75	3	45	1	15	
J/651/6931	Secure system administration	15	5	75	3	45	1	15	
							Total points		

Section 2: unit content and assessment guidance

This section provides details of the structure and content of this qualification.

Within learners' portfolios, a range of evidence types are acceptable if all learning outcomes (LOs) are covered, and if the evidence generated can be internally and externally quality assured. For approval of methods of internal assessment other than portfolio building, please contact your external quality assurer (EQA).

The explanation of terms explains how the terms used in the unit content are applied to this qualification. This can be found in section 3.

Behavioural framework

Embedded within higher technical qualifications (HTQs) is the opportunity for learners to develop behaviours relevant to their chosen discipline, in line with the qualification's knowledge and skills.

The following table identifies opportunities to demonstrate the behaviours – embedded within the knowledge and skills – that will be assessed as part of this HTQ. Learners may also naturally demonstrate these behaviours elsewhere, beyond the listing below. All listed behaviours are subject to assessment.

B1: Work independently and demonstrate initiative, being resourceful when faced with a problem and taking responsibility for solving complex problems within their own level of responsibility.
B2: Work within the goals, vision and values of the organisation.
B3: Work to meet or exceed customers' requirements and expectations.
B4: Commit to continued professional development, in order to ensure growth in professional skill and knowledge.
B5: Work under pressure showing resilience.
B6: Work collaboratively with external stakeholders and others across the organisation.

	Behaviours					
Unit	B1	B2	B3	B4	B5	B6
01: Cloud networking protocols, services and topologies	N/A	N/A	LO4 LO5	N/A	N/A	N/A
02: Cyber security threats and risk management	N/A	N/A	N/A	N/A	LO1	N/A
03: Network performance, optimisation, and maintenance	LO2 LO3	N/A	N/A	N/A	N/A	N/A
04: Change management and business continuity in network infrastructure	N/A	N/A	LO3	N/A	N/A	LO3
05: Security compliance and legislation	N/A	LO1 LO2	N/A	LO1 LO2	N/A	N/A
06: Secure system administration	N/A	N/A	N/A	N/A	LO4	N/A

Unit 01 Cloud networking protocols, services and topologies (R/651/6926)

Unit summary				
This unit provides a strong foundation for cloud networking fundamentals by examining network architecture, protocols, and services. The unit sets the foundation for cloud services by providing learners with the knowledge of cloud computing concepts and how various elements of IT infrastructure (for example, hardware, operating system, protocols, network services) operate and how they can be secured. Understanding the flow of data across network layers, and managing services securely is key to preventing vulnerabilities and attacks.				
Assessment				
Internally assessed unit				
Mandatory	**Graded P/M/D**	**Level 5**	**30 credits**	**130 GLH**

Learning outcomes (LOs)	Mandatory teaching content
1. Explore cloud computing concepts and their use within organisations	**Knowledge**: The characteristics of cloud computing in line with the National Institute of Standards and Technology (NIST) (for example, resource pooling). Different deployment models (for example, public, private) and how these meet business and security requirements. The key technical considerations when selecting a cloud environment. Use cases, benefits and limitations of cloud service solutions: • Software as a Service (SaaS) • Infrastructure as a Service (IaaS) • Platform as a Service (PaaS). Key considerations when selecting and implementing cloud service solutions: • business and strategic fit • technical requirements • security and risk management • data governance and compliance.
2. Explore components of IT system architecture and their role in supporting organisational IT solutions	**Knowledge**: Key components of IT system architecture and their role in delivering IT services: • hardware (for example, servers, switches) • software (for example, server operating systems). The role of network architecture in supporting system connectivity, performance and scalability.

Learning outcomes (LOs)	Mandatory teaching content
	The role and benefit of virtual machines: • workload consolidation • DR • sandboxing • flexible resource allocation. The function of hypervisors in managing virtual machines and allocating resources. How cloud integration (for example, SaaS) changes traditional IT architecture by enabling: • scalability • elasticity • service abstraction. IT architectural design decisions and how they affect: • system availability • redundancy • fault tolerance • disaster recovery (DR) planning. The impact IT architectural choices have on long-term system maintenance. How communication services (for example, Voice over Internet Protocol (VoIP)) are integrated within IT architectures. The role of operating system tools and services in managing, monitoring, and securing system components (for example, process management, system logs, resource monitoring).
3. Examine devices, applications, protocols and services within the context of conceptual models	**Knowledge**: How devices interact with conceptual models (for example, Open Systems Interconnection (OSI) model and the Transmission Control Protocol/Internet Protocol (TCP/IP) stack). How applications integrate within conceptual models: • operation at different layers (for example, application, transport) • their relationship to protocols and services. How socket pairs are used to uniquely identify and manage network communications between the sending device (for example, source IP address and port) and the receiving device (for example, destination IP address and port) using a specified protocol (for example, TCP).

Learning outcomes (LOs)	Mandatory teaching content
	The function of network protocols (for example, Hypertext Transfer Protocol (HTTP), TCP/IP, Domain Name System (DNS)) within the context of conceptual models. How network protocols enable communication across different layers and support data transmission. The role of network and cloud services (for example, Dynamic Host Configuration Protocol (DHCP), DNS) in conceptual models and how this links to network layers. The integration of devices, applications, ports, protocols, and services within conceptual models.
4. Explore and apply the key concepts of routing and switching	**Knowledge**: The concept of routing tables and the decision-making process used by routers to forward packets. The different use cases of static and dynamic routing to meet requirements. How to configure and manage common routing protocols (for example, RIP, EIGRP, OSPF). How routers enable communication between devices in different network segments. How switches operate at the data link layer (layer 2) of the OSI model. How to create and manage Virtual LANs (VLANs) and apply inter-VLAN routing techniques. The types and applications of network redundancy and load balancing techniques. The impact of routing and switching on network performance. The application of network addressing schemes (for example, IPv4, IPv6) and number system conversions (for example, decimal, binary) to support IP-based communication. The conversion of decimal and binary representations of IP addresses and subnet masks to support configuration and troubleshooting. How to develop network diagrams through the use of network modelling techniques to support effective network infrastructure planning. **Skills**:

Learning outcomes (LOs)	Mandatory teaching content
	Apply appropriate network addressing and numerical systems to meet specification requirements.
5. Explore network topologies and networking technologies and their ability to provide a secure, scalable, and efficient IT infrastructure	**Knowledge**: How cloud-based networks differ from traditional on-premises networks: • virtualisation • abstraction • software-defined networks (SDN). The function and configuration of virtual switches, routers, gateways, and firewalls in cloud platforms (for example, Azure, AWS). The use of different cloud network architecture (for example, hub-and-spoke, mesh, hybrid cloud) to meet organisational requirements. The use of technologies (for example, virtual private networks (VPNs), Direct Connect, Azure ExpressRoute) to establish secure connections between on-premises infrastructure and cloud environments. The application of cloud network segregation to isolate resources and manage traffic within virtual networks. How cloud providers implement security at the network layer and the additional controls organisations can implement. The application of core networking and security technologies used in cloud infrastructure to support secure organisation IT solutions (for example, virtual private cloud (VPC), SD-WAN). **Skills**: Interpret and implement information from internal or external stakeholders regarding network requirements.
6. Examine the functions and configurations of core network services in supporting IT operations	**Knowledge**: The role of DNS and DHCP in ensuring seamless communication within a network. How directory services (for example, Active Directory) centralise authentication and authorisation: • enforcing security policies • access control (for example, role-based access control (RBAC)) • enabling auditing • monitoring of user activities.

Learning outcomes (LOs)	Mandatory teaching content
	The importance of network time protocol (NTP) for time synchronisation across all network devices (for example, co-ordinated network operations). Approaches to provide secure, encrypted channels for users to access networks remotely (for example, VPN). Use of security measures for communication services (for example, email, VoIP) necessary to prevent data breaches and service disruption. Approaches to securing web services (for example, HTTPS) to protect sensitive data from attacks (for example, SQL injection). Approaches to securing print and file services to prevent unauthorised access. How monitoring and logging services (for example, Simple Network Management Protocol (SNMP), Syslog) are used to track network health, performance, and security.

Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
LO1: Explore cloud computing concepts and their use within organisations	**P1**: explain fundamental cloud computing concepts and their use by organisations	**M1**: explain how different cloud deployment and service models meet specific organisational business and security requirements	**D1**: critically evaluate strategic cloud service selections and associated IT architectural choices
LO2: Explore components of IT system architecture and their role in supporting organisational IT solutions	**P2**: describe key components of IT system architecture and their roles in delivering IT services	**M2**: analyse virtualisation technologies with operating systems in a cloud infrastructure	
LO3: Examine devices, applications, protocols and services within the context of conceptual models	**P3**: describe the purpose of the OSI and TCP/IP models and the protocols and services that operate at each layer	**M3**: explain the integration of devices, applications, protocols, and services across layers of conceptual models	**D2**: evaluate the integration of components within conceptual models for efficiency and security in a complex network environment
	P4: describe how socket pairs are used to manage network	**M4**: explain how socket pairs identify and manage network communications	

Learning outcomes (LOs)	Pass	Merit	Distinction
	communications between devices	between a sending device and a receiving device using a specified protocol	
LO4: Explore and apply the key concepts of routing and switching	**P5**: apply fundamental routing, switching, and network addressing concepts including required numerical conversions and the use of network diagrams and models	**M5**: apply routing, switching and network addressing concepts by developing and interpreting network models and diagrams	**D3**: justify optimal routing, switching, and addressing solutions for complex networks
LO5: Explore network topologies and networking technologies and their ability to provide a secure, scalable, and efficient IT infrastructure	**P6**: interpret basic stakeholder requirements to identify appropriate cloud networking topologies and technologies	**M6**: implement network solutions based on interpreted stakeholder requirements	**D4**: design a secure, scalable, and adaptable cloud network architecture for complex business, compliance, and security requirements
LO6: Examine the functions and configurations of core network services in supporting IT operations	**P7**: describe core network services in traditional and cloud-based systems	**M7**: explain configuration and security considerations for core network services supporting IT operations	**D5**: evaluate the effectiveness of secure configuration for core network services in maintaining service continuity and mitigating risk in cloud environments

Unit 02 Cyber security threats and risk management (T/651/6927)

Unit summary				
This unit focuses on identifying and analysing a wide range of threats to IT systems including internal, external and environmental risks. It will allow learners to explore vulnerabilities in networks, endpoint devices and at application level. Additionally, learners will explore threats specifically targeting wireless technology and system misconfigurations allowing them to examine how different IT components can be targeted by an attack. It covers threat modelling and the application of frameworks like the Confidentiality, Integrity, and Availability (CIA) triad allowing learners to develop skills to classify threat actors, assess social engineering risks, and apply mitigation strategies.				
Assessment				
Internally assessed unit				
Mandatory	**Graded P/M/D**	**Level 5**	**20 credits**	**90 GLH**

Learning outcomes (LOs)	Mandatory teaching content
1. Explore how different cyber threats affect IT systems and infrastructure	**Knowledge**: Security threats to IT systems: • internal • external • environmental. Network-based attacks and how they may compromise availability and data integrity. Characteristics and behaviours of endpoint threats. The ways in which application-layer vulnerabilities can be exploited by attackers. Threats associated with wireless technologies and unsecured wireless communications. The ways in which system vulnerabilities can be exploited by attackers: • poor configuration • outdated software. The ways in which different types of IT infrastructure assets can be targeted by threats. The ways to test and assess systems for vulnerabilities that can be exploited by attackers (for example, penetration testing, vulnerability scanning). **Skills**:

Learning outcomes (LOs)	Mandatory teaching content
	Apply appropriate testing tools and techniques to ensure system security and operational status of a network.
2. Evaluate human and organisational factors in cyber threats and actor behaviour	**Knowledge**: Social engineering attacks and how humans may contribute to security breaches. Classification of threat actors and their motivations: • insiders • cyber criminals • hacktivists • state-sponsored groups. The Tactics, Techniques, and Procedures (TTPs) used by cyber threat actors to compromise IT systems. How organisations may use TTPs to inform detection, incident response, and defensive strategies. The effectiveness of security training and areas where human error may lead to vulnerabilities.
3. Apply threat modelling and mitigation strategies to reduce organisational cyber risk	**Knowledge**: How to assess the potential impact of threats using the Confidentiality, Integrity, and Availability (CIA) triad. The techniques to detect and mitigate threats using: • appropriate tools • configuration hardening • defensive techniques. The application of threat modelling to identify, categorise, and prioritise threats to organisational IT assets. The application of mitigation strategies and the process of continuous monitoring to ensure that defensive measures are effective. **Skills**: Install and configure hardware and software, as required, to maintain and manage security. Monitor and manage network systems to prevent threats from affecting a network.

Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
LO1: Explore how different cyber threats affect IT systems and infrastructure	**P1**: describe common cyber threats to IT systems and the tools used for vulnerability detection	**M1**: develop a cyber risk management plan for an organisation	**D1**: justify a cyber risk management plan including tools and configurations
	P2: apply testing tools and techniques to identify vulnerabilities resulting from various cyber threats to IT systems and infrastructure		
LO2: Evaluate human and organisational factors in cyber threats and actor behaviour	**P3**: describe common threat actors, their motivations, and human factors that contribute to cyber threats	**M2**: analyse the TTPs of different threat actors and the influence of organisational factors on security posture	
LO3: Apply threat modelling and mitigation strategies to reduce organisational cyber risk	**P4**: install basic security configurations to mitigate common threats as part of a given risk treatment plan	**M3**: configure security elements and adapt system monitoring to mitigate identified organisational threats, informed by threat modelling	

Unit 03 Network performance, optimisation, and maintenance (Y/651/6928)

Unit summary				
Performance monitoring and network optimisation are crucial for ensuring both efficiency and security. Learners will explore how proactive maintenance helps prevent cyber incidents. This unit focuses on maintaining and optimising network performance, which directly ties into cyber security by preventing security risks, improving system efficiency, and ensuring continuous monitoring. Proactive maintenance, troubleshooting, and optimisation are key to detecting and mitigating vulnerabilities and ensuring that the network remains secure and functional, including the use of automated systems.				
Assessment				
Internally assessed unit				
Mandatory	**Graded P/M/D**	**Level 5**	**20 credits**	**90 GLH**

Learning outcomes (LOs)	Mandatory teaching content
1. Explore and apply techniques for optimising system performance	**Knowledge**: The factors that can affect a network and the impact these have on a network's performance. The application and impact of system performance techniques for optimisation: • traffic shaping • Quality of Service (QoS) • load balancing • caching. **Skills**: Use identifying, analysing and recording tools and techniques to monitor and optimise system performance.
2. Explore network maintenance that ensures network functionality	**Knowledge**: The types and implementation of network maintenance strategies: • proactive • reactive. The potential issues with not applying proactive network maintenance strategies. **Skills**: Identify and monitor appropriate system maintenance. Implement maintenance procedures to support network functionality (for example, cloud incident management and root cause analysis (RCA)).

Learning outcomes (LOs)	Mandatory teaching content
3. Apply troubleshooting methodologies for network and IT infrastructure	**Knowledge**: The application of troubleshooting methodologies to identify and resolve issues within network and IT infrastructure (for example, Top-Down Approach, divide and conquer). Potential impacts of not using a methodical approach to troubleshoot network and IT infrastructure issues. The application of troubleshooting techniques used in network and IT infrastructure (for example, isolate, repair or escalate faults). Use of root cause analysis techniques to diagnose system performance issues: • the five 'whys' • fishbone diagram • failure mode and effects analysis (FMEA) • event tree analysis (ETA) • Pareto chart. Use of diagnostic tools and techniques to gather and interrogate information on system performance: • packet analyser/sniffer software • network orchestration software • management console and dashboards • vendor-specific hardware management tools • cloud native security tools. Responsibilities and remit of internal and external stakeholders for network maintenance. **Skills**: Apply appropriate tools and techniques to gather information to support troubleshooting. Apply the appropriate diagnostic tools and techniques to identify system performance or security issues. Isolate, resolve or escalate faults as appropriate. Communicate responsibilities and diagnostic outcomes to internal and external stakeholders as required: • using appropriate language (for example, technical terminology) • considering accessibility and diversity requirements.

Learning outcomes (LOs)	Mandatory teaching content
4. Explore cloud management of wireless networks	**Knowledge**: How factors affect wireless network technologies used in cloud computing: • latency • bandwidth. How secure network and device configurations are applied to wireless technologies. Benefits and risks of wireless management in the cloud. How cloud management tools can help manage wireless infrastructure.

Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
LO1: Explore and apply techniques for optimising system performance	**P1**: apply identifying, analysing and recording tools and techniques for system performance optimisation and monitoring	**M1**: apply identifying, analysing and recording tools and techniques to monitor, and optimise system performance in line with defined specifications	**D1**: develop a comprehensive operational network management strategy for a complex IT infrastructure, integrating proactive performance optimisation techniques, risk-based maintenance schedules, and advanced troubleshooting methodologies
LO2: Explore network maintenance that ensures network functionality	**P2**: describe different types of network maintenance strategies and the importance of proactive maintenance for network functionality	**M2**: implement required network maintenance procedures to support network functionality, based on identified system needs	
LO3: Apply troubleshooting methodologies for network and IT infrastructure	**P3**: employ basic diagnostic tools to gather information regarding a reported network issue	**M3**: apply systematic troubleshooting methodologies and diagnostic tools to identify, isolate, and resolve network and IT infrastructure faults	
	P4: describe how to use root cause analysis techniques to diagnose system performance issues	**M4**: explain how to use a range of root cause analysis techniques to diagnose system performance issues	
LO4: Explore cloud management of wireless networks	**P5**: describe key factors affecting wireless network technologies in cloud computing and	**M5**: explain how cloud management tools are used to configure and manage wireless network infrastructure	**D2**: evaluate cloud-based wireless network management solutions for a specific organisational scenario

Learning outcomes (LOs)	Pass	Merit	Distinction
	common secure configurations for these networks		

Unit 04 Change management and business continuity in network infrastructure (A/651/6929)

Unit summary				
This unit focuses on the causes and consequences of failures within networks and the measures used to support business continuity. Learners will develop strategies for maintaining operations during cyber incidents and IT system failures. The unit covers maintaining business continuity and effectively managing IT changes, which is crucial for cyber security. Understanding disaster recovery and change management helps ensure that systems can be quickly restored after an attack, while secure change management practices prevent vulnerabilities from being introduced into the network. Additionally, recording and communicating actions taken during recovery processes are vital for compliance and transparency in security practices.				
Assessment				
Internally assessed unit				
Mandatory	**Graded P/M/D**	**Level 5**	**20 credits**	**90 GLH**

Learning outcomes (LOs)	Mandatory teaching content
1. Explore common failures within cloud infrastructure systems	**Knowledge**: The causes and consequences of failures within wireless and wired networks. Considerations for appropriate preventative measures to meet identified failures. Components and application of redundancy systems to support business continuity (BC). **Skills**: Interpret information from employer/end users when planning and prioritising network tasks and securely implement to maintain BC.
2. Explore how to integrate services into a network	**Knowledge**: The role of network services in supporting organisational operations: • reducing downtime • scalability • cost reduction • security • compliance. Methods to integrate services into the network: • manual administration • automation tools • cloud-based.

Learning outcomes (LOs)	Mandatory teaching content
	How factors (for example, cost, security and existing infrastructure) affect the selection of server infrastructure and its location: • virtual • physical • cloud-based. The process of upgrading, installing, configuring and testing servers to maintain BC.
3. Explore the role of organisational procedures in maintaining compliance with industry practices and stakeholder requirements	**Knowledge**: How disaster recovery (DR) and BC processes and procedures are implemented to restore operational functionality (for example, preservation of system configurations). How to manage and communicate non-compliance with service-level agreements (SLAs). The importance of establishing SLAs prior to the commencement of tasks. The potential impacts of not complying with SLAs (for example, contractual or financial penalties). **Skills**: Organise and prioritise internal and external stakeholders' requests in line with SLAs and organisation processes. Record and communicate key information to stakeholders, in line with SLAs and organisational process requirements.
4. Explore and apply approaches to change management	**Knowledge**: The role of a Change Advisory Board (CAB) within change management: • change requests • redundancy planning • security and risk analysis • CAB automation. How to verify outputs against the requirements of the change management process. Approaches to the implementation of Secure Access Service Edge (SASE): • zero trust principles.

Learning outcomes (LOs)	Mandatory teaching content
	Skills: Compare outputs against original change management requests and confirm compliance for SASE: • zero trust principles.

Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
LO1: Explore common failures within cloud infrastructure systems	**P1**: describe common causes of failures in cloud infrastructure systems and preventative measures for BC	**M1**: implement preventative measures against cloud infrastructure failures, based on employer/end user information	**D1**: evaluate the effectiveness of redundancy systems and preventative strategies for ensuring BC
LO2: Explore how to integrate services into a network	**P2**: describe the role of network services in supporting organisational operations	**M2**: explain techniques for integrating network services within a networked system	**D2**: justify a network service integration strategy for a complex organisational scenario
LO3: Explore the role of organisational procedures in maintaining compliance with industry practices and stakeholder requirements	**P3**: explain organisational procedures for BC, DR, and managing SLAs	**M3**: apply organisational procedures for managing stakeholder requests, SLAs, and BC communications effectively	**D3**: develop a comprehensive framework for restoring operational functionality and managing IT changes within an organisation
LO4: Explore and apply approaches to change management	**P4**: describe a common approach to IT change management	**M4**: apply a change management process for a specified IT system modification	
	P5: describe approaches to the implementation of Secure Access Service Edge (SASE)	**M5**: explain the zero trust principles within a SASE implementation strategy	**D4**: compare outputs against original change management requests and confirm compliance for SASE, including zero trust principles

Unit 05 Security compliance and legislation (H/651/6930)

Unit summary				
Learners will gain an understanding of legal and regulatory requirements for cyber security, focusing on compliance frameworks, data protection laws, and security policies. This unit focuses on the essential area of security compliance and legislation, which is critical to cyber security. Understanding the impact of legal requirements and regulations on security practices ensures that IT professionals can design and implement systems that not only meet security needs but also adhere to legal and regulatory standards. This knowledge and skillset are vital for ensuring data protection, privacy, and compliance within organisations, and mitigating the risk of penalties due to non-compliance.				
Assessment				
Internally assessed unit				
Mandatory	**Graded P/M/D**	**Level 5**	**15 credits**	**70 GLH**

Learning outcomes (LOs)	Mandatory teaching content

1. Assess how current legislation influences operational practice	**Knowledge**:
	
	How current legislation informs operational practice and the impact of non-compliance:
	
	• legislation:
	  ○ UK General Data Protection Regulation (UK GDPR)
	  ○ Data Protection Act 2018
	  ○ Computer Misuse Act 1990
	  ○ Waste Electrical and Electronic Equipment (Amendment, etc.) Regulations 2025.
	
	How to design and review organisational policies and procedures for the recording, handling and storing of data in line with legislation.
	
	Skills:
	
	Operate securely in compliance with appropriate legislation, policies, industry frameworks and procedures when completing network tasks, handling, recording and storing data.

2. Apply industry-recognised frameworks for cloud compliance	**Knowledge**: Key features of compliance frameworks (for example, ISO/IEC 27001, NIST Cybersecurity Framework (CSF) 2.0, CIS controls). Role of frameworks in managing risk, data protection, and regulatory compliance. How cloud providers align services with compliance standards.

Learning outcomes (LOs)	Mandatory teaching content
	Skills: Interpret and apply relevant compliance requirements to cloud operations in line with organisational and regulatory standards. Operate securely in line with recognised frameworks and internal policies.
3. Assess the implications of international legislation and cloud provider policies on data handling	**Knowledge**: Key features of international data protection laws (for example, UK GDPR, the US CLOUD Act 2018). The influence of cloud provider policies on data residency, access, and sovereignty. Legal considerations for cross-border data transfer and storage.

Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
LO1: Assess how current legislation influences operational practice	**P1**: describe key UK legislation relevant to cloud networking and its influence on operational practice	**M1**: explain how organisational data-handling procedures must align with specific articles of current UK legislation to ensure compliant operation	**D1**: develop an organisational strategy to ensure cloud networking operations comply with relevant UK legislation and an industry-recognised framework, justifying the necessary policies and procedural controls
LO2: Apply industry-recognised frameworks for cloud compliance	**P2**: explain key features of an industry-recognised compliance framework and their role in guiding secure cloud operations	**M2**: apply relevant controls from an industry-recognised compliance framework to meet defined security and compliance requirements	
LO3: Assess the implications of international legislation and cloud provider policies on data handling	**P3**: describe key elements of an international data protection law and common cloud provider data policies affecting data handling	**M3**: explain the implications of a specified international data protection law and cloud provider policies on data handling	**D2**: assess the data governance challenges for an organisation operating internationally

Unit 06 Secure system administration (J/651/6931)

Unit summary				
This unit focuses on securely configuring and managing IT systems. Learners will explore best practices for access control, patch management, and system hardening. It focuses on secure system administration, which is directly tied to cyber security practices. Configuring and maintaining systems securely involves ensuring that all components are regularly updated and tested, as well as managing access controls to safeguard against security breaches. By applying best practices for secure system administration, organisations can maintain robust security measures and ensure system integrity.				
Assessment				
Internally assessed unit				
Mandatory	**Graded P/M/D**	**Level 5**	**15 credits**	**70 GLH**

Learning outcomes (LOs)	Mandatory teaching content
1. Explore methods of configuring and administering network security	**Knowledge**: How to configure and administer network security: • access control • patch management • system hardening.
2. Explore secure scripting techniques to automate administrative tasks and performance	**Knowledge**: How automation tools (for example, configuration management, security management) support with network tasks and performance. The application of scripting languages (for example, PowerShell, Python, Bash) in cloud administration to automate routine administrative functions. The application of secure scripting practice (for example, input validation, error handling, secure credential management, and appropriate logging practices). Potential benefits and limitations of using automation tools for network administrative tasks. How artificial intelligence (AI) may be used in network automation to enhance performance, security, and reliability.
3. Explore system hardening measures and their impact on availability and security	**Knowledge**: The use of system hardening techniques (for example, disabling services, patching, removing defaults). How hardening improves security and reduces attack surfaces. The application of system hardening techniques to secure cloud environments.

Learning outcomes (LOs)	Mandatory teaching content
	Potential impacts on system availability, usability, and maintenance.
4. Apply techniques for upgrading and testing components	**Skills**: Select and use the appropriate tools to upgrade, apply and test components within a network to meet organisational requirements and comply with organisational policies and processes, to ensure minimal downtime and loss of data.

Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
LO1: Explore methods of configuring and administering network security	**P1**: describe common methods for configuring network security, including access control, patch management, and system hardening	**M1**: explain how specific methods of network security configuration address identified security threats in cloud environments	**D1**: evaluate the effectiveness of an integrated network security architecture, encompassing access control, patch management, and system hardening
LO2: Explore secure scripting techniques to automate administrative tasks and performance	**P2**: describe common scripting languages and secure scripting practices for automating administrative tasks and performance in cloud environments	**M2**: explain the application of scripts using a common language to automate routine administrative functions and performance	**D2**: implement key elements of a comprehensive secure system administration and performance plan for a complex cloud service
	P3: describe how artificial intelligence (AI) may be used in network automation	**M3**: explain how artificial intelligence (AI) may be used in network automation to enhance performance, security and reliability	
LO3: Explore system hardening measures and their impact on availability and security	**P4**: describe common system hardening techniques and their impact on system security and operational availability	**M4**: explain the application of system hardening techniques to a specified cloud component	
LO4: Apply techniques for upgrading and testing components	**P5**: explain a process for upgrading and testing system components in compliance with organisational policies	**M5**: execute the upgrade and testing of system components according to a defined plan	

NCFE assessment strategy

The key requirements of the assessment strategies or principles that relate to units in this qualification are summarised below.

The centre must ensure that individuals undertaking assessor or quality assurer roles within the centre conform to the assessment requirements for the unit they are assessing or quality assuring.

Knowledge LOs

- Assessors will need to be both occupationally knowledgeable and qualified to make assessment decisions.
- Internal quality assurers (IQAs) will need to be both occupationally knowledgeable and qualified to make quality assurance decisions.

Competence/skills LOs

- Assessors will need to be both occupationally competent and qualified to make assessment decisions.
- IQAs will need to be both occupationally knowledgeable and qualified to make quality assurance decisions.

The centre with which the learners are registered will be responsible for making all assessment decisions. Assessors must be **contracted** to work directly with the centre, contributing to all aspects of standardisation. The centre must ensure a process of training is followed, including during induction and quality assurance activities. Occupationally competent and qualified assessors from the centre must use direct observation to assess practical skills-based outcomes.

Section 3: explanation of terms

This table explains how the terms used at **level 5** in the unit content are applied to this qualification (not all verbs are used in this qualification).

Act (as a role model)	Serve as a model in a particular behavioural or social role for another person to emulate.
Adapt (approaches)	Modify, adjust, make suitable for purpose.
Adhere to	Follow, keep, maintain, respect, abide by, give support to (for example, adhere to a strict code of practice).
Analyse	Break down the subject or complex situations into separate parts and examine each part in detail, identify the main issues and show how the main ideas are related to practice and why they are important (reference to current research or theory may support the analysis).
Critically analyse	This is a development of 'analyse' that explores limitations as well as positive aspects of the main ideas in order to form a reasoned opinion.
Apply	Use knowledge, understanding, or skills in a practical context or given scenario to achieve a specified outcome.
Ascertain	Find out for certain.
Assess	Estimate and make a judgement.
Automate	To program or configure a system or process to operate without manual intervention.
Clarify	Explain the information in a clear, concise way showing depth and understanding.
Collaborate (L7)	Work jointly with.
Communicate	To convey information, ideas, or feelings effectively through various means to a specific audience.
Compare	Examine the subjects in detail looking at similarities and differences.
Compare and contrast	Examine the subjects in detail, looking at similarities and differences and distinguish between (identify) striking differences.
Demonstrate	Apply skills in a practical situation and/or show an understanding of the topic.
Describe	Provide an extended range of detailed information about the topic or item in a logical way.
Design	Plan and create a detailed specification or solution for a system, process, or product to meet defined requirements.

Develop	Identify, build and extend a topic, plan or idea.
Discuss	To examine or talk about a subject in detail, considering different opinions or perspectives.
Distinguish between	Discuss identified differences between more than one item, product, object or activity.
Empower	Equip or supply with an ability; enable or permit.
Enable	Supply with the means, knowledge, or opportunity; make able.
Establish (L5 and L6)	Set up on a permanent basis; get generally accepted; place beyond dispute.
Evaluate	Examine strengths and weaknesses, arguments for and against and/or similarities and differences; judge the evidence from the different perspectives and make a valid conclusion or reasoned judgement; apply current research or theories to support the evaluation when applicable.
Critically evaluate	To make a judgement about the value, validity or effectiveness. The additional word 'critically' includes analysis, reflection and evidence-based reasoning.
Evidence	To provide facts, data, or observations that support a claim, conclusion, or action.
Explain	Apply reasoning to account for how something is or to show understanding of underpinning concepts (responses could include examples to support the reasons).
Explore	Investigate, examine, or discuss a topic, concept, or system in detail to gain a deeper understanding.
Facilitate (L6)	Make easier; assist the progress of.
Formulate (L5, L6 and L7)	Draw together; set forth in a logical way; express in systematic terms or concepts.
Give constructive feedback	Provide commentary that serves to improve or advance; be helpful.
Identify	Ascertain the origin, nature, or definitive characteristics of.
Implement (L5 and L6)	Put into practical effect; carry out.
Initiate	Originate/start a process.
Intervene effectively	Change an outcome.
Investigate	Detailed examination or study; enquire systematically.

Justify	Give a comprehensive explanation of the reasons for actions and/or decisions.
Mentor	Serve as a trusted counsellor or teacher to another person; help others succeed.
Monitor	Maintain regular surveillance.
Negotiate	Discuss with a view to finding an agreed settlement.
Perform	To carry out a task, action, or function as required or specified.
Produce	To create or generate something, such as a document, report, or output, according to given specifications.
Recognise	Acknowledge the validity of.
Recommend	Revisit and judge the merit of; endorse a proposal or course of action; advocate in favour of.
Refine	To improve something by making small changes, making it more precise, effective, or elegant.
Reflect on	Consult with oneself, recognising implications of current practice with a view to changing future practice.
Represent views of	Act as an advocate; speak, plead or argue in favour of.
Research (L5 and L6)	A detailed study of a subject to discover new information or reach a new understanding.
Resolve	Solve; settle; explain.
Review	To examine a subject or process, issue or body of work, with the aim of summarising key points, highlighting strengths and weaknesses and making recommendations or judgements.
Critically review	Revise, debate and judge the merit of.
Review and revise	Revisit, judge the merit of and make recommendations for change.
Secure	Make safe; obtain (information or evidence).
Set objectives (L6)	Identify the outcomes required.
Signpost	Point the way; indicate.
Summarise	Select the main ideas, arguments or facts and present in a precise, concise way.
Support	Strengthen, support or encourage; corroborate; give greater credibility to.
Triangulate (L7)	Identify three aspects to ensure validity.

Work in partnership	Work in association with two or more individuals (this may include stakeholders, service users and/or carers).

Section 4: support

Support materials

The following support materials are available to assist with the delivery of this qualification and are available on the NCFE website:

- Qualification Factsheet.

Useful websites

Centres may find the following websites helpful for information, materials and resources to assist with the delivery of this qualification:

- The National Cyber Security Centre (ncsc.gov.uk)
- MITRE ATT&CK (attack.mitre.org)
- Cloud architecture center (cloud.google.com/architecture)
- NIST: Cyber security (nist.gov/cybersecurity)

These links are provided as sources of potentially useful information for delivery/learning of this subject area. NCFE does not explicitly endorse these websites or any learning resources available on these websites.

Other support materials

The resources and materials used in the delivery of this qualification must be age-appropriate and due consideration should be given to the wellbeing and safeguarding of learners in line with your institute's safeguarding policy when developing or selecting delivery materials.

Products to support the delivery of this qualification may be available. For more information about these resources and how to access them, please visit the NCFE website.

Reproduction of this document

Contact us

NCFE
Q6
Quorum Park
Benton Lane
Newcastle upon Tyne
NE12 8BT

Tel: 0191 239 8000*
Fax: 0191 239 8001
Email: customersupport@ncfe.org.uk
Website: www.ncfe.org.uk

Version 1.0 May 2026
Information in this Qualification Specification is correct at the time of publishing but may be subject to change.

NCFE is a registered charity (Registered Charity No. 1034808) and a company limited by guarantee (Company No. 2896700).

To continue to improve our levels of customer service, telephone calls may be recorded for training and quality purposes.

Appendix A: units

To simplify cross-referencing assessments and quality assurance, we have used a sequential numbering system in this document for each unit.


Knowledge-only units are indicated by a star. If a unit is not marked with a star, it is a skills unit or contains a mix of knowledge and skills.

Mandatory units

Unit number	Regulated unit number	Unit title	Level	Credit	GLH
Unit 01	R/651/6926	Cloud networking protocols, services and topologies	5	30	130
Unit 02	T/651/6927	Cyber security threats and risk management	5	20	90
Unit 03	Y/651/6928	Network performance, optimisation, and maintenance	5	20	90
Unit 04	A/651/6929	Change management and business continuity in network infrastructure	5	20	90
Unit 05	H/651/6930	Security compliance and legislation	5	15	70
Unit 06	J/651/6931	Secure system administration	5	15	70

The units above may be available as stand-alone unit programmes. Please visit the NCFE website for further information.

Change history record

Version	Publication date	Description of change
1.0	01 May 2026	First published version