Qualification Specification

Level 2 Award in Cyber Security Awareness For Critical National Infrastructure

Contents

Introduction

This qualification is appropriate for individuals employed in all levels of an organisation across a critical national infrastructure 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 awarding organisation for this qualification is ProQual Awarding Body and the regulatory body is the Office of Qualifications and Examinations Regulation (Ofqual).

Entry Requirements

There are no formal entry requirements for this qualification. Centres should carry out an **initial assessment** of candidate skills and knowledge to identify any gaps and help plan the assessment.

Qualification Profile

Qualification title	**ProQual Level 2 Award in Cyber Security Awareness for Critical National Infrastructure**
Ofqual qualification number	610/0705/5
Level	2
Total Qualification Time	10 hours
Assessment	Pass or fail Internally assessed and verified by centre staff External quality assurance by ProQual verifiers
Qualification start date	1/4/2022
Qualification end date	

Qualification Structure

Candidates must complete the 2 Mandatory units.

J/650/2007	Understanding cyber security risks for a critical national infrastructure (5 GLH)
K/650/2008	Understanding the effective implementation of cyber security policies for a critical national infrastructure (5 GLH)

Centre Requirements

Centres must be approved to offer this qualification. If your centre is not approved please complete and submit form **ProQual Additional Qualification Approval Application**.

Staff
Staff delivering this qualification must be appropriately qualified and occupationally competent.

Assessors/Internal Quality Assurance
For each competence-based unit centres must be able to provide at least one assessor and one internal quality assurance verifier who are suitably qualified for the specific occupational area. Assessors and internal quality assurance verifiers for competence-based units or qualifications will normally need to hold appropriate assessor or verifier qualifications, such as:

- ProQual Level 3 Certificate in Teaching, Training and Assessing
- Level 3 Award in Assessing Competence in the Work Environment
- Level 3 Award in Assessing Vocationally Related Achievement
- Level 3 Certificate in Assessing Vocational Achievement
- Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practices
- Level 4 Certificate in Leading the Internal Quality Assurance of Assessment Processes and Practices

Support for Candidates

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

Assessment

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

Assessment guidance is included to assure consistency.

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

Evidence can include:

- assignments/projects/reports
- worksheets
- portfolio of evidence
- record of oral and/or written questioning

Learning outcomes set out what a candidate is expected to know, understand or be able to do.

Assessment criteria specify the standard a candidate must meet to show the learning outcome has been achieved.

Learning outcomes and assessment criteria for this qualification can be found from page 7 onwards.

Internal Quality Assurance

An internal quality assurance verifier confirms that assessment decisions made in centres are made by competent and qualified assessors, that they are the result of sound and fair assessment practice and that they are recorded accurately and appropriately.

Adjustments to Assessment

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.

Results Enquiries and Appeals

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

Certification

Candidates who demonstrate achievement of the qualification will be awarded 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 required number of credits for a qualification. All certificates will be issued to the centre for successful candidates.

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 certificates.

Learning Outcomes and Assessment Criteria

Unit J/650/2007
Understanding cyber security risks for a critical national infrastructure

Learning Outcome - The learner will:	Assessment Criterion - The learner can:
1. Understand the principles of Cyber Security within a critical national infrastructure.	1.1 Identify the principles of cyber security for a critical national infrastructure environment. 1.2 Identify the purpose of cyber security awareness within a critical national infrastructure environment.
2. Understand the cyber threats to organisational and personal security.	2.1 Identify the following current and emerging cyber threat actors, to include: - State-sponsored (APT) - Individual (lone actor) - Hackers and Hacktivists - Cyber Terrorist - Cyber Criminal / Organised Crime - Organisational (business) - Insiders (intentional and unintentional) 2.2 Summarise current and emerging cyber threat motivations and drivers, to include: - Supporting National Objectives - Financial Reward - Improve Personal Technical Skills - Support Political/Ideological Goals - Supporting Business Objectives 2.3 Summarise current and emerging cyber threat tactics, techniques and procedures, to include: - Social Engineering - Malicious Software (Malware) - Network Attack / Intrusion - Local Physical Access - Supply Chain Corruption 2.4 Identify current and emerging cyber threat targets within an organisational and personal setting, to include: - Administrator (privileged access) - Social / Professional Network accounts - Financial Accounts - Customer Credentials - User / Employee Accounts - Storage Devices and Removable Media - Internet (websites, web apps) - Network (includes WiFi, routers etc) - Communication Information Systems (CIS)

Learning Outcome - The learner will:	Assessment Criterion - The learner can:
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 Summarise 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 recovery and business continuity.	5.1 Define cyber incident response 5.2 Define disaster recovery 5.3 Define business continuity in a cyber context. 5.4 Identify effective approaches to cyber incident response.
6. Understanding 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 and professional networking site use within a critical national infrastructure environment. 6.3 Identify examples of positive social media use within a critical national infrastructure environment. 6.4 Identify actions that can be taken to reduce the risk of exploitation via social and professional networking sites.

Unit K/650/2008
Understanding the effective implementation of cyber security policies for a critical national infrastructure

Learning Outcome - The learner will:	Assessment Criterion - 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 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 Summarise security methods that can be used to safeguard systems. 3.2 Explain specific security methods to protect against cyber threats.
4. Understand the importance of cyber security policy compliance at all levels of an organisation.	4.1 Summarise the need for an organisational approach to cyber security. 4.2 Identify the key content of an effective cyber security policy. 4.3 Summarise the responsibilities for ensuring effective communication of cyber security information and policies within their area of responsibility. 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 Summarise the processes that should be taken following a cyber incident.
6. Understand how to ensure effective compliance with organisational acceptable usage policies within area of responsibility.	6.1 Identify the key features of an acceptable usage policy to include: - Removable media policies - Home and mobile working 6.2 Explain how these policies are implemented effectively.

Learning Outcome - The learner will:	Assessment Criterion - The learner can:
7. Understand how to identify cyber risks specific to their organisational role or business area.	7.1 Identify processes used to identify cyber risks to an organisation. 7.2 Explain the importance of remaining cyber security aware in business. 7.3 Summarise processes used to ensure organisational cyber security.
8. Understand the principles of access control and management.	8.1 State the purpose of access control. 8.2 Define the principles of access control.
9. Understand the importance of cyber incident response, disaster recovery and business continuity.	9.1 Define cyber incident response 9.2 Define disaster recovery 9.3 Define business continuity in a cyber context. 9.4 Identify effective approaches to cyber incident response.
10. Understanding the safe usage of social and professional networks within an organisation.	10.1 Identify and explain risks associated with social media use in a business environment. 10.2 Identify examples of negative social and professional networking site use within a business environment. 10.3 Identify examples of positive social media use within a business environment. 10.4 Identify actions that can be taken to reduce the risk of exploitation via social and professional networking sites.

Assessment

There must be valid, authentic and sufficient for all the assessment criteria. However, one piece of evidence may be used to meet the requirements of more than one learning outcome or assessment criterion.

www.proqualab.com

enquiries@proqualab.com

Tel: +44 (0)1430 423822

ProQual AB Limited, ProQual House, Unit 1, Innovation Drive, Newport HU15 2HG
Company Registration Number: 07464445