Qualification Specification

QNUK Level 5 Certificate in Security Management (RQF)

603/7313/1

Developed in collaboration with:

Contents

1. Introduction

Qualifications Network Limited (QNUK) is an Awarding Organisation recognised and regulated by the Office of Qualifications and Examinations (Ofqual) in England, the Council for Curriculum, Examinations and Assessment (CCEA) in Northern Ireland and Qualifications Wales.

This specification outlines key information required by users of the qualification to ensure they can make an informed decision about the suitability of the qualification they are taking or proposing to take for the purposes that they intend to use it.

2. Contact Us

Please get in touch if you need any advice or guidance with this qualification.

Head Office:

Qualifications Network
First Floor Offices
86A Lancaster Road
Enfield
Middlesex
EN2 0BX

Email: centres@qnuk.org
Tel: 020 3795 0559

3. Version Number

Centres should make sure they are using the most up to date document by checking the footer which will confirm the current version number.

Document owner	Qualifications Manager
Date last updated	24/03/2021
Next review	25/03/2024
Status	Final
Version	1
Document control number	QS|L5SM

4. Qualification Objective

This qualification is developed for individuals working in the Private Security Sector, particularly those intending to provide security management functions within a business. The qualification aims to develop an understanding of approaches to security management, considering current and emerging threats, risk mitigation, convergence and the role of security management during an incident. Learners will also develop an awareness programme on security management for managers and staff. This qualification will support a role in the workplace.

5. Sector Support and Industry Recognition

This qualification has been developed in collaboration with ASTA, CTR Secure Services in partnership with iSMTA.

6. Geographical Coverage of this Qualification

This qualification is available in England.

7. Benefit for Learners

This qualification develops learner's knowledge and understanding of security management in light of current and emerging criminal and terrorist threats to business. Research skills are developed allowing the learner to explore a range of security management concepts including business continuity management, security investigations and IT forensics, risk mitigation, convergence and incident management. Learners will develop communication skills through developing and delivering a security management awareness programme to managers and staff. This qualification develops transferrable skills that will support the Security Manager in the workplace.

8. Progression

This qualification is primarily for progression within the workplace, learners could progress to:

- Employment as a Security Manager or similar roles
- Higher education courses in Management, Security Management, Risk and Security Management and similar

9. Recognition of Prior Learning

QNUK are unable to accept requests for recognition of prior learning (RPL) for this qualification.

10. Qualification Information

Qualification Number (QN)	603/7313/1
Learning Aim	
Total Qualification Time (TQT)	168
Guided Learning Hours (GLH)	22
Credit value	17
Level	5
Validity	Lifetime
Assessment	Portfolio of evidence

Achieving the qualification	Learners must achieve the 7 mandatory units

11. Qualification Structure

Unit No.	Unit Title	Level	GLH	TUT	Credit
Mandatory units					
L/618/6817	Security for Business	5	2	12	1
R/618/6818	Traditional and Emerging Security Threats	5	4	30	3
R/618/6821	Understanding Security Management	5	6	45	5
H/618/6824	Security Management and Risk Mitigation	5	4	30	3
M/618/6826	Security Management and Convergence	5	2	13	1
T/618/6827	Security's Role in Incident Management	5	2	15	2
A/618/6828	Creating a Security Management Programme	5	2	18	2

The learning outcomes for the qualification may be found in Appendix 1. The Assessment Guidance details the assessment criteria which are used to determine if a learner has met the requirements of the learning outcomes. Further depth of coverage is also provided in the Assessment Guidance.

12. Learner Entry Requirements

There are no specific recommended prior learning requirements for this qualification. Entry is at the discretion of the centre, however, learners should be aged 18 years and over to take this qualification.

It is the centre's responsibility to ensure that each learner is sufficiently competent in the use of the English language. All assessments must be conducted in English. Centres must ensure that learners have sufficient language skills before putting the learners forward for assessment.

As a guide, learners should as a minimum have language skills equivalent to the following:

- a C1 level qualification on the Home Office's list of recognised English tests and qualifications
- an ESOL qualification at (Level 2) on the Ofqual register taken in England, Wales or Northern Ireland
- an ESOL qualification at Scottish Credit and Qualifications Framework level 6 awarded by the Scottish Qualifications Authority (SQA) and taken in Scotland
- Functional Skills Level 2 in English
- SQA Core Skills in Communication at Scottish Credit and Qualifications Framework level 6

Learners must have a basic understanding of ICT to fully engage with this qualification.

There are no other pre-requisites for this qualification. However, learners should be able to work at level 3 and above.

13. Delivery

This qualification is delivered in a face-to-face setting over a 5-day period. Learners should complete the qualification within 12 months of the date of enrolment on the qualification. All learners must be registered with QNUK as soon as possible following enrolment.

13.1. Venue Requirements

The training venue should be suitable for learning and meet all relevant Health and Safety requirements.

13.2. Blended Learning

Blended learning is acceptable for this qualification provided suitable controls are in place to ensure learners complete all elements. The qualification may be delivered via e-learning, through a virtual classroom or traditional face-to-face settings.

13.3. Trainer to Learner Ratio

The maximum Trainer to learner ratio for this qualification is 1:20

14. Centre Personnel Requirements

This qualification is delivered by suitably qualified trainers.

All those who deliver and assess this qualification must:

1. Minimum 5 years out of the last 10 years working in a Security Management, Risk Management, Business Continuity roles or similar;
2. Minimum level 5 occupational qualification, such as Level 5 Security Management or higher level qualifications such as Security Management, Risk and Security Management, Business Continuity or similar;
3. Hold a recognised teaching qualification as outlined in our centre resource manual;
4. Show current evidence of continuing professional development in teaching, assessment and the subject matter.

Internal Quality Assurance Requirements

Each centre must have access to a suitably qualified IQA. The IQA cannot verify the delivery or assessment of individual learners or cohorts of learners where the IQA has been involved in the delivery or assessment of the qualification for those learners.

All those who are involved with the quality assurance of these qualifications **internally** must:

1. have up-to-date working knowledge and experience of best practice in assessment and quality assurance;
2. meet the delivery staff requirements for this qualification;
3. hold, or be working towards a recognised qualification related to the Internal Quality Assurance of Assessment;
4. show current evidence of continuing professional development in assessment, quality assurance and the subject matter.

Please note whilst centre personnel may be approved for both roles, those assigned the role of Trainer/Internal Verifier are not permitted to operate in both these roles for any learner.

15. Assessment Requirements

Learners are assessed for this qualification through:

15.1. Portfolio of evidence

Learners are assessed for this qualification using a portfolio of evidence. The portfolio can include a range of assessment methods including:

- Assignments
- Record of professional discussions
- Observation of practical tasks/activities
- Product of work

Language of assessment	English
Duration	As required
Pass mark	100%
Grading	Pass/Fail

16. Moderation

The level of external moderation required for this qualification will be risk based and in line with the Centre Assessment Standards Scrutiny Strategy applicable to this qualification.

There may be situations within the centre devised assessment methodology that require observations, in these situations QNUK EQA Department will also require to conduct verification visits to ensure the accuracy and consistency of assessment decisions.

QNUK EQA Department will advise the centre of the required levels of moderation/verification to anticipate for this qualification upon centre approval for delivery.

17. Resits

As this qualification is evidence based, resits are not required; however, appropriate referral of submitted work from the learner may be used where additional detail or depth of knowledge is required.

18. Reasonable Adjustments

Learners are required to complete the assessments in a manner appropriate to the purpose of the qualification.

The prescribed assessment methods for this qualification should not unfairly disadvantage learners who would otherwise be able to demonstrate competence in line with the purpose of the qualification. Learners should contact their centre to discuss reasonable adjustment if they feel the prescribed assessment methods would disadvantage them.

19. Results

The centre is required to submit learner results within 10 working days of assessment to Qualifications Network UK for moderation. We will issue verified results and appropriate certification to the approved centre within 7 working days of receiving the results. Centres will forward results and/or certificates to learners, who can expect to receive them within 20 working days of taking the assessment. If learners have not received results and/or certificates within 25 working days, they should contact the centre in the first instance.

Appendix 1: Units

Unit 1 Security for Business (X/XXX/XXXX)

Unit Summary

This unit develops understanding of how security management can help protect the business or client's needs. Learners will develop a security management strategy that supports business or client's priorities, budget and culture and encourages growth and profit. Learners will conduct secondary research to gather information to complete the security strategy.

1. The learner will: Know how to protect the business or client's strategy		
Assessment Guidance The learner must:		**Types of Evidence**
1.1	Evaluate how security management needs are met by a strategy that fully supports the business or client's requirements	Assignment

What needs to be learnt?	
1.1	Security management needs in an organisation How to develop an effective security strategy that aligns to business or client needs How to design security measures that meet business or client priorities, budget and culture How to design security measures that encourage growth and profit How to ensure employees support security measures

Rationale for level			
	Level	**Emphasis**	**Comments**
Knowledge	5	Strong	Learners may have a practical and technical understanding of the field of security management, probably based on workplace experience. Learners will interpret and evaluate relevant information gathered through secondary research to develop a security strategy that meets business/client requirements and encourages profit and growth.
Skills	5	Strong	Learners will use their research findings and evaluation of how the developed security strategy meets business needs to communicate the strategy to employees to ensure their support.
Overall	5		

Rationale for TUT and credit			
	Hours	**Comments**	
Guided learning	**2**	Learners may have a practical and technical understanding of the field of security management. The GLH provides time for deliverers to introduce the unit and outline the theme of security management meeting the needs of business.	
Directed study	2	Building on classroom delivery, learners will undertake directed study as they work through the requirements of the unit.	
Independent study	8	Learners are expected to undertake secondary research to explore the topic of security management and gather the relevant information to support their evaluation of how security management needs are met through a strategy that fully supports the business or client's requirements.	
Work-based learning	N/A		
Non invigilated assessment	N/A		
TUT:	**12**	**Credit:**	**1**

Unit 2 Traditional and Emerging Security Threats (X/XXX/XXXX)

Unit Summary

This unit develops understanding of traditional threats to a business or client and supports understanding of emerging trends in security threats. Learners will conduct secondary research into current and emerging criminal and terrorist threats to complete the assignment.

1. The learner will: Understand the traditional threats to a business or client		
Assessment Guidance The learner must:		**Types of Evidence**
1.1	Evaluate the traditional threats facing a Security Manager	Assignment

2. The learner will: Understand the security threats of tomorrow and emerging trends		
Assessment Guidance The learner must		**Types of Evidence**
2.1	Critically analyse emerging criminal and terrorist threats potentially harmful to business interests, reputation and physical wellbeing	Assignment

What needs to be learnt?	
1.1	Traditional threats: • who commits such crimes? • how they do it • why they do it • when they do it Threat analysis Methods of protection against threats
2.1	Emerging criminal and terrorist trends of tomorrow and how to prepare for them How to maintain awareness of emerging trends that may affect and potentially threaten your client

Rationale for level			
	Level	**Emphasis**	**Comments**
Knowledge	5	Strong	Learners will have a practical and technical understanding of the field of security management, probably based on workplace experience. Learners will interpret and evaluate relevant information gathered through secondary research on traditional and emerging threats to businesses and how to protect against them.
Skills	5	Strong	Learners will use relevant research to identify criminal and terrorist threats and apply their findings to various ways to protect their businesses or clients. Building on the research, learners will develop their own methodologies for maintaining awareness of criminal and terrorist risks to businesses.
Overall	5		

Rationale for TUT and credit			
	Hours	**Comments**	
Guided learning	**4**	Learners may have a practical and technical understanding of the field of security management. The GLH provides time for deliverers to introduce the unit and outline the theme of criminal and terrorist threats that can affect businesses today.	
Directed study	6	Building on classroom delivery, learners will undertake directed study as they work through the requirements of the unit.	
Independent study	20	Learners are expected to undertake secondary research to explore the topic of criminal and terrorist threats and gather the relevant information to support their evaluation of threats security management face and analysis of emerging threats that are harmful to businesses today.	
Work-based learning	N/A		
Non invigilated assessment	N/A		
TUT:	**30**	**Credit:**	**3**

Unit 3 Understanding Security Management (X/XXX/XXXX)

Unit Summary

This unit develops knowledge and understanding of the value and effectiveness of security functions that apply to Data Centre protection, Business Continuity Management, security investigations and IT forensics. Learners will conduct secondary research into Data Centre security functions, Business Continuity Management and security investigations and IT forensics to complete the assignment.

1. The learner will: Know the value and effectiveness of security functions that apply to Data Centre protection		
Assessment Guidance The learner must:		**Types of Evidence**
1.1	Evaluate the value and effectiveness of the Information Protection Specialist as part of your security task force support to the Data Centre work force	Assignment

2. The learner will: Know the value and effectiveness of Business Continuity Management		
Assessment Guidance The learner must:		**Types of Evidence**
2.1	Critically analyse the effectiveness of Business Continuity Management in supporting the resilience of a business	Assignment

3. The learner will: Know the value and effectiveness of modern Security Investigations and IT Forensics		
Assessment Guidance The learner must:		**Types of Evidence**
3.1	Evaluate the value and effectiveness of Security Investigations and IT Forensics within the Data Centre workforce	Assignment

What needs to be learnt?	
1.1	• Physical Security protection • Information Protection • Difference between Data and Information Protection • Cyber Security • Connection between IT and Cyber Security • Main value and effectiveness of Physical Security, Information Protection and Cyber Security • Strengths and weakness of Physical Security, Information Protection and Cyber Security
2.1	• Business Continuity • Business Resilience • Crisis Management • Main value and effectiveness of Business Continuity, Resilience and Crisis Management • Strengths and weaknesses of Business Continuity, Resilience and Crisis Management
3.1	• Fraud Prevention • Security Investigations • IT Forensic Investigations • Main value and effectiveness of Fraud Prevention, Investigations and IT Forensic Investigations • Strengths and weaknesses of Fraud Prevention, Investigations and IT Forensic Investigations

Rationale for level			
	Level	**Emphasis**	**Comments**
Knowledge	5	Strong	Learners will have a practical and technical understanding of the field of security management, probably based on workplace experience. Learners will interpret and evaluate relevant information gathered through secondary research on Data Centre security functions, Business Continuity Management and Security Investigations and IT forensics
Skills	5	Strong	Learners will use relevant research to build their knowledge of Data Centre security functions, Business Continuity Management, Security Investigations and IT Forensics and develop skills in evaluating the value and effectiveness of each in supporting effective security management in a business.
Overall	5		

Rationale for TUT and credit			
	Hours	**Comments**	
Guided learning	**6**	Learners may have a practical and technical understanding of the field of security management. The GLH provides time for deliverers to introduce the unit and outline the topics of Data Centre security functions, Business Continuity Management and Security Investigations and IT forensics that can affect businesses today.	
Directed study	8	Building on classroom delivery, learners will undertake directed study as they work through the requirements of the unit.	
Independent study	36	Learners are expected to undertake secondary research to explore the topic of security management in general and gather the relevant information to support their evaluation and analysis of Data Centre security functions, Business Continuity Management and Security Investigations and IT forensics that can affect businesses today.	
Work-based learning	N/A		
Non invigilated assessment	N/A		
TUT:	**50**	**Credit:**	**5**

Unit 4 Security Management and Risk Mitigation (X/XXX/XXXX)

Unit Summary

This unit develops understanding of the methodology required to produce a security risk assessment and learners will develop their knowledge of how to design out or reduce crime through effective security management. Learners will conduct secondary research into security risk assessments and designing out crime through security management.

1. The learner will: Understand the methodology of producing a security risk assessment		
Assessment Guidance The learner must:		**Types of Evidence**
1.1	Evaluate the methodology and processes used when designing a security management risk assessment within a business environment	Assignment

2. The learner will: Know how to design out or reduce crime through effective security management		
Assessment Guidance The learner must:		**Types of Evidence**
2.1	Critically analyse different ways to design out or reduce crime within a business through the use of a range of security measures	Assignment

What needs to be learnt?	
1.1	• Reasons and methods for recording crime and crime analysis • Recording of crimes, damage and impact • Effective Security Risk Assessment • Importance of a Security Risk Register • How Security Management uses the Risk Register to implement risk reduction • How security measures combine in layers to reduce risk • Communication and use of Security Risk Assessment results
2.1	• Approaches to designing out crime for a variety of common scenarios • Using crime prevention techniques as a proactive approach • Using crime prevention as a reactive approach • How Security Management enables other security functions to work together

Rationale for level			
	Level	**Emphasis**	**Comments**
Knowledge	5	Strong	Learners will have a practical and technical understanding of the field of security management, probably based on workplace experience. Learners will interpret and evaluate relevant information gathered through secondary research on security risk assessment methodologies and designing out or reducing crime through effective security management.
Skills	5	Strong	Learners will evaluate their research of security risk assessment methodologies and designing out or reducing crime through effective security management and demonstrate how this may be achieved.
Overall	5		

Rationale for TUT and credit			
	Hours	**Comments**	
Guided learning	**4**	Learners may have a practical and technical understanding of the field of security management. The GLH provides time for deliverers to introduce the unit and outline the topic of risk assessment and risk mitigation that are necessary in businesses today.	
Directed study	6	Building on classroom delivery, learners will undertake directed study as they work through the requirements of the unit.	
Independent study	20	Learners are expected to undertake secondary research to explore the topic of risk assessment and risk mitigation and gather the relevant information to support their evaluation and analysis of risk assessment methodologies and processes and ways to design out or reduce crime through effective security management.	
Work-based learning	N/A		
Non invigilated assessment	N/A		
TUT:	**30**	**Credit:**	**3**

Unit 5 Security Management and Convergence (X/XXX/XXXX)

Unit Summary

This unit develops understanding of how security management adds value when converged with other security functions across the business. Learners will conduct secondary research into the range of security functions that are available to businesses.

1. The learner will: Understand how Security Management adds value when converged with other security functions across the business		
Assessment Guidance The learner must:		**Types of Evidence**
1.1	Evaluate how Security Management and other security functions work together to add value to the business	Assignment

What needs to be learnt?	
1.1	• How other security functions need to be converged to mitigate against convergent threats • Role of Security Management in converging security functions • Best Practice Security Standards for business and how convergence of security functions is necessary to achieve it • Different ways to achieve security function convergence • Business functions that relate directly to security functions • Business functions that indirectly relate to security functions

Rationale for level			
	Level	**Emphasis**	**Comments**
Knowledge	5	Strong	Learners will have a practical and technical understanding of the field of security management, probably based on workplace experience. Learners will interpret and evaluate relevant information gathered through secondary research on security threats and different ways to achieve security convergence.
Skills	5	Strong	Learners will evaluate their research of convergent security threats and will use this information to show how different security functions can be converged into an overarching security management strategy for the business.
Overall	5		

Rationale for TUT and credit			
	Hours	**Comments**	
Guided learning	**2**	Learners may have a practical and technical understanding of the field of security management. The GLH provides time for deliverers to introduce the unit and outline the topic of convergence of security functions that are necessary in businesses today.	
Directed study	1	Building on classroom delivery, learners will undertake directed study as they work through the requirements of the unit.	
Independent study	10	Learners are expected to undertake secondary research to explore the topic of convergence of security functions and gather the relevant information to support their evaluation and analysis of how this supports a business or client's security strategy.	
Work-based learning	N/A		
Non invigilated assessment	N/A		
TUT:	**13**	**Credit:**	**1**

Unit 6 Security's Role in Incident Management (X/XXX/XXXX)

Unit Summary

This unit develops understanding of how security management works as part of an Incident Management Team, and the role of the Security Manager in managing incidents. Learners will conduct secondary research into the incident management and the role of security during an incident.

1. The learner will: Understand how Security Management works as part of an Incident Management Team		
Assessment Guidance The learner must:		**Types of Evidence**
1.1	Evaluate the role of the Security Manager in managing incidents	Assignment

What needs to be learnt?	
1.1	• How security is designed to prevent and detect criminal activity • Definition of 'crisis' • Types of incidents that impact on security within a business • How to manage an incident • Role of security when incidents and situations escalate to crisis • Security actions in a crisis • Organising and managing executive protection • Organising, implementing and managing employee protection • Changes to business practices after an incident • Incident 'aftercare' • Role of centralised security control rooms • Use of alarm receiving centres

Rationale for level			
	Level	**Emphasis**	**Comments**
Knowledge	5	Strong	Learners will have a practical and technical understanding of the field of security management, probably based on workplace experience. Learners will interpret and evaluate relevant information gathered through secondary research on incident management and actions businesses take post incident.
Skills	5	Strong	Learners will evaluate their research of incident management and will use this information to show security management plays a key role during a security incident and how it can support the business to resume their normal operations afterwards, with or without changes to normal business practice.
Overall	5		

Rationale for TUT and credit			
	Hours	**Comments**	
Guided learning	**2**	Learners may have a practical and technical understanding of the field of security management. The GLH provides time for deliverers to introduce the unit and outline the topic of incident management that should be considered by all businesses.	
Directed study	3	Building on classroom delivery, learners will undertake directed study as they work through the requirements of the unit.	
Independent study	10	Learners are expected to undertake secondary research to explore incident management and gather the relevant information to support their evaluation of Security Management's role during an incident.	
Work-based learning			
Non invigilated assessment			
TUT:	**15**	**Credit:**	**2**

Unit 7 Creating a Security Management Programme (X/XXX/XXXX)

Unit Summary

Learners will develop a security awareness programme for managers and staff, drawing on secondary research to understand relevant legislation, current threats and changes in security, technology, society, economy and crime and terrorist threats that businesses may face.

1. The learner will: Understand how to develop a security awareness programme for managers and staff		
Assessment Guidance The learner must:		**Types of Evidence**
1.1	Evaluate ways of achieving an accepted security approach within a corporate culture	Assignment
1.2	Produce a Security Management awareness programme to be delivered to managers and staff	Awareness Programme

What needs to be learnt?	
1.1	• Current ways and methods for security management to meet current and emerging threats • Changing trends within security • How security changes following the development of technology, society, economy and crime methods • Current legislation, including potential changes to legislation anticipated in coming months • Importance of security convergence to mitigate current and emerging threats • Which business security related functions should be part of a converged security approach? • Methods and techniques for training / raising awareness of security to managers and staff • Current business language and terminology
1.2	Key information to be included in an awareness programme to deliver key security management message

Rationale for level			
	Level	**Emphasis**	**Comments**
Knowledge	5	Strong	Learners will have a practical and technical understanding of the field of security management, probably based on workplace experience. Learners will interpret and evaluate relevant information including legislation, current threats and changes in security, technology, society, economy and crime and terrorist threats that businesses may face when creating the awareness programme.
Skills	5	Strong	Learners will evaluate their research of legislation, current threats and changes in security, technology, society, economy and crime and terrorist threats that businesses may face and will create an awareness programme to support managers and staff.
Overall	5		

Rationale for TUT and credit			
	Hours	**Comments**	
Guided learning	**4**	Learners may have a practical and technical understanding of the field of security management. The GLH provides time for deliverers to introduce the unit and outline the topic producing and delivering an awareness programme to managers and staff. The remaining GLH should be available to participate in the learner's security management awareness programme.	
Directed study	4	Building on classroom delivery, learners will undertake directed study as they work through the requirements of the unit.	
Independent study	10	Learners are expected to undertake secondary research to explore incident management and gather the relevant information to support their evaluation of Security Management's role during an incident.	
Work-based learning	N/A		
Non invigilated assessment	N/A		
TUT:	**18**	**Credit:**	**2**

Appendix 2: Command Verbs

To ensure that learners can meet the requirements of each criterion, they should be explained to the learner prior to assessment and fully understood by the Assessor for this qualification.	
Critically analyse	This is a development of 'analyse' which explores limitations as well as positive aspects of the main ideas in order to form a reasoned opinion
Evaluate	Review evidence from different perspectives and come to a valid conclusion or reasoned judgement
Produce	Carry out or do; take an action; follow an instruction