Cyber Security Engineer Sample Assessment Brief

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

Unit 01 Principles of cyber security (Y/651/0932)

Unit 02 Cyber security architecture (D/651/0934)

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

Student name / ID number	
Unit number, title and learning outcomes (LOs)	**Unit 01** Principles of cyber security (Y/651/0932) **LO3**: Apply programming and scripting languages to design or end user requirements **Unit 02** Cyber security architecture (D/651/0934) **LO2**: Apply the characteristics of digital system components, implementing security controls **LO3**: Apply the concepts of cryptography **Unit 05** Risk assessment in cyber security (J/651/0937) **LO2**: Assess risk management in cyber security
Assignment title	System creation

Scenario

You work for a company who specialise in creating information communication technology (ICT) software solutions for small independent companies. You lead the Systems team, and it is your job to create bespoke secure systems for your clients. You have been approached to create a brand-new secure system for a company. They are a small company of 11 full-time staff who have recently had a data scare. They have already had a full security audit undertaken, and this has given a list of findings and recommendations that are urgently needed. Your job is to study the security audit and build a brand-new system for them that resolves the issues.

Tasks

Below you will find the list of issues found by the client's security audit. You are to research and implement new systems / procedures that will resolve these issues.

Issue 1

To help the company moving forward, design and create a custom tool that can perform a vulnerability scan of their network and identify any potential issues. You can use supporting libraries such as Nmap or versatile authentication server and service (VAS) to support the work. Ensure you evaluate the suitability of your code.

Issue 2

The audit gives a list of system components and their issues (see resources). Your job is to resolve the issues found for each of the components listed. For example, the firewall is not configured on their server, so you need to correctly configure it. Document and justify your decisions.

Issue 3

The audit found no evidence of cryptography to secure any data. This is an essential upgrade requirement. You need to evidence a secure way of sending data within this company; for example, creating a secure file transfer protocol. It must apply appropriate cryptographic algorithms and key management techniques. Consider industry-standard options and suitable libraries for implementation.

Note any security trade-offs made for further analysis.

Issue 4

Once issues 1 to 3 have been resolved, look at the security audit and identify any remaining risks that the company still face and evidence this in a risk assessment document.

Note: your solutions may create new risks. Ensure you include mitigation strategies as a final step to best secure the data from the company.

Include a justification for any risk treatment and mitigation strategies to be implemented by staff in the future.

Evidence requirements

For each issue, you should include:

Issue 1

- designs of a custom vulnerability tool
- packaged vulnerability tool
- a written evaluation of the suitability of the code including recommendations.

Issue 2

- system and security plan, including:
  - list of system components and their issues
  - list of fixes for all components
- a written justification of your fixes for the security components.

Issue 3

- evidence of secure data transfer system
- a written analysis of any trade-offs made between encryption algorithms and key management approaches.

Issue 4

- risk assessment documentation
- a written justification of your selected risk treatment strategies.

Unit learning outcomes (LOs)

Unit 01 Principles of cyber security (Y/651/0932)
LO3: Apply programming and scripting languages to design or end user requirements

Unit 02 Cyber security architecture (D/651/0934)
LO2: Apply the characteristics of digital system components, implementing security controls
LO3: Apply the concepts of cryptography

Unit 05 Risk assessment in cyber security (J/651/0937)
LO2: Assess risk management in cyber security

Grading criteria

Unit 01 Principles of cyber security (Y/651/0932)

Learning outcomes (LOs)	Pass	Merit	Distinction
LO3: Apply programming and scripting languages to design or end user requirements	**P4**: Produce a program code or script, taking into account end user requirements **P5**: Explain variations when producing clean and maintainable code	**M3**: Assess the suitability of the program code or script produced	**D2**: Evaluate the suitability of the program code or script in terms of suitability for the end user, making recommendations of suggested improvements

Unit 02 Cyber security architecture (D/651/0934)

Learning outcomes (LOs)	Pass	Merit	Distinction
LO2: Apply the characteristics of digital system components, implementing security controls	**P4**: Identify common digital system components (switches, routers, firewalls, servers) and their functions	**M2**: Propose a comprehensive security plan for a complex digital system	**D2**: Justify the selection of components and controls in a security plan
	P5: Design and test a system that incorporates appropriate security controls based on a given security case study	**M3**: Outline mitigation techniques for identified vulnerabilities	
LO3: Apply the concepts of cryptography	**P6**: Describe the principles of symmetric and asymmetric encryption and hashing	**M4**: Differentiate between various encryption algorithms in terms of strength and use cases	**D3**: Analyse security trade-offs between different encryption algorithms and key management approaches
	P7: Design a basic encryption scheme to protect data based on specific security requirements		
	P8: Develop a secure key management plan, including rotation, storage and archival strategies, addressing potential vulnerabilities		

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

Learning outcomes (LOs)	Pass	Merit	Distinction
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

Issue 2 examples could include:

- outdated software:
  - operating systems (Windows, Linux) running versions with known security patches missing
  - out-of-date web server, database, or other critical applications with published vulnerabilities
- configuration errors:
  - firewall disabled or rules too permissive (allowing risky traffic)
  - default passwords left unchanged on administrative interfaces
  - unnecessary services running, increasing the attack surface
- poor access controls:
  - excessive user permissions or lack of separation of duties
  - shared accounts or weak password practices.