Qualification Specification

ProQual Level 2 Award in Cyber Security Awareness for Business

ProQual Level 2 Award in Cyber Security Awareness for Business

This qualification is part of ProQual's broad offer of qualifications in the Cyber Security and Intelligence 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 Business provides a nationally recognised qualification for individuals employed in all levels of an organisation across any sector in which ICT systems are used as part of the business. Topics include the principles of cyber security, threats to organisational security, safe ICT use and the importance of implementing cyber security policies

The aims of this qualification are:

- To develop knowledge and skills of individuals to enable them to support their organisations with cyber security.
- To increase awareness of the current issues in cyber security.
- To provide career progression opportunities for individuals interested in entering the cyber security 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 Business
Qualification Number:	601/8257/X
Level:	2
Total Qualification Time (TQT):	10
Guided Learning Hours (GLH):	8
Assessment:	Pass/Fail
	Internally assessed and verified by centre staff
	External quality assurance by ProQual verifiers
Qualification Start Date:	01/01/2016
Last Review Date	18/09/2024
Next Review Date:	18/09/2027

Learner Profile

There are no formal academic entry requirements for this qualification. Centres should perform an initial assessment of candidate's knowledge and skills to identify any gaps and to help determine the assessment plan.

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

Candidates who complete this qualification may progress onto higher level qualifications within the Cyber Security and Intelligence Suite.

Qualification Structure

This qualification consists of **two** mandatory unit/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.				
M/507/9765	Understanding the Cyber Security Risks to Business.	2	5	4
T/507/9766	Understanding the Effective Implementation of Cyber Security Policies for Business.	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 of Business

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 of the 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.
- ProQual Level 3 Award in Assessing Vocational Achievement.

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 to Business			Level:	2
Unit Number:	M/507/9765	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 an organisation.	1.1	Identify the principles of cyber security for a business environment.
		1.2	Describe the purpose of cyber security awareness within a business environment.
2	Understand the threats to organisational security.	2.1	Identify activities associated with cyber-crime.
		2.2	Explain how cyber espionage is relevant to organisational cyber security.
		2.3	Summarise the risk of terror attacks on own organisation's cyber assets.
		2.4	Identify the insider risk.
		2.5	Describe how potential customer activities can impact cyber security.
3	Understand how to identify cyber risks specific to own organisational role.	3.1	Identify processes used to identify cyber risks to an organisation.
		3.2	Explain the importance of remaining cyber security aware in business, including potential consequences for own organisation.
4	Understand the principles of access Management.	4.1	State the purpose of access management
		4.2	Identify the principles of access management.

5	Understand how to secure end points.	5.1	Define the meaning of the term "end point".
		5.2	Identify the end points relevant to own role.
6	Understand the security risks associated with WIFI zones.	6.1	Explain basic WiFi security concepts.
		6.2	Identify the security risks associated with WiFi.
		6.3	Identify actions that can can be taken to increase WiFi security within own organisation.
7	Understand the importance of cyber incident response and disaster recovery.	7.1	Define the term **cyber incident response**.
		7.2	Define the term **disaster recovery.**
		7.3	Identify effective approaches to cyber incident response.
		7.4	Identify effective approaches to disaster recovery.
8	Understand the safe usage of social media networks within an organisation.	8.1	Explain the risks associated with social media use in a business environment.
		8.2	Identify examples of negative social media use within a business environment.
		8.3	Identify examples of positive social media use within a business environment.
		8.4	Identify actions that can be taken to reduce the risk of exploitation via social media.

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.

Centres may use the appropriate ProQual Candidate Workbook, or their own, centre devised, assignments. Candidates must provide evidence that they have met **all** of the assessment criteria, although a single piece of evidence may be used to demonstrate achievement of multiple assessment criteria.

Title:	Understanding the Effective Implementation of Cyber Security Policies for Business			**Level:**	2
Unit Number:	T/507/9766	**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 business 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 for cyber security policy.
		2.2	Identify sources of information to ensure currency with cyber security issues.
3	Know how to select and use appropriate security methods to safeguard systems and data.	3.1	Identify security methods that can be used to safeguard systems.
		3.2	Explain how to apply security methods for specific threats.
4	Understand the importance of cyber security policy compliance at all levels of an organisation.	4.1	Explain the need for an organisational approach to cyber security.
		4.2	Identify the key content of an effective cyber security policy.
		4.3	Identify potential issues with non-compliance of cyber security policy at departmental and individual levels.

5	Understand how to effectively report and mitigate against further cyber attacks.	5.1	Identify key content required for a cyber incident report.
		5.2	Explain the processes that should be taken following a cyber incident.
		5.3	List the measures that should be taken to prevent further attacks of the same nature.
6	Understand the security risks associated with WIFI zones.	6.1	Identify the key features of a removable media policy.
		6.2	Summarise how effective removable media policies should be implemented.
7	Understand how to ensure the implementation secure use of ICT policy for home and mobile working.	7.1	Identify the key features of a home and mobile working policy.
		7.2	Summarise how effective home and mobile working policies should be implemented.

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.

Centres may use the appropriate ProQual Candidate Workbook, or their own, centre devised, assignments. Candidates must provide evidence that they have met **all** of the assessment criteria, although a single piece of evidence may be used to demonstrate achievement of multiple assessment criteria.

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