BIIAB

Qualification Specification

BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6

Qualification Number: R667 04

BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6

Version and date	Change, alteration or addition	Section
Version 2, April 2021	Launch version	

Table of Contents

1. About the BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6

BIIAB Qualifications Limited is regulated to deliver this qualification by the Scottish Qualifications Authority (SQA). The qualification has a unique code which is shown below. The code will be displayed on the final certificate for the qualification.

Qualification Title	Code
BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6	R667 04

2. Objective and Purpose of this Qualification

The BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6 is designed to show that learners have obtained and can demonstrate the knowledge and skills required to be a Security Officer.

The primary purpose of the qualification is to confirm occupational competence. However, employers can also rely on the knowledge provided as meeting nationally recognised standards within security at this level. As such the sub-purpose is to confirm the ability to meet a 'licence to practise' or other legal requirements made by the relevant sector, professional or industry body.

Under the Private Security Industry Act 2001, all security officers must hold a licence to practise issued by the Security Industry Authority (SIA). Successful completion of this course enables a security officer to meet one of the requirements to apply for their licence.

Due to constant regulatory, policy and funding changes, users are advised to check this qualification is funded for use with individual learners before making registrations. If you are unsure about the qualification's status, please contact BIIAB Qualifications Limited head office.

3. About this Specification

This specification has been developed to provide guidance for learners, assessors and quality assurers undertaking, delivering, or quality assuring this qualification.

The purpose of the specification is to provide the majority of the key information that may be needed to prepare for, and help support, the successful delivery of the qualification, in one place.

If this specification is updated, centres will be notified by BIIAB Qualifications Limited.

4. BIIAB Qualifications Limited Customer Service

BIIAB Qualifications Limited is committed to giving the highest possible levels of customer service. BIIAB Qualifications Limited's Service Level Agreement is available via www.biiab.org.

Our Customer Service team can be contacted between the hours of 0900 and 1700 Monday to Friday by using the contact details below, or outside those hours, by leaving a message on our voicemail service.

Customer Service Contact Details: 01276 684449

Email: customersupport@bii.org

Our Customer Service team will be happy to assist with any administration related enquiries you may have. For example:

- registration and certification enquiries
- re-certification issues
- centres available in the local area
- appeals
- whistleblowing.

5. What are Rules of Combination?

Under the Regulatory Framework, qualifications can be made up of a combination of mandatory and/or optional units. The units and credits required to complete a qualification are set out by the rules of combination. These allow for flexibility and transferability.

The rules of combination will specify:

- The total credit value of the qualification
- The amount of credit that must be achieved within specific groupings of units (e.g. Mandatory, Optional Unit, and Optional groups)
- The minimum credit which must be achieved at the level or above the level of the qualification
- The Total Qualification Time (TQT)
- The title, Unit Regulation Number and BIIAB Qualifications Limited Unit number for each unit, alongside its level, credit, and Guided Learning Hours (GLH)
- Any barred units (units that cannot be taken together as part of the qualification).

When choosing the appropriate route for a learner or group of learners, it is the responsibility of the centre to ensure the rules of combination are adhered to.

6. BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6 Rules of Combination and Structure

To achieve the BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6, learners **must** complete all units within the qualification. This **must** consist of:

- Minimum total credit: **4**
- Mandatory Group A **minimum** number of units: **3**
- Minimum Guided Learning Hours: **38 hours**
- Total Qualification Time: **42 hours**

The qualification has been developed based upon industry feedback as to the fundamental knowledge and skills required to work in the sector at the level.

Listed overleaf are the qualification units.

BIIAB unit number	URN	Unit title	Credit	Level	Guided learning hours (total learning and assessment time)	SIA minimum contact time (hours)	SIA maximum permitted self-study time (hours)	Total time	Assessment method
PWPSI	UP11 04	Principles of Working in the Private Security Industry	2	2	17	9	8	17	Multiple-choice questions and practical assessment
PWSOPSI	UP16 04	Principles of Working as a Security Officer in the Private Security Industry	1	2	10	10	Not permitted	12	Multiple-choice questions and practical assessment
ACMIPSI	UP13 04	Application of Conflict Management in the Private Security Industry	1	2	11	11	Not permitted	13	Multiple-choice questions and practical assessment
				Total	**38 hours (minimum 5 days)**	**30 hours (minimum 4 days)**	**8**	**42**	

Note: The minimum of 4 days only applies where self-study can be evidenced. If no self-study can be evidenced, the qualification must be delivered for a minimum of 38 hours over 5 days.

Order of delivery and assessment of the units

It is a requirement that learners undertaking the BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6 are trained in the Application of Conflict Management in the Private Security Industry **before**:

- The practical assessment of Principles of Working as a Security Officer in the Private Security Industry
- The practical assessment of Principles of Working as a Door Supervisor in the Private Security Industry
- The delivery of Application of Physical Intervention Skills in the Private Security Industry

The **assessment** of the Application of Conflict Management in the Private Security Industry unit can be done **after** the physical intervention training has been delivered.

7. Grading

The qualification is graded either a pass or fail. In order to achieve the qualification, the learner must pass all four mandatory units. If a learner does not pass every unit, the qualification will not be awarded.

8. Age Restriction

This qualification is appropriate for learners aged 16 and over, however learners cannot possess a licence until the age of 18.

9. Entry Requirements

English Language Pre-requisite for Learners

In the course of their work, security operatives are likely to be required to make calls to the emergency services, or for example communicate to resolve conflict. It is essential that security operatives can communicate effectively.

It is the Centre's responsibility to ensure that each learner is sufficiently competent in the use of the English and/or Welsh language. All assessments must be conducted in the medium of English and/or Welsh as appropriate.

Learners should, as a minimum, have language skills in reading, writing, speaking and listening equivalent to the following:

- A B2 Level qualification on the Home Office's list of recognised English tests and qualifications
- A B2 Common European Framework of Reference for Languages (CEFR)
- An ESOL qualification at (Level 1) on the Ofqual register taken in England, Wales or Northern Ireland
- An ESOL qualification at Scottish Credit and Qualifications Framework Level 5 awarded by the Scottish Qualifications Authority (SQA) and taken in Scotland
- Functional Skills Level 1 in English
- SQA Core Skills in Communication at Scottish Credit and Qualifications Framework Level 5
- Essential Skills Wales Communication Level 1.

Training centres must ensure that all learners have sufficient reading, writing, speaking and listening language skills before putting the learners forward for training and assessment. All English/Welsh language assessments used by Centres must be agreed with BIIAB Qualifications Limited as part of security centre approval.

Centres must retain this information for all learners against all four competencies for a minimum of three years in line with retention of assessment evidence requirements.

First Aid Training Requirements

Learners taking their Door Supervision or Security Officer training for the first time will need to show that they hold a current and valid First Aid or Emergency First Aid certificate that meets the requirements of the Health and Safety (First Aid) Regulations 1981. It is an SIA requirement that training centres must confirm that each learner is sufficiently qualified in First Aid or Emergency First Aid.

Learners should, as a minimum, have achieved an Emergency First Aid at Work qualification covering the following outcomes:
- understand the role of the first aider, including reference to:
  - the importance of preventing cross-infection
  - the need for recording incidents and actions
  - use of available equipment
- assess the situation and circumstances in order to act safely, promptly and effectively in an emergency
- administer first aid to a casualty who is unconscious (including seizure)
- administer cardiopulmonary resuscitation and use of an automated external defibrillator
- administer first aid to a casualty who is choking
- administer first aid to a casualty who is wounded and bleeding
- administer first aid to a casualty who is suffering from shock
- provide appropriate first aid for minor injuries (including small cuts, grazes and bruises, minor burns and scalds, small splinters).

Learners should present their First Aid or Emergency First Aid certificate to their training provider before they start training. This certificate must be valid for at least 12 months from course start date.

It is the centre's responsibility to check the learner's First Aid certificate and maintain relevant records of how a learner meets this requirement.

Training centres must retain this information for a minimum of three years in line with retention of assessment evidence requirements.

10. Assessment

Overview of Assessment Strategy

The qualification contains units that cover both knowledge and competency which are all assessed. The competence elements of the units are assessed through practical assessments and require learners to demonstrate their competence through observation by an assessor. Knowledge assessments provided by BIIAB Qualifications Limited will ensure that effective learning has taken place and that learners have the opportunity to:

- meet the assessment criteria
- achieve the learning outcomes.

Assessments will be accessible and will produce results that are valid, reliable, transparent and fair. BIIAB Qualifications Limited will ensure that the result of each assessment taken by a learner in relation to a qualification reflects the level of attainment demonstrated by that learner in the assessment, and will be based upon the achievement of all of the specified learning outcomes.

In order to assess formally the learners' knowledge, BIIAB Qualifications Limited has developed externally set, externally marked paper-based **multiple-choice assessments**.

Details of the ordering process, assessment documentation, invigilation requirements to centres and the documentation to be completed can be found in the Centre Manual for the Administration of BIIAB Qualifications within the Security Portfolio document, available in the password protected area of CentreZone.

BIIAB Qualifications Limited will make every effort to ensure that it allows for assessment to:

- Be up to date and current
- Reflect the context from which the learner has been taught
- Be flexible to learner needs

BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6

Assessment Principles

The Assessment Principles for BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6 have been designed by the Security Industry Authority (SIA) in conjunction with all SIA approved Awarding Organisations. While BIIAB Qualifications Limited has not itself solely designed the strategy, it agrees with the principles and their suitability as an Assessment Strategy for this qualification, it has agreed that this strategy will be applied for this qualification, and it has agreed that it will monitor the compliance of BIIAB Qualifications Limited centres offering this qualification against the criteria. As such all centres and their assessment must adhere to the current Assessment Principles for this qualification.

The Assessment Principles for this qualification can be seen in the section which follows and it provides details of the key requirements for the qualification and the assessors and quality assurers delivering, quality assuring and certificating the qualification.

Principles of Working in the Private Security Industry

This unit will be assessed by both knowledge and practical assessment. The knowledge assessment is an externally set and marked multiple choice question paper consisting of 70 questions. The examination will last for 105 minutes and learners will be required to answer correctly 49 of the 70 questions (70%) in order to pass. The practical assessment is an externally set, internally assessed activity based on the completion of an evidential statement and learners will be required to achieve a pass mark of 100%. Training centres are required to retain copies of the evidential statements completed on record for a minimum of 3 years, the BIIAB Qualifications Limited EQA will sample this activity during a quality assurance visit.

Principles of Working as a Security Officer in the Private Security Industry

This unit will be assessed by both knowledge and practical assessment. The knowledge assessment is an externally set and marked multiple choice question paper consisting of 60 questions. The examination will last for 90 minutes and learners will be required to answer correctly 42 of the 60 questions (70%) in order to pass. The practical assessment is an externally set, internally assessed observation of searching with observation sheet and an externally set and internally assessed observation of using communications devices. The practical assessment must be visually recorded for each learner and is recommended to take approximately 15 minutes. Learners will be required to achieve a pass mark of 100% for the practical assessment.

Application of Conflict Management in the Private Security industry

This unit will be assessed by both knowledge and practical assessment. The knowledge assessment is an externally set and marked multiple choice question paper consisting of 20 questions. The examination will last for 30 minutes and learners will be required to answer correctly 14 of the 20 questions (70%) in order to pass. The practical assessment is an externally set, internally assessed practical scenario with observation sheet. The practical assessment must be visually recorded for each learner and is recommended to take approximately 15 minutes. Learners will be required to achieve a pass mark of 100% for the practical assessment.

Facilities

BIIAB Award for Security Officers in the Private Security Industry (Scotland) at SCQF Level 6

Training and assessment for approved licence-linked qualifications must be undertaken in an environment appropriate for training and learning. The environment must be adequately equipped for training, conducive to effective learning and must comply with current Health and Safety requirements.

Equipment for practical demonstrations must be readily available and fit for purpose. For practical scenarios, it is best practice to provide a realistic work environment for the training and assessing aspects of all practical activities. For full details of arrangements for the assessment and examination environment, please refer to BIIAB Qualifications Limited's Centre Manual for the Administration of BIIAB Qualifications within the Security Portfolio.

Trainers/Assessors involved in the delivery of Licence-linked qualifications

All trainers/assessors seeking to deliver licence-linked qualifications must have achieved as a minimum:

Trainer Qualifications

1. Award in Education and Training (Level 3 QCF/RQF) (Level 6 SCQF) or a teaching or training qualification at Level 3 (QCF/RQF), Level 6 (SCQF) (or equivalent or above), which has been accredited by SQA Accreditation/QCA/Ofqual or validated by a HEI, or equivalent such as:
   - Level 4 Award in Education and Training (QCF/RQF)
   - Certificate in Education
   - Post Graduate Certificate in Education
   - SVQs in Learning and Development at SCQF Level 8 and 9
   - NVQ Levels 3 and 4 in Learning and Development
   - Scottish Training Qualification for Further Education (TQFE)
   - PTLLS, CTLLS or DTLLS
   - Master's in Education

   AND
2. A National Counter Terrorism Security Office (NaCTSO) / SIA endorsed counter terrorism programme such as the ACT (Action Counters Terrorism) Awareness training which must be completed annually.

Assessor Qualifications

Assessors must hold any of the following qualifications:
- Level 3 Award in Understanding the Principles and Practices of Assessment (RQF)
- Level 3 Award in Assessing Competence in the Work Environment (RQF)
- Level 3 Award in Assessing Vocationally Related Achievement (RQF)
- A1 Assessing Learners Using a Range of Methods
- D32 Assess Learner Performance
- D33 Assess Learner Using Different Sources of Evidence
- L&D 9D Assess workplace competence using direct methods
- L&D 9DI Assess workplace competences using direct and indirect methods

OR the following unit from an Assessor qualification:

- Unit 1 Understanding the Principles and Practices of Assessment

OR the following units from a Teaching Qualification:
- Understanding Assessment in Education and Training unit from a Level 3 Award in Education and Training
- Understand the Principles and Practices of Assessment from a 12 credit Preparing to Teach in the Lifelong Learning Sector
- Principles of Assessment in Lifelong Learning from a 12 credit Preparing to Teach in the Lifelong Learning Sector qualification
- Understanding the Principles and Practices of Assessment from a Level 3 Certificate/Level 4 Diploma in Learning and Development
- Assess Occupational Competence in the Work Environment from a Level 3 Certificate/Level 4 Diploma in Learning and Development
- Assess Vocational Skills, Knowledge and Understanding Level 3 Certificate/Level 4 Diploma in Learning and Development.

It is expected that in most cases the trainer and the assessor will be the same person. If assessors do not hold any of these qualifications/units at the launch of the security qualifications, they will have until 30 September 2022 to achieve them.

Internal Quality Assurer (IQA) requirements

All those seeking to undertake internal quality assurance activities for licence-linked qualifications must have achieved as a minimum one of the following:
- Level 4 Award in Understanding the Internal Quality Assurance of Assessment Processes and Practices (RQF)
  - Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practices (RQF)
  - Level 4 Certificate in Leading the Internal Quality Assurance of Assessment Process and Practices (RQF)
  - V1 Conduct Internal Quality Assurance of the Assessment Process
  - D34 Internally Verify the Assessment Process
  - L&D 11 Internal Quality Assurance

OR the following unit from an IQA qualification:
- Unit 2/Unit 4 Understanding the principles and practices of internally assuring the quality of assessment.

If IQAs do not hold any of these units by the launch of the security qualifications, they will have until 30 September 2022 to achieve one.

The Centre is required to have access to at least one qualified IQA by 30 September 2022 with security sector competency relevant to the area they are quality assuring and who is familiar with the course content of the units that they are quality assuring.

Centre personnel who wish to check their eligibility may do so by contacting BIIAB Qualifications Limited.

Additional qualifications required by Trainers, Assessors and IQAs of the Conflict Management unit

The SIA requires all trainers and assessors involved in the delivery of the Application of Conflict Management in the Private Security Industry unit to have received relevant training. Trainers are required to hold a qualification at NQF/QCF/RQF Level 3 Deliverers of Conflict Management Training.

The IQA does not need to hold a formal conflict management qualification but does need to have appropriate competence in conflict management. Appropriate competency could come from employment in:
- Armed services
- Police service
- Security industry
- Prison service

BIIAB Qualifications Limited will require sufficient information about an IQA's occupational competence which will be considered on a case by case basis.

Occupational Competence required by Trainers and Assessors

Trainers and assessors delivering licence-linked qualifications must demonstrate that they have the necessary experience, knowledge and understanding of the sector in which they are providing training.

BIIAB Qualifications Limited will require sufficient information about a trainer's and assessor's occupational competence for consideration in the approval process. Occupational competence will normally come from working in the private security industry but other relevant experience may be acceptable and will be considered by BIIAB Qualifications Limited on a case by case basis. There is no requirement for a trainer or assessor to have a current SIA licence.

Other relevant experience could come from employment in:
- Armed services
- Police service
- Security industry
- Prison service

To ensure that trainers and assessors have the right occupational competence, the SIA and BIIAB Qualifications Limited require trainers and assessors new to the sector (i.e. this is their first role as a trainer or assessor in the security sector as identified from their CV) to have two years' frontline operational experience in the last five years in the UK, relevant to the qualifications that they are delivering. This operational experience can be achieved from full/part-time/weekend employment and achieved in blocks of employment as long as it meets the threshold above.

Existing trainers and assessors must demonstrate to BIIAB Qualifications Limited that they are taking sufficient steps to keep their occupational competence up to date. Suitable steps would include attendance at relevant conferences and seminars, and continuing work experience in

the sector. Trainers and assessors must be able to demonstrate evidence of a suitable level of continued professional development (CPD) in the sector. This should include the equivalent of at least 40 hours every year spent in a combination of training, increasing professional knowledge through other means or working in the industry. This CPD record must show that the National Counter Terrorism Security Office (NaCTSO) / SIA endorsed counter terrorism programme such as the ACT (Action Counters Terrorism) awareness training has been completed on an annual basis.

It is the responsibility of training centres to retain the CPD information of trainers and assessors. BIIAB Qualifications Limited and the SIA reserve the right to spot check this information for accuracy and quality assurance purposes. This evidence must be retained for a minimum of three years for audit purposes.

The SIA may publish additional requirements for trainers as and when they are agreed. Trainers looking to deliver licence-linked qualifications should ensure that they are fully familiar and compliant with the requirements as communicated by BIIAB Qualifications Limited.

Appeals

If learners are dissatisfied with an assessment outcome, they have the right to appeal. The **main** reasons for an appeal are likely to be:

- Learners do **not** understand why they are **not** yet regarded as competent, because of unsatisfactory feedback from the assessor
- Learners believe they are competent and that the assessor has misjudged them, or has failed to utilise some vital evidence

BIIAB Qualifications Limited expects most appeals from learners to be resolved within the centre. BIIAB Qualifications Limited will only consider a learner's appeal after the centre's internal appeals procedure has been fully exhausted.

For full details of the BIIAB Qualifications Limited's appeals procedure please refer to https://www.biiab.org/useful-information/biiab-policies/

11. Initial Assessment and Induction

Prior to the start of any programme, centres should make an initial assessment of each learner. This is to ensure that the learners are entered for an appropriate type and level of qualification.

The initial assessment should identify the specific training needs that the learner has, and the support and guidance that they may require when working towards their qualification.

The centre must also identify any units the learner has already completed, or credits they have accumulated, relevant to the qualification.

BIIAB Qualifications Limited suggests that centres provide an induction programme to ensure the learner fully understands the requirements of the qualification they will work towards, their responsibilities as a learner, and the responsibilities of the centre.

12. Reasonable adjustments and special considerations

BIIAB Qualifications Limited has a duty to ensure that the integrity of their qualifications and assessments is maintained at all times. At the same time they and their centres have a duty to ensure that the rights of individual learners to access qualifications and assessment in a way most appropriate for their individual needs are upheld.

Learners who require reasonable adjustments for their assessments **must** inform their assessor at the beginning of their course of their requirements.

During the initial assessment of the learner, or after the commencement of their qualification, it may be considered or determined that reasonable adjustments need to be made to allow access to qualifications and / or assessments.

If it is believed that a learner may require a reasonable adjustment or special consideration, the BIIAB Qualifications Limited policy 'BIIAB Qualifications Limited Reasonable Adjustments and Special Considerations Policy' must initially be referred to in order to determine if the adjustment or consideration can be made, can be made but only following express permission from BIIAB Qualifications Limited, or is unsuitable.

BIIAB Qualifications Limited's reasonable adjustments and special considerations policy is provided to all BIIAB Qualifications Limited approved centres and can be found at https://www.biiab.org/useful-information/biiab-policies/

13. Resources

BIIAB Qualifications Limited provides the following additional resources for this qualification:

- Multiple-choice assessments (externally set, externally marked)
- Documentation for the practical assessments
- Sample assessments
- Access to the units
- Learning support materials

All of these resources are available for download via https://www.biiab.org/

Assessments are available through CentreZone which is a password-protected area of the BIIAB website which centres approved for the qualification can access.

Access to the Units

Units form the qualification and the standard that **must** be achieved in order to be awarded each unit. This is covered within the learning outcomes, assessment criteria and the indicative content that form part of the delivery. BIIAB Qualifications Limited includes the mandatory units within this specification.

14. Design and Delivery

Centres **must** refer to the units that form the qualification and the standard that **must** be achieved in order to be awarded each unit. This is covered within the learning outcomes and assessment criteria that form part of the delivery.

Each unit within this qualification has been allocated a number of Guided Learning Hours (GLH).

This can include activities such as training/classroom based sessions, tutorials, supervised study or supervised 'on-the-job' learning and face-to-face or other pre-arranged 1:1 teaching sessions (e.g. simultaneous electronic communication such as webcam contact or internet messaging). It could also include time spent undertaking assessments.

The qualification will be assigned Total Qualification time (TQT) which, as well as GLH, will include the estimated number of hours spent in preparation, study or any other unsupervised learning, study or assessment for an average learner.

When planning how to deliver the qualification it is important to refer to this definition.

BIIAB Qualifications Limited will not prescribe how the qualification is delivered, but centres **must** ensure the delivery chosen meets their learners' needs.

Use of self-study

The SIA and BIIAB Qualifications Limited recognise that there is some learning that contributes to the achievement of the licence-linked qualifications that can be completed through self-study.

Where a Centre wishes to use self-study in this way, they must firstly inform BIIAB Qualifications Limited. The Centre must detail within their quality management processes each of the following:

- The areas of learning to be delivered by self-study
- The method of self-study to be used
- The number of hours to be covered by the self-study material
- A robust and auditable method for determining that learners have undertaken the self-study

It is important the materials used clearly show learners how many hours of learning they are expected to undertake and that they are given sufficient time to allow them to complete it before their course begins. It is also a requirement that the centre checks these during training to ensure appropriate learning has occurred. This will be quality assured by BIIAB Qualifications Limited through external quality assurance processes.

Self-study may be used to deliver up to **eight** hours of Principles of Working in the Private Security Industry (PWPSI). The Learning Outcomes that can be delivered via distance learning are:

- LO1: Know the main characteristics and purposes of the Private Security Industry (2 hours)
- LO2: Understand legislation as it applies to a security operative (2 hours)
- LO4: Understand the importance of safe working practices (2 hours)
- LO5: Understand fire procedures in the workplace (1 hour)
- LO11: Understand good practice for post incident management (1 hour)

Suitable methods of self-study include prepared, high quality:

- On-line learning materials or courses that the learner must navigate
- Workbooks that the learner must work through and complete
- Learning materials that the learner can use to cover specified areas of content

Training centres are reminded that any self-study material used must be retained for a minimum of 3 years in line with retention of assessment evidence requirements.

15. Format of Units

All units within this qualification will be presented in a standard format that is consistent with the format for all units of assessment. The format will give tutors and learners guidance as to the requirements of the unit for successful completion. Each unit within this specification will be in the format below:

Unit Title

This will be shown as it appears on the SQA computer system

Unit Reference Number (URN)

The Unit Reference Number is the unique code that the unit is given by the Regulator. This unit will be referenced on the final qualification certificate. The same unique code for the unit applies in whichever qualification the unit is included within. BIIAB Qualifications Limited also assign unique unit numbers which normally is consistent when the unit is used in multiple BIIAB qualifications.

Level

This identifies the level of demand for the unit, but may be a different level to that of the overall qualification. The level of the units will be set according to National Occupational Standards and the level descriptors.

Credit

When a whole unit is completed the learner will achieve credits specified by the number of hours' learning time it will take an average learner to complete the unit including the assessment.

Guided Learning Hours (GLH)

The required number of hours that learning should take place under the immediate guidance or supervision of a lecturer, supervisor, tutor or other appropriate provider of education or training.

Total Qualification Time (TQT)

Total Qualification Time (TQT) is defined as the number of notional hours which represents an estimate of the total amount of time that could reasonably be expected to be required in order for a Learner to achieve and demonstrate the achievement of the level of attainment necessary for the award of a qualification. TQT is comprised of the following two elements:

- The number of hours which an awarding organisation has assigned to a qualification for Guided Learning, and
- An estimate of the number of hours a Learner will reasonably be likely to spend in preparation, study or any other form of participation in education or training, including assessment, which takes place as directed by – but, unlike Guided Learning, not under the Immediate Guidance or Supervision of – a lecturer, supervisor, tutor or other appropriate provider of education or training.

TQT is always assigned to the qualification however a similar calculation may on occasions also be assigned to a unit.

Learning Outcomes and Assessment Criteria

Learning Outcomes are what the learner is expected to know, understand or be able to do upon successful completion of the unit.

Assessment Criteria are descriptions of the requirements that a learner is expected to meet in order to demonstrate that a learning outcome has been achieved.

16. Initial Registration

Registration and Certification

Learners should be registered and certificated via BIIAB Qualifications Limited's On-line Registration and Certification Service (ORCS) www.orcs.biiab.org. Please refer to BIIAB Qualifications Limited's Centre Guidance for using ORCS.

Equal Opportunities and Diversity Policy

BIIAB Qualifications Limited has in place an equal opportunities policy, a copy can be found at centrezone.bii.org .

BIIAB Qualifications Limited is committed to ensure that:

- Approved centres operate an equal opportunities policy
- Approved centres communicate the policy to staff and learners
- Approved centres have an effective complaints and appeals procedure of which both staff and learners are made aware
- Approved centres are aware of their responsibilities in providing equality of opportunity, particularly with regard to provision for learners with particular assessment requirements.

17. Qualification Review and Feedback

BIIAB Qualifications Limited is committed to the ongoing review of this qualification to ensure it remains fit for purpose.

This review approach involves the collation of evidence in the form of any information, comments and complaints received from users of this qualification in relation to its development, delivery and award.

BIIAB Qualifications Limited will give due regard to any credible evidence received which suggests that a change in approach to the development, delivery and award of this qualification is required in order to ensure that no adverse effects will result. This qualification will be periodically reviewed and revised to ensure the content remains relevant, the assessment approach remains appropriate and that it remains valid and fit for purpose.

18. Mandatory Units

The following units are mandatory for this qualification.

Principles of Working in the Private Security Industry
UP11 04

Level   6
Credit   2
GLH   17 (8 hours allowed for Distance Learning)
TQT   17

Learning Outcomes The learner will	Assessment Criteria The learner can	Indicative Content
1. Know the main characteristics and purposes of the Private Security Industry	1.1 Identify the key purposes of the private security industry	• Prevent and detect crime and unauthorised activities • Prevent and reduce loss, waste and damage • Monitor and respond to safety risks • Provide personnel and appropriate protection systems for people, property and premises • Raise standards in the industry
	1.2 State the aims and functions of the Security Industry Authority (SIA)	• Protect the public and regulate the security industry through licensing • Raise standards (through the Approved Contractor Scheme) Monitor the activities and effectiveness of those working in the industry • Set and approve standards of conduct, training and supervision within the industry • Keep under review the private security industry and the operation of the legislative framework
	1.3 Recognise the required standards of behaviour of a security operative	• Main qualities required for security industry operatives: reliability and integrity; politeness; professional attitude and appropriate personal appearance; being prepared to take responsibility • Skills: communication skills; observational skills; problem solving; ability to handle sensitive situations; team-working skills • Adherence to SIA Standards; adherence to organisation/company values and standards

	1.4 Identify the benefits of community safety initiatives	- Examples of community safety initiatives: police liaison officers, police community links, initiatives to radio link with other venues e.g. National PubWatch, local PubWatch initiatives, sharing information, red and yellow cards - Aim: to reduce the opportunity for crime to take place - Activities: include improving physical security of vulnerable targets, improving the environment, removing the means to commit crime; improving the visibility in an area e.g. lighting; controlling access to areas so unauthorised people cannot gain access to commit crime; initiatives to radio link with other venues e.g. National PubWatch, local PubWatch initiatives, sharing information, red and yellow cards - Benefits: include better partnership working, cooperating with Local Authority and police, liaison with other venues, reduction of risk of crime to own employer or other employers, promotion of safer communities
	1.5 Recognise how assignment instructions support the Security Operative role.	- Describes the security operative's roles and duties for specific location - Outlines actions to take in an emergency including obtaining contact numbers - Part of a contract between client/customer and the security company
	1.6 Recognise how each security operative role may use CCTV	- Benefits of using CCTV e.g. - Prevents crime - Cuts down on incidents - Reduces costs by not having to employ additional staff - Can provide clear evidence for investigations - Can provide evidence which can be used in a court of law - Understand the legal implications of using CCTV e.g. - Must be registered

		- o Must have a named person who is responsible and accountable for its use - o Must display signs to inform people that CCTV is in operation - o Must not record in private spaces such as toilets • Must comply with current data protection legislation e.g. - o when storing data including any recordings - o restricting access to certain staff - o by using recordings appropriately
	1.7 Identify the limitations of CCTV within the security operative role	• Privacy issues and concerns • Vulnerable to damage and vandalism • Misuse • Cannot prevent crime • Cost • Familiarity with scope of cover • Technology vulnerabilities
	1.8 State the purpose of the Approved Contractor Scheme	• Raise performance standards • Assist the SIA to develop new opportunities • Increased customer confidence
2. Understand legislation as it applies to a security operative	2.1 Identify the differences between Civil and Criminal Law	Main features of Civil law: • Purpose to right a wrong • Individual brings the cases • Remedy by compensation for loss or damage • Standard of proof on balance of probabilities Examples of civil offences: • Libel • Defamation • Breach of contract • Employment Law • Family and matrimonial disputes • Property disputes • Personal injury cases • Trespass Main features of Criminal Law: • Purpose to deter and punish • State brings the cases

		• Remedy is fines/imprisonment • Standard of proof is beyond reasonable doubt Examples of Criminal offences: • Driving under the influence • Assault • Murder • Rape • Child abuse • Theft • Domestic abuse • Wilful Fire Raising • Kidnapping or holding someone against their will
	2.2 State the main aims of the Private Security Industry Act 2001	• Raise standards in the private security industry • Increase public confidence in the private security industry • Increase public safety • Remove criminal elements from the private security industry • Established the SIA (Security Industry Authority) • Established licensing

	2.3 Identify key legislation relating to promoting equality and diversity in the workplace	• Key Legislation: Equalities Act 2010; Human Rights Act 1998
		• Protection from discrimination in the workplace:
		  o protected characteristics: race/ethnicity/nationality, gender, religion or belief, disability, sexual orientation, gender reassignment, marriage/civil partnership, age, pregnancy and maternity
		  o direct and indirect discrimination
		• Areas where equal opportunities legislation applies: recruitment; access to training; pay and benefits; promotion opportunities; terms and conditions; redundancy; dismissal
		• Employer's duty to make reasonable adjustments

	2.4 Identify licensable roles under the Private Security Act	Licensable roles

		Licensed sectors in manned guarding: vehicle immobilisation; security guarding, door supervision; CCTV; close protection, cash and valuables in transit (CVIT), key holding
	2.5 Identify how data protection regulation impacts on the security operative	Have an understanding of current data protection regulation Include the general principles • The use of body worn cameras and restrictions e.g. o Images must be stored to comply with GDPR and can only be viewed by authorised personnel • Recording and documenting in notebooks
3. Understand arrest procedures relevant to security operatives	3.1 State the meaning of arrest	o Arrest is to take away someone's liberty o There is no legal definition for citizen's arrest o Police and non-police arrest o Arrest with a warrant o Arrest without a warrant

	3.2 Identify offences for which a security operative can make an arrest	o Security operatives have no special powers of arrest, only the same powers of arrest as every other citizen.
		o Arrestable offences and Breach of the Peace
		o Arrestable offences are usually tried at Sheriff Court/High Court in Scotland.
		o Powers of arrest under the common law
		• Offences include:
		    o Culpable Homicide
		    o Serious Assault
		    o Assault
		    o Rape
		    o Sexual Assault
		    o Firearms offences
		    o Robbery
		    o Housebreaking
		    o Theft
		    o Drugs offences
		    o Fraud
		    o Vandalism

	3.3 Identify the limitations to a security operative's powers of arrest.	• Must be within powers of citizen's arrest • Section 24a of the Police and Criminal Evidence Act 1984 • Indictable offence must be either being committed or have already been committed • Arrest can only be made to prevent the person from:

		○ (a) causing injury to himself or another; ○ (b) suffering injury himself; ○ (c) causing loss of or damage to property; ○ (d) making off before a constable can assume responsibility for him
	3.4 State procedures to follow when making an arrest	- Inform person that they are under arrest, provide the reason for arrest, and that the police will be called - Detain the person and ensure their safety - Use witnesses wherever possible - Only use reasonable and necessary force to prevent: ○ escape of individual under arrest or assault against security operatives or others
	3.5 State why an arrest should only be made as a last resort	- Taking someone's liberty is a serious matter - Can only arrest for Arrestable Offences - False arrest can lead to civil or criminal prosecution of the security operative making the arrest - Personal safety of the security operative can be at risk
	3.6 State procedures following an arrest	- The arrested person is now the security operatives responsibility - Ensure own safety - Ensure the person's safety - Ensure any evidence is preserved and not disposed of - Hand person over to police, explaining reason for arrest - Inform police of any extra evidence of offence (witnesses, CCTV, property) - Record arrest in line with local policy - Assist police with a statement if required - Attend court at a later date if required - Identify how to work with the Police in relation to arrest procedures
	3.7 State what is meant by 'reasonable' and 'necessary' force	- Reasonable force is the amount of force that can be used to protect yourself or your property from attack. It can be used to prevent crime or when detaining someone through a citizen's arrest. It can also be classed as "legal force" - Necessary force is an opinion of the level of force that was carried out in any situation

4. Understand the importance of safe working practices	4.1 Identify responsibilities under the Health and Safety at Work etc. Act	Responsibilities of employees and the self-employed: • To take responsibility for own health and safety, to co-operate with employer, to take reasonable care and not put themselves or public at risk, to report injuries and accidents to employer • To follow instruction, processes and procedures put in place by their employer Responsibilities of employers: • To maintain the safety of employees and anyone who visits the premises • To provide safe access and egress • To assess and reduce risk, to provide first aid facilities, to tell staff about hazards, to provide training if required, to record injuries and accidents, to provide and maintain necessary equipment and clothing and warning signs • To comply with legislation: consequences of failure to comply e.g. prosecution, business closure

	4.2 Identify the risks of lone working within the private security industry	• Being isolated and having to rely on technology for back up
		• Being vulnerable:
		   o Injury / ill-health
		   o Violence
		   o Lack of support
		   o Lack of communication
		   o Lack of welfare facilities for rest

	4.3 Identify typical workplace hazards and risks	Definition of 'hazard': • potential source of harm or adverse health effect on a person or persons Typical workplace hazards: • accidents due to poor lighting, uneven surfaces, steps, etc. • risk of infection from body fluids • risk of dealing with aggressive or violent behaviour

		- Injuries from poor manual handling - Misuse/abuse of machinery - Sharp objects (needles and knives) - Diseases - Hazardous chemicals - Noise pollution - Moving vehicles - Obstructions - Poor lighting - Fire/floods and other emergencies Definition of 'risks': - likelihood that a person may be harmed or suffer adverse health effects if exposed to a hazard Identify risks: - Level of Risk (High, Medium or Low impact) - Assess the risk of the hazard by identifying who may be harmed and how, what controls are already in place, what additional controls are needed to control the risk, who is required to do this and when is it required to be completed by.
	4.4 State how to minimise risk to personal safety at work	- Risk assessment: developing awareness of risks and how to minimise them - Following health and safety and organisational procedures in relation to health and safety - Use of protective equipment, personal alarms and mobile phones - Importance of following safe routines and being systematic - Identify methods for safe manual handling - Assessment of load; know own limits; plan route; use of mechanical aid; stable base; correct positioning of head, feet and back; correct positioning of load; smooth movements; avoidance of twisting; push rather than pull

		• Follow health and safety and organisational procedures in relation to global (or critical) incidents
	4.5 Identify safety signs and signals	• Different categories of sign: e.g. prohibition, warning, mandatory, safe condition, fire-fighting, hazard/chemical warning plates
	4.6 State procedures to be followed for recording and reporting accidents and health and safety incidents	• Reportable incidents and accidents under RIDDOR: work-related, dangerous occurrence, resulting in injury, occupational disease or death; gas related incident • Procedures: in line with organisational procedures; record in accident book; RIDDOR reporting – 'responsible person', online, telephone, by post • Remember to include who, what, when, how and where

	4.7 Identify ways to keep personal information safe	• When handling any personal information or data (either their own or someone else's) Security Operatives must:
		   o Comply with current data protection legislation
		   o Follow organisational procedures
		   o Follow assignment instructions
		   o Maintain confidentiality of information
		• Security Operatives should:
		   o Use personal social media responsibly including managing privacy settings
		   o Not wear anything identifiable outside the workplace
		   o keep personal vigilance e.g. not completing surveys
		   o Not discuss work issues outside the workplace
		   o Not discuss work information with colleagues

5. Understand fire procedures in the workplace	5.1 Identify the elements that must be present for fire to exist	• Components of fire: the fire triangle (oxygen, fuel, heat - chemical chain reaction)

	5.2 State the actions to be taken upon discovering a fire	• Follow organisation's policies and procedures • Sound the alarm and inform emergency services • FIRE (Find, Inform, Restrict, Evacuate or Extinguish). Do not attempt to put out a fire if it puts you in danger. • Identify area where fire is, isolate other areas • Control panel: Important to ensure full understanding of extent of area of incident, to pass on correct message to emergency services e.g. with regard to materials, chemical stored in affected area
	5.3 Identify basic fire safety controls	• Be observant and vigilant • Control of fuel and ignition sources e.g. bins and waste disposal • Safe storage of flammables • Inspection and maintenance of electrical equipment • Avoidance of overloading electrical points • Follow staff training • Adhere to fire plan
	5.4 Identify classifications of fire	• A – Ordinary combustible: includes paper, wood, textiles, rubber • B – Flammable liquids e.g. petrol, paint, solvents • C – Flammable gas e.g. butane, propane • D – Metal fires e.g. powdered and metal shavings, alkali-based metals • Electrical fires (no classification as electricity is a source of ignition as opposed to a fuel). • F – Hot cooking oils
	5.5 Identify the different types of fire-fighting equipment	Extinguishers: • Water for use with paper, wood • General Foam for use with paper, wood; specialist foam for use with industrial alcohol • CO_2 Gas for use with electrical fires (primary); flammable liquids (secondary) • Wet Chemical, for cooking oil fires • Powder for use with most fires including liquid and electrical fires

		Other equipment: • fire blankets, fire hose, sprinkler system
	5.6 Identify the role of a fire marshal in the event of an emergency	• sound the alarm • check allocated area to ensure that everybody has left, take roll call • take control of the evacuation and ensure that anybody with evacuation difficulties is aided • proceed to the assembly area and report to the Fire officer in charge
6. Understand emergencies and the importance of emergency procedures	6.1 Identify the key emergency terms	Emergency is: • a situation that is unexpected, threatens safety or causes serious disruption and requires immediate action Emergencies can include incidents, occurrences, accidents. Examples are listed below. • Incident/Occurrence – this could include a fight, power cut or drug overdose, etc. • Emergency – this could include health emergencies such as epileptic seizure, anaphylactic shock, heart attack, etc. • Accident – this could include someone falling down steps, someone slipping on a wet floor, etc.
	6.2 Identify different types of emergencies within the workplace	Types of emergency: • power, system or equipment failure; flood; actual or threatened serious injury; serious illness; bomb threat, fire, terror threat
	6.3 Recognise how people react when emergencies occur	Types of reactions: • Public/human responses – fight or flight • Panic, freeze • Crowd control, danger of crushing
	6.4 Identify actions to be taken in an emergency situation	Security operative responses to emergencies: • follow correct procedures depending on emergency • ensure safety of self and others

		- report to appropriate authorities - act quickly, be authoritative, remain calm, encourage others to remain calm - follow procedures for making emergency calls - follow escalation procedures if required - document clearly what happened and your response - review and evaluate incident - Identify how a graduated response can be applied to incidents
	6.5 Identify the role of the security operative in relation to first aid incidents	List actions to be taken when first aid is required - If necessary, contact designated first aider or the emergency services - Know the limits of your own ability and authority to deal with personal injury - Record the injury in the accident book - Keep people safe, including onlookers - Provide privacy whenever possible
	6.6 Recognise evacuation principles	Evacuation – this is a controlled process of emptying an area or premises of people. Evacuation can be to an adjoining area within a building or outside depending on the severity of the incident. Examples for evacuation could be flood, fire or terror threat. Invacuation – this is a controlled process of getting people into safe premises due to an incident which could cause harm to people who were outside. For example, if a person with a firearm started to shoot people in the street you would encourage everyone into the building and lock the doors for safety. Basic principles are to keep people safe and to follow the organisation's policies and procedures.

		Importance of knowing venue specific requirements
7. Understand how to communicate effectively as a security operative	7.1 Identify the different types of communication	• non-verbal communication: gesture, stance, eye contact, facial expression, • verbal communication: speaking, listening, reading, pitch, tone of voice • written communication: pictures, signs, script, text messages
	7.2 State the importance of effective communication	• to ensure that the message being sent is received and understood by the recipient • Features of effective communication include choosing language and medium appropriate for message and recipient, delivering message clearly, checking understanding • Promotes effective teamwork • Promotes a professional establishment and service • Prevents misinterpretation which could lead to aggressive behaviour • Prevents misunderstanding which could lead to mistakes • Importance of effective communication: to ensure organisational effectiveness and effective team working, to provide effective service to customers • NATO phonetic alphabet: Call signs: correlate to each letter from phonetic alphabet; local policies regarding call signs allocated • Uses of phonetic alphabet: enables quick identification of individuals; enables spelling of words during transmissions to avoid misunderstandings
	7.3 Identify the benefits of teamwork in the private security industry	• Promotes safety • Provides a professional and safe service and establishment • Supports colleagues • Promotes efficiency
	7.4 State the principles of customer service	• Establishing rapport, acknowledging the customer, communicating information effectively, showing respect, listening to the customer and trying to meet their expectations

		• Dealing with problems: acknowledge the customer, establish the customer's needs, put yourself in the customer's position, accept responsibility, involve the customer in the solution, see it through
	7.5 Recognise diverse customer needs and expectations	• Types of customer: internal and external, direct and indirect • Customer needs/expectations: e.g. information, assistance, directions • Customers with particular needs: e.g. physical difficulties, learning difficulties, sensory impairment, English as second language, under influence of drugs and/or alcohol
8. Understand record keeping relevant to the role of the security operative	8.1 State the importance of accurate record keeping	• To comply with the law • To provide a clear audit trail of the incident or accident • To prevent you from having to rely on your memory
	8.2 Identify the types of records that may need to be completed	• Incident records • Accident records • Searches and checks • Logbooks • Pocket notebooks • Search / visitor / key registers • Duty sheets • accident reports • Lost/found property registers • Message books • Handover reports • Other site-specific reports
	8.3 Identify what information to include in records	• Who – the report is for / it was written by • What – happened / action was taken / was the result • When – Day/date/time • How – did it happen • Where – place of incident • Details of any other witnesses/people/injuries or property

	8.4 Demonstrate the accurate completion of an evidential statement (Section 9 Statement)	**Statement to be completed as part of the training and internally assessed with a sign off sheet submitted to AO to say completed.** • The implications of failing to complete the section 9 statement or using the required documents. • PACE (Police and Criminal Evidence Act 1984) • Incidents requiring physical intervention/use of force, must be • fully reported – including: • description of subject/s behaviour • other 'impact factors' • staff responses including description of physical • interventions and level of force used • description of any injuries sustained • first aid and/or medical support provided • details of admission to hospital • support to those involved and follow up action required
	8.5 State the process of attending court to give evidence	• Follow organisation's policies and procedures • Follow any legal advice from representative • Be punctual and prepared
9. Understand terror threats and the role of the security operative in the event of a threat	9.1 Identify the different threat levels	• The official source of UK Threat Level is (MI5) and their website is https://www.mi5.gov.uk/threat-levels. As well as knowing what each level means an operative would ideally need to know how it may impact the response level their location may have. • LOW means an attack is highly unlikely • MODERATE means an attack is possible, but not likely • SUBSTANTIAL means an attack is likely • SEVERE means an attack is highly likely • CRITICAL means an attack is highly likely in the near future • Have an understanding of how UK threat level may impact the response level for the location in which you are working.

	9.2 Recognise the common terror attack methods	- Awareness of attack planning phases. - Most current terrorist attack methodologies: - Marauding Terror Attack (MTA), including firearms, knife, blunt objects, etc. - Explosive device, including Improvised Explosive Device (IED), Person-Borne Improvised Explosive Device (PBIED). Vehicle-Borne Improvised Explosive Device (VBIED), Leave Behind Improvised Explosive Device (LBIED) - VAAW (Vehicle As A Weapon) also known as vehicle ramming - Chemical, Biological, Radiological and Nuclear (CBRN), including acid attacks. - Cyber attacks - Insider threat
	9.3 Recognise the actions to take in the event of a terror threat	- Understand the role security operatives have to play during a terror attack. - Understand what Run, Hide, Tell means for a security operative: keeping yourself safe and encouraging members of the public, who will look up to you, to follow you to a safe place - Know and follow relevant procedure for your place of work, including the company's evacuation plan within the limits of your own authority. - Use your knowledge of the location and making dynamic decisions based on available information to keep yourself and the public safe. - Know the difference between evacuation and invacuation (lock down), including the pros and cons of both options. - In both of these situations, the pros can very easily become cons. For example, evacuating a building due to fire tries to keep people safe but the con can be that people rush out and get injured or stand around outside which could result in accident. Conversely, taking people into a building for safety due to a terrorist act on the street can mean that they are all grouped together and could be seen as an

| | | easy target for other forms of terrorist activities.
Report incidents requiring immediate response from the police on 999 Know what information emergency response require: What you have seen and what has happened. Who you saw, what they looked like, what they were wearing. Where did the situation happen and where you are. When did it happen. Awareness of emergency services response time Reporting suspicious activity that does not need immediate response to the Anti-Terrorist Hotline. Know who the public sector counter-terrorism experts are and how to access their information; Centre for the protection of national infrastructure (CPNI) National Counter Terrorism Security Office (NaCTSO) Awareness of current initiatives: Run, hide, tell keeping themselves safe and encouraging members of the public, who will look up to a person wearing a yellow vest, to follow them to a safe place. ACT - Action Counter Terrorism SCaN - See, Check and notify |
| | 9.4 identify the procedures for dealing with suspicious items | Hot Principles: Hidden Obviously suspicious Typical Four Cs: Confirm, Clear, Communicate and Control

Safety distance, including: |

		• distance v suspicious item size (small items: 100 m - large items or small vehicle: 200 m - large vehicle: 400 m) • how to visually represent safety distance (e.g. football field) • difficulty involved in setting up a safety distances and not use radio/mobile phone within 15 m

	9.5 Identify behaviours that could indicate suspicious activity	• Suspicious activity is any observed behaviour that could indicate terrorism or terrorism related crime.
		• Hostile reconnaissance is the observing of people, places, vehicles and locations with the intention of gathering information to plan a hostile act.
		• Understand examples of what this might look like, including:
		   o Individuals taking particular interest in security measures, making unusual requests for information, testing security by breaching restricted areas, loitering, tampering with utilities
		   o Individuals avoiding security staff.
		   o Individuals carrying out activities inconsistent with the nature of the building or area.
		   o Individuals with forged, altered or stolen identity documents, documents in different names, with large amounts of cash, inappropriately dressed for season/location; taking photos or making drawings
		   o Parked vehicles with people inside, empty parked vehicles left unattended for long period
		   o Multiple sightings of same suspicious person, vehicle, or activity
		• Understands actions that can deter or disrupt hostile reconnaissance, including:
		   o Ensuring a visible presence of vigilant security staff; frequent patrols but at irregular intervals

		- Maintaining organised search procedures - Ensuring emergency exits are secured when not in use to prevent unauthorised entry
	9.6 Identify how to respond to suspicious behaviour	- Use your customer service skills to disrupt potential hostile reconnaissance. - Understand the importance of showing professional behaviour and visible security as a tool to deter hostile reconnaissance. - Know where to report suspicious behaviour including: - Internal procedure for site - Confidential (Anti-Terrorist) Hotline: 0800 789 321 - British Transport police (BTP) "See it, Say it, Sorted": text 61016 or call 0800 40 50 40 - Non-emergency: 101 - ACT online reporting - Life threatening emergency or requiring immediate response: 999
10. Understand how to keep vulnerable people safe	10.1 Recognise duty of care with regard to vulnerable people	- Duty of care is: "a moral or legal obligation to ensure the safety or well-being of others" - People may not always appear to be vulnerable so best practice would be to have a duty of care for everyone
	10.2 Identify factors that could make someone vulnerable	- Vulnerable: being under the influence of alcohol or drugs; alone or receiving unwanted attention; separated from friends; appearing lost or isolated; being followed or threatened; victims of domestic violence; young people under the age of 18, mental ill-health, learning disabilities, physical disabilities, being elderly, being acutely ill, Key behaviours associated with a range of invisible disabilities (physical, mental or neurological condition that limits a person's movements, senses or activities that is invisible to the onlooker). - Indicators of child sexual exploitation: children and young people in the company of older people or antisocial groups, acting

		in an inappropriate and sexualised way; intoxicated; arriving and departing a location with different adults; getting into and out of a number of different cars
	10.3 Identify actions that the security operative should take towards vulnerable individuals	- Seeking help from other professionals, police, ambulance, street pastors, street marshals or representatives from any other scheme active in the area to help people - Offer to call a relative or friend to give assistance - Offer to call a licensed taxi to take the vulnerable person home - Using 'safe havens' or other local initiatives run by organisations such as St John's Ambulance - Be aware of current safety initiatives e.g. Ask Angela campaign - Reporting indicators of child sexual exploitation: - Contact the police or call Crimestoppers - Report as soon as possible
	10.4 Identify behaviours that may be exhibited by sexual predators	- Close monitoring of vulnerable people - Buying drinks or gifts for vulnerable people - Suspicious behaviour around certain times and venues - Inappropriate use of technology e.g. upskirting with phones
	10.5 Identify indicators of abuse	- Restricting freedom of individuals - Unexplained bruising - Lack of confidence and insecurity - Change in circumstances e.g. cleanliness, appearance
	10.6 State how to deal with allegations of sexual assault	- Follow organisation's policies and procedures - Notify police - Safeguard victim - Separate victim from assailant - Record and document all information
	10.7 State how to deal with anti-social behaviour	- Follow your organisation's policies and procedures - Speak to the person - Explain the situation and the risks of the anti-social behaviour

		• Explain the consequences if the anti-social behaviour continues • Remain calm • Ensure that your colleagues know about the situation and that you have back-up if needed • Vigilance; • High-profile patrols; • Early intervention; • Positive non-aggressive communication; • Prompt reporting of incidents; • Accurate recording of incidents; • Liaison with police and other appropriate agencies.
11. Understand good practice for post incident management	11.1 Identify sources of post incident support available	• Sources of support through colleagues, management and counsellors • Publications, internet • Help lines (e.g. Samaritans) • Other support e.g. Citizen's advice/ Trade Unions
	11.2 State why accessing support following an incident is important	• Reducing the chances of long-term problems such as depression, anxiety, fear, post-traumatic stress • Helps you to reflect on the incident and evaluate your actions
	11.3 State the benefits of reflecting on incident	• Areas for improvement can be identified • Preventing reoccurrence of the same problem • Organisations can use data for licensing hearings • Recognising trends • Recognising poor practice • Recognising good practice • Sharing good practice • Making improvements • Improving procedures for incident management • Identifying common response to situations
	11.4 Identify why it is important for security operatives to contribute to improving practice	• Promotes professional service • Increases safety for staff • Promotes teamwork • Increases safety for customers • Identifies procedures or methods to deal with situations effectively

Principles of Working as a Security Officer In The Private Security Industry

UP16 04

Level: 6

Credit: 1

GLH: 10

TQT: 12

Unit aim: This unit covers the knowledge and the practical skills required for a security officer working in the private security industry.

Learning Outcomes The learner will	Assessment Criteria The learner can	Indicative Content
1. Understand the roles and responsibilities of security officers	1.1 Identify different security officer roles within the private security industry.	• Retail • Corporate • Asset Protection • Educational establishments • Health and Care Sector (NHS)
	1.2 Identify the main responsibilities of a security officer.	• Protect life • Prevent and deter crime • Prevent loss • Protect property and assets • Respond to incidents and emergencies • Control site access/egress • Provide assistance to employees and customers • Provide a safe and secure environment • Maintain confidentiality of site and personal data/information • Ensure compliance with current Data Protection legislation • Customer Liaison • Process deliveries
	1.3 Recognise how the control room supports the security officer.	• Monitors activity on a site using systems such as CCTV / Clocking devices and Radios • Provides assistance and emergency back up support for security officers • Around the clock/out of hours support • Central point of contact • Management of frontline staff • Storage and issue point for equipment (e.g. PPE, body worn cameras (BWC) etc.)
2. Understand the control of access and egress.	2.1 State the purpose of access and egress control.	• Controls the entry and exit of all staff/visitors and customers • Records who is on site at any given time

		• Provides information in the event of evacuation /emergencies • Protects safety of staff and visitors. • Safeguards site and assets • Allows entry to authorised persons only etc.

	2.2 Identify the security officer's duties and responsibilities when controlling access and egress.	• **Relating to:**
		  o People including statutory agencies
		  o Vehicles
		  o Property
		
		• Operating queuing systems
		• Checking authority to enter premises
		• Operating access/egress control equipment
		• First point of contact, so creates visitor/customer impression
		• Providing directions and guidelines for site access to third parties
		• Controlling the entry and exit of all staff/visitors and customers
		• Searching people, their belongings and vehicles
		• Staffing access points/checkpoints
		• Controlling issue/return of visitors passes
		• Recording visitor information
		• Refusing entry and removing unauthorised persons
		• Recording who is on site at any given time
		• Provide information in the event of evacuation, emergencies
		• Protects safety of staff and visitors

	2.3 State the powers of statutory agencies relating to access and egress control.	• Statutory agencies include HM Revenue and Customs; police officers; Health and Safety Inspectors; Fire Officers; local authority trading standards officers; local authority food safety inspectors • Do not have to give advance notice of visit • Must provide valid proof of identity • Statutory agencies must not be prevented from carrying out their duties
	2.4 Identify ways of attempting to gain unauthorised access.	• Unauthorised use of keys, cards, codes etc. • Using false / outdated credentials / ID • Unsecured access points • Tailgating • Door propping • Physical breach

	2.5 State the responsibilities of a security officer in relation to crowd management and queue control at access and egress points.	• Decreasing the potential for conflict outside the site • Demonstrating good customer service • Allowing assessment of attitude and behaviour of different customers while queuing • Enforcement of admissions policy • Improving the safety of self, customers and others • Reducing likelihood of crushing • Working with traffic management to keep pedestrians safe and avoid traffic collisions • Enhance customer satisfaction and enjoyment • Understand current government guidance as applied to sites
3. Know the different types of electronic and physical protection systems in the security environment.	3.1 Identify how the different types of electronic and physical protection systems can support the security officer role.	• Provide information of incidents on site requiring action, • Detecting change of state and/or fault • Access/egress control systems: to control entry/exit of site/premises • CCTV systems: to show images an officer may not otherwise easily be able to see • Electronic Article Surveillance (EAS): to alert officer if tag hasn't been removed before exiting retail premises • Intruder alarms: display location / type of breach • Enable large area to be covered • Give enhanced vision in low light • Identify objects not visible to the naked eye • Enable faster response times • Reduce manning numbers • Safer searching

	3.2 Identify different types of protection measures.	• Access/egress control these control access to/entry from premises:
		  o Visitor logs and passes
		  o Signing in/signing out
		  o Swipe cards/fob entry;
		  o Biometric readers;
		  o Hostile vehicle mitigation;
		  o Video intercoms;
		  o Keypads;
		  o Facial recognition;
		  o Mail/baggage Scanners;
		  o Mail and delivery logs
		
		• Physical controls: Fences / walls incl those with climb deterrent, gates, raised kerbs;

		• Intruder detection and alarms e.g. infrared sensors; break resulting in ink/smoke deployment • Mechanical devices (e.g. cat's claws; turnstiles; locks; control barriers) • Automatic Number Plate Recognition (ANPR) • Metal detectors (walk-through/ handheld etc.) • Fire: heat/smoke detectors; audible alarms; flashing lights. Detect a change of 'state' • CCTV: PTZ cameras; fixed cameras. Monitor and record activity on site • Maintenance systems: alert staff to faults with systems • Electronic Article Surveillance (EAS) tagging, • Key management systems
	3.3 Identify potential risks to protection systems.	• Sabotage from either external parties or insider threat • Malfunction • Absence of or poor maintenance • User error • Systems failure e.g. electrical outage, • Force Majeure /accidental damage (e.g. natural disaster)
	3.4 Identify types of alarm activations and the actions to take in response to them.	• Follow assignment instructions • Intruder alarm: check panel; contact control; use CCTV to investigate/ in person if safe to do so; call emergency services if appropriate • Fire (heat/smoke); check panel; contact control; if genuine, start official fire evacuation process including calling emergency services • Gas leak: raise the alarm; evacuate; contact supplier • False alarms: activations resulting in emergency services attending unnecessarily. Include alarms activated in error or maliciously activated • Building Maintenance System (BMS) activations: check panel; contact control • Awareness of the implication of excessive 'false alarms' on the emergency service response

4. Know how to minimise risk to personal safety at work.	4.1 Identify responsibilities for personal safety at work.	• **Employer responsibilities:**
		   ○ Provision of assignment instruction
		   ○ Importance of contractor responsibilities
		   ○ Risk assessment
		   ○ Training needs analysis
		   ○ Provision of PPE and other essential equipment
		   ○ Application of current employment legislation

		o Provision of Health and Safety procedures and policies • **Employee responsibilities:** o Follow assignment instructions o Identification of training needs o Attend appropriate training o Fit and well for work/duties o Use of PPE and other essential equipment o Follow company HR policies and procedures
	4.2 Identify situations that might compromise personal safety.	• Lone working • Interrupting a crime in progress • Dealing with intoxicated individuals • High risk locations (e.g. construction sites; remote and higher value site)
	4.3 Identify the risks of ignoring personal safety in conflict situations.	• Increased risk of escalation • Places self and others at increased risk of violence and/or injury • Risk of being considered negligent for any resultant harm
	4.4 State the personal safety benefits of undertaking dynamic risk assessments.	• Ensures a process of analysing risk and the best course of action prior to action, then during and after the incident. • Increases own ability to assess and react to the changing situations
	4.5 List ways to minimise risk to personal safety at work.	• Good communication • Keeping the control room / colleagues informed • Working within the limits of own knowledge and skillset • Prompt action • Control measures including the appropriate use of PPE • Keeping own knowledge and skills up-to-date via CPD
	4.6 Recognise the different types of personal protective equipment relevant to the role of a security officer	• Wearables o Waterproof clothing o High-visibility clothing o headwear o Stab vests o Gloves (needle/slash resistant) o Rubber gloves and face shields o Ear defenders o Eye protection o Safety footwear o Dust mask o Face coverings

		• Equipment o Metal detectors o Body worn cameras (BWC) o Radios, mobile phones o Personal alarms o Torches o Equipment to help control infections
	4.7 State the purpose of using body-worn cameras (BWC)	• Securing evidence against an offender • Deterring crimes • Self-protection • Curbing behaviour (Security Officer or customer) • Identifying offenders
	4.8 Identify strategies that can assist personal safety in conflict situations.	• Awareness • Using dynamic risk assessments • Building rapport • Active listening • Using problem solving techniques • Using CCTV • Working in teams • Knowing when to involve the emergency services
	4.9 Describe limits of own responsibility in physical intervention situations.	• Work within own training, skillset and physical capabilities • Request assistance when appropriate • Legal responsibility for actions and omissions • Current legal framework and responsibilities
	4.10 Identify types of harm that can occur during physical interventions.	*Types of harm:* • Serious injury or death can result from: o strikes and kicks o an individual falling or being forced to ground o interventions involving the neck, spine or vital organs o restraint on the ground (face up and face down) or other position that impairs breathing and/or circulation and increases risk of death through positional asphyxia o any forceful restraint can lead to medical complications, sudden death or permanent disability especially where situational and individual risk factors are present o non-weapon items could cause harm to individual if they were to fall (e.g. glass objects, tools carried on person etc.) • Stress and emotional trauma
	4.11 Identify the personal safety advantages of mental alertness at work.	• Quick reaction time • Awareness of potential hazards • Accurate assessment of situation • Increased potential to prevent escalation

		• Clear identification of hazards and necessary actions to mitigate risk.

	4.12 State the benefits of reflecting on personal safety experiences.	• Improving safety of:
		  ○ Self
		  ○ Staff
		  ○ Visitor/customer
		
		• Learning from what went well and what could have been handled better
		• Informing/identifying improvements to personal and organisational practices and procedures
		• Preventing reoccurrence of the same/similar problem
		• Recognising trends to prevent reoccurrence of the same/similar problems
		• Importance of sharing good practice to improve personal, team and organisational performance
		• Recognising good and poor practice
		• Identifying common responses to situations
		• Identifying procedures or methods to deal with situations effectively.

5. Understand drug-misuse legislation, issues and procedures relevant to the role of a security officer.	5.1 Recognise the signs and symptoms of drug use	• Awareness of Misuse of Drugs Act 1971 including:
		  ○ Possession of drugs
		  ○ Possession of controlled drugs with intent to supply
		  ○ Supplying controlled drugs
		  ○ Manufacturing controlled drugs
		  ○ Allowing the premises to be used to take controlled drugs
		  ○ Class A, B and C drugs
		• Uncoordinated / unusual behaviour
		• Repetitive movement (especially mouth and hands)
		• Dilated or constricted (pinpoint) pupils
		• Excessive sweating
		• Anxiety
		• Feeling drowsy
		• Unconsciousness

	5.2 Identify the signs that may indicate drug dealing	• Suspicious behaviour • Frequent trips to toilets • Meetings with lots of strangers • Lots of people approaching one individual • Covert exchanges of items/cash • Hiding in areas out of view of staff and CCTV • Information from other customers or members of staff / neighbouring property

		• Unusual activity in car park/vicinity of site (especially out of hours) • Drug litter found around the perimeter and or on site
	5.3 State how to dispose of drug related litter and contaminated waste	• Use personal protective equipment (i.e. safety gloves) • Use sharps boxes or bottles for needles • Dispose of blood-stained tissues down the toilet or place in contaminated waste bags
6. Know how to conduct effective search procedures.	6.1 Identify the different type of searches carried out by a security officer.	• General: when everyone is searched • Random: when a random selection of people is searched (e.g. search every fourth person) • Specific: when specific individuals or vehicles are searched for specific reasons (Suspicious people, vehicles / packages etc). • Vehicle • Premises
	6.2 Identify a security officer's right to search.	• As a part of the site admissions policy • As a condition of entry • In accordance with employees' contracts (for entry / exit) • As a loss prevention technique to ensure staff / visitors are not stealing; where sensitive data/industrial espionage is risk to ensure data / intellectual property is not taken off site • Follow same sex searching policy (inc. searches of transgender individuals should be performed according to the 'SIA Trans customers: A guide for door supervisors' guidance) • Only with permission from the person prior to the search • As stated in assignment instructions
	6.3 Identify different types of searching equipment.	• Handheld metal detector (Search wand), ensure sensitivity of equipment is known • Archway Metal detectors (know calibration settings) • Baggage / Packages x-ray scanning, trays for smaller belongings • Search mirrors with lights • Gloves • Torch Search dogs (trained to detect specific threats of concern)
	6.4 Recognise possible hazards when conducting a search.	• Drugs coming into contact with skin • Needles/ Sharp objects • Infectious Diseases

		• Weapons • Violence • Malicious allegations • Un co-operative visitor/client/customer

	6.5 State precautions to take when carrying out a search.	• Use of personal protective equipment (PPE), e.g. safety gloves
		• Use of a dedicated search area with good lighting
		• Carry out searching in pairs if possible
		• Carry out searching in view of CCTV if possible
		• Use self-search techniques
		
		Infectious diseases
		• Use of personal protective equipment (PPE), e.g. safety gloves
		• Use self-search techniques
		
		For Vehicles
		• Ensure own health and safety:
		   o use appropriate PPE including high-visibility clothing and safety footwear etc.
		   o avoid inhaling vehicle fumes
		   o be aware of other moving vehicles
		   o be visible to other motorists
		   o constantly monitor for hazards and risk in the search area)
		• Ensure engine is off and keys are controlled
		• Vehicle is parked in a safe designated location with parking brake applied
		• Ensure driver and any passengers are visible and in a safe location
		• Search location to have good lighting, CCTV and witness where possible.

	6.6 State actions to take if an incident or an accident occurs during searching.	• Contact emergency services • Follow assignment instructions • Summon assistance from first aider (if necessary) • Cordon area off • Complete notebook / report / search log
	6.7 Demonstrate how to search people, and their property.	• Explain the search policy • Obtain permission of person being searched prior to the search • Use effective communication throughout the search • Follow site policy / assignment instructions • Follow same sex searching policy (inc. searches of transgender individuals. These searches should be performed according to the SIA guidance document "Trans customers: A guide for door supervisors' which is located at:

		 • Use appropriate PPE (e.g. protective gloves) • Search with a witness or in view of CCTV • Designated search area / table with good lighting • Consider dignity in front of others • Never ask to remove clothing, other than outer garments e.g. coats, gloves, jumpers. • Use self-searching techniques (where appropriate) • Consideration must be given to protected characteristics o age o disability o gender reassignment o marriage and civil partnership o pregnancy and maternity o race o religion or belief o sex/gender • When searching children and young people: o two staff should be present during search o never ask to remove clothing, other than outer garments like coats, gloves, jumpers o avoid touching o encourage parents/ guardians to assist
	6.8 State typical areas of vehicles to be searched	**Types of Vehicles:** • Cars • Vans • Motorcycles/Cycles • Heavy Goods Vehicles Carry out level/type of search according to assignment instructions Areas to be searched: • Interior (inc. under seats; door pockets; under carpet) • Boot or cargo area • Engine compartment (inc. behind battery) • Outside • Underneath • Toolbox • Voids (in manufacturer-made storage areas and/or voids that may have been altered/customised)
	6.9 Identify reasons for carrying out a premises search.	• Pre-entry check to ensure safety on opening • Identifying potential hazards • Search for drugs, weapons, suspicious packages, missing persons • Find potential lost property

		• Closing check to ensure no personnel remain in toilets, or areas where it is easy to hide/stow away • Lock down to ensure all windows and doors are secure etc.
	6.10 Recognise actions to take in the event of a search refusal.	• Politely explain reasons for search: o condition of entry / employment contract • If visitors/customers do not give consent for a search, then they should be denied entry, inform person they are due to visit • Follow site policy / assignment instructions • Record details in search register / other report
	6.11 Identify reasons for completing search documentation.	• Protection against allegations of misconduct • Protect person who is being searched. • Proof of lawful search for evidential reasons • To capture time, date, people present, reason for search • Search book/ register • Search report • Incident book/ report
	6.12 Identify actions to take if a prohibited or restricted item is found during a search.	• Follow site policy / assignment instructions • If item is against entrance policy but is not illegal, follow the site's policy/assignment instructions. • Consider holding/looking after non-illegal but restricted item(s) before granting entry is and returning item on exit. • Consider seizing / securing the illegal item, refusing entry, recording the find and informing the police. Or; • Consider seizing the illegal item, arresting the individual, calling the police and handing over both the person and the item to the police. • Record the find in line with the site policy / assignment instructions and record details of the find • Inform control room / senior management • If the individual is an employee contact line manager/ Human Resources as detailed in assignment instructions
7. Understand how to patrol designated areas safely.	7.1 State the purposes of patrolling.	• To ensure all is in order • Visual deterrent • Identifies weaknesses in site security and actions needing to be taken
	7.2 Identify types of patrol undertaken by a security officer.	• First or Initial: Those patrols carried out at the beginning of a shift, (or takeover/handover) to identify problems/incidents that need to be dealt with

		• Final: The last patrol carried out before the security officer goes off duty, to ensure that any areas requiring attention have been identified/dealt with
		• Snap, or "one-off" patrol: An additional patrol carried out to respond to a specific incident or situation
		• Lock up/unlock patrols, when required to ensure:
		   o all entry points are secure;
		   o alarms set;
		   o fire precaution measures in place.
		• Unlock patrols ensure safe access/ to staff/ public; emergency exits accessible

	7.3 State patrolling procedures.	• Follow assignment instructions • Ensure radio equipment is tested, fully charged and programmed to correct channel prior to use • Check assignment instructions for frequency / requirements / route • If clocking devices are to be used in what order/ timings • Inform relevant people at beginning (and end) of patrol frequency patterns of patrols and their safety implications. • Vary routes and times • Use relevant (mechanical or electronic) clocking devices to record patrol information • Be vigilant, e.g. for opportunities for intruders/fire; checking fire exits; checking doors and windows are secure etc. • Maintain contact with colleagues/control room • Identify site security breaches • Challenge the unusual/unexpected • Identify the reasons for of using local and site knowledge when patrolling. • Awareness of any local crime issues that may affect security of site Identify suspicious persons, vehicles, packages

	7.4 Identify how to communicate effectively using relevant equipment.	• Equipment
		   o Radio's and earpieces
		   o Mobile phones
		   o Internal telephone systems
		• Communication occurring between:
		   o internal and external colleagues
		   o professionals i.e. within the site or police/external agencies
		• Methods used to communicate clearly and accurately over a radio network:
		   o use of radio protocols to signal start/end of transmissions;
		   o use of clear and concise language;

		o ensure clear and effective communication; o ensure urgent incidents are dealt with quickly

	7.5 Demonstrate effective use of communication devices.	• Accurate, brief and clear
		 • Use of call-signs, pro-words, local code words
		 • Use of the NATO phonetic alphabet
		 • Correct pronunciation of numbers
		 • Professional local radio etiquette
		 • Equipment used:
		    o Radios
		    o Mobile phone
		    o Internal telephone systems
		    o Internal tannoy systems/public address systems
		 • Ensure radio equipment is tested, fully charged and programmed to correct channel prior to use

	7.6 Recognise the importance of check calls.	• Maintains contact with colleagues/control room • Contributes to safety of security officer • Checks that all radio systems are functioning • Provides opportunity to identify any areas of poor radio transmission

	7.7 State how to respond to an incident.	• Follow assignment instructions
		 • Report to control room
		 • Carry out dynamic risk assessment
		 • Cordon off area
		 • Protect evidence
		 • Call the emergency services (if appropriate)
		 • Direct CCTV coverage to area (if possible)
		 • If an indictable offence has been committed, consider arrest
		 • For suspected theft, follow assignment instructions and apply an appropriate method of control e.g. ASCONE
		    o Approach, Select, Conceal, Observe, Non-payment Exit
		 • For cases of trespass follow assignment instructions and apply an appropriate method of control e.g. 5 step appeal to ask them to leave
		    o Ask them to leave
		    o Explain why request has been made
		    o Inform person of potential consequences
		    o Final request and confirmation that they refuse to leave under their own steam
		    o Action, use reasonable force to remove the trespasser from site
		 • For medical incidents, consider using privacy screening
		 • Obtain witness details

		- Corroboration required i.e. two independent sources of evidence - Record details in notebook as soon as possible - Write an incident report and other reporting methods set out in assignment instructions as soon as possible following the incident - Provide statement to Police if required - Take part in debrief - Support colleagues post incident
	7.8 State reasons for recording and preserving crime scenes	- Permanent written record of the event - For evidential purposes - To assist in identifying offenders - To assist outside agencies or court cases - To justify actions taken - To prevent malicious allegations or civil actions
	7.9 State actions to take to preserve evidence after an incident	- Contact the emergency services - Cordon off the area - Contain potential evidence - Control the area - Call for support and inform management - Restrict access - Show police any potential evidence - Record actions
	7.10 Identify circumstances when a security officer should call the police	- Following an arrest - To report: - a serious crime - a serious public order offence - other serious incidents inside or outside of the site - Concern for the welfare of self and others - Suspicious activity with terrorism concerns.

Application of Conflict Management in the Private Security Industry

UP13 04

Level   6
Credit   1
GLH   11
TQT   13

Unit aim:
This unit forms part of the SIA licence-to-practise qualifications for door supervisors, security officers.
It covers application of the principles of conflict management which security operatives are required to know, understand and demonstrate

Essential resources: Access to appropriate scenarios for role play related to specific security role

Learning Outcomes The learner will	Assessment Criteria The learner can	Indicative Content
1 Understand the principles of conflict management appropriate to the role	1.1 Identify situations that can lead to conflict	Common situations leading to conflict • Misunderstandings • Poor communication • Lack of planning • Unrealistic/ unfair expectations • Attitudes • Frustration and stress • Substance and alcohol use
	1.2 State how positive and constructive communication can be used to manage conflict	• Importance of positive and constructive communication • Being positive, professional, calm, clear and polite • Using effective communication skills (vital to defuse and avoid conflict)
	1.3 Recognise why it is important to be familiar with policies and procedures relating to workplace violence	• Employer policies, guidance and procedures relating to workplace violence • Meeting Health and Safety at Work legislation • Setting an expectation for both staff and customers as to what behaviour is and is not acceptable • Making staff aware of their responsibilities in regard to workplace violence

		• Ensuring staff are aware of the procedures to follow in the event of a violent situation • Detailed reporting procedures • Helps reduce risk of litigation and harm to self and others
	1.4 Identify the stages of escalation in conflict situations	Stages of conflict escalation • Frustration leads to • Anger leads to • Aggression leads to • Violence
	1.5 Recognise the stages of the attitude and behaviour cycle	Attitude and behaviour cycle • importance of adopting an appropriate initial response to conflict situations • Link between attitude and behaviour • Positive attitude constructs positive behaviour • Negative attitude constructs negative behaviour • Effective behaviour and communication influencing attitude and behaviour of others
2 Understand how to recognise, assess and reduce risk in conflict situations	2.1 Recognise the potential risk posed in a conflict situation	Risks in potential conflict situations • Identifying potential risk to self and others (staff, customers, bystanders) • Dynamic risk assessment (definition; identifying and assessing risk, taking action to eliminate or reduce risk, monitoring and reviewing, recognise escalation in risk and reacting appropriately) • Possible measures to reduce risk (ensuring staff are trained, effective communication, identifying and assessing potential threats, adapting conflict response to situation • Minimising risk of violence and aggression towards self and others by using communication skills and de-escalation techniques
	2.2 Identify factors that can trigger or inhibit a range of responses in self and others	Factors • Actions • Behaviours (self and others) • Situations • Emotions Triggers • Perceptions • Conflicting goals

		• Different personal values • Misunderstandings • Poor communication Inhibitors • Self-control • Personal values • Fear of retaliation • Social or legal consequences • Body worn cameras and any other technology

	2.3 Identify a range of responses to conflict situations	Range of responses
		• Feeling insulted
		• Feeling threatened
		• Anger
		• Loss of face
		• Being ignored
		• Peer pressure
		• Feeling patronised
		• The feeling of not being taken seriously
		• Alcohol, drugs and medical conditions
		• angry response
		• Fight or flight response
		   o Fear
		   o Adrenaline
		   o Shock
		• fear of being "blocked in"

	2.4 Recognise the stages in de-escalating conflict	Stages in de-escalating conflict • Assess emotional state • Identify trigger factors • Reassure to reduce anxiety • Speak calmly and actively listen • Empathise and check understanding • Problem solving - resolve the issue • Explain what, when, how • Keep informed
	2.5 State the importance of positioning and exit routes	Positioning and exit routes • Maintaining personal space • Demonstrating non-aggressive stance • Ensuring an escape route is visible for all parties • Awareness of exit routes
3 Understand the use of problem-solving techniques when resolving conflict	3.1 Recognise how to use empathy to resolve conflict	Empathy • ability to share someone else's feelings or experiences • imagining being in that person's situation Customer perspective/ resolving conflict

		- what the customer thinks and feels; sees; says: does - customer pain (fears, frustrations, obstacles) - potential gain (goals, wants, needs) - understanding the customer's point of view
	3.2 Identify the benefits of using problem solving techniques	Problem solving techniques - Identify issues - Understand everyone's interests - Identify possible solutions/options - Evaluate options - Select option or options - Document agreement(s) - Agree on contingencies, monitoring, and evaluation Benefits - Managing customer expectations - Building rapport - Building trust - Finding mutual understanding - Demonstrating empathy - Explaining reasons
	3.3 Recognise how win-win approaches work to resolve conflict situations	Win-win situation - Outcome where everyone is satisfied Win-win approaches - Active listening - Empathy - Problem solving - Negotiation
4 Be able to communicate to de-escalate conflict	4.1 Recognise verbal and non-verbal communication techniques	Range of communication techniques Verbal communication - Speaking – pitch, tone, clarity, language - Listening Non-verbal communication - Stance - Body language - Eye contact - Gestures - Signalling non-aggression through non-verbal communication - Personal space awareness
	4.2 Explain how to deal with communication barriers in conflict situations	Barriers heat, pain, fear, noise, shock, language, mental illness, culture, fear of authority, attitude, belief Substance and/or alcohol use

		Overcoming communication barriers • speak clearly, adopt non-aggressive stance, maintain space, move to quieter/lighter space, make sure you are non-threatening, explain what you are doing
	4.3 Identify different behaviour types	Aggressive behaviour • threatening tone • threatening positioning • angry gestures • angry words • concerns of violence • Staring/ uncomfortable eye contact Assertive behaviour • Firm but fair • Calm • Normal positioning • Relaxed body language • Polite/rational speech • Listening • Acknowledging Passive behaviour • Hesitant, apologetic speech patterns • Overly seeking approval • Always agreeing with others • Broken speech pattern • Self-deprecation or self-criticism • Overly quiet speech • Discomfort in groups • Lack of eye contact
	4.4 Demonstrate approaches to take when addressing unacceptable behaviour	Approaches • Non-aggressive body language • Empathy • Be positive and assertive • Actively listen • Problem solving • Follow appropriate organisational policies and procedures
	4.5 Demonstrate ways to de-escalate conflict situations	Conflict de-escalation • Manging communication barriers • Using positive communication • Active listening • Non-verbal communication • Verbal communication • Non-aggressive • Empathy

		• Building rapport/trust • Problem solving • Providing assistance e.g. calling a taxi • Including management in discussions
	4.6 Demonstrate working with colleagues to de-escalate conflict situations	• Positioning • Switching to or from a colleague

Notices

This book does not purport to contain an authoritative or definitive statement of the law or practice on any subject and the publishers supply the information on the strict understanding that no legal or other liability attaches to them in respect of it. References to sources of further guidance or information have been made where appropriate.

Robins Wood House
Robins Wood Road
Nottingham
NG8 3NH