Qualification Specification

Level 4 Certificate in Cyber Security and Intrusion For Business

Contents

Introduction

This qualification builds on the fundamental principles of cyber security and is a natural progression for individuals working in an IT role, helping them to qualify as cyber security professionals. The qualification also provides a clear route of progression for individuals seeking to move from IT support roles, into better paid and more testing cyber security positions.

The awarding organisation for this qualification is ProQual Awarding Body and the regulatory body is the Office of Qualifications and Examinations Regulation (Ofqual). The specification for these qualifications has been approved by the Welsh Government for use by centres in Wales.

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 4 Certificate in Cyber Security and Intrusion for Business**
Ofqual qualification number	601/8167/9
Level	4
Total Qualification Time	70 hours
Assessment	Pass or fail Internally assessed and verified by centre staff External quality assurance by ProQual verifiers
Qualification start date	1/12/15
Qualification end date	

Qualification Structure

Candidates must complete the 3 Mandatory units.

T/507/9458 Cyber Security for Business Networks
A/507/9459 Managing Cyber Security in Business
M/507/9460 Cyber Intrusion for Business

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 verifier who are suitably qualified for the specific occupational area. Assessors and internal 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
- 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.

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
- candidate test papers

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 4 Certificate in Cyber Security and Intrusion for Business

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

T/507/9458 Cyber Security for Business Networks

Learning Outcomes – the learner will:		Assessment Criteria – the learner can:	
1.	Understand how to securely configure ICT systems	1.1	Explain the importance of securely configuring all ICT systems
		1.2	Explain the application of security patches
		1.3	Explain the purpose of a systems inventory
2.	Be able to securely configure ICT systems	2.1	Demonstrate the secure configuration of an ICT system
		2.2	Demonstrate the application of security patches
		2.3	Define a security baseline for all ICT devices
3.	Understand how to test and monitor network security	3.1	Explain the purpose of penetration testing
		3.2	Explain the processes involved in penetration testing
		3.3	Evaluate software that can be used for penetration testing
		3.4	Explain the purpose of a network perimeter
		3.5	Explain why security controls must be monitored and tested
4.	Be able to test and monitor organisational network security	4.1	Demonstrate penetration testing
		4.2	Identify network security issues through penetration testing
		4.3	Manage the network perimeter including wireless access
		4.4	Demonstrate the use of software setup related to malware and other monitoring products
		4.5	Analyse the monitoring and testing of security controls
5.	Understand the importance of compliance with organisational Malware Protection Policy	5.1	Explain the risks associated with a range of malware
		5.2	Evaluate a range of malware defences
		5.3	Explain the purpose of malware scanning
6.	Be able to demonstrate compliance with organisational Malware Protection Policy	6.1	Establish adequate malware defences
		6.2	Demonstrate malware scanning and secure backup of ICT systems

A/507/9459 Managing Cyber Security in Business

Learning Objectives – the learner will:		Assessment Criteria – the learner can:	
1.	Understand the requirement to determine the risks to an organisations information	1.1	Evaluate the need for an effective governance structure relating to cyber risk
		1.2	Explain a range of information risks
2.	Understand the use of account management processes	2.1	Explain the potential approaches to account management processes
		2.2	Explain control procedures relating to activity and audit logs
		2.3	Explain the importance of monitoring user activities
3.	Be able to demonstrate the use of account management processes	3.1	Demonstrate the use of account management processes
		3.2	Develop reports related to user privileges and accounts
		3.3	Demonstrate control procedure evidence related to activity and audit logs
		3.4	Monitor user activity, providing evidence and reports
4.	Understand the implementation of user security policies within organisations	4.1	Explain the importance of organisational level user security policies
		4.2	Identify examples of acceptable and secure use policies
		4.3	Explain why staff training is essential for effective cyber security policies
		4.4	Identify current back door cyber threats
5.	Be able to develop user security policies within organisations	5.1	Develop organisational level user security policies
		5.2	Determine the acceptable and secure use of organisational ICT systems
6.	Understand how to manage cyber incident response and disaster recovery	6.1	Explain potential disaster recovery activities
		6.2	Explain the requirement for incident management plans
		6.3	Describe the reporting process for criminal incidents
7.	Be able to manage cyber incident response and disaster recovery	7.1	Demonstrate an effective response to incidents and disaster recovery activities
8.	Understand how to monitor organisational ICT systems and networks	8.1	Explain the purpose of an ICT monitoring strategy
		8.2	Summarise the content of ICT security logs
		8.3	Explain how to secure ICT systems further to the indication of an attack

Learning Objectives – the learner will:		Assessment Criteria – the learner can:	
9.	Be able to monitor organisational ICT systems and networks	9.1	Determine an ICT Monitoring Strategy
		9.2	Develop an ICT Monitoring Policy
		9.3	Demonstrate the monitoring of ICT systems and networks
		9.4	Analyse security logs
		9.5	Secure all ICT systems further to the indication of an attack
10.	Be able to manage organisational Access to Removable Media Policy	10.1	Explain the necessity for an Access to Removable Media Policy
		10.2	Develop an Access to Removable Media Policy
11.	Understand how to manage organisational Secure Use of ICT Policy for Home and Mobile Working	11.1	Evaluate current government legislation and frameworks relevant to the control of digital data
		11.2	Identify the types of staff training events suitable for Home and Mobile Working policies.
		11.3	Explain how to apply a secure baseline build to all their organisation's ICT devices
12.	Be able to manage organisational Secure Use of ICT Policy for Home and Mobile Working	12.1	Develop a Secure Use of ICT Policy for Home and Mobile Working for all employees

M/507/9460 Cyber Intrusion for Business

Learning Outcomes – the learner will:		Assessment Criteria – the learner can:	
1.	Understand how to establish a security perimeter in a Wifi zone	1.1	Explain the use of hardware and software related to security in Wifi zones Identify current back door threats
		1.2	Explain the importance of mobile device policies for Wifi zones
		1.3	Explain how hardware and software can be utilised in relation to securing a Wifi
		1.4	perimeter
		1.5	Explain what rogue access points are
		1.6	Identify applications that are of high risk to a network area
2.	Know how to establish a security perimeter within a Wifi zone	2.1	Develop and demonstrate a mobile policy for Wifi zones
		2.2	Demonstrate the use of appropriate hardware and software in relation to securing a Wifi perimeter
		2.3	Provide an analysis of a Wifi zone
		2.4	Develop a policy on the detection of rogue access points and applications that are of risk to a network area
		2.5	Develop a policy to counter back door threats to networks
3.	Understand the regulatory frameworks associated with cyber intrusion	3.1	Identify regulatory frameworks associated with Wifi monitoring
		3.2	Explain the legislation relating to hacking or breaking into user networks
		3.3	Evaluate the problems that can be encountered when monitoring Wifi zones
		3.4	Explain the risk associated with managing Wifi zones within an International context
4.	Be able to analyse activities within Wifi zones	4.1	Analyse potential problems that could be encountered when monitoring Wifi zones

	Learning Objectives – the learner will:		Assessment Criteria – the learner can:
5.	Know how to utilise technology to secure networks from hacking	5.1	Explain the use of VPN functionality and application tunnelling to promote security
		5.2	Critically evaluate at least three commercial products that are available to secure LAN and other mobile networks
		5.3	Explain encryption methods such as TLS/SSL
		5.4	Explain the features of account lock out
		5.5	Explain host isolation in relation to Wifi networks
		5.6	Explain network separation in relation to Wifi networks
		5.7	Explain what a man in the middle attack is and how it affects network users
		5.8	Explain how to establish secure passwords
6.	Be able to utilise technology to secure networks from hacking	6.1	Use VPN functionality and application tunnelling to promote security
		6.2	Secure a LAN using commercially available products
		6.3	Demonstrate the use of encryption methods such as TSL/SSL
		6.4	Demonstrate account lock out and show how to enable and secure this setting
		6.5	Establish secure passwords for network users

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.

ProQual Awarding Body
ProQual House
Annie Med Lane
South Cave
HU15 2HG
UK

Tel: +44(0)1430 423822

www.proqualab.com

enquiries@proqualab.com