QNUK Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry (RQF)
603/7303/9

Contents

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

1. Introduction

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

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

2. Contact Us

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

Head Office:

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

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

3. Version Number

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

Document owner	SJD Director
Date last updated	17/02/2021
Next review	17/02/2024
Status	Draft
Version	1
Document control number	QS|L2SIACCTV

4. Qualification Objective

This qualification has been developed by the Security Industry Authority (SIA) in collaboration with all endorsed Awarding Organisations and various expert working groups. Learners who are successful in achieving this qualification will become eligible to apply for an SIA licence to practice within the private security industry in the United Kingdom, supporting a role in the workplace.

5. Sector Support and Industry Recognition

This qualification is directly supported and developed by the Security Industry Authority and their endorsed Awarding Organisations (QNUK, Pearson, NOCN, Laser, SFJ Awards, Highfield Qualifications and BIIAB)

6. Geographical Coverage of this Qualification

This qualification is available in England, Wales, Scotland and Northern Ireland.

The legal systems of Scotland and Northern Ireland differ from that of England and Wales. Differences in the legal systems are reflected in the delivery of relevant sections of the qualifications. Employers however may not know which version of the qualification an employee may have taken, so the SIA advises that operatives and their employers remain responsible for being familiar with the laws and legal system relating to the area in which they will be working

7. Benefit for Learners

This is an SIA licence linked qualification, meaning that successful learners will be notified to the SIA which provides a necessary requirement towards obtaining a licence to perform the role of a CCTV Operator in the private security industry.

8. Progression

Learners could progress to the:

QNUK Level 3 Award in Understanding Security Management (RQF)

QNUK Level 3 Award in Security Management (RQF)

QNUK Level 3 Award in Retail Loss Prevention (RQF)

9. Recognition of Prior Learning

QNUK would welcome requests for recognition of prior learning (RPL) where a learner is able to provide sufficient, reliable and valid evidence of achievement for the following units if they have been achieved after 1st April 2021 and accompanied by either a Unit credit or full qualification, issued by an SIA Endorsed Awarding Organisation, containing them:

- Principles of Working in the Private Security Industry

10. Qualification Information

Qualification Number (QN)	603/7303/9
Learning Aim	
Total Qualification Time (TQT)	30
Guided Learning Hours (GLH)	30
Credit value	3
Level	2
Validity	Lifetime, subject to SIA 'Top Up' requirements for relicensing
Assessment	Invigilated MCQ paper (MCQ), practical observations (Obs)
Achieving the qualification	Learners must achieve the 2 mandatory units

11. Qualification Structure

Unit No.	Unit Title	Level	GLH	TQT	Credit
Mandatory units					
H/618/6791	Principles of Working in the Private Security Industry	2	17	17	2
F/618/6796	Principles and Practices of Working as a CCTV Operator in the Private Security Industry	2	13	13	1

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

12. Learner Entry Requirements

12.1. Learner Age

Only those aged 18 or over may hold an SIA licence. Learners aged 16 or over may take this qualification, however they must be made aware that they may not apply for an SIA licence until they are 18 years old. 16-17-year-olds are exempt from the requirement of video recording their practical assessment. In these cases, alternative evidence, such as a transcript, must be provided.

12.2. English Language

Security operatives are likely, in the course of their work, to be required to make calls to the emergency services, or for example, communicate to resolve conflict. It is therefore 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 assessment 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.

13. Delivery

This qualification is delivered in a face-to-face setting over a 3-or-4-day period (depending if distance learning is used for the applicable units). Learners should complete the qualification within 5 weeks of commencement of the course.

13.1. Venue Requirements

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

- The assessment room for MCQ examinations must meet QNUK SIA Examination and Invigilation Policy requirements.

- To be able to deliver and assess the learning outcomes and assessment criteria of unit Principles and Practices of Working as a CCTV Operator in the Private Security Industry, training centres must ensure.

- As a minimum a CCTV system should have at least two PTZ cameras and associated recording and monitoring equipment within a control room. If a control room is not available a simulated control room environment must be used.

- A simulated control room environment is a room that during training and assessment can be used solely for this purpose.

- The ratio of trainers to learners; one trainer to maximum 12 learners for the delivery of practical skills with the assessment completed on a 1 – 1 basis.

- The completion of documentation and portfolio creation can be conducted within a classroom (group) environment.

- These practical assessments must take place after the delivery of the following units.
    - Principles of Working in the Private Security Industry.
    - Principles and Practices of Working as a CCTV Operator in the Private Security Industry.

13.2. Equipment Requirements

Please see 13.1 for CCTV equipment requirements. Additionally, the centre is required to provide a minimum of two handheld radios for the communication element of assessment.

13.3. Blended Learning

Virtual Learning Environments (VLE) are acceptable for the knowledge elements of this qualification; however, the practical requirements still require face to face learning and assessment. Centres wishing to deliver via VLE must gain pre-authorisation from QNUK prior to delivery.

13.4. Trainer to Learner Ratio

The maximum Trainer to learner ratio for this qualification is 1: 12

13.5. Recommended Resources

- Security Industry Authority website
  https://www.gov.uk/government/organisations/security-industry-authority

- ACT (Action Counters Terrorism) Awareness e-learning:

https://www.gov.uk/government/news/access-to-online-counter-terrorism-training-made-easier-for-home-users

- Information Commissioner's Office (ICO)

  https://ico.org.uk/

14. Centre Personnel Requirements

14.1. Trainer/Assessors delivering licence-linked qualifications

Approved trainers/assessors seeking to deliver licence-linked qualifications must have successfully completed a range of formal qualifications. These are detailed below.

All trainers/assessors must have achieved as a minimum.

Trainer Requirements
- 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

- 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.

14.2. Assessor Qualifications

Assessors to 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.

- 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 these qualifications, they will have until 30th September 2022 to achieve them.

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

14.3. Internal Quality Assurer

Internal Quality Assurer (IQA) to hold any of the following qualifications.

- 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 at the launch of these qualifications, they will have until 30th September 2022 to achieve one.

15. Assessment Requirements

Learners are assessed for this qualification through:

15.1. Multiple-Choice Question Papers (MCQ)

The MCQ papers will be taken under examination conditions, i.e. learners will sit a minimum of 1.25 metres apart, will not confer during the examination and no electronic devices (such as mobile phones) or books, including dictionaries, will be permitted.

Principles of Working in the Private Security Industry

Language of assessment	English
Duration	110 minutes
Pass mark	70% (51 / 72)
Grading	Pass / Fail

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

Language of assessment	English
Duration	60 minutes
Pass mark	70% (28 / 40)
Grading	Pass / Fail

Example MCQ is included at Appendix 3, page 35.

15.2. Practical Observations (Obs)

Externally set, internally assessed activities across both units based on the completion of set tasks. Activities are identified in Appendix 1 as Obs within the Types of evidence column

Pass Mark = 100%

15.3. Short Answer Questions (SAQ)

Externally set and internally assessed workbook

Pass mark = 80% for the short answer element of workbook

16. External Marking

All SIA licence linked qualification MCQ exams are externally marked by QNUK.
Practical observations and portfolios of evidence are externally set and internally marked by the centre but subject to 100% moderation in the case of written assignments and verified via risk assessed modelling in the case of practical observations.

QNUK use a combination of video recorded evidence and centre quality assurance visits to verify practical observations and assessments.

17. Resits

Learners who require to resit any failed unit/s MCQ may do so for one further attempt without incurring cost to the centre or learner, however it is the centre's responsibility to ensure the learner has a realistic chance of success and provide additional coaching and learning support where required. Any resit examination must be taken within 3 weeks of the centre receiving the result, outside of 3 weeks the learner will require to attend the full learning for that unit prior to attempting the examination.

18. Reasonable Adjustments

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

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

19. Results

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

Appendix 1: Units

Unit 1 Principles of Working in the Private Security Industry

Unit Summary

This unit provides the learner with basic knowledge which supports development into specialist units. Establishing the roles, responsibilities and general legislation which is applicable to all individuals operating within the licenced private security sectors is the key objective of this important unit.

1. The learner will: Know the main characteristics and purposes of the Private Security Industry		Types of Evidence
Assessment Guidance The learner must		**Types of Evidence**
1.1	Identify the key purposes of the private security industry	MCQ
1.2	State the aims and functions of the Security Industry Authority (SIA)	MCQ
1.3	Recognise the required standards of behaviour of a security operative	MCQ
1.4	Identify the benefits of community safety initiatives	MCQ
1.5	Recognise how assignment instructions support the Security Operative role	MCQ
1.6	Recognise how each security operative role may use CCTV	MCQ
1.7	Identify the limitations of CCTV within the security operative role	MCQ
1.8	State the purpose of the Approved Contractor Scheme	MCQ

2. The learner will: Understand legislation as it applies to a security operative		Types of Evidence
Assessment Guidance The learner must		**Types of Evidence**
2.1	Identify the differences between Civil and Criminal Law	MCQ
2.2	State the main aims of the Private Security Industry Act 2001	MCQ
2.3	Identify key legislation relating to promoting equality and diversity in the workplace	MCQ
2.4	Identify licensable roles under the Private Security Act	MCQ
2.5	Identify how data protection regulation impacts on the security operative	MCQ

3. The learner will: Understand arrest procedures relevant to security operatives		Types of Evidence
Assessment Guidance The learner must		**Types of Evidence**
3.1	State the meaning of arrest	MCQ
3.2	Identify offences for which a security operative can make an arrest	MCQ
3.3	Identify the limitations to a security operative's powers of arrest.	MCQ
3.4	State procedures to follow when making an arrest	MCQ
3.5	State why an arrest should only be made as a last resort	MCQ
3.6	State procedures following an arrest	MCQ
3.7	State what is meant by 'reasonable' and 'necessary' force	MCQ

4. The learner will: Understand the importance of safe working practices		
Assessment Guidance The learner must		**Types of Evidence**
4.1	Identify responsibilities under the Health and Safety at Work etc. Act	MCQ
4.2	Identify the risks of lone working within the private security industry	MCQ
4.3	Identify typical workplace hazards and risks	MCQ
4.4	State how to minimise risk to personal safety at work	MCQ
4.5	Identify safety signs and signals	MCQ
4.6	State procedures to be followed for recording and reporting accidents and health and safety incidents	MCQ
4.7	Identify ways to keep personal information safe	MCQ

5. The learner will: Understand fire procedures in the workplace		
Assessment Guidance The learner must		**Types of Evidence**
5.1	Identify the elements that must be present for fire to exist	MCQ
5.2	State the actions to be taken upon discovering a fire	MCQ
5.3	Identify basic fire safety controls	MCQ
5.4	Identify classifications of fire	MCQ
5.5	Identify the different types of fire-fighting equipment	MCQ
5.6	Identify the role of a fire marshal in the event of an emergency	MCQ

6. The learner will: Understand emergencies and the importance of emergency procedures		
Assessment Guidance The learner must		**Types of Evidence**
6.1	Identify the key emergency terms	MCQ
6.2	Identify different types of emergencies within the workplace	MCQ
6.3	Recognise how people react when emergencies occur	MCQ
6.4	Identify actions to be taken in an emergency situation	MCQ
6.5	Identify the role of the security operative in relation to first aid incidents	MCQ
6.6	Recognise evacuation principles	MCQ

7. The learner will: Understand how to communicate effectively as a security operative		
Assessment Guidance The learner must		**Types of Evidence**
7.1	Identify the different types of communication	MCQ
7.2	State the importance of effective communication	MCQ

7.3	Identify the benefits of teamwork in the private security industry	MCQ
7.4	State the principles of customer service	MCQ
7.5	Recognise diverse customer needs and expectations	MCQ

8. The learner will: Understand record keeping relevant to the role of the security operative	
Assessment Guidance The learner must	**Types of Evidence**
8.1	State the importance of accurate record keeping	MCQ
8.2	Identify the types of records that may need to be completed	MCQ
8.3	Identify what information to include in records	MCQ
8.4	Demonstrate the accurate completion of an evidential statement (Section 9 Statement)	Obs
8.5	State the process of attending court to give evidence	MCQ

9. The learner will: Understand terror threats and the role of the security operative in the event of a threat	
Assessment Guidance The learner must	**Types of Evidence**
9.1	Identify the different threat levels	MCQ
9.2	Recognise the common terror attack methods	MCQ
9.3	Recognise the actions to take in the event of a terror threat	MCQ
9.4	Identify the procedures for dealing with suspicious items	MCQ
9.5	Identify behaviours that could indicate suspicious activity	MCQ
9.6	Identify how to respond to suspicious behaviour	MCQ

10. The learner will: Understand how to keep vulnerable people safe	
Assessment Guidance The learner must	**Types of Evidence**
10.1	Recognise duty of care with regard to vulnerable people	MCQ
10.2	Identify factors that could make someone vulnerable	MCQ
10.3	Identify actions that the security operative should take towards vulnerable individuals	MCQ
10.4	Identify behaviours that may be exhibited by sexual predators	MCQ
10.5	Identify indicators of abuse	MCQ
10.6	State how to deal with allegations of sexual assault	MCQ
10.7	State how to deal with anti-social behaviour	MCQ

11. The learner will: Understand good practice for post incident management	
Assessment Guidance The learner must	**Types of Evidence**
11.1 Identify sources of post incident support available	MCQ
11.2 State why accessing support following an incident is important	MCQ
11.3 State the benefits of reflecting on incident	MCQ
11.4 Identify why it is important for security operatives to contribute to improving practice	MCQ

What needs to be learnt?	
1.1	• 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	• 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	• 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	• 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	• 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	• Benefits of using CCTV e.g. o Prevents crime o Cuts down on incidents o Reduces costs by not having to employ additional staff

2.2 *(continued from previous)*		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		• Privacy issues and concerns • Vulnerable to damage and vandalism • Misuse • Cannot prevent crime • Cost • Familiarity with scope of cover • Technology vulnerabilities
1.8		• Raise performance standards • Assist the SIA to develop new opportunities • Increased customer confidence
2.1		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 (defamation in Scotland) • 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 (wilful fire raising in Scotland) • Kidnapping or holding someone against their will
2.2		• 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	• 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	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	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
3.1	• 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	• 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
	• Indictable offences are usually tried at the Crown Court (Arrestable offences are usually tried at Sheriff Court/High Court in Scotland)
	• Powers of arrest under the common law
	• Offences include:
	    ○ Murder/Homicide (Culpable Homicide in Scotland)
	    ○ Aggravated Assault (Serious Assault in Scotland)
	    ○ Assault
	    ○ Rape
	    ○ Sexual Assault
	    ○ Firearms offences
	    ○ Robbery
	    ○ Burglary (Housebreaking in Scotland)
	    ○ Theft
	    ○ Drugs offences
	    ○ Fraud
	    ○ Criminal damage (Malicious mischief in Scotland)

3.3	• 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	• 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	• Taking someone's liberty is a serious matter • Can only arrest for indictable offences (Arrestable offences in Scotland) • 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	• 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	• 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
4.1	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	• Being isolated and having to rely on technology for back up
	• Being vulnerable:
	    ○ Injury / ill-health
	    ○ Violence
	    ○ Lack of support
	    ○ Lack of communication
	    ○ Lack of welfare facilities for rest

4.3	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	• 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	• Different categories of sign: e.g. prohibition, warning, mandatory, safe condition, fire-fighting, hazard/chemical warning plates
4.6	• 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	• 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
5.1	• Components of fire: the fire triangle (oxygen, fuel, heat - chemical chain reaction)
5.2	• 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	• 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	• 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	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	• 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
6.1	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	Types of emergency: • power, system or equipment failure; flood; actual or threatened serious injury; serious illness; bomb threat, fire, terror threat

6.3	Types of reactions: • Public/human responses – fight or flight • Panic, freeze • Crowd control, danger of crushing
6.4	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	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	• 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
7.1	• 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	• 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	• Promotes safety • Provides a professional and safe service and establishment • Supports colleagues

	• Promotes efficiency
7.4	• 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	• 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
8.1	• 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	• 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	• 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	**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	• Follow organisation's policies and procedures • Follow any legal advice from representative • Be punctual and prepared

9.1	• 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	• 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	• 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.
	   o 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	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	• 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	• 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

10.1	• 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	• 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	• 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	• 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	• Restricting freedom of individuals • Unexplained bruising • Lack of confidence and insecurity • Change in circumstances e.g. cleanliness, appearance
10.6	• Follow organisation's policies and procedures • Notify police • Safeguard victim • Separate victim from assailant • Record and document all information
10.7	• 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.
11.1	• 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	• 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	• 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	• Promotes professional service • Increases safety for staff • Promotes teamwork • Increases safety for customers • Identifies procedures or methods to deal with situations effectively

Rationale for level			
	Level	**Emphasis**	**Comments**
Knowledge	2	Very Strong	High volume of Level 2 command verbs
Skills	2	Weak	A single entry for a practical task
Overall	2	Strong	Whole unit is within the cognitive domain range expected at level 2. Very little stretch, challenge or reflection deviating from Level 2

Rationale for TQT and credit		
	Hours	**Comments**
Guided learning	**17**	**8 hours of this can be directed study**
Directed study	Optional 8	
Independent study	N/A	
Work-based learning	N/A	
Non invigilated assessment	N/A	
TQT:	17	**Credit:** 2

Unit Summary

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

1. The learner will: Understand the purpose of a surveillance (CCTV) systems and the roles and responsibilities of control room team and other stakeholders.		
Assessment Guidance The learner must		**Types of Evidence**
1.1	Identify the different uses of public space surveillance (CCTV) systems	MCQ
1.2	State the roles and responsibilities of each member of the control room team.	MCQ
1.3	Identify the roles of other stakeholders in public space surveillance (CCTV) systems.	MCQ
1.4	State how to work effectively with a range of stakeholders and other agencies	MCQ

2. The learner will: Understand the different types of legislation and how they impact on Public Space Surveillance (CCTV) operations.		
Assessment Guidance The learner must		**Types of Evidence**
2.1	Identify how the Data Protection Act impacts on to the role of a CCTV Operator	MCQ
2.2	Identify how the Freedom of Information Act impacts on public space surveillance (CCTV) operations	MCQ
2.3	Identify how the Protection of Freedoms Act impacts on public space surveillance (CCTV) operations	MCQ
2.4	Identify how human rights impact on public space surveillance (CCTV) operations	MCQ
2.5	Identify how the principles of covert surveillance impact on public space surveillance (CCTV) operations	MCQ
2.6	Identify how the offence of voyeurism impacts on public space surveillance (CCTV) operations	SAQ
2.7	Recognise the impact of Codes of Practice on public space surveillance (CCTV)	MCQ
2.8	Identify how the use of unmanned aerial vehicles (UAV) is controlled	MCQ

3. The learner will: Understand the importance of operational procedures in public space surveillance (CCTV) operations.		
Assessment Guidance The learner must		**Types of Evidence**
3.1	State why operational procedures are necessary to public space surveillance (CCTV) operations	MCQ
3.2	Identify the key elements of an operational procedures' manual	MCQ
3.3	State how the operational procedures manual impacts on public space surveillance (CCTV).	MCQ
3.4	State the procedure for creating an evidential audit trail	MCQ

4. The learner will: Understand how public space surveillance (CCTV) systems equipment operates.		
Assessment Guidance The learner must		**Types of Evidence**
4.1	Identify how the different components of a surveillance system operate.	MCQ
4.2	Identify the purpose of functional checks on control room equipment	MCQ

5. The learner will: Understand Surveillance techniques		
Assessment Guidance The learner must		**Types of Evidence**
5.1	Explain a range of surveillance techniques	SAQ
5.2	State the standards for capturing evidential images	SAQ
5.3	State actions to take when dealing with multiple incidents	SAQ

6. The learner will: Understand different types of incidents and how to respond to them		
Assessment Guidance The learner must		**Types of Evidence**
6.1	Recognise the difference between a crime and non-crime incident	MCQ
6.2	Identify the CCTV Operators response to a crime and non-crime incident	MCQ

7. The learner will: Understand health and safety in the CCTV environment.		
Assessment Guidance The learner must		**Types of Evidence**
7.1	State the guidelines for CCTV operators under the display screen equipment regulations	MCQ
7.2	Identify the factors in CCTV operations which may create stress for operators and how to deal with them	MCQ
7.3	Identify specific risks and controls when working in CCTV operations.	SAQ

8. The learner will: Demonstrate operational use of CCTV equipment		
Assessment Guidance The learner must		**Types of Evidence**
8.1	Demonstrate functional checks on control room equipment	Obs
8.2	Demonstrate how to use surveillance equipment	Obs
8.3	Demonstrate surveillance techniques	Obs
8.4	Demonstrate effective use of communication devices	Obs
8.5	Obtain an evidential image	Obs

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

9. The learner will: Produce evidential documentation		
Assessment Guidance The learner must		**Types of Evidence**
9.1	Produce documents required for the audit trail	Obs

What needs to be learnt?	
1.1	• 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	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	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	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

© Qualifications Network Ltd 2021   QS|L2SIACCTV: v1   Page | 26

	Utilising: • radio, phone, personnel • dedicated person in room / dedicated telephone line
2.1	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	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	The role of Surveillance Camera Commissioner: • To promote the Surveillance Camera Code of Practice and review its operation and impact.
2.4	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	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	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	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	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
3.1	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	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	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	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
4.1	Main components of a surveillance system are: • Cameras, lenses, operator control, • 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	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

5.1	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	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	• 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
6.1	**Non-criminal** • Crowd control • Evacuation • Missing person • Accident • Fire, traffic • Flood • Safety issues **Criminal** • Theft • Robbery • Burglary • Assault • Criminal damage • Drug related
6.2	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.
7.1	Health and Safety (Display Screen Equipment) Regulation 1992. • Carry out risk assessment of work station • Regular breaks • Eye sight test
7.2	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	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
8.1	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	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	• 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	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	Produce images of quality/size that could be used as evidence: • Identification 100% • Recognition 50% • Observation 25% • Detection 10% • Vehicles 50%
9.1	• 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

Rationale for level			
	Level	**Emphasis**	**Comments**
Knowledge	2	Strong	High volume of Level 2 command verbs
Skills	2	Strong	Multiple skills entries
Overall	2	Strong	Whole unit is within the domain range expected at level 2. Very little stretch, challenge or reflection deviating from Level 2

Rationale for TQT and credit			
	Hours	**Comments**	
Guided learning	13		
Directed study	N/A		
Independent study	N/A		
Work-based learning	N/A		
Non invigilated assessment	N/A		
TQT:	13	**Credit:**	1

Appendix 2: Command Verbs

To ensure that learners can meet the requirements of each criterion, they should be explained to the learner prior to assessment and fully understood by the Assessor for this qualification.	
Conduct	Carry out
Demonstrate	Apply skills in a practical situation and/or show an understanding of the topic
Describe	Write or speak about the topic or activity giving detailed information
Establish	Set up on a permanent basis; Get generally accepted; Place beyond dispute
Explain	Make clear. Give reasons for
Identify	Provide brief information about a subject, specific process or activity
Implement	Put into practical effect; Carry out
Produce	Carry out or do / Take an action / Follow an instruction
Provide	Supply relevant information, products or resource

(this list is not exhaustive)

Appendix 4: Specimen Assessment Material

1	Which one of the following activities does not require an SIA licence to perform

    A   Checking identity prior to admission

    B   Searching a person's bag

    C   Removing a trespasser

    D   Providing customers with directions

2	When a vehicle is used to contain an improvised explosive device, it is known as a

    A   VBIED

    B   PBIED

    C   ABIED

    D   MBIED

3	Which one of the following statements is true?

    A   Intrusive surveillance can happen if the CCTV operator suspects criminal activity

    B   Intrusive surveillance requires authorisation under RIPA from a senior police officer

    C   Intrusive surveillance can be authorised by the CCTV room supervisor

    D   Intrusive surveillance cannot be conducted in any circumstances