Cyber Security Engineer Sample Assessment Brief

NCFE Level 4 Diploma: Cyber Security Engineer
QN: 603/7748/3

Unit 05 Risk assessment in cyber security (J/651/0937)

Version 1.0 September 2024

Student name / ID number	
Unit number, title and learning outcomes (LOs)	**Unit 05** Risk assessment in cyber security (J/651/0937) **LO1**: Examine operating system security features **LO2**: Assess risk management in cyber security
Assignment title	Risk within cyber security

Scenario

You have recently joined a company as a cyber security intern. This small non-profit organisation provides support and advocacy for victims of domestic abuse. They rely heavily on donations and have a very limited IT budget.

Key details

Staff: five full-time employees and several volunteers. Some staff members are less tech-savvy than others.

Current systems: a mix of older laptops (Windows 7 Professional and Windows 10 Professional) and a donated server (running an outdated version of Windows Server).

Data: sensitive donor information (names, addresses, contact details, and sometimes financial information). Additionally, they store case notes with potentially identifying information about the people they help.

Operations: heavy reliance on email, web browsing for research and outreach, and basic office software. Volunteers sometimes use their personal devices to access the organisation's shared file storage.

Challenges

Tight budget: limited funds for new hardware or software.

Compliance: there is a concern about potential compliance issues with data protection regulations, as their practices are not very formalised.

Threats: the sensitive nature of their work makes them a potential target for cyber attacks aimed at disrupting services or stealing information.

Tasks

Task 1

Write a report describing the security features of Windows Professional (7 and 10). Ensure you recommend specific security features of the operating system for the company. You may consider including the use of third-party applications, such as antivirus software.

Task 2

You have been given access to a simulated environment mirroring your company network and systems. Conduct a risk assessment, paying close attention to vulnerabilities stemming from outdated operating systems, user practices (personal devices), and potential lack of security awareness. Create a prioritised mitigation plan with specific recommendations, keeping in mind the cost constraints.

Evidence requirements
You must provide: • a written report • risk assessment documentation, including a mitigation plan.
Unit learning outcomes (LOs)
LO1: Examine operating system security features LO2: Assess risk management in cyber security

Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
LO1: Examine operating system security features	**P1**: Describe fundamental security features offered by different operating systems	**M1**: Explain how the choice of operating system impacts an organisation's overall security posture	
LO2: Assess risk management in cyber security	**P2**: Define the scope of cyber security risk assessment and identify common risk assessment methodologies	**M2**: Explain how risk assessment documentation supports risk treatment decisions and suggest appropriate risk treatment options	**D1**: Design a comprehensive risk assessment plan, tailoring it to meet the requirements of a recognised cyber security standard
	P3: Apply a basic risk assessment process to identify security risks and vulnerabilities in a given scenario	**M3**: Apply a risk assessment process, analysing results and prioritising risks based on likelihood and impact	**D2**: Justify proactive risk treatment strategies, considering both technical and organisational countermeasures

Resources

Example vulnerabilities:

- outdated operating systems – Windows 7 and Windows Server 2010 R2 are no longer supported by Microsoft, making them highly vulnerable to known exploits
- personal devices (bring your own device) – unmanaged personal devices connecting to the network introduce risks of malware infection and unauthorised data access
- lack of security awareness – staff might be susceptible to phishing scams, poor password practices, or accidental data leaks.

Other common issues:

- unsecured Wi-Fi network
- lack of encryption on sensitive data
- poor incident response procedures.