Qualification Specification

Level 3 Award in Dealing with a Cyber Attack or Data Breach

Contents

	Page
Introduction	3
Qualification profile	3
Centre requirements	5
Support for candidates	5
Assessment	6
Internal quality assurance	6
Adjustments to assessment	6
Results enquiries and appeals	7
Certification	7
Learning Outcomes and Assessment Criteria	8

Introduction

This qualification is aimed at senior managers of organisations with boardroom level responsibility. It is centred around a simulation exercise where delegates, working together as an imaginary Board, are drip-fed pieces of information that they will need to review and discuss before deciding upon an appropriate course of action. Topics include:

- The role of the Board in preventing cyber crime
- Dealing with an incident in real time
- Crisis management - critical thinking and decision-making
- Developing Pre and Post-incident Response Plans
- Embedding cyber security as a Boardroom issue

The Regulated Qualifications Framework (RQF) is the single framework for regulated qualifications, the regulatory body for this qualification is the Office of Qualifications and Examinations Regulation (Ofqual). This qualification has been accredited onto the RQF.

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 3 Award in Dealing with a Cyber Attack or Data Breach**
Ofqual qualification number	603/3700/X
Level	3
Total Qualification Time	25 hours (12 GLH)
Assessment	Pass or fail Internally assessed and verified by centre staff External quality assurance by ProQual verifiers
Qualification start date	15/10/2018
Qualification end date	

Qualification Structure

Candidates must complete two Mandatory units.

Unit Reference Number	Unit Title	Unit Level	GLH
H/617/2602	An introduction to cyber crime	3	6
M/617/2604	Dealing with a Cyber Attack or Data Breach	3	6

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 quality assurance verifier qualifications, such as:

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

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
- observation report by assessor

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 8 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 3 Award in Dealing with a Cyber Attack or Data Breach

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 H/617/2602
An introduction to cyber crime

Learning Outcome - The learner will:	Assessment Criterion - The learner can:
1 Understand the scale and scope of cyber crime in the UK	1.1 Explain what cyber crime and fraud are and how they affect UK businesses
	1.2 Identify key terminology and relevant legislation
	1.3 Explain why awareness of cyber crime and fraud is so important to the business they work in
2 Understand how and where their organisation is vulnerable to cyber crime and fraud	2.1 Identify the most common threats/areas of vulnerability and be able to explain how each one affects their business
	2.2 explain how their organisation may be put at risk of a cyber attack or breach by customers and suppliers
3 Understand what their role is as a senior decision-maker in preventing or reducing their vulnerability to cyber crime	3.1 Demonstrate the attributes and competencies of what makes a good cyber security leader
	3.2 Demonstrate how they can increase staff awareness of cyber crime and fraud within their organisation
	3.3 Explain how social media and other platforms can be used to promote good cyber security practice
4 Know how to implement technical and non-technical solutions to reduce their vulnerability to cyber crime and fraud	4.1 demonstrate knowledge of a wide range of preventative measures that protects their business, their suppliers and customers
	4.2 Explain the importance of having good cyber security policies in place
	4.3 Demonstrate how they can reduce their personal risk to cyber attack or breach
	4.4 Explain where they get reliable and trusted advice on cyber security
	4.5 Explain the benefits of good cyber security

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.

Unit M/617/2604
Dealing with a Cyber Attack or Data Breach

Learning Outcome - The learner will:	Assessment Criterion - The learner can:
1 Understand how their organisation may be compromised by a cyber attack or data breach	1.1 Recognise when an attack or breach has taken place
	1.2 Spot risk factors
2 Understand how decision-making models can support senior managers in dealing with an attack or breach	2.1 Make justifiable decisions based on a consistent decision-making framework
	2.2 Use information from a range of sources to support decision-making
	2.3 Demonstrate how to coordinate resources in responding to an attack or breach
	2.4 Demonstrate how they make justifiable decisions at a time of rapid change with a constant stream of information
3 Understand how to deal effectively with customers, suppliers and others, including internal/external governance bodies, regulators, the media and staff	3.1 Develop clear communications to keep people informed during a cyber attack or data breach
	3.2 Demonstrate how different communication channels can be used effectively to keep people informed
4 Know how to develop, implement and test a pre and post cyber incident response plan	4.1 Explain how an incident response plan works within their organisation, identifying roles and responsibilities and its fit with wider business continuity plans
	4.2 Explain how their organisation can regularly test their response plan

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, Westbridge Court, Annie Med Lane, South Cave HU15 2HG
Company Registration Number: 07464445