Standard Draft Preview

Standard in development
L4: Protective Security Adviser
Version 0.0

Title of occupation

Protective Security Adviser

UOS reference number

ST1401

Core and options

No

Level of occupation

Level 4

Occupational maps data

Route: Protective services
Pathway: Protective Services
Cluster: Protective service manager

Typical duration of apprenticeship

18 months

Does professional recognition exist for the occupation?

No

Regulated occupation

Is this a statutory regulated occupation?

No

Occupation summary

This occupation is found in the public and private sectors and focuses on the mitigating actions/policies required to meet prevailing threats and protect assets from compromise across the enterprise using a combination of physical security; personnel security; technical security and cyber security. This occupation is found in every organisation that holds assets of value that require protection. An asset is anything with value, tangible or intangible, in need of protection, and which can include but not be exclusive to People- employees, contractors, visitors and communities; Physical – property and items of value that can be seen, touched or held; Information - data bases, financial data, research, trade secrets and intellectual property; Processes and Systems - anything that enables the enterprise to function. These groupings can be further broken down into tangible assets (buildings, equipment, raw materials); intangible assets (intellectual property, contracts, copyrights, reputation) or mixed assets (individuals and their knowledge, physical assets that contain intangible assets.) The range of sectors that this occupation applies to includes all Critical National Infrastructure (CNI) sectors: Chemicals; Civil Nuclear; Communications; Defence; Emergency Services; Energy; Finance; Food; Government; Health; Space; Transport; Water and Supply chains of these sectors. This occupation also applies to (but is not exclusive to) the following sectors: Construction; Property management; Science/Technology centres; Academia; Retail; Tourism; Stadia and sporting arenas; Hotels and hospitality; Events sector and Night-time economy.

The broad purpose of the occupation is to protect assets from identified threats by assessing protective security risks and developing mitigations to reduce these risks. This may comprise, amongst other things, the deployment of security personnel, conditioning of enterprise personnel to ensure a positive security culture, target hardening, use of technology and policies and procedures to mitigate the identified threats and associated risks. In essence the apprenticeship will enable delegates to develop an understanding of an organisation's assets, the threats they face and assessment of the risk this poses. This apprenticeship will then support delegates to then develop plans to mitigate these risks and implement security measures, with a review process which provides continuous improvement. The occupation will provide delegates with the fundamentals of protective security and lay the foundations towards 'security convergence'. Protective security is a combination of the four security disciplines of personnel, physical, cyber and technical security. Protective security is where all four disciplines have been considered together to ensure threats that seek to find gaps between the disciplines cannot be exploited. This is often referred to as security convergence. The Government Functional Standard GovS 007: Security, describes the purpose of each of the protective security disciplines: Physical Security: The purpose of physical security measures is to ensure a safe and secure working environment for staff and visitors, protecting them against a wide range of threats (including theft, terrorism and espionage). Personnel Security: The purpose of personnel security is to assure organisations that the people it employs are suitable for work in sensitive roles. It also safeguards employees from exploitation as a result of their personal circumstances. Technical Security: The purpose of technical security measures is to holistically protect sensitive information and technology from close access acquisition or exploitation by hostile actors, as well as any other form of technical manipulation. Cyber Security: The purpose of cyber security is to ensure the security of data and information.

In their daily work, an employee in this occupation interacts with a variety of internal and external stakeholders as protective security practitioners do not work alone, with the focus on security being a business enabler. To achieve this protective security practitioners, need

to work with a wide range of stakeholders within a business to ensure business needs are met and externally to support and work with partners and the communities they are based in. In the role of the Protective Security Adviser they will be expected to communicate effectively and provide protective security briefings and subject matter expertise to mitigate protective security risks to a wide variety of stakeholders. Such stakeholders may include: senior risk owners; employees; customers; suppliers; distributors; enterprise risk management (ERM) professionals; corporate threat/intelligence analysts; business continuity/resilience professionals; business development management; information security officers; human resource departments; health and safety professionals; physical security teams; 3rd party supply; chains; Police/law enforcement; community representatives; and the National Technical Authorities i.e. National Protective Security Authority (NPSA), UK National Authority for Counter Eavesdropping (NACE) and National Cyber Security Centre (NCSC).

An employee in this occupation will be responsible for the identification of security vulnerabilities to enable organisations to provide a converged security and risk mitigation approach employing National Technical Authority (NTA) guidance. This may include developing asset registers; records of threat actors and potential threat vectors employed against organisational assets; vulnerability assessments; security risk assessments (SRA); protective security mitigations; protective security risk registers; protective security planning and review and assurance processes.

Typical job titles

Deputy security adviser, Security adviser, Security consultant, Security contract manager, Security manager, Security officer, Security practitioner, Security specialist, Security supervisor

Are there any statutory/regulatory or other typical entry requirements?

No

Occupation duties

DUTY	KSBS
Duty 1 Identify and assess assets and their criticality.	K7 K10 K12 K14 K18 K19 K20 K21 K22 K23 K27 K29 K30 K32 K34 K37 K41 K42 K43 K44 K45 K46 K47 K50 K53 K56 K58 K59 S1 S3 S4 S5 S7 S8 S15 S16 S18 S19 S20 S21 S23 S28 S29 S30 S31 S32 B1 B2 B3 B4
Duty 2 Evaluate the range of threat actors and potential threat vectors employed against organisational assets.	K3 K7 K11 K12 K13 K14 K18 K19 K20 K21 K22 K23 K25 K26 K27 K28 K29 K30 K31 K32 K33 K34 K35 K36 K38 K39 K40 K41 K42 K43 K44 K45 K46 K47 K49 K50 K53 K56 K58 K59 S1 S3 S4 S5 S7 S8 S9 S10 S15 S16 S18 S19 S20 S21 S23 S28 S29 S30 S31 S32 B1 B2 B3 B4
Duty 3 Conduct Security Risk Assessments (SRA).	K1 K3 K4 K5 K7 K8 K10 K11 K12 K14 K15 K16 K18 K19 K20 K21 K22 K23 K24 K25 K26 K27 K28 K29 K30 K32 K33 K34 K35 K36 K37 K38 K41 K42 K43 K44 K45 K46 K47 K49 K50 K53 K56 S1 S3 S4 S5 S6 S7 S8 S9 S10 S11 S12 S13 S14 S15 S16 S17 S18 S19 S20 S21 S23 S28 S29 S30 S31 S32 S33 B1 B2 B3 B4
Duty 4 Implement a security plan.	K1 K3 K5 K7 K8 K10 K11 K12 K14 K16 K17 K18 K19 K20 K21 K22 K23 K24 K25 K26 K27 K28 K29 K30 K31 K32 K33 K34 K35 K36 K37 K38 K47 K49 K50 K51 K52 K53 K56 S1 S2 S3 S4 S5 S6 S7 S8 S9 S10 S11 S12 S13 S14 S15 S16 S17 S18 S19 S20 S21 S22 S23 S27 S28 S29 S30 S31 S32 S33 B1 B2 B3 B4
Duty 5 Manage protective security mitigations.	K1 K3 K5 K7 K8 K10 K11 K12 K14 K16 K18 K19 K20 K21 K22 K23 K24 K25 K26 K27 K28 K29 K30 K32 K33 K34 K35 K36 K37 K38 K47 K49 K50 K51 K52 K53 K56 S1 S2 S3 S4 S5 S6 S7 S8 S9 S10 S11 S12 S13 S14 S15 S16 S17 S18 S19 S20 S21 S22 S23 S28 S29 S30 S31 S32 B1 B2 B3 B4
Duty 6 Maintain a protective security risk register.	K3 K4 K5 K6 K7 K10 K11 K12 K14 K15 K16 K17 K25 K26 K27 K29 K30 K32 K34 K37 K47 K49 K50 K53 K56 S1 S2 S3 S4 S5 S7 S8 S9 S10 S11 S12 S13 S14 S15 S16 S17 S18 S19 S20 S21 S22 S23 S28 S29 S30 S31 S32 B1 B2 B3 B4

DUTY	KSBS
Duty 7 Implement and maintain a review and assurance process.	K3 K5 K6 K7 K8 K10 K11 K12 K14 K16 K22 K23 K27 K29 K30 K32 K34 K35 K36 K37 K47 K48 K49 K50 K53 K55 K56 K58 K59 S1 S2 S3 S4 S5 S7 S8 S9 S10 S11 S12 S13 S14 S15 S16 S17 S18 S19 S20 S21 S22 S23 S24 S28 S29 S30 S31 S32 B1 B2 B3 B4
Duty 8 Develop and embed a healthy security culture.	K1 K7 K9 K10 K11 K12 K13 K14 K16 K25 K26 K27 K28 K29 K30 K31 K32 K33 K34 K35 K36 K37 K38 K44 K47 K49 K50 K53 K54 K56 K57 K59 S1 S3 S5 S7 S9 S10 S11 S15 S16 S18 S19 S20 S21 S22 S23 S24 S28 S29 S30 S31 S32 S33 B1 B3 B4
Duty 9 Provide briefings covering physical, personnel, technical and cyber security.	K3 K5 K6 K7 K9 K10 K11 K12 K13 K14 K16 K25 K26 K27 K29 K30 K31 K32 K33 K34 K35 K36 K37 K47 K49 K50 K53 K54 K56 K57 K58 K59 S1 S2 S3 S5 S7 S9 S10 S11 S15 S16 S18 S19 S20 S21 S22 S23 S25 S26 S28 S29 S30 S32 S34 B1 B2 B3 B4
Duty 10 Apply underpinning national technical authority advice to respond to dynamic security needs.	K2 K7 K10 K11 K12 K14 K16 K24 K25 K26 K27 K28 K29 K30 K31 K32 K33 K34 K35 K36 K37 K38 K39 K40 K41 K42 K43 K44 K45 K46 K47 K48 K49 K50 K53 K54 K55 K56 K57 K58 K59 S1 S2 S3 S5 S7 S8 S9 S10 S11 S12 S13 S14 S15 S16 S17 S18 S19 S20 S21 S22 S23 S25 S26 S28 S29 S30 S32 S33 S34 B1 B2 B3 B4
Duty 11 Manage stakeholder expectations and provide appropriate subject matter expertise to mitigate protective security risks.	K2 K4 K5 K6 K7 K9 K10 K11 K12 K14 K15 K16 K18 K19 K20 K21 K22 K23 K24 K25 K26 K27 K29 K30 K32 K33 K34 K35 K36 K37 K41 K42 K43 K44 K45 K46 K47 K48 K49 K50 K51 K52 K53 K54 K55 K56 K57 K58 K59 S1 S2 S3 S4 S5 S6 S7 S9 S10 S11 S15 S16 S17 S18 S19 S20 S21 S22 S23 S24 S25 S26 S27 S28 S29 S30 S32 S33 S34 B1 B2 B3 B4

KSBs

Knowledge

K1: Crime and security science theories and how they underpin protective security design to provide a layered security approach and why security matters to protect businesses and society: Routine Activity Theory, Rational Choice Theory, Offender Typologies, Crime Mapping, Broken Windows Theory, the security triangle of detection, response and delay, Situational Crime Prevention, Social Crime Prevention, adversary path analysis, Crime Prevention through Environmental Design and Defence in depth based on National Protective Security Authority (NPSA) deter, detect, delay, mitigate, respond principles.
K2: The protective security eco-system, the role played by key organisations and how each National Technical Authority (NTAs) contributes to the protective security of business and society: the Register of Security Engineering Specialists (RSES) and Chartered Security Professionals (CSyP).
K3: How the security convergence of the four main disciplines of protective services Cyber, Personnel, Physical and Technical can mitigate vulnerabilities of the siloed approach to security risk management.
K4: Importance of a single overview of risk for senior risk owners by employing security convergence.
K5: The main features and how to apply significant law to individual organisations: the Occupiers Liability, Health and Safety, Management of Health and Safety at Work Regulations, Fire Safety, Data Protection, the National Security Act, the National Security Investment Act, the Security Services Act, Common Law and Criminal Law, the Digital Online Resilience Act, UK AI Act, Communications Act, Computer Misuse Act, Data Protection Act, GDPR, Network and Information Systems Regulations, Privacy and Electronic Communications Regulation.
K6: Principles of good governance, governance structure and protective security oversight of cyber, physical, personnel and technical security including two-way communication channels, security risk registers, an accountable board level risk owner and structure for dissemination of information and decisions.
K7: The influence of organisational objectives and differing protective security approaches taken in the context of government, Critical National Infrastructure, multi-nationals, academia, start-ups and emerging technology.
K8: The requirements of ISO standards and their application in protective security.
K9: The challenges faced by individuals from diverse backgrounds, with differing social-economic and societal perceptions when seeking and interacting with colleagues and stakeholders.
K10: Principles of asset identification and classification: physical, information, people assets and anything that enables a business to operate e.g. a process, system, document or person and brand and reputation.
K11: The influence of intent and capability on threat actor actions.
K12: Information sources and the types of information of potential threats to security: the National Protective Security Authority (NPSA), National Cyber Security Centre (NCSC), UK National Authority for Counter Eavesdropping (UK NACE), National Counter Terror Security Office (NaCTSO), MI5, Police, local crime statistics and external stakeholders.
K13: Threat Intelligence Cycle and how to use threat assessments to conduct threat analysis based on a range of threat scenarios that organisations would potentially face based on their assets, services provided and locations.

K14: Principles of security risk management including how threat, vulnerability and impact determines the risk posed to an organisation, its assets and people and how mitigating threat, vulnerabilities and impact can be supported with protective security.
K15: The principles of quantitative, qualitative and semi-qualitative risk assessment methodologies to develop risk statements including threat actors, assets targeted, attack vectors used, and potential impact aligned to organisational assets, threat, vulnerability and impact.
K16: The concepts, main functions and benefits of security risk registers for governance, mitigations, risk tolerance and corporate memory and how they support the production of Operational Requirements.
K17: Common security standards to mitigate forcible attack vectors including Loss Prevention Standards (LPS) 1673, LPS 1178 Issue 8, NPSA Marauding Terrorist Attack Standard and NPSA Manual Forced Entry Standards (MFES).
K18: The main types of postal/courier attack vectors and mitigations and the principles of the PAS 97: 2021 Mail Screening and Security-Specification.
K19: The main types of glazing specification, glazing systems vulnerabilities and mitigation against forcible attack and blast.
K20: NPSA principles on threats to security posed by vehicles: Vehicle as a Weapon (VAW), Vehicle Borne Improvised Explosive Device (VBIED) and the Layered Vehicle Attack and the potential risk they provide to organisations, businesses and society and how ISO 22343-1: 2023 Vehicle security barriers supports building resilience for security threats with Hostile Vehicle Mitigation strategies.
K21: Methodology used by threat actors during marauding terrorist attacks and NPSA recommended measures to minimise the impact of Marauding Terrorist Attack to save lives.
K22: Principles of the NPSA Surreptitious Threat Mitigation Process (STaMP) employing NPSA Surreptitious Attack Protective Security Philosophy.
K23: Principles of the Cyber Assurance Physical Security Systems (CAPSS).
K24: Governmental, Independent and third-party certification of physical security products and standards e.g. NPSA Catalogue of Security Equipment (CSE), Redbook LIVE.
K25: How organisations can manage potential insider threat, insider risk and insider events: leadership, governance, pre-employment screening and vetting, ongoing personnel security, employee monitoring and assessment, investigation and disciplinary practices, an security culture with security focused behaviour embedding NPSA's 5 Es, effective and line management, organisational insider threat stakeholder group utilising the NPSA ten steps of insider risk assessment and isomorphic learning.
K26: How the threat landscape and societal challenges influence motivations and methods used by insiders and insider event typologies: unauthorised disclosure of sensitive information, process corruption, unauthorised provision of third-party access to organisational assets, financial gain through financial corruption and workplace violence.
K27: The integration of personnel, cyber, physical and technical security controls to mitigate insider risk.
K28: Principles of hostile reconnaissance and hostile planning stages, and how protective security can be used to disrupt hostile reconnaissance employing the principles of NPSA DENY, DETECT and DETER strategy and the integration of Security Minded Communications, See Check and Notify (SCaN) and Project Servator.
K29: The role individuals can play to ensure their personal security and safety when working for an organisation: personal situational awareness, online vigilance, maintain residential security, planning prior to travel, managing own digital footprint, protect sensitive information, follow organisational personal security emergency procedures.
K30: The principles of technical security and why and how organisations may be targeted.
K31: The required elements of a technical surveillance device.

K32: The principles of information egress via spatial, physical and conductive methods used during standoff and close access technical collection operations.
K33: How existing protective security may encourage threat actors to employ technical attack vectors.
K34: The convergence of physical, personnel and people security to mitigate standoff attacks and close access technical collection operations.
K35: The technical security attack vectors: overt access of visitors and contractors, commercial off the shelf 'quick plant' products, human interface devices, mobile telephones, smart devices, long lensing, drones, laser microphones and deep plant devices, 'man-in-the-middle', Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST) attacks, and lip-reading attack vectors.
K36: How to mitigate against technical attacks during 'overt access': quick plant devices, human interface devices, remote access trojans, international mobile subscriber Identification catchers, man-in-the-middle, vulnerabilities created by smart devices, long lensing, lip reading, drones, laser microphones and deep plants.
K37: The concept and applicability of Confidentiality, Integrity and Availability (CIA) for cyber security.
K38: The main features of malware and how they can get into a computer via human and technical factors.
K39: The threat vectors used by threat actor and mitigations: phishing, spam, spoofing, click-fraud and botnets and attacks on 'End of Life' software, anti-virus software, sandboxes and code-signing.
K40: The principles of how the internet works including Transmission Control Protocol (TCP), Internet Protocol (IP), how datagrams, packets work, and the principles of wireless Local Access Networks.
K41: The methods employed by threat actors to gain data including employing Wi-Fi hotspots, packet sniffing and man-in-the middle attacks.
K42: The principles of encryption, cryptography, asymmetric cryptography, encryption keys, secure web browsing, and methods to protect data on the network.
K43: The vulnerabilities of short encryption keys, and the Network Intrusion Detection Systems and Host Intruder Detection Systems.
K44: The consequences of common network security threats and insider threats on data loss: recreating lost data, purchasing new hardware, purchasing new software, cost of continuing without the available data, the cost involved with informing others of the data loss.
K45: How cyber security supports authentication and access to organisational systems including good password practice, salting in collaboration with hashing, use of hardware tokens.
K46: Attack vectors used including hashes and brute force attack.
K47: The principles of incident response and incident management.
K48: The principles of investigation for security incidents including gathering and grading information to be used in investigations, processing information and making recommendations for decision making.
K49: The principles of a Return on Security Investment (ROSI) and cost benefit analysis and its alignment with organisational aims and objectives and impact on security decision making.
K50: The concept of organisational resilience and learning and its interdependency with protective security to enable organisational resilience in a changing environment.
K51: The principles to promote sustainable working practices in protective security.

K52: How glazing systems can impact the carbon footprint of buildings: laminated glass, annealed/float glass, tough/tempered glass, heat strengthened glass, laminated glass sandwich and polycarbonate.
K53: The use of reflective practice theories and techniques to inform professional development of an individual and improve approaches to own practice and operational activities.
K54: Techniques for managing challenging communications using language and style that reflect the situation and audience.
K55: The use of digital technology to support investigations and assist decision making.
K56: Problem solving tools and techniques.
K57: Principles of influencing techniques to achieve goals and objectives.
K58: Methods for reporting, in accordance with organisational procedure.
K59: Presentation methods for different audiences using communication skills and strategies to maximise understanding of intended purpose.

Skills

S1: Utilise crime and security science knowledge and theory in the planning of organisational protective security to address protective security requirements and meet organisational needs.
S2: Apply the principles of security convergence to protective security planning.
S3: Comply with legislation, local and national policies and practice within limits of own role.
S4: Engage and influence the governance process to enable security risk decisions.
S5: Interpret organisational needs in the application of protective security.
S6: Follow ISO standards within limits of own role with consideration of the implications of non-compliance.
S7: Support individuals with differing social-economic and diverse backgrounds who are faced with challenges when interacting with colleagues and stakeholders.
S8: Produce asset registers for organisations, applying asset identification and classification principles.
S9: Produce 'Threat Analysis' based on an organisation's assets, services and location, applying asset identification and classification principles.
S10: Assess vulnerability and impact to the organisation within protective security risk documentation.
S11: Produce a security risk assessment.
S12: Develop physical security mitigations for forcible attack vectors.
S13: Develop physical security mitigations for surreptitious attack vectors.
S14: Utilise assured products to mitigate protective security risk.
S15: Develop measures to mitigate against organisational insider risk.
S16: Develop mitigations against hostile reconnaissance.
S17: Apply personal security and safety protocols in the work environment.
S18: Develop mitigations, using converged security, to mitigate technical security attack vectors.
S19: Develop mitigations for technical security attack vectors.
S20: Review identified vulnerabilities that could be exploited by malware in organisational assets to develop mitigations to protect confidentiality, integrity and availability of data.
S21: Develop mitigations to prevent data loss within organisations.
S22: Utilise organisational cyber security approaches for authentication and access with full consideration of password good practise mitigations and for potential attack vectors.

S23: Review Incident Response and Incident Management plans to ensure efficiency contributing to organisational resilience.
S24: Review information gathered through investigations to make recommendations for decision making.
S25: Make recommendations to senior leadership for protective security.
S26: Utilise organisational learning to enhance protective security and resilience.
S27: Incorporate sustainable practise when designing security mitigations.
S28: Engage in self-reflection, feedback and professional development activities to improve own professional practice.
S29: Manage challenging communications using language and style that reflect the situation and audience.
S30: Assess information gained through digital technology to inform decisions.
S31: Apply logical thinking and problem-solving tools and techniques, identifying issues and proposing solutions to problems.
S32: Apply influencing techniques to achieve goals and objectives.
S33: Follow organisational reporting protocols.
S34: Create and deliver presentations using communication skills and strategies to maximise understanding of intended purpose.

Behaviours

B1: Committed to supporting a strong security posture.
B2: Works independently and takes responsibility working diligently regardless of supervision levels.
B3: Effective time management.
B4: Embraces Equality, Diversity and Inclusion treating everyone with dignity and respect.

Qualifications

English and Maths

Does the apprenticeship need to include any mandated qualifications in addition to the above-mentioned English and maths qualifications?

No

Progression Routes

This apprenticeship provides a progression opportunity for those that have progressed through the Level 2 Professional Security Operative and/or Level 3 Security First Line Manager apprenticeships and onto academic and vocational qualifications on regulated frameworks: Level 4 Cyber Security Technologist, Level 6 Cyber Security Technical Professional (Integrated Degree).

Involved employers

Protective Security Centre, Linx International Group/Mitie, Canary Wharf Group, Arqiva, Securigroup, British Museum, City of London Police, Ineos UK Limited, Chubb Insurance, Corps Security, Travis Perkins plc, HM Revenues & Customs (HMRC), Department for Business and Trade, Department for Health and Social Care, Northern Ireland Office, Foreign, Commonwealth & Development Office (FCDO) Services, HM Treasury, Nuclear Waste Services, Gallagher Insurance, Department for Work and Pensions, Nuclear Waste Services, Canary Wharf Management Ltd, Dakin Security Services, Department of Health and Social Care, Government Legal Department, North East Regional Special Operations Unit, National Cyber Security Centre, Security Institute, Cabinet Office, National Protective Security Authority (NPSA), National Authority for Counter-Eavesdropping, Training and Development Unit Counter Terrorism, Home Office.

Subject sector area

1.4 Public services