Sample Assessment Brief: full unit

NCFE Level 5 Diploma: Cloud Networking and Secure Networking
QN: 610/5971/7- full
Unit 02 Cybersecurity Threats and Risk Management **(T/651/6927)**

Student name / ID number	
Unit number, title and learning outcomes (LOs)	**Unit 02** Cybersecurity threats and risk management (T/651/6927) **LO1**: Explore how different cyber threats affect IT systems and infrastructure **LO2**: Evaluate human and organisational factors in cyber threats and actor behaviour **LO3**: Apply threat modelling and mitigation strategies to reduce organisational cyber risk
Assignment title	Cybersecurity strategy

Scenario

You are a cybersecurity consultant at a growing startup specialising in cloud-native application development. The organisation has experienced several concerning security events, including phishing attempts, suspicious activity logs, and a recent audit highlighting misconfigured cloud resources. They need a comprehensive cybersecurity strategy that addresses technical vulnerabilities, human factors, and ensures robust mitigation.

Tasks

Task 1

Conduct a detailed threat and vulnerability assessment of the organisation simulated cloud infrastructure (or a provided test environment that mimics a segment of it).

- as part of your assessment process, describe common cyber threats relevant to a cloud-native startup (misconfigurations, data breaches, insecure APIs, insider threats, phishing). Explain how these threats could impact IT systems and infrastructure and outline the tools you used for vulnerability detection during your assessment
- apply testing tools and techniques (cloud vulnerability scanners, configuration checkers, network reconnaissance tools) to identify vulnerabilities resulting from various cyber threats within the simulated environment. Document your methodology, findings, and provide evidence of the vulnerabilities identified.

Task 2

Based on a provided case study, you must produce an incident analysis report. In your report ensure that you;

- describe common threat actors that would target a company such as the case study organisation, outlining their motivations
- describe the human factors that contributed to the incident
- analyse the tactics, techniques, and procedures (TTPs) used by the threat actors in the case study
- analyse the influence of organisational factors on the organisation's security posture.

You are required to produce a threat modelling document including security configurations. Ensure that you;

- apply threat modelling to a critical component identified in the case study or your previous assessment
- identify, categorise, and prioritise threats to this component
- install basic security configurations on a simulated system or network component to mitigate common threats relevant to your threat model
- configure security elements and adapt system monitoring informed by your threat modelling to mitigate the identified organisational threats at an advanced level.

Ensure that you provide evidence of your configurations and adapted monitoring.

Task 3

Building upon your detailed assessments and analyses from task 1 and task 2, develop a cyber risk management plan for the organisation.

- your plan must identify, assess, and propose treatments for key cyber risks across their cloud infrastructure and operations. It should reflect your understanding of specific threats, human and organisational factors, and incorporate appropriate mitigation strategies.
- justify your cyber risk management plan, including the specific tools and configurations recommended. This justification should include why each component of the plan is necessary and effective in mitigating the identified risks.

Evidence requirements

Task 1:
- threat and vulnerability assessment report

Task 2:
- incident analysis report
- threat modelling document
- security configurations (logs, config files / commands)

Task 3:
- cyber risk management plan document
- justification report

Unit LOs

LO1: Explore how different cyber threats affect IT systems and infrastructure
LO2: Evaluate human and organisational factors in cyber threats and actor behaviour
LO3: Apply threat modelling and mitigation strategies to reduce organisational cyber risk

Grading criteria

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	