Qualification Specification

BIIAB Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry

Qualification Number: 603/7001/4

BIIAB Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry

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

BIIAB Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry

Table of Contents

1. About the BIIAB Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry

BIIAB Qualifications Limited is regulated to deliver this qualification by Ofqual in England. The qualification has a unique Qualification Number (QN) which is shown below. Each unit within the qualification will also have a regulatory Unit Reference Number (URN).

The QN code will be displayed on the final certificate for the qualification.

Qualification Title	Qualification Number (QN)
BIIAB Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry	603/7001/4

2. Objective and Purpose of this Qualification

The BIIAB Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry is designed to show that learners have obtained and can demonstrate the knowledge and skills required to be a CCTV Operator.

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, and more specifically CCTV operation, 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 CCTV operators must hold a licence to practise issued by the Security Industry Authority (SIA). Successful completion of this course enables a CCTV operator 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.

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 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 Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry Rules of Combination and Structure

To achieve the BIIAB Level 2 Award for CCTV Operators in the Private Security Industry, learners **must** complete all units within the qualification. This **must** consist of:

- Minimum total credit: **3**
- Mandatory Group A **minimum** number of units: **2**
- Minimum Guided Learning Hours: **30 hours**
- Total Qualification Time: **31 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 Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry

Mandatory Group A

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	L/618/5957	Principles of Working in the Private Security Industry	2	2	17	9	8	17	Multiple-choice questions and practical assessment
PPWCCTVO	Y/618/6030	Principles and Practices of Working as a CCTV Operator in the Private Security Industry	1	2	13	13	Not permitted	14	Multiple-choice questions and practical assessment
				Total	30 hours (minimum 4 days)	22 hours (minimum 3 days)	8	31	

Note: The minimum of 3 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 30 hours over 4 days.

It is a requirement that learners undertaking the Level 2 Award for CCTV Operators in the Private Security Industry are trained in:

- Principles of Working in the Private Security Industry
- Principles and Practices of Working as a CCTV Operator in the Private Security Industry

Before the one-to-one CCTV practical assessment is undertaken.

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.

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

Assessment Principles

BIIAB Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry

The Assessment Principles for the Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry 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 and Practices of Working as a CCTV Operator 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 40 questions. The examination will last for 60 minutes and learners will be required to answer correctly 28 of the 40 questions (70%) in order to pass. The practical assessment is an externally set, internally assessed practical CCTV scenario with portfolio and oservation sheet. The practical assessment must be visually recorded for each learner and is recommended to take approximately 25 minutes. Learners will be required to achieve a pass mark of 100% for the practical assessment. Learners are also required to complete a workbook with short answer questions, the pass mark for these is 80%.

Facilities

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/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
   - SVQ/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

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

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.

BIIAB Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry

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 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 'The Application of Reasonable Adjustments and Special Consideration for BIIAB Qualifications' 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 Qualifications Limited 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 Register of Regulated Qualifications (http://register.ofqual.gov.uk).

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
L/618/5957

Level   2
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.
		   o Prevents crime
		   o Cuts down on incidents
		   o Reduces costs by not having to employ additional staff
		   o Can provide clear evidence for investigations
		   o Can provide evidence which can be used in a court of law
		• Understand the legal implications of using CCTV e.g.
		   o 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 • Slander • 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 • Arson • 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: ○ protected characteristics: race/ethnicity/nationality, gender, religion or belief, disability, sexual orientation, gender reassignment, marriage/civil partnership, age, pregnancy and maternity ○ 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. ○ 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	○ Arrest is to take away someone's liberty ○ There is no legal definition for citizen's arrest ○ Police and non-police arrest ○ Arrest with a warrant ○ Arrest without a warrant
	3.2 Identify offences for which a security operative can make an arrest	○ Security operatives have no special powers of arrest, only the same powers of arrest as every other citizen. ○ Arrestable offences, indictable offences and Breach of the Peace

		o Indictable offences are usually tried at the Crown Court
		o Powers of arrest under the common law
		• Offences include:
		   o Murder/Homicide
		   o Aggravated Assault
		   o Assault
		   o Rape
		   o Sexual Assault
		   o Firearms offences
		   o Robbery
		   o Burglary
		   o Theft
		   o Drugs offences
		   o Fraud
		   o Criminal damage

	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:
		   o (a) causing injury to himself or another;
		   o (b) suffering injury himself;
		   o (c) causing loss of or damage to property;
		   o (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: o 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 indictable 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 o 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

		○ Maintain confidentiality of information • Security Operatives should: ○ Use personal social media responsibly including managing privacy settings ○ Not wear anything identifiable outside the workplace ○ keep personal vigilance e.g. not completing surveys ○ Not discuss work issues outside the workplace ○ 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:
		     o What you have seen and what has happened.
		     o Who you saw, what they looked like, what they were wearing.
		     o Where did the situation happen and where you are.
		     o 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;
		     o Centre for the protection of national infrastructure (CPNI)
		     o National Counter Terrorism Security Office (NaCTSO)
		 • Awareness of current initiatives:
		     o 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.
		     o ACT - Action Counter Terrorism
		     o 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
		   o Maintaining organised search procedures
		   o 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:
		   o Internal procedure for site
		   o Confidential (Anti-Terrorist) Hotline: 0800 789 321
		   o British Transport police (BTP) "See it, Say it, Sorted": text 61016 or call 0800 40 50 40
		   o Non-emergency: 101
		   o ACT online reporting
		   o 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:
		  o Contact the police or call Crimestoppers
		  o 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	• Promotes professional service • Increases safety for staff • Promotes teamwork

	operatives to contribute to improving practice	• Increases safety for customers • Identifies procedures or methods to deal with situations effectively

Principles and Practices of working as a CCTV operator in the private security industry

Y/618/6030

Level   2
Credit   1
GLH   13
TQT   14

Unit aim: The learner will be able to understand the role and legal implications attributed to a CCTV Operator and enable the operator to demonstrate that they are able to use the equipment, identify and respond appropriately to multiple incidents and produce supporting evidence for an audit trail

Essential resources: Relevant scenarios**,** CCTV equipment, recording and printing facility, evidence bag, statement template, handover log

Learning Outcomes The learner will	Assessment Criteria The learner can	Indicative Content
Understand the purpose of a surveillance (CCTV) systems and the roles and responsibilities of control room team and other stakeholders.	1.1 Identify the different uses of public space surveillance (CCTV) systems	• Assisting in the prevention, detection and reduction of crime, disorder and anti-social behaviour • Assisting in promotion of community/public safety • Monitoring traffic flow and assist in traffic management issues • Assisting in civil emergencies and counter terrorism • Assisting in the prosecution of offenders
	1.2 State the roles and responsibilities of each member of the control room team.	Roles include: • Team worker: operator, supervisor, manager, systems manager, technical support staff; responsibilities of each; • include observing, recording, reporting

		Other responsibilities include: • Following Home Office guidance • Knowing the difference between private and public areas • Privacy blanking • Knowing what can/cannot be recorded
	1.3 Identify the roles of other stakeholders in public space surveillance (CCTV) systems.	Other stakeholders: • police, customs, health and safety, ambulance, fire and other members of the team during CCTV operations Communication in response to CCTV operations
	1.4 State how to work effectively with a range of stakeholders and other agencies	Working effectively can include: • Pass and receive information from other stakeholders: Police, other members of the CCTV team and other emergency services during CCTV operations • Dealing with a multi-incident and multi-agency operation. Third parties to include: • Emergency services • Statutory agencies • Media Types of assistance: • providing intelligence and information • tracking, searching and securing areas • crowd control/evacuation • recording evidence Utilising: • radio, phone, personnel • dedicated person in room / dedicated telephone line

Understand the different types of legislation and how they impact on Public Space Surveillance (CCTV) operations.	2.1 Identify how the Data Protection Act impacts on to the role of a CCTV Operator	The meaning of "confidentiality" as it applies to the role of a CCTV operator • Compliance with 6 principles of the Data Protection Act** • not disclosing information to any unauthorised persons relating to all operational aspects of the system and data security, • no unauthorised recording e.g. using mobile phones or similar devices • no unauthorised copying of footage. • Body worn cameras • UAVs - Drones Repercussions of breaches e.g; • dismissed, fines and potential prosecution
	2.2 Identify how the Freedom of Information Act impacts on public space surveillance (CCTV) operations	Who it applies to: • local councils and other public bodies only • who can request information under the Act • who and what type of information, only data held on individuals (subject access); • exemptions national security
	2.3 Identify how the Protection of Freedoms Act impacts on public space surveillance (CCTV) operations	The role of Surveillance Camera Commissioner: • to promote the Surveillance Camera Code of Practice and review its operation and impact.
	2.4 Identify how human rights impact on public space surveillance (CCTV) operations	The articles of the Human Rights Act, that impact on role Main articles: • Article 6: right to a fair trial • Article 8: right to privacy and family life • Article 14: prohibition of discrimination

		• Articles are: Absolute, limited and qualified • Impact on CCTV operations such as necessity, proportionate, legal and non-discriminatory
	2.5 Identify how the principles of covert surveillance impact on public space surveillance (CCTV) operations	Purpose of RIPA (Regulation of Investigatory Powers Act); • authorisation of covert/ directed surveillance. Circumstance for authorisation; • who can authorise e.g. police Definition of surveillance (difference between Directed and Intrusive Surveillance) Directed: • Directed surveillance is covert surveillance that is not intrusive and is carried out in relation to a specific investigation or operation. Intrusive: • Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device)
	2.6 Identify how the offence of voyeurism impacts on public space surveillance (CCTV) operations	Safeguarding requirements: • safeguarding children and young people, and others including voyeurism, limits what can view and record • what considerations to take before viewing CCTV material. • Voyeurism falls under the Sexual Offences Act 2003

	2.7 Recognise the impact of Codes of Practice on public space surveillance (CCTV)	Information contained in the Information Commissioner's CCTV Code of Practice • is a public document that governs how processes and procedures for CCTV operators are developed? • ensures evidence admissible in court • increases protection and confidence of the public • ensures compliance with legislation, • raise standards • improve efficiency Surveillance camera code of practice: • the 12 guidance principles and how each principle affects the operator's actions and the procedures they must follow. • SIA Standards of Behaviour • Company procedures, manuals and assignment instructions; industry standards
	2.8 Identify how the use of unmanned aerial vehicles (UAV) is controlled	Role of the CAA (Civil Aviation Authority) and the Air Navigation Order is to • monitor the use of UAV within restricted airspace (Airports) The CCTV operative needs to be • aware of the reporting process and • Communicate sightings to the appropriate services
Understand the importance of operational procedures in public space surveillance (CCTV) operations.	3.1 State why operational procedures are necessary to public space surveillance (CCTV) operations	Value of codes, procedures and guidelines: • public: reassurance, protects; partners: improving efficiency, clear working relationships. • Ensuring integrity of system and personnel that run the system • reassuring the public Definition of operational procedures: • establishes best practice • compliance with legislation • protection of public • protect the CCTV system and staff from complaints and allegations of

		malpractice and expectations under the Data Protection Act
	3.2 Identify the key elements of an operational procedures' manual	Information found in CCTV Operations manual can include the following: • Access control to control room • Emergency Procedures • Health and Safety • Proactive use of CCTV • Duties and Shift Patterns • Image management • Communications and Radios • Legal guidance • Key Handling • Fault reporting methods • System failure and actions • System Maintenance • Essential/useful contact numbers • Releasing Recorded Information
	3.3 State how the operational procedures manual impacts on public space surveillance (CCTV).	System must be: • operated, controlled, maintained within a control room to a set procedure • enables standardisation and consistency to for all operatives work in the same manner • Establishes the boundaries of the procedures
	3.4 State the procedure for creating an evidential audit trail	Importance of accurate and detailed note taking and record keeping: • admissible in court, audit trail, • guidelines for writing notes and records. • consequences of incorrect record keeping Ensure rough notes also kept as can be used as evidence: • Master, copy, bag & tag
Understand how public space surveillance (CCTV)	4.1 Identify how the different components of a surveillance system operate.	Main components of a surveillance system are: • cameras, lenses, operator control,

systems equipment operates.		• keyboard/ touch screen; • display screens, • transmission system • video management system (VMS) recording systems. Emerging technologies are: • AI (Artificial Intelligence) • AFR (automatic Facial Recognition) • ANPR (Automatic Number Pate Recognition) • Biometrics, BWC (Body Worn Cameras) • UAV (Drone)
	4.2 Identify the purpose of functional checks on control room equipment	Ensure all equipment is operational and in full working order: • Minimises system failures Equipment to be checked: • cameras • control equipment (keyboards/joystick) • monitors • recording equipment and computers Log faulty equipment in accordance with operational procedures

Understand Surveillance techniques	5.1 Explain a range of surveillance techniques	Surveillance techniques include:
		• pattern recognition
		• activity profiling
		• pro-active and reactive surveillance techniques
		• Planning surveillance
		• Hotspots (high risk areas)
		• Human behaviours:
		  Suspicious Activity
		  Body Language
		• Situational awareness
		• Incidents & Occurrence
		• Lost contact drills

	5.2 State the standards for capturing evidential images	Images dimensions for evidential purposes. quality/size that could be used; • Identification 100% • Recognition 50%

		• Observation 25% • Detection 10% • Vehicles 50% Quality and frame rate can affect evidential image through high compression levels, low quality and frame rate**.** System performance in adverse conditions: • fog/mist • snow • obstructions (foliage, signs) • low light
	5.3 State actions to take when dealing with multiple incidents	• Work as a team • prioritising of incidents • maximise use of available equipment • communication with team and statutory enforcement agencies (includes notifying if applicable), • completing relevant documentation • post incident actions
Understand different types of incidents and how to respond to them	6.1 Recognise the difference between a crime and non-crime incident	**Non-criminal** • crowd control • evacuation • missing person • accident • fire, traffic • flood • safety issues **Criminal** • theft • robbery • burglary • assault • criminal damage • drug related
	6.2 Identify the CCTV Operators response to a crime and non-crime incident	Actions to be taken when dealing with multiple incidents to a crime and non-crime incident; • communication with police, emergency services, supervisors,

		health & safety executive and local authority Graded Response • Immediate – Risk to life • Routine – May need action • Deferred – No immediate action required Maintain a record of all incidents in the appropriate incident log.
Understand health and safety in the CCTV environment.	7.1 State the guidelines for CCTV operators under the display screen equipment regulations	Health and Safety (Display Screen Equipment) Regulation 1992. • Carry out risk assessment of work station • regular breaks • eye sight test
	7.2 Identify the factors in CCTV operations which may create stress for operators and how to deal with them	Different causes: • work-related • non-work related key indicators: • physical – aches and pains etc • behavioural – mood swings etc • emotional – worrying, anxiety etc • alleviating stress • stress management
	7.3 Identify specific risks and controls when working in CCTV operations.	Specific risks; inside and outside the control room can include: • Fire • Bomb Threats/IED (Improvised Explosive Device) • Trip/slip hazards • Electrical hazards Purpose or risk assessments to include: • identifying and determining risk • minimising risk to reduce and prevent accident • responsibility of complying with health & safety regulations

Demonstrate operational use of CCTV equipment	8.1 Demonstrate functional checks on control room equipment	Functional checks on CCTV control room equipment: • Cameras • control equipment (keyboard/joystick) • monitors • recording equipment • computer • workstation Produce a completed fault log, (include in folder) Communicate using a range of devices
	8.2 Demonstrate how to use surveillance equipment	Use CCTV control room equipment including the use of: • controllers • recording devices • monitors • Video Management Systems (VMS) • Use of Pan, Tilt, Zoom (PTZ) • BWC (Body worn camera) -as applicable • UAV (Drone) as applicable • Overcome problems caused by weather
	8.3 Demonstrate surveillance techniques	• Prioritise during multiple incidents Detect and track/follow suspect on foot or in a vehicle: • locate, track • secure evidence and images • use of Pan, Tilt, Zoom (PTZ) Lost contract drill and searching • last location check • use of multiple cameras • methodical and systematic searching • use of Pan, Tilt, Zoom (PTZ) to conduct zoom in/out 360 degree checks
	8.4 Demonstrate effective use of communication devices	Use different communication methods to pass and receive information

		Give clear and accurate descriptions of people, vehicles and events: • Suspicious activity • description of individual persons • a group • a vehicle • an incident • provide location and directions, individual: • gender • age • build/weight • height • clothing • distinguishing features • ethnicity, hair etc. Vehicle • car colour • registration • make/type (as a minimum) type of incident: • location • who /what is involved • describe event as unfolds • complete relevant documentation
	8.5 Obtain an evidential image	Produce images of quality/size that could be used as evidence: • Identification 100% • Recognition 50% • Observation 25% • Detection 10% • Vehicles 50%
Produce evidential documentation	9.1 Produce documents required for the audit trail	• Copy of rough notes taken during the incident • Incident report • Copy of recorded images (practical assessment) • Print log • Evidence labels • Evidence review log • Evidence handover document • Fault log (as 8.1) • Statement detailing actions

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.

© BIIAB Qualifications Limited January 2021

Infor House
1 Lakeside Road
Farnborough
Hampshire
GU14 6XP