# Sample Assessment Brief: holistic

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

**Unit 01 Cloud Networking Protocols, Services and Topologies (R/651/6926)**

**Unit 03 Network Performance, Optimisation, and Maintenance (Y/651/6928)**

**Unit 05 Security Compliance and Legislation (H/651/6930)**

**Unit 06 Secure System Administration (J/651/6931)**

| | |
|---|---|
| **Student name / ID number** | |
| **Unit number, title and learning outcomes (LOs)** | Unit 01 Cloud networking protocols, services and topologies (R/651/6926) (LO5)<br>Unit 03 Network performance, optimisation, and maintenance (Y/651/6928) (LO1, LO3)<br>Unit 05 Security compliance and legislation (H/651/6930) (LO2)<br>Unit 06 Secure system administration (J/651/6931) (LO1) |
| **Assignment title** | Cloud network implementation, optimisation, and security |

**Scenario**

You are a cloud network specialist working for CloudSecure Solutions, a consultancy firm that specialises in designing, deploying, and managing secure and efficient cloud networks for various clients. Your new client, GlobalTech Innovations, is expanding its operations and requires a new cloud-based network infrastructure to host a critical business application.

GlobalTech Innovations has provided you with the following high-level requirements:

- the application needs to be hosted on a public cloud platform (Azure or AWS)
- the network must be secure, scalable, and highly available
- all deployments must adhere to industry-recognised compliance frameworks (NIST CSF or ISO 27001)
- the client has reported occasional performance bottlenecks with their existing on-premises network, so network optimisation is a key concern
- they also require a robust troubleshooting approach for future issues.

**Task**

**Task 1**

You are required to design and implement a basic cloud network infrastructure for GlobalTech Innovations.

Create a network design document outlining the proposed cloud network architecture. This should include:

- chosen cloud platform (Azure or AWS)
- network topology (for example, hub-and-spoke, VPC / VNet with subnets)
- function and configuration of virtual switches, routers, gateways, and firewalls
- proposed secure connection technologies (for example, VPN Gateway, ExpressRoute / Direct Connect – conceptual if not implemented).

You should;

- describe the chosen cloud networking topology and technologies, and outline common methods for configuring network security, including proposed access control measures
- implement the network solution based on your design, using virtualised cloud network components and secure connection technologies
- explain how your specific network security configurations address identified security threats

- justify your design choices, explaining why this specific secure, scalable, and adaptable cloud network architecture is optimal for GlobalTech Innovations' business, compliance, and security requirements.
- evaluate the effectiveness of your integrated network security architecture.

**Implementation and configuration**

- implement the designed cloud network infrastructure on your chosen cloud platform
- configure virtual switches, routers, and firewalls
- apply initial access control measures (for example, network security groups, security groups) to secure key components
- provide screenshots and configuration details as evidence.

**Task 2**

GlobalTech Innovations is concerned about network performance and effective troubleshooting.

Using appropriate tools establish a baseline of network performance within your deployed cloud environment. To effectively establish a baseline, you are required to;

- apply at least two common optimisation techniques to improve the network's performance
- re-test network performance after applying optimisation technique
- describe key factors that affect cloud network performance and apply common optimisation techniques in your deployed scenario
- analyse the effectiveness of your selected optimisation techniques in improving system performance, providing evidence from your before-and-after tests.
- explain how root cause analysis techniques could be used in the future to help diagnose system performance issues.

**Troubleshooting scenario**

Your assessor will introduce a simulated network fault within your deployed cloud environment (for example, a misconfigured firewall rule blocking traffic, a routing issue).

You are required to apply a systematic troubleshooting methodology and use diagnostic tools to identify, isolate, and resolve the fault.

Document the troubleshooting steps taken, the tools used, the identified cause of the fault, and the resolution implemented. Ensure you apply systematic troubleshooting methodologies and diagnostic tools to identify, isolate, and resolve the network fault.

**Task 3**

GlobalTech Innovations requires their cloud environment to be compliant with industry standards. You are required select one industry-recognised compliance framework and produce a compliance alignment report that:

- describes at least three relevant controls from the chosen framework that are applicable to your deployed cloud network infrastructure
- describes how your implemented network design and security configurations (from task 1) align with these selected controls

- explains key features of your chosen industry-recognised compliance framework and its role in guiding secure cloud operations
- applies relevant controls from the industry-recognised compliance framework to meet defined security and compliance requirements within your deployed cloud network.

**Evidence requirements**

**Task 1:**

- Cloud network design document (report format).
- Screenshots and configuration output from your chosen cloud platform evidencing the deployed network infrastructure, virtual components, and initial security configurations.

**Task 2:**

- Performance analysis report (including baseline and post-optimisation performance data / graphs).
- Troubleshooting fault resolution report.
- Screenshots / command line output demonstrating tool usage during troubleshooting.

**Task 3:**

- Compliance alignment document (report format)

**Unit learning outcomes (LOs)**

- Unit 01: Cloud Networking Protocols, Services and Topologies (LO5)
- Unit 03: Network Performance, Optimisation, and Maintenance (LO1, LO3)
- Unit 05: Security Compliance and Legislation (LO2)
- Unit 06: Secure System Administration (LO1)

**Grading criteria**

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

| Learning outcomes (LOs) | Pass | Merit | Distinction |
|---|---|---|---|
| **Unit 01, LO5**: Explore network topologies and networking technologies and their ability to provide a secure, scalable, and efficient IT infrastructure | **P6**: **i**nterpret 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 |

**Unit 03 Network performance, optimisation, and maintenance (Y/651/6928) (LO1, LO3)**

| Learning outcomes (LOs) | Pass | Merit | Distinction |
|---|---|---|---|
| **Unit 03, 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 |
| **Unit 03, LO3**: Apply troubleshooting methodologies for network and IT infrastructure | **P3**: employ basic diagnostic tools to gather information regarding a reported network issue | **M3**: **a**pply 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 | |

**Unit 05 Security compliance and legislation (H/651/6930) (LO2)**

| Learning outcomes (LOs) | Pass | Merit | Distinction |
|---|---|---|---|
| **Unit 05, 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 | **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 |

**Unit 06 Secure system administration (J/651/6931) (LO1)**

| Learning outcomes (LOs) | Pass | Merit | Distinction |
|---|---|---|---|
| **Unit 06, 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 |