Qualification Specification

ProQual Level 2 Award in Cyber Security Awareness for Critical Infrastructure

ProQual Level 2 Award in Cyber Security Awareness for Critical National Infrastructure

This qualification is part of ProQual's broad offer of qualifications in the Digital Technology Sector.

To find out more about other qualifications in this, or any other sector, or for our latest fees; check our Fees Schedule via the QR code below:

Scan Here

Contents

Introduction

The ProQual Level 2 Award in Cyber Security Awareness for Critical National Infrastructure provides a nationally recognised qualification for those currently working in, or who want to work in the Digital Technology sector.

The aims of this qualification are:

- To raise awareness and change behaviour to improve Cyber Security in for people working within Critical National Infrastructure.
- To gain awareness of the policies and key legislation that impact their role within the industry.

The awarding body for this qualification is ProQual AB. This qualification has been approved for delivery in England. The regulatory body for this qualification is Ofqual, and this qualification has been accredited onto the Regulated Qualification Framework (RQF) and has been published in Ofqual's Register of Qualifications.

Qualification Profile

Qualification Title:	ProQual Level 2 Award in Cyber Security Awareness for Critical National Infrastructure
Qualification Number:	610/0705/5
Level:	2
Total Qualification Time (TQT):	10 Hours 1 Credit
Guided Learning Hours (GLH):	8 Hours
Assessment:	Pass/Fail
	Internally assessed and verified by centre staff
	Externally quality assured by ProQual Verifiers
Qualification Start Date:	01/04/2022
Qualification Review Date:	03/06/2026
Next Review Due:	03/06/2029

Learner Profile

There are no formal academic entry requirements for this qualification. Centres should carry out their own assessment to establish candidate's existing knowledge and skills in order to develop the assessment plan.

Candidates must be aged at least 16 years old on the day that they are registered for this qualification. Centres are reminded that no assessment activity may take place until a candidate has been registered.

Qualification Structure

This qualification consists of **2 mandatory units.** Candidates must complete all mandatory units to complete this qualification.

Unit Number	Unit Title	Level	TQT	GLH
Mandatory Units – Candidates must complete **all** units in this group.				
J/650/2007	Understanding Cyber Security Risks for a Critical National Infrastructure	2	5	4
K/650/2008	Understanding the Effective Implementation of Cyber Security Policies for a Critical National Infrastructure	2	5	4

Centre Requirements

Centres must be approved to deliver this qualification. If your centre is not approved to deliver this qualification, please complete and submit the **ProQual Additional Qualification Approval Form.**

Materials produced by centres to support candidates should:

- Enable them to track their achievements as they progress through the learning outcomes and assessment criteria.
- Provide information on where ProQual's policies and procedures can be viewed.
- Provide a means of enabling Internal and External Quality Assurance staff to authenticate evidence.

Centres must have the appropriate equipment to enable candidates to carry out the practical requirements of this qualification.

Certification

Candidates who achieve the requirements for this qualification will be awarded:

- A certificate listing all units achieved, and
- A certificate giving the full qualification title:

ProQual Level 2 Award in Cyber Security Awareness for Critical National Infrastructure

Claiming certificates

Centres may claim certificates for candidates who have been registered with ProQual and who have successfully achieved the qualification. All certificates will be issued to the centre for successful candidates.

Unit certificates

If a candidate does not achieve all of the units required for a qualification, the centre may claim a unit certificate for the candidate which will list all of the units achieved.

Replacement certificates

If a replacement certificate is required a request must be made to ProQual in writing. Replacement certificates are labelled as such and are only provided when the claim has been authenticated. Refer to the Fee Schedule for details of charges for replacement.

Assessment Requirements

Each candidate is required to produce a portfolio of evidence which demonstrates their achievement of all learning outcomes and assessment criteria for each unit.

Evidence can include:

- Observation report by assessor.
- Assignments/projects/reports.
- Professional discussion.
- Witness testimony.
- Candidate product.
- Worksheets.
- Record of oral and written questioning.
- Recognition of Prior Learning.

Candidates must demonstrate the level of competence described in the units. Assessment is the process of measuring a candidate's skill, knowledge and understanding against the standards set in the qualification.

Centre staff assessing this qualification must be **occupationally competent** and qualified to make assessment decisions. Assessors who are suitably qualified may hold a qualification such as, but not limited to:

- ProQual Level 3 Certificate in Teaching, Training and Assessment.
- ProQual Level 3 Award in Education and Training.
- ProQual Level 3 Award in Assessing Competence in the Work Environment. *(Suitable for assessment taking place in a working environment only.)*
- ProQual Level 3 Award in Assessing Vocational Achievement. *(Suitable for assessment taking place in a simulated training environment only.)*

Candidate portfolios must be internally verified by centre staff who are **occupationally knowledgeable** and qualified to make quality assurance decisions. Internal verifiers who are suitably qualified may hold a qualification such as:

- ProQual Level 4 Award in the Internal QA of Assessment Processes and Practice.
- ProQual Level 4 Certificate in Leading the Internal QA of Assessment Processes and Practice.

Occupationally competent means capable of carrying out the full requirements contained within a unit. **Occupationally knowledgeable** means possessing relevant knowledge and understanding.

Enquiries, Appeals and Adjustments

Adjustments to standard assessment arrangements are made on the individual needs of candidates. ProQual's Reasonable Adjustments Policy and Special Consideration Policy sets out the steps to follow when implementing reasonable adjustments and special considerations and the service that ProQual provides for some of these arrangements.

Centres should contact ProQual for further information or queries about the contents of the policy.

All enquiries relating to assessment or other decisions should be dealt with by centres, with reference to ProQual's Enquiries and Appeals Procedures.

Units – Learning Outcomes and Assessment Criteria

Title:	Understanding Cyber Security Risks for a Critical National Infrastructure			Level:	2
Unit Number:	J/650/2007	TQT:	5	GLH:	4

Learning Outcomes *The learner will be able to:*		Assessment Criteria *The learner can:*	
1	Understand the principles of cyber security within a Critical National Infrastructure (CNI).	1.1	Identify the principles of cyber security for a Critical National Infrastructure environment.
		1.2	Identify the purpose of cyber security within a Critical National Infrastructure environment.
2	Understand the cyber threats to organisational and personal security.	2.1	Identify common types of cyber threat actors, including: • State-sponsored actors. • Cyber criminals. • Hackers or hacktivists. • Insider threats (intentional or unintentional).
		2.2	Describe common reasons why cyber-attacks occur, including: • Financial gain. • Political or ideological reasons. • Disruption or damage to services. • Personal challenge or recognition.

2	*Continued*	2.3	Identify common cyber-attack methods and indicators of suspicious activity, including: • Phishing and social engineering. • Malware (including ransomware). • Unauthorised access to systems or networks. • Physical access to devices.
		2.4	Identify common targets of cyber-attacks, including: • User accounts (including privileged access). • Sensitive or financial data. • Devices and storage media. • Systems and networks.
3	Understand how to identify cyber risks specific to their organisational role or business area.	3.1	Identify processes used to identify cyber risks to an organisation.
		3.2	Explain the importance of remaining cyber security aware in a Critical National Infrastructure environment.
		3.3	Describe processes used to ensure organisational cyber security.
4	Understand the principles of access control and management.	4.1	State the purpose of access control.
		4.2	Define the principles of access control.
5	Understand the importance of cyber incident response, disaster and business continuity.	5.1	Describe cyber incident response and why this is important to a Critical National Infrastructure environment.
		5.2	Describe disaster recovery and why this is important to a Critical National Infrastructure environment.
		5.3	Describe business continuity in a cyber context and its importance to a Critical National Infrastructure environment.
		5.4	Identify effective approaches to cyber incident response.

6	Understand the safe usage of social and professional networks within an organisation.	6.1	Identify and explain risks associated with social media use in a Critical National Infrastructure environment.
		6.2	Identify examples of negative social media and professional networking site use within a Critical National Infrastructure environment.
		6.3	Identify examples of positive social media and professional networking site use within a Critical National Infrastructure environment.
		6.4	Identify actions that can be taken to reduce the risk of exploitation via social media and professional networking sites.

Additional Assessment Information

This unit is **knowledge based.** This means that evidence is expected to take the form of candidate's written work and/or records of appropriate professional discussions.

Candidates are expected to demonstrate basic knowledge and understanding appropriate to Level 2. Responses should be clear, accurate, and expressed in the learner's own words.

Centres may use their own, centre devised, assignments to organise candidate evidence or may use their own portfolio templates.

Assessors may wish use to use a checklist or evidence matrix to organise and track the assessment outcomes that have been achieved, but these **do not,** in themselves, constitute evidence of achievement.

Title:	Understanding the Effective Implementation of Cyber Security Policies for a Critical National Infrastructure			**Level:**	2
Unit Number:	K/650/2008	**TQT:**	5	**GLH:**	4

Learning Outcomes *The learner will be able to:*		**Assessment Criteria** *The learner can:*	
1	Understand the legislation associated with information assurance and cyber security within an organisation.	1.1	Identify the key legislation relevant to cyber security in a Critical National Infrastructure environment.
		1.2	Explain the importance of effective cyber security policies to ensure compliance with key legislation.
2	Understand how to provide guidance and obtain resources to ensure an effective cyber awareness strategy.	2.1	Identify appropriate sources of guidance on cyber security policy.
		2.2	Identify sources of information to stay up to date with cyber security issues.
3	Know how to select and use appropriate security methods to safeguard systems and data.	3.1	Describe security methods that can be used to safeguard systems.
		3.2	Explain specific security methods that can be used to safeguard systems.
4	Understand the importance of cyber security policy compliance at all levels of an organisation.	4.1	Describe why organisations need an overall approach to cyber security.
		4.2	Identify the key elements of an effective cyber security policy.

5	Understand how to effectively report and mitigate against further cyber-attacks.	5.1	Describe the processes that should be taken following a cyber incident.
6	Understand how to ensure effective compliance with organisational acceptable use policies within area of responsibility.	6.1	Identify the key features of an acceptable usage policy to include: • Removeable media polices. • Home and mobile working.
		6.2	Explain how these polices are implemented effectively.

Additional Assessment Information

This unit is **knowledge based.** This means that evidence is expected to take the form of candidate's written work and/or records of appropriate professional discussions.

Candidates are expected to demonstrate basic knowledge and understanding appropriate to Level 2. Responses should be clear, accurate, and expressed in the learner's own words.

Centres may use their own, centre devised, assignments to organise candidate evidence or may use their own portfolio templates.

Assessors may wish use to use a checklist or evidence matrix to organise and track the assessment outcomes that have been achieved, but these **do not,** in themselves, constitute evidence of achievement.

Appendix One – Command Verb Definitions

The table below explains what is expected from each **command verb** used in an assessment objective. Not all verbs are used in this specification

Apply	Use existing knowledge or skills in a new or different context.
Analyse	Break a larger subject into smaller parts, examine them in detail and show how these parts are related to each other. This may be supported by reference to current research or theories.
Classify	Organise information according to specific criteria.
Compare	Examine subjects in detail, giving the similarities and differences.
Critically Compare	As with compare, but extended to include pros and cons of the subject. There may or may not be a conclusion or recommendation as appropriate.
Describe	Provide detailed, factual information about a subject.
Discuss	Give a detailed account of a subject, including a range of contrasting views and opinions.
Explain	As with describe, but extended to include causation and reasoning.
Identify	Select or ascertain appropriate information and details from a broader range of information or data.
Interpret	Use information or data to clarify or explain something.
Produce	Make or create something.
State	Give short, factual information about something.
Specify	State a fact or requirement clearly and in precise detail.

ProQual Awarding Body
ProQual House
Unit 1, Innovation Drive
Newport, Brough
HU15 2GX

Tel: 01430 423 822
enquiries@proqualab.com
www.proqualab.com