Protective Security Advisers

SFJ Awards Level 4 Certificate for Protective Security Advisers

Qualification Handbook

Qualification Number: 610/5561/X

Operational Start Date: 1st May 2025

Contents

Document Control

Revisions and Amendment Register

Date of Issue	Page No	Revision	Version
April 2025	--	--	1
May 2025	41-52	Added indicative content / guidance to unit 9	2
June 2025	10	Updated section 2.6 to include Northern Ireland	3
April 2026	1, 6, 10	Added HTQ logo, section 2.2 and updated wording in section 2.6	4
May 2026	9, 10	Added in section 2.10	5

1. Introduction

1.1. About SFJ Awards

SFJ Awards is part of the Workforce Development Trust group, together with Skills for Justice, Skills for Health and People 1st International. The Workforce Development Trust is a not-for-profit organisation helping employers to continually improve their workforce through increasing productivity, improving learning solutions and helping to boost the skills for staff across a wide range of industries throughout the UK and internationally.

SFJ Awards is an independent Awarding Organisation, regulated by the UK qualifications regulators, including Ofqual, CCEA and Qualifications Wales, to assess, quality assure and certificate learners and employees, helping training providers and employers to continue developing a highly skilled workforce for the future. Our values are 'For Skills, For Flexibility and For Jobs' and our work embodies the core charitable aims of the wider Workforce Development Trust group that ultimately supports better jobs. We add value to employers and training providers by delivering a wide range of sector-specific regulated qualifications, bespoke learner certification and quality assurance; SFJ Awards is also an End-Point Assessment Organisation for Apprenticeships in England.

Whilst predominantly delivering qualifications and assessments to meet the needs of Policing, Fire and Rescue, Community Justice, Custodial Care, Armed Forces, Security and Emergency Services, we continue to grow into markets that require a robust, and quality assured certification solution.

1.2. Customer Service Statement

Our Customer Service Statement is published on the SFJ Awards website giving the minimum level of service that centres can expect. The Statement will be reviewed annually and revised as necessary in response to customer feedback, changes in legislation, and guidance from the qualifications regulators.

1.3. Centre Support

SFJ Awards works in partnership with its customers. For help or advice contact:

SFJ Awards
Consult House
Meadowcourt Business Park
4 Hayland Street
Sheffield
S9 1BY

Tel: 0114 284 1970
Email: info@sfjawards.com
Website: www.sfjawards.com

2. The Qualification

2.1. Qualification Objective

This handbook relates to the following qualification:

SFJ Awards Level 4 Certificate for Protective Security Advisers

This qualification was designed in collaboration with and is endorsed by the Protective Security Centre (Home Office). In addition, the qualification is also endorsed by all three of the government's National Technical Authorities: National Protective Security Authority (NPSA), UK National Authority for Counter Eavesdropping (NACE) and National Cyber Security Centre (NCSC).

The role of a Protective Security Adviser is to safeguard an organisation's assets –people, information, physical property, systems – by identifying threats and implementing integrated security measures across physical, personnel, technical, and cyber domains. Found in both public and private sectors Protective Security Advisers conduct risk assessments, develop and review mitigations, and promote a converged security approach to close gaps between security disciplines. They collaborate with internal and external stakeholders, from senior leaders to law enforcement, and follow national standards and guidance to ensure resilience, continuity, and a strong security culture across the enterprise.

The objective of this qualification is to provide learners with the baseline of knowledge and skills required to carry out the role of a protective security adviser. This qualification equips delegates with the competencies to understand how the protective security disciplines dovetail to provide the foundations of 'security convergence'. Completion of this qualification will provide an understanding of how threat actors target us with a converged approach, and the importance of protecting organisational assets with robust converged security mitigations providing organisational seniors with a single overview of protective security risk.

2.2. Higher Technical Qualification (HTQ) Status

The SFJ Awards Level 4 Certificate for Protective Security Advisers has been approved as a Higher Technical Qualification (HTQ). HTQs are level 4 and 5 qualifications that have been developed in line with employer-led occupational standards, ensuring they meet the knowledge, skills and behaviours required for specific technical occupations.

As a HTQ, this qualification provides assurance to both employers and learners of its quality and relevance. It supports the development of specialist, industry-recognised skills that are aligned to current workforce needs, helping learners to progress into, or advance within, skilled employment.

HTQs offer a flexible approach to learning, enabling study on a full-time or part-time basis. They provide a valuable pathway for individuals looking to enter a new career, progress within their current role, or continue their professional development. Achievement of an HTQ can support access to well-paid, secure and sustainable employment.

Please note that recognition of this qualification as a HTQ applies in **England only**.

For more information about HTQs, please visit the Skills England website.

2.3. Pre-entry Requirements

There are no pre-entry requirements for this qualification. However, centres must ensure that learners are able to complete this qualification, for example, through completing a skills scan to ensure they can work at the appropriate level.

2.4. Qualification Structure

To be awarded this qualification the learner must achieve **all 14** mandatory units as shown in the table below.

Mandatory Units				
Unit Number	**Odyssey Reference**	**Unit Title**	**Level**	**GLH**
1	6718	Crime and Security Science	4	7
2	6719	Legislation and Governance	4	10
3	6720	Asset, Threat and Vulnerability	4	8
4	6721	Security Risk	4	8
5	6722	Physical Security Standards and Mitigations	4	12
6	6723	Personnel Security	4	10
7	6724	People Security	4	7
8	6725	Personal Security	4	6
9	6726	Technical Security	4	6
10	6727	Cyber Security	4	10
11	6728	Incident Response and Management	4	5
12	6729	Investigations	4	10
13	6730	Security as a Business Enabler	4	6
14	6731	Effective Communication and Reflective Practice for Professional Development	4	6

2.5. Total Qualification Time (TQT)

Values for Total Qualification Time[1], including Guided Learning, are calculated by considering the different activities that Learners would typically complete to achieve and demonstrate the learning outcomes of a qualification. They do not include activities which are required by a Learner's Teacher based on the requirements of an individual Learner and/or cohort. Individual Learners' requirements and individual teaching styles mean there will be variation in the actual time taken to complete a qualification. Values for Total Qualification Time, including Guided Learning, are estimates.

Some examples of activities which can contribute to Total Qualification Time include:

- Independent and unsupervised research/learning
- Unsupervised compilation of a portfolio of work experience
- Unsupervised e-learning
- Unsupervised e-assessment
- Unsupervised coursework
- Watching a pre-recorded podcast or webinar
- Unsupervised work-based learning
- All Guided Learning

Some examples of activities which can contribute to Guided Learning include:

- Classroom-based learning supervised by a Teacher
- Work-based learning supervised by a Teacher
- Live webinar or telephone tutorial with a Teacher in real time
- E-learning supervised by a Teacher in real time
- All forms of assessment which take place under the Immediate Guidance or Supervision of a lecturer, supervisor, tutor or other appropriate provider of education or training, including where the assessment is competence-based and may be turned into a learning opportunity.

The Total Qualification Time and Guided Learning Hours for this qualification are as follows:

Qualification Title	TQT	GLH
SFJ Awards Level 4 Certificate for Protective Security Advisers	140	111

2.6. Grading

This qualification is graded pass / fail.

2.7. Age Range and Geographical Coverage

This qualification is recommended to learners aged **18** years and over and is regulated in England, Wales and Northern Ireland.

[1] Total Qualification Time, Ofqual
https://www.gov.uk/guidance/ofqual-handbook/section-e-design-and-development-of-qualifications

2.8. Opportunities for Progression

This qualification creates a number of opportunities for progression as completion of this course will enable learners to progress their career as a qualified security adviser and progress onto the next step of developing a deep specialism in their chosen field.

2.9. Use of Languages

SFJ Awards business language is English and we provide assessment materials and qualification specifications that are expressed in English. Assessment specifications and assessment materials may be requested in Welsh or Irish and, where possible, SFJ Awards will try to fulfil such requests. SFJ Awards will provide assessment materials and qualification specifications that are expressed in Welsh or Irish and support the assessment of those learners, where the number of learners makes it economically viable for SFJ Awards to do so. More information is provided in the SFJ Awards' Use of Language Policy.

For learners seeking to take a qualification and be assessed in British Sign Language or Irish Sign Language, please refer to SFJ Awards' Reasonable Adjustments Policy. A learner may be assessed in British Sign Language or Irish Sign Language where it is permitted by SFJ Awards for the purpose of Reasonable Adjustment.

Policies are available on our website sfjawards.com or on request from SFJ Awards.

2.10. Post Nominals

Use of Post Nominal Letters

Learners who have successfully achieved the SFJ Awards Level 4 Certificate for Protective Security Advisers are entitled to use the post-nominal letters:

CertPSA4

Purpose

The post-nominal CertPSA4 recognises that the holder has achieved this regulated qualification and has demonstrated the knowledge and skills required of a Protective Security Adviser at Level 4.

Entitlement

Use of the post-nominal is restricted to individuals who have been formally awarded the:

610/5561/X SFJ Awards Level 4 Certificate for Protective Security Advisers

It must not be used by learners who are still undertaking the qualification or who have not achieved a pass.

Use in Practice

Holders may use CertPSA4 after their name in professional and relevant contexts, including:

- curriculum vitae and job applications
- professional profiles
- email signatures
- business correspondence and documentation

Example:

Jane Smith CertPSA4

Format

The post-nominal must be presented as CertPSA4, without spaces or punctuation. It should be written after the individual's name and, where multiple post-nominals are used, in an appropriate order reflecting level and/or relevance.

Misuse

The post-nominal must not be used in any way that could mislead others regarding an individual's qualification status, role, or professional competence. SFJ Awards reserves the right to take appropriate action where misuse is identified.

3. Qualification Units

Title	Crime and Security Science
Level	4
Unit Number	1
GLH	7

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand the development of Crime and Security Science as a discipline	1.1	Evaluate the role of key criminological theories in shaping protective security strategies	• Routine Activity Theory • Rational Choice Theory • Broken Windows Theory • What are their applicability's and limitations?
	1.2	Analyse how spatial and situational strategies support protective security	• Crime Mapping • Situational crime prevention • Crime Prevention through Environmental Design (CPTED) • Social crime prevention
	1.3	Assess the importance of Defence in Depth when designing Protective Security	
2. Understand the contribution the National Technical Authorities provide to Crime and Security Science	2.1	Evaluate how the roles of the National Technical Authorities contribute to Crime and Security Science	• The protective security eco-system • National Protective Security Authority • UK National Authority for Counter Eavesdropping • National Cyber Security Centre • Who We Work With | NPSA

	2.2	Describe how Accreditation bodies support the work of National Technical Authorities	• NPSA Working with Security Professionals | NPSA • The Register of Chartered Security Professionals (CSyP) | NPSA • Register of Security Engineers and Specialists (RSES) | NPSA
3. Understand the concept of security convergence	3.1	Describe the four disciplines of protective security	• Cyber – National Cyber Security Centre - NCSC.GOV.UK • Personnel – Personnel and People Security | NPSA • Physical – Physical Security Advice | NPSA • Technical security – UK NACE Operations - FCDO Services
	3.2	Evaluate the importance of convergence of the cyber, personnel, physical and technical security when designing Protective Security	• Security Convergence • Level 4 protective security apprenticeship brings a converged approach - City Security Magazine
4. Be able to apply crime science and security convergence principles to meet organisational protective security needs	4.1	Produce an organisational protective security plan addressing protective security requirements and organisational needs	Risk-based and proportionate security strategy | NPSA
	4.2	Apply the principles of security convergence to protective security planning	Protective Security Risk Management PSRM | NPSA
	4.3	Determine best communication practices for cross-functional security teams within protective security planning	
Additional information about the unit			

Delivery Guidance	This unit covers key crime theories (e.g. Routine Activity, Rational Choice) and the role of National Technical Authorities in protective security. Learners will explore security convergence across cyber, personnel, physical, and technical domains and apply these principles in creating a security plan. To deliver this unit, centres should adopt a blend of theoretical instruction and practical activities to ensure learners develop both the knowledge and practical ability of the Protective Security Adviser role.
Assessment Guidance	Assessment for this unit should combine theoretical understanding with practical application, allowing learners to demonstrate their ability to critically evaluate crime theories and apply integrated security approaches effectively.
Links	Below YouTube channel will provide further indicative learning: Sustainable Security - YouTube

Title	Legislation and Governance
Level	4
Unit Number	2
GLH	10

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand relevant legislation relating to protective security	1.1	Describe the responsibility of organisations towards the relevant occupiers' liability legislation	• Occupiers' Liability Act 1957 (England and Wales) • Occupiers' Liability (Scotland) Act 1960 • Occupiers' Liability Act (Northern Ireland) 1957
	1.2	Analyse how health and safety legislation can be used to support protective security	• Health and Safety at Work Act 1974 • Health and Safety at Work (Northern Ireland) Order 1978 • Management of Health and Safety at Work Regulations 1999
	1.3	Explain the importance of fire safety legislation	• The Regulatory Reform (Fire Safety) Order 2005 • Regulatory Reform (Scotland) Act 2014 • Fire Safety Act 2021 (Wales) • The Fire Safety Regulations (Northern Ireland) 2010
	1.4	Assess the impact of current and emerging security legislation on protective security	• The Terrorism (Protection of Premises) Bill • Data Protection Act • General Data Protection Regulation (GDPR) • The National Security Act • National Security Investment Act

			• Security Services Act
	1.5	Analyse how key elements of regulatory and common law govern security practices	• Criminal Law • Common Law • The Private Security Industry Act
	1.6	Summarise organisational responsibilities related to duty of care and risk management	• Duty of Care • Guard Dog Act
2. Understand why effective governance is paramount to protective security	2.1	Assess the importance of organisations having an individual(s) at board level who is accountable for cyber, personnel, physical and technical security risk	• Passport to Good Security for Senior Executives | NPSA • Leadership and Governance | NPSA
	2.2	Explain the importance of a clear organisational structure in effectively managing protective security risks	• Principles of good governance • Identifying those responsible and accountable for protective security risk management • Identifying those with authority and resource to action mitigations
3. Understand how organisational objectives and international standards influence the development and implementation of protective security measures	3.1	Evaluate how organisational objectives impact the protective security approach for organisations	To include: • Government • Critical National Infrastructure (CNI) • Multinationals • Academia • Start-ups • Emerging technology
	3.2	Identify the ISO standards that are relevant to protective security	ISO - Search
4. Understand the challenges and positive	4.1	Identify legislation and organisational policies relating to equity, diversity and inclusion within the workplace	

impact embracing equity, diversity and inclusion has on protective security	4.2	Explain the impact of socio-economic diversity on workplace interactions with colleagues and stakeholders	What is diversity, equity, and inclusion (DE&I)? | McKinsey
5. Understand how to apply security policies and governance practices to meet organisational needs effectively while fostering an inclusive environment	5.1	Explain how an organisation should meet compliance legislation, local and national policies in relation to the organisations objectives	
	5.2	Evaluate how Protective Security Advisers can influence Senior Risk Owners to enable informed risk decisions to be made to protect and add value to an organisation	
	5.3	Assess organisational needs for implementing protective security measures that are aligned to the organisations mission, assets, threat and risk	
	5.4	Identify relevant ISO standards used within the context of protective security and consider the implications of non-compliance	
	5.5	Explain how to provide support for individuals from diverse socio-economic and cultural backgrounds	

Additional information about the unit	
Delivery Guidance	This unit introduces learners to key legislation such as health and safety, fire safety, and data protection as well as governance, ISO standards and equality, diversity and inclusion. To deliver this unit a range of both theoretical and practical activities should be used, for example, case studies, group discussions or workshops.
Assessment Guidance	Assessment for this unit could include a range of different methods such as written reports, reflective journals or professional discussions to allow learners to demonstrate their ability to comply with governance and legislation as well as their willingness to support individuals with differing backgrounds.

Title	Asset, Threat and Vulnerability
Level	4
Unit Number	3
GLH	8

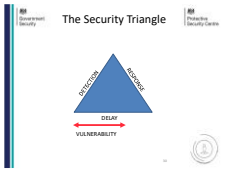
Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand the types of organisational assets and identify which assets and people require protection	1.1	Describe the range of assets that organisations may hold using the NPSA Asset Identification Guide	To include: • Physical • Information • Systems • People • Other (brand, reputation) Assets can be: • Tangible • Intangible • Mixed
	1.2	Explain how people and assets are ranked by how much their loss could harm the business or its stakeholders	Protective Security Risk Management PSRM | NPSA
	1.3	Explain how information assets should be classified based on their level of sensitivity and the impact of compromise, loss or misuse	Protective Security Risk Management PSRM | NPSA
2. Understand the concept of threat and how to access and use relevant	2.1	Explain how Intent and Capability contribute to threat	Protective Security Risk Management PSRM | NPSA

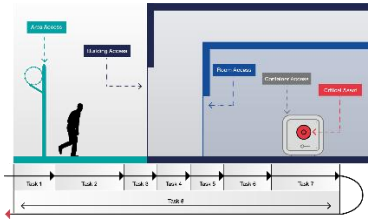
sources of threat information			See also: Book: Paul Martin, The Rules of Security - Staying Safe in a Risky World, Oxford University Press
	2.2	Define the term 'Threat Actor'	Glossary | NPSA
	2.3	Identify the primary sources of threat information available	To include: • National Protective Security Authority (NPSA) • National Cyber Security Centre (NCSC) • UK National Authority for Counter Eavesdropping (UK NACE) • National Counter Terrorism Security Office (NaCTSO) • MI5 • Police • Local crime statistics • External stakeholders
	2.4	Identify the component parts of the 'Threat Intelligence Cycle'	Threat Intelligence Cycle
3. Understand how to identify threats to an organisation	3.1	Assess how an organisation's location, assets, and services may attract potential threat actors and identify which threat actors could be interested based on these factors	Protective Security Risk Management PSRM | NPSA
	3.2	Identify threat scenarios that an organisation may face	Threat Landscape and Assessment Information | NPSA
	3.3	Define the terms 'Vulnerability' and 'Impact' in the context of protective security risk management	Glossary | NPSA

4. Be able to develop comprehensive protective security plans by documenting assets, analysing threats, and assessing vulnerabilities	4.1	Produce an asset register for own organisation	Should apply: • Asset identification • Classification principles
	4.2	Produce a 'Threat Analysis' based on own organisation's assets, services and location	Should apply: • Asset identification • Classification principles
	4.3	Assess vulnerability and impact to own organisation	
	4.4	Implement the NPSA's Guide to Using Threat Assessments when developing a security plan	
Additional information about the unit			
Delivery Guidance	This unit introduces learners to the identification and classification of organisational assets using the NPSA Asset Identification Guide, covering physical, informational, and intangible assets. To deliver this unit a range of discussions and practical exercises should be used to provide learners with an overview of threat definitions, including intent, capability, and the roles of various threat actors. Learners should be familiarised with sources of threat information and facilitating an analysis of threat scenarios related to an organisation's location, assets, and services would be beneficial.		
Assessment Guidance	Assessment for this unit should include a combination of practical and theoretical assessment methods. This could include the learner producing an asset register or threat analysis alongside evaluating a range of threat scenarios and analysing vulnerability to demonstrate comprehensive risk management understanding.		

Title	Security Risk
Level	4
Unit Number	4
GLH	8

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand the importance of security risk components, including the methods of risk assessment, risk statement construction, and the role of a risk register	1.1	Analyse how threat, vulnerability and impact contribute to security risk	See book: Paul Martin, The Rules of Security - Staying Safe in a Risky World, Oxford University Press
	1.2	Summarise the strengths and weaknesses of quantitative, qualitative and semi-qualitative risk assessment methodology	May include: • Residual risk See also: Book: Paul Martin, The Rules of Security - Staying Safe in a Risky World, Oxford University Press
	1.3	Describe how the threat actor, asset targeted, vector used, and potential impact are used to form a risk statement	Operational requirements | NPSA
	1.4	Outline how security risk registers enable practitioners and stakeholders to develop appropriate risk mitigations	
	1.5	Explain why timely reviews of the security risk register are required	Align to: • Asset • Threat • Risk

	1.6	Assess the importance of security risk registers in providing effective audit trails of decision making	Considering corporate memory
	1.7	Analyse how a security risk register can provide a business-as-usual mechanism for managing protective security good practice	
	1.8	Explain the benefits of conducting the Operational Requirements process	Operational requirements | NPSA
	1.9	Explain the importance of providing a single overview of security risk to senior risk owners through the use of security convergence	
2. Understand the benefits and key principles of developing a protective security plan and the importance of regular risk review	2.1	Explain the organisational benefits of developing a protective security plan to mitigate risks identified and optimise the implementation process	
	2.2	Explain how the 'Security Triangle' of detection, response and delay combine to aid protective security	 A suitable delay is determined by the time required to both detect and respond to an incident, if the combined detection and response time is longer than that of the delay provided by security measures, this provides a vulnerability.

	2.3	Describe how Adversary Path Analysis can be used to identify and communicate detection, delay and response	 The delay should start at the first point of detection and can be influenced by the installation of security rated products that provide a level of assurance to the delay they provide. The Adversary Path Analysis which highlights the importance of deterrence, the use of detection, ideally to trigger an alert as soon as possible and the provision of enough delay to enable an appropriate response. Security_Brochure.pdf See also Book: Mary Lynn Garcia, The Design and Evaluation of Physical protection Systems, Elsevier
	2.4	Describe how the security principles of deter, detect, delay, mitigate, and respond enhance protective security and support the 'Security Triangle' approach	Learners should consider: • Beyond the perimeter • The perimeter • Within the perimeter • The building • The asset
	2.5	Explain the importance of regularly reviewing protective security risks to ensure the effectiveness of security measures over time	• On a cyclical basis • When the threat changes, • When a breach has occurred, • When there is a change to the operational

			environment • When new security measures are implemented
	2.6	Explain why the appropriate identified risks need to be communicated to those responsible and accountable for security risk	• Passport to Good Security for Senior Executives | NPSA • Leadership and Governance | NPSA
3. Be able to use and produce security risk assessments and registers	3.1	Calculate the security risk posed to an organisation aligned to the organisation's assets and threats	
	3.2	Produce a converged security risk assessment	Learners should incorporate: • Cyber • Personnel • Physical • Technical
	3.3	Define how effective implementation of a security risk register can provide senior risk owners with the information to make informed judgements on risk tolerance	

Additional information about the unit	
Delivery Guidance	This unit introduces learners to the components of security risk (threat, vulnerability and impact) as well as risk assessment methods (quantitative, qualitative, semi-qualitative), the security triangle (detection, response, delay) and principles such as deter, detect, and mitigate. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.
Assessment Guidance	Assessment for this unit could include exercises where learners construct risk statements and calculate security risk based on given assets and threats. Learners could also complete a practical task to create and review a security risk register, highlighting its value in decision-making and corporate memory. Additionally, learners could demonstrate understanding through a written assignment on applying the principles of deter, detect, delay, mitigate, and respond.

Links	• Protective Security Risk Management PSRM | NPSA Below YouTube channel will provide further indicative learning: • Sustainable Security - YouTube

Title	Physical Security Standards and Mitigations
Level	4
Unit Number	5
GLH	12

Learning Outcomes *The learner will:*	Assessment Criteria *The learner can:*		Guidance and/or Indicative Content
1. Understand Forcible Attack Standards that enhance security through delay tactics	1.1	Evaluate how Loss Prevention Standards support protective security	• LPS 1673 • LPS 1673: Issue 1 • LPS 1175 Issue 8 • Security Brochure.pdf
	1.2	Assess how standards support protective security	• National Protective Security Authority (NPSA) • Marauding Terrorist Attack Standard (MTAS) • Manual Forced Entry Standard (MFES)
2. Understand how to mitigate postal threats	2.1	Identify the purpose of screening mail and courier deliveries	Screening mail and courier deliveries | NPSA
	2.2	Examine standards for mail screening and security	• PAS 97: 2021 Mail Screening and Security - Specification • Screening mail and courier deliveries | NPSA
3. Understand the risk posed by building glazing systems and the benefits of blast	3.1	Identify the various specifications of glazing and their vulnerability against forcible attack and blast	Windows and Glazed Facades | NPSA
	3.2	Evaluate the mitigation measures and protective measures available for glazing systems	Windows and Glazed Facades | NPSA

mitigation for safety and carbon reduction	3.3	Explain how glazing mitigation and protective measures can potentially reduce a buildings carbon footprint	• Laminated glass • Annealed/float glass • Tough/tempered glass • Heat strengthened glass • Laminated glass sandwich • Polycarbonate
4. Understand what risk attack vectors employing vehicles could pose to organisations	4.1	Describe how vehicle as a weapon (VAW) attacks may impact an organisation	Hostile Vehicle Mitigation (HVM) | NPSA
	4.2	Explain what a Vehicle Borne Improvised Explosive Device (VBIED) is	Hostile Vehicle Mitigation (HVM) | NPSA
	4.3	Evaluate how a Layered Vehicle Attack may impact an organisation	Hostile Vehicle Mitigation (HVM) | NPSA
5. Understand how HVM measures are the integrated deployment of security processes, procedures and physical obstructions to counter vehicle borne threats	5.1	Explain why an integrated approach is required to mitigate vehicle borne threats	Hostile Vehicle Mitigation (HVM) | NPSA
	5.2	Identify the key aspects of the international standard for security and resilience — vehicle security barriers	• ISO 22343-1: 2023 • Hostile Vehicle Mitigation (HVM) | NPSA
	5.3	Explain how vehicle security barriers contribute to building resilience against security threats through Hostile Vehicle Mitigation (HVM) strategies	Hostile Vehicle Mitigation (HVM) | NPSA
6. Understand what a Marauding Terrorist Attack is and how to mitigate the impact to an organisation	6.1	Describe the variations of Marauding Terrorist Attacks	Marauding Terrorist Attacks | NPSA
	6.2	Explain the range of potential measures that can be employed to mitigate a Marauding Terrorist Attack	Marauding Terrorist Attacks | NPSA
	6.3	Describe the range of lockdown measures that organisations could employ to safeguard personnel	Marauding Terrorist Attacks | NPSA

	6.4	Assess why Marauding Terrorist Attack Standard products should be used as part of a mitigation strategy	Marauding Terrorist Attacks | NPSA
7. Understand what the surreptitious threat is and how to mitigate against surreptitious attack vectors	7.1	Describe what is meant by surreptitious attacks	STaMP
	7.2	Describe when STaMP should be considered to support protective security within an organisation	
	7.3	Evaluate the National Protective Security Authority (NPSA) Surreptitious Attack Protective Security Philosophy	
	7.4	Outline the National Protective Security Authority (NPSA) CLASS standard	NPSA Product Grading Systems | NPSA
	7.5	Explain how the BAD principles are used to mitigate the surreptitious attack vector	
8. Understand how the Cyber Assurance of Physical Security Systems (CAPSS) can support organisations with protective security	8.1	Describe the purpose of CAPSS	Cyber Assurance of Physical Security Systems | NPSA
	8.2	Explain what organisations should consider CAPSS products	Cyber Assurance of Physical Security Systems | NPSA
9. Understand where to source security rated products to mitigate forcible and surreptitious attacks	9.1	Explain what products can be found in the Redbook live	RedBook Live - LPCB Red Book
	9.2	Describe what standard of products can be found in the National Protective Security Authority (NPSA) Catalogue of Security Equipment	The Catalogue of Security Equipment | NPSA

10. Be able to produce designs for physical security mitigations	10.1	Develop physical security mitigations for forcible attack vectors	
	10.2	Develop physical security mitigations for surreptitious attack vectors	
	10.3	Apply assured products to mitigate protective security risk	
Additional information about the unit			
Delivery Guidance	This unit introduces learners to the key standards for physical security, such as the Loss Prevention Standards and NPSA guidelines as well as mitigating various threats, including postal, vehicle, and surreptitious attacks. The unit also covers security protocols like mail screening and vehicle-borne threat countermeasures and standards like ISO 22343-1 and CAPSS. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.		
Assessment Guidance	Assessments for this unit could include the development of a comprehensive physical security mitigation plan addressing both forcible and surreptitious attack vectors. Learners could also demonstrate knowledge through case-based assignments that evaluate risk reduction strategies for glazing systems, vehicle attacks, and other attack vectors.		

Title	Personnel Security
Level	4
Unit Number	6
GLH	10

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand the key definitions of personnel in the context of protective security	1.1	Define key terms related to personnel security, including 'insider,' 'insider risk,' 'insider threat,' and 'insider event'	• Personnel and People Security | NPSA • NPSA Changes to Insider Risk Definitions | NPSA
	1.2	Explain how insider risks, threats, and events contribute to protective security considerations	Insider Risk | NPSA
2. Understand the typologies, motivations, and methods associated with insider events	2.1	Explain how unauthorised disclosure of sensitive information may impact an organisation	Introduction to Insider Risk | NPSA
	2.2	Describe how Process Corruption or Sabotage may impact an organisation	Introduction to Insider Risk | NPSA
	2.3	Assess the impact that the unauthorised provision of third-party access to organisational assets and people may provide	Introduction to Insider Risk | NPSA
	2.4	Outline the impact on an organisation by insiders with privileged access who seek financial gain through financial corruption	Introduction to Insider Risk | NPSA
	2.5	Describe how workplace violence committed by employees could potentially impact organisations	Introduction to Insider Risk | NPSA

	2.6	Define key insider types, including 'deliberate insider,' 'recruited/pressured insider,' 'self-initiated insider,' and 'unintentional insider'	Insider Risk Mitigation | NPSA See also Book: Paul Martin, Insider Risk & Personnel Security - Insider Risk and Personnel Security | An introduction | Paul Martin |
3. Understand the current societal and cultural challenges that may encourage threat actors to undertake insider events	3.1	Analyse the role of social and cultural challenges in fostering conditions for insider threats	Consider how for example COVID-19, the Cost-of-Living Crisis etc. impact insider events
4. Understand what is required for an Insider Risk Mitigation Programme to be effective	4.1	Explain how good governance and leadership is required to implement effective personnel security	Insider Risk Mitigation | NPSA
	4.2	Assess the benefits that an Insider Stakeholder Group would provide to an organisation	Insider Risk Mitigation | NPSA
	4.3	Identify steps to effective insider risk assessment and how they support organisational risk management	10 Steps to Effective Insider Risk Assessment | NPSA
	4.4	Describe the role which Pre-Employment Screening and Vetting provides to support personnel security	• Pre-employment screening | NPSA • Insider Risk Mitigation | NPSA
	4.5	Assess how ongoing personnel security can mitigate insider events within organisations	• Ongoing Personnel Security | NPSA • Insider Risk Mitigation | NPSA
	4.6	Describe how the monitoring and assessment of employees can mitigate insider events within organisations	Insider Risk Mitigation | NPSA

	4.7	Evaluate how investigation and disciplinary practices provide a response to potential insider events	Insider Risk Mitigation | NPSA
	4.8	Analyse how Security Culture and Behaviour Change can mitigate insider events	Security culture | NPSA
	4.9	Explain how converging personnel, cyber, physical, and technical security controls can mitigate insider risk	• Security Convergence • Level 4 protective security apprenticeship brings a converged approach - City Security Magazine
5. Be able to mitigate Insider Risk	5.1	Discuss how effective line management can support the insider risk mitigation	• Insider Risk Mitigation Framework | NPSA • Insider Risk Mitigation | NPSA
	5.2	Assess how physical security controls can support the mitigation of insider risk	Insider Risk Mitigation Framework | NPSA
	5.3	Develop measures to mitigate against organisational insider risk	Insider Risk Mitigation Framework | NPSA

Additional information about the unit	
Delivery Guidance	This unit introduces learners to personnel security by defining key concepts, including insider threats and types of insider events, societal and cultural challenges that may lead to insider risks and effective Insider Risk Mitigation Programme. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.
Assessment Guidance	Assessments could include a written analysis of insider threat types and their potential impact on organisations or learners could develop a brief insider risk mitigation plan, incorporating screening, role-based risk assessment, and employee monitoring. Centres should devise assessments that reflect real-world scenarios relevant to the learners' contexts.
Links	Below YouTube channel will provide further indicative learning: Sustainable Security - YouTube

Title	People Security
Level	4
Unit Number	7
GLH	7

Learning Outcomes *The learner will:*	Assessment Criteria *The learner can:*		Guidance and/or Indicative Content
1. Understand what a security culture is	1.1	Describe what is meant by the term 'security culture'	Security culture | NPSA
	1.2	Determine how an effective security culture can contribute to protective security	Security culture | NPSA
	1.3	Consider how organisations can effectively re-enforce the required security behaviours for all site users	Security culture | NPSA
	1.4	Evaluate how organisations can embed behaviour change using an established framework	Embedding Security Behaviour Change | NPSA
2. Understand hostile reconnaissance and disruptive effects, and how protective security measures and communication strategies can be used to mitigate threats	2.1	Describe what is meant by the terms 'Hostile' 'Reconnaissance' and 'Disruptive Effects'	• Hostile Reconnaissance | NPSA • Disrupting Hostile Reconnaissance | NPSA
	2.2	Describe the methods and planning stages associated with hostile reconnaissance	• Online • Onsite • Insider • Hostile Reconnaissance | NPSA
	2.3	Explain how protective security measures can exploit vulnerabilities in hostile actors	• Including anxiety and paranoia • The use of the NPSA DENY, DETECT, and DETER strategy

	2.4	Explain how a Security Minded Communications, See, Check and Notify (SCaN) implementation and Project Servator can be used to create disruptive effects at a site/location	• Security-Minded Communications guidance | NPSA • See, Check and Notify (SCaN) | NPSA • Disrupting Hostile Reconnaissance | NPSA
	2.5	Describe how Project Servator can amplify a site's security posture	Disrupting Hostile Reconnaissance | NPSA
3. Be able to develop and implement mitigations against hostile reconnaissance	3.1	Conduct a hostile reconnaissance assessment to identify the places hostiles would need to position themselves to gain detailed information about your site/building	
	3.2	Develop mitigations against hostile reconnaissance	
	3.3	Implement proactive security measures that disrupt hostile reconnaissance activities	

Additional information about the unit	
Delivery Guidance	This unit introduces the concept of security culture, emphasizing how a strong culture supports protective security and shapes user behaviour. It also covers the NPSA 5Es Framework for embedding behaviour change, hostile reconnaissance and the NPSA DENY, DETECT, and DETER strategy. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.
Assessment Guidance	Assessment could include a written analysis of security culture's role in protective security and how behaviour change can be embedded using the NPSA 5Es Framework. Learners could also develop a plan outlining strategies to disrupt hostile reconnaissance, applying the DENY, DETECT, and DETER framework and proposing specific mitigations to enhance security. A combination of practical and knowledge-based assessment methods should be used.

Title	Personal Security
Level	4
Unit Number	8
GLH	6

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand the principles of personal security and safety	1.1	Describe what is meant by the term 'Personal Situational Awareness'	Personal Safety and Security for High-Risk Individuals
	1.2	Explain how 'Online Vigilance' can support personal security	• Stay Vigilant Online • Protect information about you
	1.3	Outline what measures an individual can take to protect their residence	• Protect your home • The Blue Book: A Guide to Personal Security | ProtectUK
	1.4	Outline the range of 'Travel Planning' measures that can be taken	Protect you away from home
	1.5	Describe how to reduce vulnerability with digital footprints	Protect information about you
	1.6	Identify methods to protect sensitive information relating to an individual	Protect sensitive information
	1.7	Outline personal security emergency procedures	Prepare for an emergency

2. Be able to apply personal security and safety protocols effectively in the work environment	2.1	Demonstrate adherence to established personal security protocols to ensure safety in various workplace scenarios	Suzy Lamplugh Trust | Personal Safety
	2.2	Identify and respond appropriately to potential security threats in the work environment using personal safety protocols	Suzy Lamplugh Trust | Personal Safety

Additional information about the unit	
Delivery Guidance	This unit introduces learners to the fundamentals of personal security by discussing key concepts such as situational awareness, online vigilance, and digital footprint management. It also covers residence security, travel planning, and protecting sensitive personal information. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.
Assessment Guidance	Assessments could include a written report on personal security strategies, covering areas like situational awareness, residence protection, and travel planning. Learners could also complete a practical exercise in which they apply personal security protocols within a work environment. Centres should devise assessments that reflect real-world scenarios relevant to the learners' contexts.

Title	Technical Security
Level	4
Unit Number	9
GLH	6

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand what technical security is and why organisations may be targeted	1.1	Explain what is meant by 'technical security'	**Purpose of Technical Security:** • To holistically protect sensitive information and technology. **Protection Against:** • Close or near access acquisition • Exploitation by hostile actors • Any other form of technical manipulation **Additional Responsibilities:** • Protecting security systems from compromise and/or external interference • Detecting and deterring eavesdropping attacks • Mitigating vulnerabilities and threat vectors
	1.2	Evaluate why organisations may be targeted with technical attack vectors	**Sources of Technical Threats:** • Foreign intelligence services • Terrorist, extremist, and subversive organisations • Criminals, investigative journalists, investigation agencies, information brokers, and commercial rivals. • Opportunists and inadvertent enthusiasts • Disgruntled employees coerced or persuaded by any of the above actors

			Specific Organisational Threats:
			• Entities involved in combating organised crime face elevated threats from Organised Criminal Groups (OCGs).
			• OCGs use eavesdropping and radio interception to protect their own activities and monitor law enforcement operations.
			
			Technical Attack Methods:
			• Can be used independently or in conjunction with physical and cyber methods
			  • Physical vectors: access, proximity, physical threat
			  • Cyber vectors: targeting of information systems, building controls, IoT devices
			• Aim to exploit gaps between security disciplines
			
			Examples of Technical Attacks:
			• **Hybrid example**: A fake burglary is staged to implant a GPS tracker in a laptop, which is later carried to a sensitive location.
			• **Technical-only example**: When physical access is highly restricted (e.g. secure site, armed protection), attackers disable a house alarm to plant concealed audio devices.

2. Understand the methods that information can be egressed from an organisation	2.1	Explain the required elements of a technical surveillance device	Including: • Why technical surveillance devices require a power source • Method of collection • How the attacker gains the information required
	2.2	Explain how information egress is achieved through spatial methods	**Wireless Eavesdropping Risks:** • Wireless tech (Wi-Fi, Bluetooth, GSM) can be exploited for eavesdropping.

			• Devices may transmit data unnoticed by blending with normal signals. • Signals often extend beyond secure areas, increasing exposure. • Sources include phones, access systems, IoT, and building controls. **TEMPEST Threats:** • TEMPEST refers to unintentional signal leaks from electronic devices. • Signals can travel via air, metal, or sound and are hard to detect. • High-risk devices: laptops, PCs, audio/video systems, radios. • Closer proximity and better equipment = higher risk of exploitation. **Illumination Attacks:** • RF energy is aimed at targets or devices; reflections can leak info. • Famous example: *The Great Seal Bug* — a passive, power-free device activated by external RF to capture sound.

	2.3	Evaluate how information egress is achieved through the physical removal of assets	• When signal-based (spatial/conductive) egress isn't possible, adversaries may target physical devices or data directly.
			• Physical recovery may align with the adversary's risk appetite.
			• Access to devices may require:
			  • A recruited insider
			  • A cyber exploit
			  • Tampered access controls

			• These are known as blended or hybrid attacks, combining multiple methods. • They exploit gaps between security domains and siloed policies for success.

	2.4	Explain how information is egressed through conductive methods	• Information like speech can travel through and interact with surrounding infrastructure.
			• Infrastructure extending beyond secure areas (e.g. power, fibre, gas, sprinklers) can unintentionally carry information outward.
			• Adversaries exploit this to collect data without needing close access, reducing their risk.
			• Eavesdropping devices may also use this infrastructure to:
			  • Transmit collected data out discreetly.
			  • Reach a safer or more suitable collection point.
			
			Example: Baby monitors send audio through mains power to remote receivers — a similar concept used in technical attacks.

	2.5	Describe what is meant by 'standoff attack'	• Conducted from a distance to avoid detection or when close access is not possible.
			• 'Stand-off' distance varies based on:
			  • Attack type
			  • Location (urban vs. rural)
			  • Adversary's risk appetite
			• Typically occurs outside the target's controlled perimeter.
			• Can be launched from:
			  • Nearby buildings
			  • Vehicles
			  • Individuals on foot

3. Understand how strong cyber, physical, personnel and people security may encourage standoff attacks	3.1	Evaluate how existing security postures may encourage standoff attacks using Crime and Security Science	• Robust cyber, personnel, and physical security may deter direct device placement.
			• Adversaries may instead choose a stand-off attack to reduce detection risk.
			• During hostile reconnaissance, adversaries assess:
			  • Security awareness and adherence by staff
			  • Overall vigilance and enforcement of security policies
			• A strong posture increases the effort, risk, and resources required for an effective attack.
			• Stand-off attacks may also be preferred due to:
			  • Time constraints (e.g. short-notice operations)
			  • Reduced need for physical access to collect intercepted data

	3.2	Explain how physical, personnel and people security can be used to mitigate standoff attacks	**Converged Security Essentials:** • Integrated security increases detection and reduces risk of technical attacks. • Use unpredictable patrols and engage neighbours to report suspicious activity. • Manage wireless infrastructure proactively. **Secure Use of Space:** • Hold sensitive meetings in interior rooms, away from windows and public areas. • Avoid locations vulnerable to visual surveillance or lip-reading. **Stand-Off Attack Mitigation:** • Know your building's infrastructure (e.g. vents, cabling) to prevent data leakage. • Relocate meetings or remove exposed infrastructure to reduce risk.

			• Requires good communication, policy awareness, and cross-discipline coordination.

4. Understand the range of technical security devices and how they are deployed	4.1	Assess the potential risk posed by overt access of visitors and contractors	**Physical Access Risks:**
			• Ease of access increases the risk of surveillance device placement.
			• Adversaries may gain access to install or retrieve devices through various methods.
			
			Common Access Points
			• Visitors, including internal staff from other areas, may bring bags, PEDs, or cameras.
			• Service staff and contractors often access:
			  • Back areas, service lifts, risers, network infrastructure
			  • Work early, often unsupervised
			
			Exploitation Tactics:
			• Adversaries may recruit insiders and pose as trusted visitors to exploit assumptions of legitimacy
			• Security complacency can lead to unchecked access if individuals appear vetted.
			
			Mitigation Measures:
			• Implement policies requiring escort of visitors and contractors in sensitive areas.
			• Define sensitive areas to include meeting rooms and zones handling classified material.

	4.2	Assess the potential risk posed by commercially available quick plant devices	**Commercial Surveillance Devices:** • Readily available from sites like Amazon, eBay, and Temu. • Range from cheap consumer gadgets to high-end, law

			enforcement-grade equipment. • Even low-cost devices can be effective with proper tradecraft and determination. **Attribution Challenges** • Devices are often bought using stolen credit cards, cash, or vouchers. • This creates distance between the adversary and the device, complicating attribution.
	4.3	Assess the potential risk posed by the deployment of Human Interface Devices (Rubber Duckies)	**Physical Access Enables Cyber Attacks:** • Once inside, adversaries can deploy devices to interact with IT systems and infrastructure. • Common method: uploading malware or scripts to enable further attacks. **Examples of Device-Based Attacks:** • STUXNET: Malware spread via infected USB stick unknowingly plugged into an official system. • Rubber Ducky mimics a USB drive and delivers keystroke injections or malware payloads. • O.M.G. Cable (Hak5) appears as a phone charger and can run preloaded scripts triggered remotely. • These tools are particularly useful for targeting isolated (air-gapped) systems with no internet access.
	4.4	Describe why mobile phones are an attractive target for threat actors	• Devices like phones, smartwatches, and tablets store highly sensitive data. • Constantly carried and used during daily interactions, making them prime targets. • Physical access and cyber-attacks can be used to exploit these devices. • Devices contain multiple microphones and cameras that can be exploited for audio recording and video

			surveillance. **Information at Risk:** • Health data • Contacts and messages • Photos and location history • Emails and browsing activity • Financial and work-related information

	4.5	Explain how Remote Access Trojan malware can be used as an attack vector	• **Zero-click attacks:** No user interaction needed; malware installs without the owner's knowledge.
			• **User-assisted attacks:** Require actions like clicking a link or opening an attachment (e.g. spear phishing).
			• Both attack types can install RATs, granting adversaries access to data, calls, microphones, cameras, and other sensors.
			• RATs may be commercially available or developed by state actors.
			• Highly sophisticated RATs often show no signs:
			  • No obvious battery drain
			  • No device warmth or glitches
			  • Remain invisible to the user

	4.6	Describe how International Mobile Subscriber Identity (IMSI) catchers can potentially be used as an attack vector	**Mobile Identifiers:** • 2G–4G: Uses IMSI (International Mobile Subscriber Identity), a unique 15-digit number. • 5G: Replaces IMSI with SUPI (Subscription Permanent Identifier). **Malicious Cell Towers (MCTs):** • Can extract IMSI/SUPI by luring a phone away from the legitimate network. • Allows adversaries to identify and track the phone,

			deploy a Remote Access Trojan (RAT) and access phone number, calls, messages, apps, and media • MCTs can act as MITM devices, intercepting traffic by rerouting it through an adversary's network.
	4.7	Explain how a man in the middle attack is actioned to enable a standoff or close access attack	• Used to gather information from multiple users or devices. • Can be a precursor to deeper cyber intrusions on individuals or organisations. • Commonly compromise wireless communications (Wi-Fi, cellular). • May also involve physical tapping of cables. • Stealthy: Victim is unaware their data is being intercepted. • Proximity matters: Being physically close increases success likelihood.
	4.8	Evaluate the security risks posed by technology within both office and home environments	Security risks associated with: • smart devices • long lensing • lip reading • drone reconnaissance • laser microphones
	4.9	Analyse the potential risk posed by Deep Plant Devices	• Pose a severe risk by exposing sensitive information to adversaries. • Difficult to detect due to concealment and passive design. • Can operate for long durations or remain dormant until activated. • Require a reliable power source to function effectively. • Often involve high-risk installation, which adversaries aim to minimise.

	4.10	Assess when organisations are vulnerable to Deep Plant Devices	• Exposed structure and infrastructure offer opportunities for device installation. • Adversaries may access service infrastructure (e.g. mains, pipes) to establish egress routes and use building materials and unsupervised access to conceal devices during refurbishment. • Devices and their egress paths are harder to detect when embedded during early stages.

	4.11	Identify the importance of securely storing construction materials when building sensitive sites	• Risk applies to:
			  • Structural elements (concrete, rebar, timber)
			  • Cabling (fibre, copper)
			  • Furnishings and system components (doors, lighting, life safety systems)
			• A secure supply chain is critical to protecting sensitive sites from compromise.

	4.12	Describe TEMPEST attacks and the common attack vectors associated with this threat	• All electronic devices emit electromagnetic fields, vibrations, sounds, and radio frequencies.
			• Adversaries can collect these emissions to infer or extract sensitive information.
			• NCSC is the UK's National Technical Authority for both TEMPEST and EMS.
			• Strict installation guidelines exist for using TEMPEST-rated equipment securely.
			• Approved vendors:
			  • Listed by the NCSC (UK)
			  • Available in the NATO Catalogue for certified products

5. Understand Technical Security Mitigations	5.1	Explain mitigation methods for managing overt access and external device threats	Including: • Quick plant devices • Human Interface Devices • Deep plant devices

	5.2	Describe mitigation approaches for digital and network-based threats	Including: • Remote Access Trojans • International Mobile Subscriber Identity (IMSI) catchers • Technical man-in-the-middle attacks
	5.3	Assess mitigation strategies for various surveillance and eavesdropping methods	Including: • smart devices • long lensing • lip reading, drone reconnaissance • laser microphones
6. Be able to develop and implement mitigations for technical security	6.1	Develop mitigations, using converged security, to mitigate technical security attack vectors	
	6.2	Design and implement mitigations to address technical security attack vectors	
Additional information about the unit			
Delivery Guidance	This unit introduces the concept of technical security, emphasizing why organisations are targeted by technical attack vectors as well as technical security devices, common vulnerabilities and mitigation strategies using converged security. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.		
Assessment Guidance	Assessment could include a report where learners evaluate technical security risks and potential attack vectors within a simulated or real organisational environment. Learners could also complete a practical exercise to develop a mitigation strategy addressing specific technical attack vectors. A combination of practical and knowledge-based assessment methods should be used.		

Title	Cyber Security
Level	4
Unit Number	10
GLH	10

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand the role of UK legislation and regulation in Cyber Security and the concept of Confidentiality, Integrity, and Availability (CIA)	1.1	Explain key elements of legislation relevant to digital security	Including: • Computer Misuse Act • Digital Online Resilience Act • UK Artificial Intelligence Act • Communications Act • Network and Information Systems Regulations 2018 • The Privacy and Electronic Communications Regulation 2003
	1.2	Describe the concept of Confidentiality, Integrity and Availability	Election Security Spotlight – CIA Triad
2. Understand the basics of malware	2.1	Describe common types of malware and their functions	Including: • Viruses • Worms • Trojans • Botnets
	2.2	Identify how malware can get into a computer	Human/technical factors
	2.3	Identify common techniques used by threat actors	Including: • Phishing • Spam

			• Spoofing • Click-fraud • Identity theft
	2.4	Describe anti-malware defences	Including: • Anti-virus software (signature and heuristics) • Zero-day vulnerabilities • Sandboxes • Code signing
	2.5	List the vulnerabilities associated with 'End of Life' software	
3. Understand the basics of the internet	3.1	Analyse the function of the internet with a focus on the Transmission Control Protocol/Internet Protocol (TCP/IP)	To include: • Its role in data transmission • Network communication • Packet management
	3.2	Identify how datagrams/packets work	
	3.3	Describe key principles of wireless local area networks	Including risks associated with: • Wi-Fi hotspots • Packet sniffing • Man-in-the-middle attacks
	3.4	Identify the principles of encryption as a method to secure data transmission	
4. Understand the basics of cryptography	4.1	Identify the principles of cryptography	Define: • Plaintext • Ciphertext • A cipher • Encryption • Decryption

	4.2	Describe encryption keys and the vulnerability posed by short keys	
	4.3	Identify the principles of asymmetric (or public key) cryptography	
	4.4	List the principles of secure web browsing	
5. Understand how to protect data on the network	5.1	Describe the basic principles of networks, with a focus on the roles of firewalls and Virtual Private Networks (VPNs)	
	5.2	Identify the principles and vulnerabilities of Network Intruder Detection Systems (NIDS) and Host Intruder Detection Systems (HIDS)	
6. Understand the impact when cyber defences fail	6.1	Identify how data loss occurs (via a network/insider)	
	6.2	Identify the consequences of a data loss	This could include: • cost of recreating the lost data • purchasing new hardware/software • cost of continuing without the data (availability) • the cost of informing others about the loss
7. Understand how authentication supports cyber security	7.1	Explain how cybersecurity measures support authentication and control access to organisational systems	• Authentication methods (e.g., passwords, multi-factor authentication, biometrics) • The role of good password practices, including the use of salting and hashing (e.g., 2fA + MFA) • Role of access control policies and techniques (e.g., role-based access control, least privilege)

	7.2	Explain how hashing and salting work together to protect passwords in transit and mitigate the risk of theft	
	7.3	Describe what a 'Brute Force Attack' is and its implications for password security	
8. Be able to assess and mitigate vulnerabilities in organisational assets to protect data confidentiality, integrity, and availability	8.1	Assess and review identified vulnerabilities in organisational assets that could be exploited by malware	
	8.2	Implement mitigations to safeguard the confidentiality, integrity, and availability of data	
	8.3	Design and implement strategies to prevent data loss within organisations	
	8.4	Apply organisational cybersecurity approaches for authentication and access control	Incorporating best practices for password security and mitigating potential attack vectors

Additional information about the unit	
Delivery Guidance	This unit introduces key UK cyber security legislation, such as the Computer Misuse Act and Network and Information Systems Regulations. It also covers core cyber security concepts like Confidentiality, Integrity, and Availability (CIA), malware types, internet functionality, and cryptography basics. As well as this, learners will also gain an understanding of network protection tools and good authentication practices, including hashing, salting, and multi-factor authentication. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.
Assessment Guidance	Assessment for this unit could involve a written report analysing cyber security threats and legislation, alongside practical exercises to identify network vulnerabilities and develop data protection strategies. Learners could also create a mitigation plan addressing data loss prevention, password security, and authentication best practices, demonstrating a solid understanding of protecting organisational data against cyber threats. A combination of practical and knowledge-based assessment methods should be used.

Links	• Intro to Cyber Security - Online Cyber Security Course - FutureLearn • National Cyber Security Centre - NCSC.GOV.UK

Title	Incident Response and Management		
Level	4		
Unit Number	11		
GLH	5		
Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand incident response and management	1.1	Describe the principles of incident response	Respond & recover - NCSC.GOV.UK
	1.2	Identify escalation and activation phases of incident response	
	1.3	Describe incident management	
	1.4	Identify how command, control, coordination and communication integrate during incident management	
2. Be able to assess and enhance Incident Response and Incident Management plans to improve organisational resilience	2.1	Review Incident Response and Incident Management plans to identify areas for improved efficiency	
	2.2	Implement adjustments to Incident Response and Incident Management plans that contribute to overall organisational resilience	
Additional information about the unit			
Delivery Guidance	This unit introduces learners to the fundamentals of incident response, covering principles such as escalation and activation phases. Learners will also gain an understanding of effective incident management, focusing		

	on command, control, coordination, and communication integration as well as developing the ability to review incident response and management plans. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.
Assessment Guidance	Assessment for this unit could include a written analysis of incident response principles, alongside a practical exercise where learners outline and evaluate an incident management plan. A combination of practical and knowledge-based assessment methods should be used.
Links	• Incident Management | NPSA • JESIP

Title	Investigations		
Level	4		
Unit Number	12		
GLH	10		
Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand how to gather and grade information to be used in investigations	1.1	Identify and access appropriate sources of information on incidents to be investigated promptly	• Investigation & Disciplinary | NPSA • Acas guide to conducting workplace investigations | Acas
	1.2	Identify how to obtain information by lawful means	
	1.3	Describe how to gather corroborative information where necessary to support investigations	
	1.4	Explain how to grade information correctly according to its usefulness and reliability	
	1.5	Identify how to gather sufficient information on which to develop an investigation	
	1.6	Describe how to handle and store information in a way which protects its confidentiality and evidential value	
2. Understand how to process information	2.1	Describe the process of establishing patterns and links in relevant information through analysis	
	2.2	Explain the process of identifying potential suspects	

	2.3	List how to record details of information accurately, completely and in approved formats	
	2.4	Explain why investigators should follow up the results of analysis of information promptly including passing on to the appropriate person	
3. Understand how to use digital technology to support investigations and inform decision-making processes	3.1	Explain how digital technology can be used to gather and analyse information in investigations	
	3.2	Explain how digital tools assist in making informed decisions based on investigation outcomes	
4. Understand how to make recommendations, based on processed information, for further investigation	4.1	Determine the need for evidence relevant to the incident or irregularity, based on analysis of available information	
	4.2	Explain how to maintain the security and confidentiality of details for investigation recommendations	
	4.3	Identify how to make presentations of recommendations to the appropriate person accurately, fully and within agreed timescales	
5. Be able to analyse and assess information for investigations	5.1	Analyse information collected from investigations to provide informed recommendations for decision-making	
	5.2	Assess information gained through digital technology to inform decisions	

	5.3	Demonstrate effective reporting methods in accordance with organisational procedures	

Additional information about the unit	
Delivery Guidance	This unit introduces the principles of gathering and grading information for investigations, with emphasis on lawful information acquisition and maintaining evidential integrity. The unit also covers information analysis, focusing on establishing links, identifying suspects, and documenting findings accurately as well as following up on analysis outcomes and making evidence-based recommendations. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required. Learners should ensure they are referring to their organisational policies where relevant.
Assessment Guidance	Assessment for this unit could include a written exercise where learners identify sources and demonstrate lawful information gathering techniques. Learners could also present investigation findings and recommendations, ensuring confidentiality and clarity in communication to relevant stakeholders. A combination of practical and knowledge-based assessment methods should be used.

Title	Security as a Business Enabler
Level	4
Unit Number	13
GLH	6

Learning Outcomes *The learner will:*	Assessment Criteria *The learner can:*		Guidance and/or Indicative Content
1. Understand how to demonstrate a Return on Security Investment (ROSI)	1.1	Identify the methods used to produce a ROSI (Return On Security Investment) which aligns to own organisations aims and objectives	Return on Security Investment (ROSI)
	1.2	Identify the method used to create a Cost Benefit Analysis	Cost Benefit Analysis
2. Understand how protective security can support organisational resilience	2.1	Explain how to influence senior leaders through protective security decision making	Protective Security Risk Management PSRM | NPSA
	2.2	Explain the principles of influencing techniques used to achieve goals and objectives	Influencing Techniques
	2.3	Describe the concept of organisational resilience	BCI Resilience Framework 1.0 – What are the universal core principles? | BCI
	2.4	Explain how organisational resilience can be supported by good protective security	Protective Security Risk Management PSRM | NPSA
	2.5	Explain how protective security and business continuity management support each other	• Business Continuity Management • Protective Security Risk Management PSRM | NPSA • The Business Continuity Institute (BCI) | A global institute for business continuity and resilience | BCI

	2.6	Identify the associated benefits of Organisational Learning	Organisational Learning
3. Understand how protective security can support sustainability	3.1	Describe how the effective planning, and use of security rated products contributes to organisational sustainability	Prior learning within this qualification
	3.2	Explain how incorporating sustainable practices in protective security measures can reduce environmental impact	Sustainability and climate change
4. Be able to provide strategic recommendations to senior leadership, applying organisational learning and sustainable practices to enhance protective security and resilience	4.1	Provide strategic recommendations to senior leadership to enhance protective security measures	
	4.2	Apply organisational learning to strengthen protective security and improve resilience	
	4.3	Apply influencing techniques to achieve goals and objective	
	4.4	Integrate sustainable practices into the design of security mitigations	

Additional information about the unit	
Delivery Guidance	This unit introduces the concept of Return on Security Investment (ROSI) and its role in aligning security measures with organisational goals. Learners will also gain an understanding of using protective security to support resilience and business continuity as well as the importance of sustainability. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.
Assessment Guidance	Assessment could include a written analysis where learners outline methods for calculating ROSI and performing a cost-benefit analysis. Learners could also complete a practical task, making recommendations to senior leadership on security measures that enhance resilience and align with sustainability objectives. A combination of practical and knowledge-based assessment methods should be used.

Title	Effective Communication and Reflective Practice for Professional Development
Level	4
Unit Number	14
GLH	6

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Be able to communicate effectively, report in line with organisational procedures, and engage in self-reflection and professional development to enhance practice	1.1	Evaluate the benefits of using a recognised model of reflection	Reflective Practice
	1.2	Describe how continuous professional development can support career progression	CPD
	1.3	Apply techniques to manage challenging communications, adapting language and style to suit the situation and audience	• Communication Styles • Conflict Management
	1.4	Present information to different audiences using strategies that enhance clarity and understanding of the intended purpose	• Communication Styles • Presentation Styles
	1.5	Apply logical thinking and problem-solving tools and techniques to identify issues and propose effective solutions	Logical Thinking
	1.6	Engage in self-reflection, seek feedback, and participate in professional development activities to improve personal practice	

Additional information about the unit

Delivery Guidance	This unit introduces learners to recognised models of reflection and helps them understand how reflective practice supports personal growth and learning. The unit also covers Continuous Professional Development (CPD) in career advancement and the importance of setting personal development goals. To deliver this unit a range of both theoretical and practical activities should be used to allow learners to fully understand the knowledge and skills required.
Assessment Guidance	Assessment could include a reflective essay where learners evaluate the benefits of using a model of reflection and outline a personal CPD plan. Learners could also engage in a practical exercise involving self-reflection and feedback, identifying areas for improvement and setting actionable goals to enhance their professional practice. A combination of practical and knowledge-based assessment methods should be used.

4. Centre Requirements

4.1. Centre Responsibilities

Centres must be approved by SFJ Awards and also have approval to deliver the qualifications they wish to offer. This is to ensure centres have the processes and resources in place to deliver the qualifications. Approved centres must adhere to the requirements detailed in the SFJ Awards Centre Handbook, which includes information for centres on assessment and internal quality assurance processes and procedures

When a centre applies to offer a qualification, they will need to provide evidence that they have sufficient resources and infrastructure in place for delivery of that qualification:

- evidence of assessor and IQA competence
- sample assessment materials and mark schemes
- scheme of work
- details of available resources.

Centres are responsible for ensuring that their assessor and internal quality assurance staff:

- are occupationally competent and/or knowledgeable as appropriate to the assessor or IQA role they are carrying out
- have current experience of assessing/internal quality assuring as appropriate to the assessor or IQA role they are carrying out
- have access to appropriate training and support
- are independent and any conflicts of interests are managed and monitored appropriately by SFJ Awards.

Information on the induction and continuing professional development of those carrying out assessment and internal quality assurance must be made available by centres to SFJ Awards through the external quality assurance process.

This handbook should be used in conjunction with the following SFJ Awards documents:

- Assessment Guidance
- Centre Handbook
- Centre Assessment Standards Scrutiny (CASS) Strategy
- Conflict of Interest Policy
- Whistleblowing Policy
- Malpractice and Maladministration Policies
- Equality and Diversity Policy
- Appeals Policy
- Complaints Policy
- Sanctions Policy
- Examinations and Invigilation Policy
- Risk and Centre Monitoring Policy
- Fair Access and Equality of Opportunity Policy
- Reasonable Adjustment and Special Considerations Policy
- Standardisation Policy
- Direct Claims Policy
- Centre Approval Process

All documents referenced in the strategy are available to centres on Odyssey, SFJ Awards learner management system, or on request from SFJ Awards.

4.2. Centre Assessment Standards Scrutiny (CASS) Strategy

Awarding Organisations are required by Ofqual to have a CASS Strategy in place to improve the controls where an assessment is devised and marked by a centre.[2] In line with our CASS Strategy, SFJ Awards will determine the most appropriate CASS approach for each qualification / qualification suite using a risk-based approach.

Any Subject Matter Experts (SMEs) used by centres to develop and/or mark assessments must declare any conflict of interest and centres must ensure that any such conflicts are mitigated. All details of such conflicts of interest must be recorded by the centre.

SFJ Awards will require sample assessments from centres to maintain confidence with our centres' approach to maintaining the integrity of our quality assurance strategy defined within the CASS strategy. Centre marking will be subject to external quality assurance.

Centres are permitted to develop and mark assessments for the qualification(s) in this handbook, in line with our CASS Strategy.

4.3. Facilities

Training and assessment for approved qualifications must take place in a suitable environment that has been approved by SFJ Awards. The environment must be adequately equipped for training, conducive to effective learning, and must comply with current Health and Safety requirements. Equipment for practical activities must be readily available and fit for purpose. All examination venues must comply with the policy, standards, and regulations specified by SFJ Awards to gain approval for knowledge-based assessment.

Training and assessment facilities must comply with the ongoing approval arrangements of SFJ Awards.

4.4. Trainers

Some sectors specify trainer requirements for qualification delivery, for example first aid and security. Details of any specific trainer requirements are included in this qualification handbook. Centres should therefore check the handbook, or with SFJ Awards, for any trainer requirements that apply to the qualification(s) they wish to deliver. Centres applying for approval with SFJ Awards will be required to provide SFJ Awards with current evidence of how each trainer meets the requirements, for example certificates of achievement, CV or CPD records.

[2] Condition H2 - Centre Assessment Standards Scrutiny where an assessment is marked by a Centre

5. Assessment

5.1. Qualification Assessment Methods

Assessment methods[3] that can be used for the SFJ Awards Level 4 Certificate for Protective Security Advisers are as follows:

- Aural Examination
- E-assessment
- Multiple Choice Examination
- Portfolio of Evidence (including for example records of professional discussions, question and answer sessions, work products)
- Practical Demonstration / Assignment
- Practical Examination
- Task-based Controlled Assessment
- Written Examination
- Observation
- Professional Discussion
- Interview
- Presentation and Questioning
- Project

5.2. Assessing Competence

The purpose of assessing competence is to make sure that an individual is competent to carry out the activities required in their work.

Assessors gather and judge evidence during normal work activities to determine whether the learner demonstrates their competence against the standards in the qualification unit(s). Competence should be demonstrated at a level appropriate to the qualification. The skills required at the different qualification levels are defined in Ofqual's level descriptors.[4] Further information on qualification levels is included in the SFJ Awards Assessment Guidance.

Evidence must be:

- Valid
- Authentic
- Sufficient
- Current
- Reliable

Assessment should be integrated into everyday work to make the most of opportunities that arise naturally within the workplace.

[3] Selected from assessment methods listed on Ofqual's regulatory system (Portal)
[4] Ofqual Handbook: General Conditions of Recognition, Section E - Design and development of qualifications www.gov.uk/guidance/ofqual-handbook/section-e-design-and-development-of-qualifications

5.3. Methods for Assessing Competence

Qualifications may be assessed using any method, or combination of methods, as stipulated either by SFJ Awards or within specific qualifications, and which clearly demonstrate that the learning outcomes and assessment criteria have been met. Some sectors may have specific assessment requirements that apply to their qualifications and where these apply, details will be included in the qualification-specific handbook.

Assessors need to be able to select the right assessment methods for the competences that are being assessed, without overburdening the learner or the assessment process, or interfering with everyday work activities. SFJ Awards expect assessors to use a combination of different assessment methods to make a decision about an individual's occupational competence. Assessment methods which are most likely to be used are outlined below. However, these are included for guidance only and there may be other methods which are suitable. Further information on assessment methods is included in the SFJ Awards Assessment Guidance.

5.3.1. Observation

SFJ Awards believe that direct observation in the workplace by an assessor or testimony from an expert witness is preferable as it allows for authenticated, valid and reliable evidence. Where learners demonstrate their competence in a real work situation, this must be done without the intervention from a tutor, supervisor or colleague.

However, SFJ Awards recognise that alternative sources of evidence and assessment methods may have to be used where direct observation is not possible or practical.

5.3.2. Testimony of Witnesses and Expert Witnesses

Witness testimonies are an accepted form of evidence by learners when compiling portfolios. Witness testimonies can be generated by peers, line managers and other individuals working closely with the learner. Witnesses are defined as being those people who are occupationally expert in their role.

Testimony can also be provided by expert witnesses who are occupationally competent **and** familiar with the qualification unit(s). Assessors will not need to spend as long assessing expert witness testimony as they would a witness testimony from a non-expert. Therefore, if expert witnesses are involved in the assessment strategy for a qualification a greater number of learners can be managed by a smaller number of assessors.

The assessor is however responsible for making the final judgement in terms of the learner meeting the evidence requirements for the qualification unit(s).

5.3.3. Work Outputs (Product Evidence)

Examples of work outputs include plans, reports, budgets, photographs, videos or notes of an event. Assessors can use work outputs in conjunction with other assessment methods, such as observation and discussion, to confirm competence and assure authenticity of the evidence presented.

5.3.4. Professional Discussion

Discussions allow the learner to describe and reflect on their performance and knowledge in relation to the standards. Assessors can use discussions to test the authenticity, validity and reliability of a learner's evidence. Written/audio records of discussions must be maintained.

5.3.5. Questioning the Learner

Questioning can be carried out orally or in written form and used to cover any gaps in assessment or corroborate other forms of evidence. Written/audio records of all questioning must be maintained.

5.3.6. Simulations

Simulations may take place in a non-operational environment which is not the learner's workplace, for example a training centre. The assessment guidance attached to each unit in section 3 of the handbook will specify where simulations are authorised. Please note that proposed simulations **must** be reviewed to ensure they are fit for purpose as part of the IQA's pre-delivery activity.

Simulations can be used when:

- the employer or assessor consider that evidence in the workplace will not be demonstrated within a reasonable timeframe
- there are limited opportunities to demonstrate competence in the workplace against all the assessment criteria
- there are health and safety implications due to the high-risk nature of the work activity
- the work activity is non-routine and assessment cannot easily be planned for
- assessment is required in more difficult circumstances than is likely to happen day to day.

Simulations must follow the principles below:

1. The nature of the contingency and the physical environment for the simulation must be realistic
2. Learners should be given no indication as to exactly what contingencies they may come across in the simulation
3. The demands on the learner during the simulation should be no more or less than they would be in a real work situation

4. Simulations must be planned, developed and documented by the centre in a way that ensures the simulation correctly reflects what the specific qualification unit seeks to assess and all simulations should follow these documented plans
5. There should be a range of simulations to cover the same aspect of a unit and they should be rotated regularly.

5.4. Assessing Knowledge and Understanding

Knowledge-based assessment involves establishing what the learner knows or understands at a level appropriate to the qualification. The depth and breadth of knowledge required at the different qualification levels are defined in Ofqual's level descriptors.[5] Further information on qualification levels is included in the SFJ Awards Assessment Guidance.

Assessments must be:

- Fair
- Robust
- Rigorous
- Authentic
- Sufficient
- Transparent
- Appropriate

Good practice when assessing knowledge includes use of a combination of assessment methods to ensure that as well as being able to recall information, the learner has a broader understanding of its application in the workplace. This ensures that qualifications are a valid measure of a learner's knowledge and understanding.

A proportion of any summative assessment may be conducted in controlled environments to ensure conditions are the same for all learners. This could include use of:

- Closed book conditions, where learners are not allowed access to reference materials
- Time bound conditions
- Invigilation.

Where assessment in controlled environments is considered appropriate for qualifications, or the use of specific assessment materials (for example, exemplars or scenarios) is required, information will be included in the qualification handbook.

5.5. Methods for Assessing Knowledge and Understanding

SFJ Awards expect assessors to use a variety of different assessment methods to make a decision about an individual's knowledge and understanding, which are likely to include a combination of the following:

a) Written tests in a controlled environment

[5] Ofqual Handbook: General Conditions of Recognition, Section E - Design and development of qualifications www.gov.uk/guidance/ofqual-handbook/section-e-design-and-development-of-qualifications

b) Multiple choice questions (MCQs)

c) Evidenced question and answer sessions with assessors

d) Evidenced professional discussions

e) Written assignments (including scenario-based written assignments).

Where written assessments are centre-devised and centre-assessed, centres must:

- maintain a sufficient bank of assignments which are changed regularly
- record how risks in tests/exams conducted in controlled environments are mitigated
- conduct assessments in line with SFJ Awards Examination and Invigilation Policy.

Centres must take into account the qualification when selecting knowledge assessment methods to ensure they are appropriate and allow the learner to evidence the assessment criteria. For example, MCQs are unlikely to be appropriate for higher levels qualifications or assessment criteria which require learners to 'explain', 'describe', 'evaluate' or 'analyse'.

5.6. Assessment Planning

Planning assessment allows a holistic approach to be taken, which focuses on assessment of the learner's work activity as a whole. This means that the assessment:

- reflects the skills requirements of the workplace
- saves time
- streamlines processes
- makes the most of naturally occurring evidence opportunities

Planning assessment enables assessors to track learners' progress and incorporate feedback into the learning process; assessors can therefore be sure that learners have had sufficient opportunity to acquire the skills and knowledge to perform competently and consistently to the standards before being assessed. The assessment is therefore a more efficient, cost-effective process which minimises the burden on learners, assessors and employers.

6. Assessor Requirements

6.1. Occupational Knowledge and Competence

Due to the risk-critical nature of the work, particularly when assessing in the public and security sectors, and the legal implications of the assessment process, assessors must understand the nature and context of the learners' work. This means that assessors must be occupationally competent. Each assessor must therefore be, according to current sector practice, competent in the functions covered by the unit(s) they are assessing. They will have gained their occupational competence by working within the sector relating to the unit(s) or qualification(s) they are assessing.

Assessors must be able to demonstrate consistent application of the skills and the current supporting knowledge and understanding in the context of a recent role directly related to the qualification unit(s) they are assessing as a practitioner, trainer or manager.

Where assessors are assessing knowledge-based qualifications, they must be occupationally knowledgeable in the sector they are assessing in.

Assessors for the SFJ Awards Level 4 Certificate for Protective Security Advisers **must** meet the following requirements:

- Hold a level 5 qualification or above in a security-related discipline OR an undergraduate degree in another discipline
- Hold a teaching qualification (examples: PTTLS, AET, PGCE)
- Have 5+ years' experience in the security and risk management domain
- Be a member of a related professional body, i.e. The Security Institute, CSyP or RSES
- Have an up-to-date record of CPD

6.2. Qualification Knowledge

Assessors must be familiar with the qualification unit(s) they are assessing. They must be able to interpret and make judgements on current working practices and technologies within the area of work.

6.3. Assessor Competence

Assessors must be able to make valid, reliable and fair assessment decisions. To demonstrate their competence, we expect assessors to be:

- qualified with a recognised assessor qualification, or
- working towards a recognised assessor qualification.

However, there may be circumstances when assessors have the equivalent competence through training to appropriate national standards, and SFJ Awards will agree this on a case-by-case basis.

Assessors' experience, knowledge and understanding could be verified by a combination of:

- curriculum vitae and employer endorsement or references

- possession of a relevant NVQ/SVQ, or vocationally related qualification
- corporate membership of a relevant professional institution
- interview (the verification process must be recorded and available for audit).

Recognised assessor qualifications include, but are not limited to:

- RQF/QCF Level 3 Award in Assessing Competence in the Work Environment
- RQF/QCF Level 3 Award in Assessing Vocationally Related Achievement
- RQF/QCF Level 3 Certificate in Assessing Vocationally Related Achievement
- An appropriate Assessor qualification in the SCQF as identified by SQA Accreditation
- A1 Assess candidates using a range of methods
- D32/33 Assess candidate performance, using differing sources of evidence.

Where assessors hold an older qualification e.g. D32/33 or A1, they must provide evidence of Continuing Professional Development (CPD) to demonstrate current competence.

Assessors must hold an assessor qualification, or equivalent competence if agreed by SFJ Awards, relevant to the type of qualification(s) they are assessing e.g.

- Level 3 Award in Assessing Competence in the Work Environment:
  For assessors who assess **competence in a work environment**, which requires the use of the following assessment methods: observation, examining work products or outputs, oral questioning, discussion, use of witness testimony, learner statements and Recognition of Prior Learning (RPL).
- Level 3 Award in Assessing Vocationally Related Achievement:
  For assessors who assess **knowledge and/or skills in vocationally related areas** using the following assessment methods: tests of skills, oral questioning, written questions, case studies, assignments, projects and RPL.

To be able to assess both knowledge and competence-based qualifications, new assessors should be working towards the **Level 3 Certificate in Assessing Vocational Achievement.**

Centres must have in place a procedure to ensure that their trainee assessors have a representative sample of their assessment decisions counter signed by a qualified and competent assessor. SFJ Awards will provide centres with guidance on the ratio of qualified/trainee assessors.

Trainee assessors working towards a qualification must be registered for the qualification with a regulated AO and achieve it within 18 months. Assessor competence will be checked through annual External Quality Assurance checks.

Centres must check the qualification handbook for assessor requirements for the qualification(s) they are approved to deliver as some sectors have different requirements e.g. security, education and training, assessor and quality assurance, and learning and development.

Centres applying for approval with SFJ Awards will be required to provide SFJ Awards with current evidence of how each assessor meets these requirements, for example certificates of achievement. Centres who apply for approval to offer additional qualifications will be required to provide evidence of assessor competence for the qualifications they wish to offer.

6.4. Continuing Professional Development

Assessors must actively engage in continuous professional development activities to maintain:

- occupational competence and knowledge by keeping up-to-date with the changes taking place in the sector(s) for which they carry out assessments
- professional competence and knowledge as an assessor.

It is the centre's responsibility to retain the CPD information of assessors. Assessor competence and CPD will be checked by External Quality Assurers at the centre's annual compliance visit.

7. Internal Quality Assurer Requirements

7.1. Occupational Knowledge

Internal quality assurers (IQAs) must be occupationally knowledgeable across the range of units for which they are responsible prior to commencing the role. Due to the risk-critical nature of the work, particularly in the justice, community safety and security sectors, and the legal implications of the assessment process, they must understand the nature and context of the assessors' work and that of their learners. This means that they must have worked closely with staff who carry out the functions covered by the qualifications, possibly by training or supervising them, and have sufficient knowledge of these functions to be able to offer credible advice on the interpretation of the units.

IQAs for the SFJ Awards Level 4 Certificate for Protective Security Advisers **must** meet the following requirements:

- Hold a level 5 qualification or above in a security-related discipline OR an undergraduate degree in another discipline
- Have 5+ years' experience in the security and risk management domain
- Be a member of a related professional body, i.e. The Security Institute, CSyP or RSES
- Have an up-to-date record of CPD
- Hold or be working towards an IQA Qualification

7.2. Qualification Knowledge

IQAs must understand the content, structure and assessment requirements for the qualification(s) they are internal quality assuring.

Centres should provide IQAs with an induction to the qualifications that they are responsible for quality assuring. IQAs should also have access to ongoing training and updates on current issues relevant to these qualifications.

7.3. Internal Quality Assurer Competence

IQAs must occupy a position in the organisation that gives them the authority and resources to:

- coordinate the work of assessors
- provide authoritative advice
- call meetings as appropriate
- conduct pre-delivery internal quality assurance on centre assessment plans, for example, to ensure that any proposed simulations are fit for purpose
- visit and observe assessment practice
- review the assessment process by sampling assessment decisions
- ensure that assessment has been carried out by assessors who are occupationally competent, or for knowledge-based qualifications occupationally knowledgeable, in the area they are assessing
- lead internal standardisation activity
- resolve differences and conflicts on assessment decisions

To demonstrate their competence, IQAs must be:

- qualified with a recognised internal quality assurance qualification, or
- working towards a recognised internal quality assurance qualification.

Recognised IQA qualifications include, but are not limited to:

- RQF/QCF Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practice
- RQF/QCF Level 4 Certificate in Leading the Internal Quality Assurance of Assessment Processes and Practice
- An appropriate IQA qualification in the SCQF as identified by SQA Accreditation
- V1 Conduct internal quality assurance of the assessment process
- D34 Internally verify the assessment process.

Where IQAs hold an older qualification e.g. D34 or V1, they must provide evidence of Continuing Professional Development (CPD) to demonstrate current competence. Approved centres will be required to provide SFJ Awards with current evidence of how each IQA meets these requirements, for example certificates of achievement.

Centres must have in place a procedure to ensure that their trainee IQAs have a representative sample of their IQA decisions counter signed by a qualified IQA who holds a minimum of the **Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practice**. SFJ Awards will provide centres with guidance on the ratio of qualified/trainee assessors.

Trainee IQAs working towards one of the above qualifications must be registered for the qualification with a regulated AO and achieve it within 18 months. IQA competence will be checked through annual External Quality Assurance checks.

7.4. Continuing Professional Development

IQAs must actively engage in continuous professional development activities to maintain:

- occupational knowledge by keeping up-to-date with the changes taking place in the sector(s) for which they carry out assessments
- professional competence and knowledge as an IQA.

8. Expert Witnesses

Expert witnesses, for example line managers and supervisors, can provide evidence that a learner has demonstrated competence in an activity. Their evidence contributes to performance evidence and has parity with assessor observation. Expert witnesses do not however perform the role of assessor.

8.1. Occupational Competence

Expert witnesses must, according to current sector practice, be competent in the functions covered by the unit(s) for which they are providing evidence.

They must be able to demonstrate consistent application of the skills and the current supporting knowledge and understanding in the context of a recent role directly related to the qualification unit that they are witnessing as a practitioner, trainer or manager.

8.2. Qualification Knowledge

Expert witnesses must be familiar with the qualification unit(s) and must be able to interpret current working practices and technologies within the area of work.

9. External Quality Assurers

External quality assurance is carried out by SFJ Awards to ensure that there is compliance, validity, reliability and good practice in centres. External quality assurers (EQAs) are appointed by SFJ Awards to approve centres and to monitor the assessment and internal quality assurance carried out by centres.

SFJ Awards are responsible for ensuring that their external quality assurance team have:

- sufficient and appropriate occupational knowledge
- current experience of external quality assurance
- access to appropriate training and support.

9.1. External Quality Assurer Competence

To demonstrate their competence, EQAs must be:

- qualified with a recognised external quality assurance qualification, or
- working towards a recognised external quality assurance qualification

Relevant qualifications include:

- Level 4 Award in the External Quality Assurance of Assessment Processes and Practice
- Level 4 Certificate in Leading the External Quality Assurance of Assessment Processes and Practice

Trainee EQAs working towards one of the above qualifications must be registered for the qualification with a regulated AO and aim to achieve it within 18 months. Whilst working towards a qualification, trainee EQAs will be supported by qualified EQA and receive training, for example by shadowing the EQA on compliance visits. EQA competence will be checked and monitored by SFJ Awards.

9.2. Continuing Professional Development

EQAs must maintain their occupational and external quality assurance knowledge. They will attend training and development designed to keep them up-to-date, facilitate standardisation between staff and share good practice.

10. Standardisation

Internal and external standardisation is required to ensure the consistency of evidence, assessment decisions and qualifications awarded over time.

10.1. Internal Standardisation

IQAs should facilitate internal standardisation events for assessors to attend and participate, in order to review evidence used, make judgments, compare quality and come to a common understanding of what is sufficient.

10.2. External Standardisation

SFJ Awards will enable access to external standardisation opportunities for centres and EQAs over time.

Further information on standardisation is available in the SFJ Awards Quality Assurance (Internal and External) Guidance and the SFJ Awards Standardisation Policy.

11. Recognition of Prior Learning (RPL)

Recognition of prior learning (RPL) is the process of recognising previous formal, informal or experiential learning so that the learner avoids having to repeat learning/assessment within a new qualification. RPL is a broad concept and covers a range of possible approaches and outcomes to the recognition of prior learning (including credit transfer where an Awarding Organisation has decided to attribute credit to a qualification).

The use of RPL encourages transferability of qualifications and/or units, which benefits both learners and employers. SFJ Awards support the use of RPL and centres must work to the principles included in Section 6 Assessment and Quality Assurance of the SFJ Awards Centre Handbook and outlined in SFJ Awards Recognition of Prior Learning Policy.

12. Equality and Diversity

Centres must comply with legislation and the requirements of the RQF relating to equality and diversity. There should be no barriers to achieving a qualification based on:

- Age
- Disability
- Gender reassignment
- Marriage and civil partnership
- Pregnancy and maternity
- Race
- Religion or belief
- Sex
- Sexual orientation

Reasonable adjustments are made to ensure that learners who are disabled or who have additional learning needs are not disadvantaged in any way. Learners must declare their needs prior to the assessment and all necessary reasonable adjustment arrangements must have been approved by SFJ Awards and implemented before the time of their assessment.

All cases where reasonable adjustment has been used must be fully documented, made available for external quality assurance and retained for a minimum of 3 years.

Further information is available in the SFJ Awards Reasonable Adjustments and Special Considerations Policy and the SFJ Awards Equality of Opportunity Policy.

SFJ Awards will conduct Equality Impact Assessments in the design and development of qualifications to minimise as far as possible any impact on learners with a protected characteristic, disability or additional learning needs.

13. Health and Safety

SFJ Awards are committed to safeguarding and promoting the welfare of learners, employees and volunteers and expect everyone to share this commitment.

SFJ Awards foster an open and supportive culture to encourage the safety and well-being of employees, learners and partner organisations to enable:

- learners to thrive and achieve
- employees, volunteers and visitors to feel secure
- everyone to feel assured that their welfare is a high priority.

Assessment of competence-based qualifications in some sectors can carry a high-risk level due to the nature of some roles. Centres must therefore ensure that due regard is taken to assess and manage risk and have procedures in place to ensure that:

- qualifications can be delivered safely with risks to learners and those involved in the assessment process minimised as far as possible
- working environments meet relevant health and safety requirements.

Copyright

SFJ Awards
Consult House
4 Hayland Street
Sheffield S9 1BY
Tel: 0114 284 1970
sfjawards.com