RightChoice
CONSULTANCY & TRAINING LTD
Security & First Aid Training Providers and ISO and Quality Management Consultants

PRINCIPLES OF WORKING IN THE PRIVATE SECURITY INDUSTRY WORKBOOK

To be read prior to the start of the course by each learner

PRINCIPLES OF WORKING IN THE PRIVATE SECURITY INDUSTRY

Introduction

This book has been written to support your learning towards an SIA licence-linked qualification. This unit is also known as the 'common unit' as it forms the foundation for three of the four qualifications within the security suite. Please keep this book safe to revise for your exams and for future reference.

Important

If this book has been allocated to you for the purposes of self-study prior to attending an SIA licence linked qualification, it is important that you spend no less than 8 hours reading, researching, and revising the content prior to attending your first day of the course.

Contents

Chapter 1 - Know the main characteristics and purposes of the Private Security Industry

What is Security?

'A state of **feeling** or **being** safe and secure'

The security industry provides manned and technical protection to premises, people, and their property. Security is provided in three ways:

- Manned Security (people)
- Physical Security (hardware)
- Systems (technology)

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

Jobs in the Private Security Industry

There are many types of jobs available within the private security industry, including (but not limited to):

- Event Steward
- Close Protection Operative
- Drone Pilot
- Guard Dog Handler
- Security Officer
- Door supervisor
- Behavioural Detection Officer
- CCTV Operator
- Private Investigator
- Cash & Valuable in Transit (CViT)
- Vehicle Immobilizer
- Alarm Engineer

Some of these are classified as **'licensable activities'**, meaning you need a licence to perform these activities, these are highlighted in red within the list above. Failing to do so is a criminal offence under the Private Security Industry Act 2001.

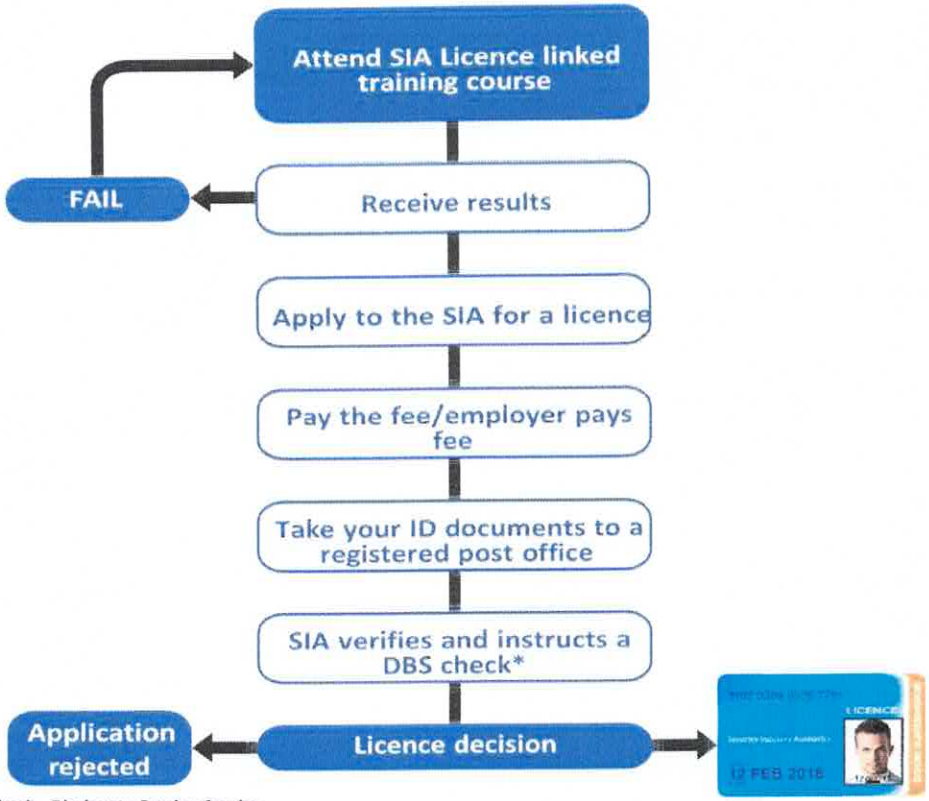
Career Paths

Some security operatives immediately find their ideal job and have many years of happy service in that role; however, many people seek to specialise or progress as they would with any organisation.

Here are some key points to know:

- You must have a licence to work
- Your licence is valid for 3 years
- Criminal offence to work without one
- Up to £5,000 fine or 6 months in prison
- Criminal offence for an employer to use an unlicensed person
- A Security Operative MUST have their SIA Licence on display at all times whilst on duty (unless there is a valid purpose or reason why it needs to be concealed i.e., plain clothes store detective, but it still must be carried.)

The process for applying for an SIA licence



*DBS check - Disclosure Barring Service

Learn more about the SIA at www.gov.uk/government/organisations/security-industry-authority

Monitoring and Partnerships

The SIA works closely with other agencies and authorities to conduct 'spot checks' to ensure all security operatives are carrying the appropriate licence for the activity they are performing, likewise the security operative will work alongside these agencies and authorities to promote the safety and security of the public.

Local authorities

The role of the local authorities surrounds the licencing of certain premises, such as nightclubs, pubs, events, restaurants, cinemas, off- licenses, certain shops etc. There are local licensing officers who act on behalf of the local authorities to ensure the premises licence conditions are being adhered to, this includes the use of appropriately licenced (SIA) security staff.

Crime reduction initiatives

There are many local initiatives and partnerships that a security operative might link into as part of their role. They form local communities with a common interest in reducing crime and increasing safety via a network of stakeholders.

Often this includes information sharing (within lawful boundaries) and communication. Live communication between retail outlets, pubs, clubs, police, town/city centre CCTV control rooms and taxis, to name but a few, provides an excellent ability to provide immediate support to prevent known offenders entering a premises or apprehend those suspected of committing a crime. The same networks enhance the ability to identify and provide support to vulnerable people and locate those who are in need of assistance.

Some example schemes are:

- Pubwatch
- Crimestoppers - Information exchange with police and other authorities for non-emergency situations
- Retail crime partnerships

Assignment Instructions (AIs)

All security operatives need to have access to a document which defines exactly what they are supposed to do in their role in relation to the contract with the client, their employer's in-house requirements and UK legislation. This document is known as the 'Assignment Instructions' which should be read from cover to cover by a new security operative to any new site and referred to in times of uncertainty, for example to know who to report to if an alarm system activates and the required steps to resolve and reset.

The assignment instructions (or sections relating to the security operative's particular role) are often provided as part of an induction programme and often required to be signed by the operative as confirmation of understanding. AIs are typically left in a secure location within the site or venue control room, however strict caution around their confidentiality and data protection must be observed at all times as in the wrong hands may compromise the site and the safety of all the staff.

Functional Information often found within AIs

- Shift times
- Site Plans
- Risk Assessments
- Contact details
- Location of high value assets
- Location of vulnerable points (VP's)
- Required patrol times/routes
- Location of equipment and PPE
- Access or ingress and egress procedures
- Search requirements/procedures
- Reporting procedures Emergency contacts
- Operating instructions for various equipment (alarm system, radios, access
- Control barriers etc) Location of check points
- Paperwork to be completed

- First Aid procedures
- Methods of communication
- Emergency procedures
- Timings of opening/closure
- Opening/closure procedures

Working with Closed Circuit Television (CCTV) systems

More than ever before it is likely that all security operatives will be working with or alongside CCTV systems. It is important to know what you can and cannot do with them to avoid criminal offences, which are easily committed if a security operative is unsure of their responsibilities.

Firstly, any CCTV system which is used to monitor members of the public for behaviour or safety must hold a valid SIA CCTV Operator licence regardless of if the cameras are in public space or on private property. Any frontline licence holder is allowed to monitor for the protection of property or premises. Similarly, 'in house' staff employed directly by the site or venue may do so without requiring an SIA licence, however they must be authorised by the owner of the system.

Some examples of this are:

- All staff in a town centre CCTV control room will have SIA CCTV licences
- Security operatives working with a Security Officer licence viewing live camera footage at the front of retail stores within their podium
- The assistant manager at a warehouse (without a CCTV licence) finding video footage of a break in to provide to the police.

In essence, if a security operative is not directly employed by the site or venue as one of their own staff, then they will need an SIA licence to operate as a third party under contract via the assignment instructions and duty register. The way they are permitted to use a CCTV system is dictated by the purposes and function of the system.

Benefits of working with CCTV

- Prevents crime
- Cuts down on incidents
- Reduces costs by not having to employ additional staff
- Can provide clear evidence for investigations
- Can provide evidence which can be used in a court of law

Legal implications of CCTV

Aside from the SIA licence requirements, there is a lot of legislation surrounding the use of CCTV systems and the data they collect. Firstly, the system itself must be registered with the Information Commissioner's Office (ICO) who act as a regulator for data collection and have very specific requirements to ensure the system is used within the boundaries of various legislation such as:

- Human rights
- Protection of the freedoms
- Data Protection
- Equality

Some of the requirements include the nomination of a person responsible for the system and its data, appropriate signage on

site to advise the public of its use, appropriate positioning of cameras avoiding areas which infringe an individual's human rights (such as toilets or changing rooms), the control of the recorded footage (data protections) and many others

There are, however, practical limitations to the use of CCTV systems which security operatives and clients must be aware of:

- Vulnerable to damage and vandalism
- Potential for misuse
- Cannot physically prevent a crime or manage conflict
- Professional systems can be expensive to set up and maintain
- Technical vulnerabilities, such as power cut, internet failure and system hacking

Learn more about the ICO at www.ico.gov.uk

Chapter 2 - Understand legislation as it applies to a security operative

The differences between Civil and Criminal law

Civil law is used to resolve disputes or arguments between two or more parties. The aim of the court is to bring a resolution to the dispute and decide through the **balance of probabilities** what the appropriate outcome should be, such as compensation, a form of injunction or residency orders.

Criminal law is used when a person or company has potentially committed a criminal offence. When guilt is proven **beyond reasonable doubt**, the court has the authority to impose a custodial sentence imprisonment) and/or community solutions such as unpaid work or fines.

Civil Law

Examples of Civil Disputes:

- Trespass
- Land disputes
- Breach of contract
- Unpaid bills
- Divorce
- Intellectual property
- Employment claims
- Probate

Criminal Law

Criminal Law is broken down into two categories:

1. **Common Law** derived from cases being tested in courts and setting the precedent
2. **Statute Law** when the government writes a particular piece of legislation, known as an 'Act of Parliament'.

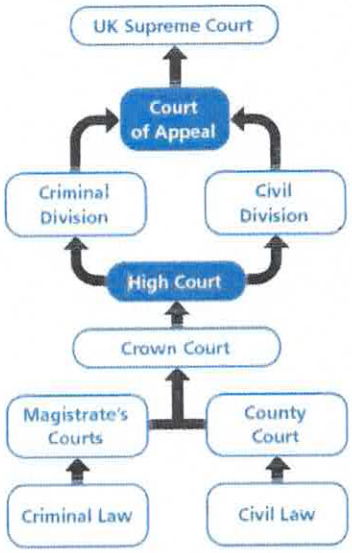
Examples of Criminal Offences:

- Common Assault
- Actual Bodily Harm
- Grievous Bodily Harm
- Manslaughter
- Murder
- Robbery
- Drug related offences
- Fraud
- Aggravated trespass
- Breach of the peace

- Theft
- Arson
- Activities without an SIA licence

English court system

The simplified diagram on the right shows the flow of the English court system. Starting from the Magistrates' and County Courts through to the High Court, the potential severity of the sentencing or fines issued increases and judgement can be made at any stage if the possible outcome is within the remit of the court to apply. Each court may refer the case to the court above if deemed proportionate.



It should be noted that the courts of appeal are to receive appeal post judgement and not make the initial judgement. The Supreme Court of the United Kingdom does not hear individual cases, they (in basic terms) help to provide guidance where there is a lack of clarity in law or there is no existing legal precedent for the judiciary to refer to.

Limitations of an SIA licence

An SIA licence does not provide the holder any additional powers of arrest other than the ability everyone has already, known as a **'Citizens Arrest'**. The purpose of an SIA licence is to enable the holder (if contracted or established on a 'Duty Register') to lawfully represent a premises owner, property owner or individual to provide safety, security and/or prevent loss damage or theft. Also, it is important to remember that the licence holder is limited to the licensable activities associated to the licence they are holding and the capacity they are contracted to provide by the client. Please note this is a generalisation and it is recommended that you should fully read 'The Private Security Industry Act (2001)' and examine 'Schedule 2' which can be found here: https://www.legislation.gov.uk/ukpga/2001/12/contents

The main aims of the Private Security Industry Act (2001)

You should now be aware that when you see the word 'Act' when associated with legislation, that it means that the law is an 'Act of Parliament' known as a Statue Law and this falls within the category of Criminal Law, meaning it is a criminal offence to operate in contrary to this legislation.

Therefore, knowledge of the Private Security Industry Act (2001) is vital to a security operative to avoid committing a criminal offence which may be punishable by criminal law, resulting in possible prison sentences and/or fines.

The Private Security Industry Act (2001) has the following main aims to:

- 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
- Establish the SIA (Security Industry Authority)
- Establish licensing

The Human Rights Act (1998)

These are the basic rights and freedoms we are all entitled to. Security operatives are entitled to their own human rights, but it is very easy to deny another person theirs whilst conducting the duties within a protective services role, so a sound working knowledge of this legislation provides another important basis for decision making. Remember it is an Act of Parliament and therefore any breach of this would be a criminal offence.

Article	Description
2	The right to life
3	The prohibition of torture
4	The prohibition of slavery and forced labour
5	The right to liberty and security
6	The right to a fair trial
7	No punishment without law
8	The right to respect of private and family life
9	Freedom of thought, conscience, and religion
10	Freedom of expression
11	Freedom of assembly and association
14	The prohibition of discrimination

The Equality Act (2010)

This is a very interesting piece of Statue legislation in its ability to draw in several items of prior legislation to meet a common goal, which can be summarised by stating that it seeks to reduce and attempt to eliminate discrimination.

In order to gain a better understanding of the Act itself, it is useful to firstly understand some of the language or terminology associated with equal opportunities.

Prejudice

Prejudice can be described as negative reconceived thoughts or opinions about an individual or group of people who share common characteristics.

Stereotyping

Stereotyping is to assume that an individual or group of people will always act or behave in the same way by associating their profile with a certain behaviour or outcome.

Neither of these two are unlawful on their own, however they can lead to something which is both undesirable and unlawful.

Discrimination

Is a physical or verbal action treating an individual or group of people unfairly compare to others based on little or no valid reason

It is also useful to understand that indirect discrimination is equally as negative, this is applying 'blanket' conditions for all but intentionally or unintentionally and unfairly, exclude or disadvantage certain individuals or groups without valid cause or reason.

The Details

As previously discussed, the Equalities Act (2010) consolidated a number of anti-discriminatory laws working towards a common aim.

This legislation is a consolidation of the following anti-discriminatory Acts of Parliament:

- The Equal Pay Act (1970)
- The Sexual Discrimination Act (1975)
- The Race Relations Act (1976)
- The Disability Discrimination Act (1995)
- The Employment Equality (Religion or Belief) Regulations (2003)
- The Employment Equality (Sexual Orientation) Regulations (2003)
- The Employment Equality (Age) Regulations (2006)
- The Equality Act (2006)
- The Equality Act (Sexual Orientation) Regulations (2007)

The Nice Protected Characteristics

- Age
- Race
- Religion or Belief
- Disability
- Gender Reassignment
- Sex
- Marriage or Civil Partnership
- Sexual Orientation
- Pregnancy and Maternity

Equal Opportunities

When we discuss equal opportunities, the focus is primarily on the Human Rights Act and the Equalities Act (others do apply).

Common situations where unlawful activity may occur in relation to equal opportunities:

Employers

- Recruitment
- Access to training
- Pay and benefits
- Promotion opportunities
- Terms and conditions
- Redundancy
- Dismissal

Security Operatives

- Access refusals
- Ejections
- Communication
- Arrests/detention
- Use of force
- Searching
- Applying restrictions
- Confiscating items
- Monitoring
- Use of CCTV
- Prioritising

It is the employer's responsibility to make reasonable adjustments to ensure all staff have an equal opportunity for success. It is the security operative's responsibility to help apply reasonable adjustments within the work environment. It is both parties' responsibility to ensure there is no direct or indirect discrimination at any time.

Data Protection Act (2018)

The Data Protection Act (2018) includes the General Data Protection Regulations (GDPR 2018). During the course of their work a Security Operative is likely to handle large amounts of personal data which must be handled according to the law. The following is a simplified summary of the Act:

1. Personal data must be fairly and lawfully processed.
2. Personal data must be obtained for specified and lawful purposes.
3. Personal data must be adequate, relevant, and not excessive.
4. Personal data must be accurate and up to date.
5. Personal data must not be kept for longer than is necessary.
6. Personal data must be processed in line with our rights.
7. Personal data must be held securely.
8. Personal data must not be transferred to other countries outside the European Economic Area unless those countries have similar data protection laws.

An organisation can face a large fine if they are found to be in breach of the Data Protection Act.

Sources of data collected by a Security Operative (examples)

Keeping Data Safe Collected Data

When handling any personal information or data (either their own or someone else's) Security Operatives must:

- Comply with current data protection legislation
- Follow organisational procedures
- Follow assignment instructions
- Maintain confidentiality of information

Personal Data

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

Chapter 3 - Understand arrest procedures relevant to security operatives

Arrest is a potential requirement for any frontline Security Operative (and citizen) should the consequences of not intervening with a situation be significant.

This option should only be considered in the following circumstances:

- A crime has been committed and it is not practical for a Police Officer to attend without the suspect escaping away from surveillance
- To prevent serious harm to themselves or others

- A crime is foreseeably imminent
- They are a known criminal unlawfully at large
- To prevent the causing loss of or damage to property
- It is safe to do so

To make things even clearer, this does not apply to minor offences, they must be serious or **indictable**.

indictable
ADJECTIVE

1. *(of an offence) rendering the person who commits it liable to be charged with a serious crime that warrants a trial by jury.*

As a general guide, these are typically crimes that would see the offender potentially receiving prison sentences of 5 years or longer if found to be guilt in court

Examples of indictable offences:

Murder
Aggravated Assault
Assault
Rape
Sexual Assault
Firearms Offences
Robbery
Theft
Drug offences
Fraud
Vandalism

Risks associated with making an arrest

Taking an individual's liberty is a direct crime in itself if not performed in the right and lawful circumstances (Article 5: The right to liberty and security). Alongside the criminal offence the Security Operative may face substantial claims levied by the innocent party in a civil court.

Any Police Officer will tell you that they often encounter violence when making an arrest. This is even with the support of a large team, a crown warrant and personal protective equipment that only the police are permitted to carry, to assist them to manage violent encounters (batons, taser, spray) alongside the criminal offences of assaulting a Police Officer and resisting arrest. A Security Operative has none of these and is often regarded with lower respect by criminals due to the absence of a crown warrant. This naturally increases the risk of assault when attempting to make an arrest.

Clearly there are significant risks, however, it is the right thing to do if there is a threat to other people's safety or a serious crime may occur. There are many professional and moral considerations which support the risk, if the operative feels it is safe to attempt.

Do:

- Conduct the arrest as discreetly as possible
- Identify self
- Do not search the individual
- Inform person that they are under arrest and give reason
- Show firmness of intent
- Advise they will be detained until the police arrive
- Use of reasonable force only if necessary, to prevent escape of individual under arrest or to prevent assault against self or others
- Detain the person safely
- Treat fairly, allow them to use toilet (do not supervise them in toilet cubical)
- Allow them water and to administer medication (if lawfully prescribed)

Avoid:

- The use of aggression
- Public humiliation Pain compliant restraint
- Any restraint on the floor or pressing against individual's diaphragm
- Any restraint on or around an individual's neck area
- Questioning the detained person
- Prolonged arrest/detention

I will

- Ensure welfare of person arrested and own safety
- Separate if more than one person
- Inform police
- Detain and supervise until police arrive
- Preserve evidence
- Produce an Incident report
- Assist police with a statement if required
- Attend court at a later date if required

Use of force

When the phrase 'use of force' is used, it often triggers thoughts of heavy-handed grappling with another person in order to maintain order or conduct a citizen's arrest.

This is inaccurate as an assault is any direct, indirect, or suggested physical contact with another person.

Common Assault – s.39 Criminal Justice Act 1988

An assault is any act (and not mere omission to act) by which a person intentionally or recklessly causes another to ***suffer*** *or* ***apprehend*** *immediate* ***unlawful violence****.*

By this definition, a security operative threatening to 'throw' somebody out or 'remove' them might raise grounds for a criminal charge against them. This would be entirely prohibitive to any operative (or citizen) acting for ethically the right reasons and would even put carers and health workers at risk of prosecution for merely helping to support a patient whilst walking. The final phrase 'unlawful violence' provides the

sensibility to the definition in that the physical contact needs to equate being unlawful to become a criminal offence.

Section 3, Criminal Law Act 1967

*'A person may use such force as is **reasonable** in the circumstances in the prevention of crime, or in the effecting or assisting in the lawful arrest of offenders or suspected offenders, or of persons unlawfully at large'*

This is not the only legislation supporting the **lawful use of force** but is arguably the most applicable to the role of security operatives. Furthermore, force may be used in self-defence if there is an honestly held belief that a risk of assault is imminent or occurring

R v Balogun [2000]

'...A man who is attacked or believes that he is about to be attacked may use such force as is both necessary and reasonable in order to defend himself. If that is what he does then he acts lawfully.'

Please read 'man' to mean all genders.

There is a lot of interrogation into 'reasonable' as this is subjective to the perceptions of the individual, the situation they find themselves in, the size, age, capability, and ferocity of the person they are applying force upon. An easy way to navigate this question is by introducing the word proportionate; applying force that is equal to the requirements at that time.

Summary of situations which may justify force being used

- When you or another person is being assaulted
- To prevent you or another person from being assaulted
- To stop a breach of the peace
- To prevent a breach of the peace
- To protect another person from harm
- Evicting a trespasser from a venue
- To detain or arrest a person who has committed a crime
- To detain or arrest a person who is suspected of committing a crime (must have valid and justifiable grounds)

Chapter 4 - Understand the importance of safe working practices

Below are some of the many implications if a health and safety culture is not adopted within the workplace.

People

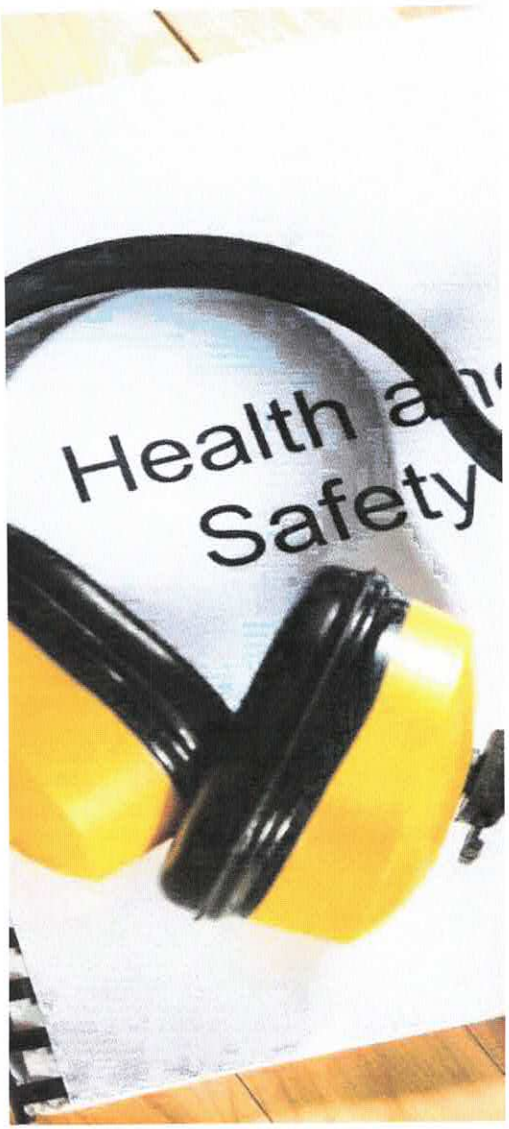
- Injury
- Illness
- Fatality
- Long-term effects

Business

- Lost productivity
- Business disruption
- Staff shortages
- Damage to reputation and public image
- Financial costs to rectify

Enforcement

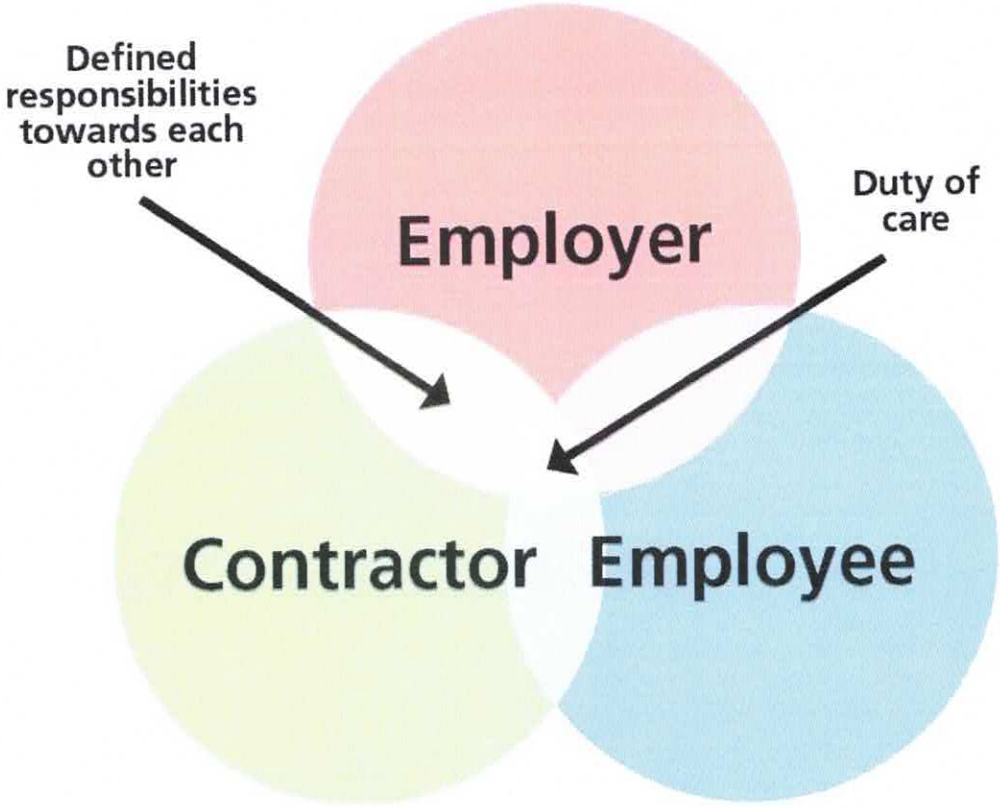
- Prosecution
- Prohibition of certain activities
- Fines
- Business closure
- Imprisonment of negligent staff or directors



Why is health & safety important in the work environment?

There is a phrase often used when discussing health and safety in the workplace and that is 'duty of care', which means that everyone has a responsibility for their own and other people's safety. There are defined tasks within the Health and Safety at Work etc. Act (1974) depending if you are the employer, employee, or contractor, but in general terms 'duty of care' encourages responsibility and discourages a 'walk on by' attitude.

Again, as this is an Act of Parliament, it is statute law (criminal) meaning any person found not to be complying with the legislation could face imprisonment and/or fines. Interestingly 'duty of care' can also be found within common law (also criminal). It is also worth noting that there is something in law called '**vicarious liability**'. This means that, if you are involved with a breach of the law and there was something you could have reasonably done to avert the situation, but failed to, then you are also liable and prosecutable.



The Health & Safety at Work etc. Act 1974

In a similar manner in which the SIA is the regulatory authority installed by the government to regulate the Private Security Industry Act (2001) on their behalf, the Health and Safety Executive (HSE) was installed by the government to regulate the Health and Safety at Work etc. Act 1974. The Act itself is a very substantial piece of legislation, which can be found here for further reading:
https://www.legislation.gov.uk/ukpga/1974/37/contents

The HSE apply interventions in proportion to the level of risk and severity presented to them from inspections. A HSE inspection can be triggered in a number of ways including complaints, self-referral, following an incident, reports from other agencies, whistleblowing or as part of a regular inspection or monitoring programme. If an inspector finds a hazard which requires attention, they can apply a range of precautionary interventions or potentially seek to bring negligence be suspected. prosecutions should serious

Improvement notices

Issued when the situation is not an immediate danger to staff or the public but needs to be addressed before it is.

Prohibition Notices

Issued to immediately halt an activity or restrict access should the risk and threat of harm are imminent.

In both cases the inspector will revisit to assure themselves that the remedies have been correctly applied by the employer before considering their escalation options. Prosecution is an option which may be applied immediately or after due attempts to allow the employer to remedy the situation have failed.

Responsibilities under the Health & Safety at Work etc. Act 1974

The two key statements below provide the focus for the requirements of this qualification to explain some of the requirements and responsibilities of the employer and the security operative.

Key responsibilities of the employer

Below list some (not exhaustive) of the responsibilities the employer has towards ensuring their premises, staff and customers are kept safe from foreseeable harm:

- Carry out risk assessments
- Take reasonable steps to eliminate or reduce the risks identified
- Provide safety equipment
- Ensure safe working practices
- Provide relevant training
- Provide suitable personal protective equipment (PPE) or clothing
- Violence and verbal abuse are also considered to be workplace hazards in some environments and are covered by this legislation.

Key responsibilities of the employee

This is covered by section 7 and also includes the self-employed and contractors working at someone else's premises, this is often the case for security operatives, however some may be direct employees of the establishment that they are protecting.

- Take reasonable care of their own and colleagues' health and safety
- Do not perform unsafe activities
- Comply with the organisation's health and safety policies/procedures
- Follow all reasonable instructions
- Use protective equipment properly
- Follow emergency procedures
- Exercise a duty of care to self, others, and the organisation

Remember that common sense plays a large part both in ensuring a safe work environment and in law. If a security operative decides to take a high-risk action (such as standing on a bar or tabletop to gain a better view and incurs an injury) then the employer is not at fault if the decision was entirely that of the security operative, who is potentially liable for any loss or injuries to others.

What are 'Risks and Hazards'?

A **hazard** is the source of harm, for example tripping over something or being electrocuted, so it is not the physical end result it is the thing that causes the injury. **Risk** is the likelihood (or chances) that the hazard will happen.

In this example the hazard is Covid-19' and the person in the image is reducing the risk(likelihood) of catching it by using a face mask (PPE)

In this example the hazard is slipping or falling down the walkway, the risk has been reduced by holding the handrails

Employer Management of Risks

The employer starts this process by conducting a risk assessment, arguably it could be called a hazard assessment as the first thing they need to do is identify the potential hazards (sources of harm) in the workplace. The word 'reasonable' is used a lot when considering health and safety as it is nearly impossible to predict and prevent all accidents, but the employer must consider all reasonably likely sources of harm. The below is an example of a very basic risk assessment:

Hazard	Who	Hazard Score	Risk Score	Risk Rating (hazard x risk)	Mitigation	Risk Score after Mitigation	Risk Rating after Mitigation
Fall down wet stairs	Staff Public	3	3	9	Anti-slip strips	1	2
Assault by aggressive customers	Staff Public	1	3	3	Staff conflict training	2	2
Being run over by moving vehicles in car park	Staff Public	3	2	6	Hi-vis for staff and separated walkways for all	1	3

Hazard Score

1: Minor cuts, bruises, abrasions
2: Serious cuts, broken bones, life-changing
3: Potential fatality

Risk Score

1: Remotely possible but unlikely
2: Infrequent likely
3: Certain/almost certain

Risk Rating

1-3: Acceptable
4-6: Requires continual physical monitoring
7-9: Unacceptable

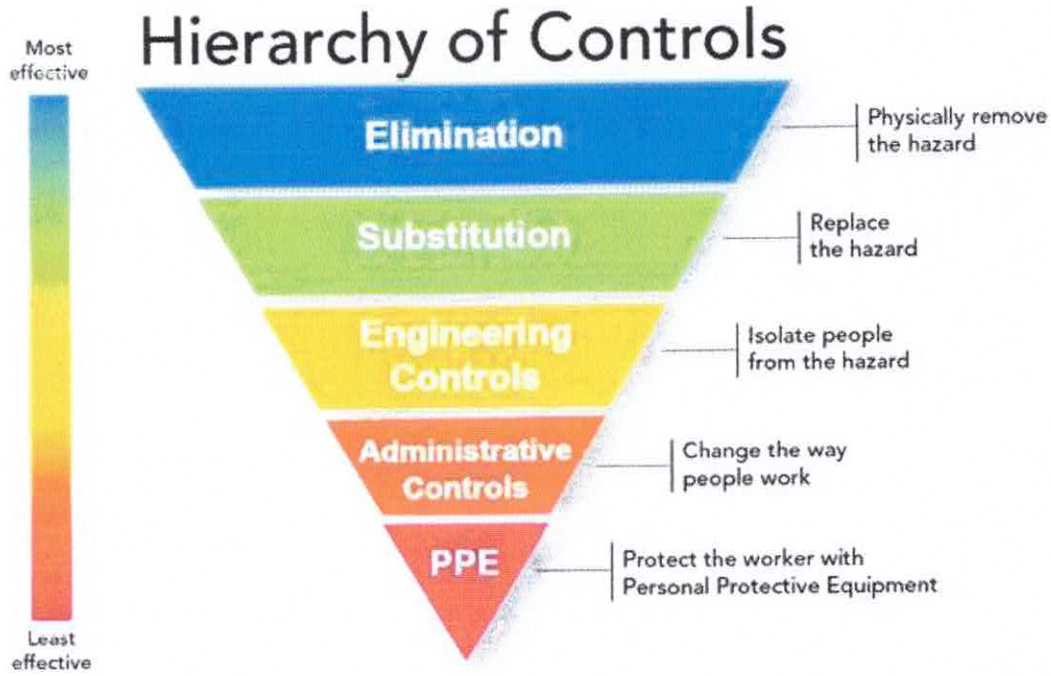
The hazard score never changes as the harm from (for example) falling down the stairs never gets less, but the employer can influence the likelihood (risk) of it happening by applying some mitigation, meaning putting things in place to reduce the risk. There are many mitigation elements that can be applied such as appropriate signage, PPE, training, barriers, tape, alarms, removal of hazard entirely, reducing time spent near to the hazard, controlling access and countless physical resources (remember the word '**reasonable**')

Mitigation of risks

There are many methods that health and safety professionals use to decide the best course of action to apply mitigation solutions to manage the risks they have identified. It is useful to understand these as, during the course of employment in protective services, a security operative is likely to encounter many hazards which randomly appear and need some form of intervention to avoid people being harmed. Examples could include:

- Broken glass
- Unsafe door
- Spillages
- Damaged equipment
- Many others

The identified hazard needs to be reported immediately and possibly some actions from the security operative to mitigate the risk in the interim may be needed until the management of the premises can resolve the situation fully.



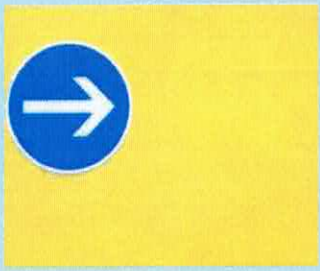
Health and safety signs

One of the mitigation techniques that the employer (or premises owner) will use is the effective use of safety signs to advise people of the hazards or direct them to safer conditions. Basic knowledge is highly effective in saving lives, for example knowing how to get out of a building in an emergency or being aware that there is a hazard to health.

As a security operative is responsible for their own and others' safety, it is absolutely necessary that safety signs are fully understood to be able to do this effectively.

Prohibition

The colour and shape of this sign is a white circular sign with ared border. The sign has a red crossbar running through it from the top left to the bottom right. The sign is usedto indicate that you **must not** do something.



Mandatory

The colour and shape of this sign is a solid blue circlewith a white symbol and/or writing, used to indicate that you **must do** something.

Warning

The colour and shape of this sign is a yellow triangle with a black border. Theinformation is given within the triangle, it does not prohibit or mandate the reader to anything apart from be **alerted** to something.

Safe condition

The colour and shape of this sign is a green background with a white symbol. The signmay be square or oblong in shape. These signsgenerally indicate conditions associated with **safety**, such as fire exits, evacuation routes and First Aid equipment.

Hazardous Chemicals

This is a diamond shaped sign which contains information about the chemicals withinthe area or container to which it is attached.

Health and safety alarms

From time to time, a security operative will be required to raise an alarm to inform other people of a situation. Alarms can be urgent or non-urgent depending on their purpose, but common ones to be aware of are as follows:

Electronic fire alarm buttons - many are traditional 'break glass' types but there are variations to be aware of that include additional stages or actions, such as requiring to lift a protective screen first.

However, there are still locations that use a manual bell to be turned by the operator. These are often used as a fall-back in case of power and back up battery/generator failure.

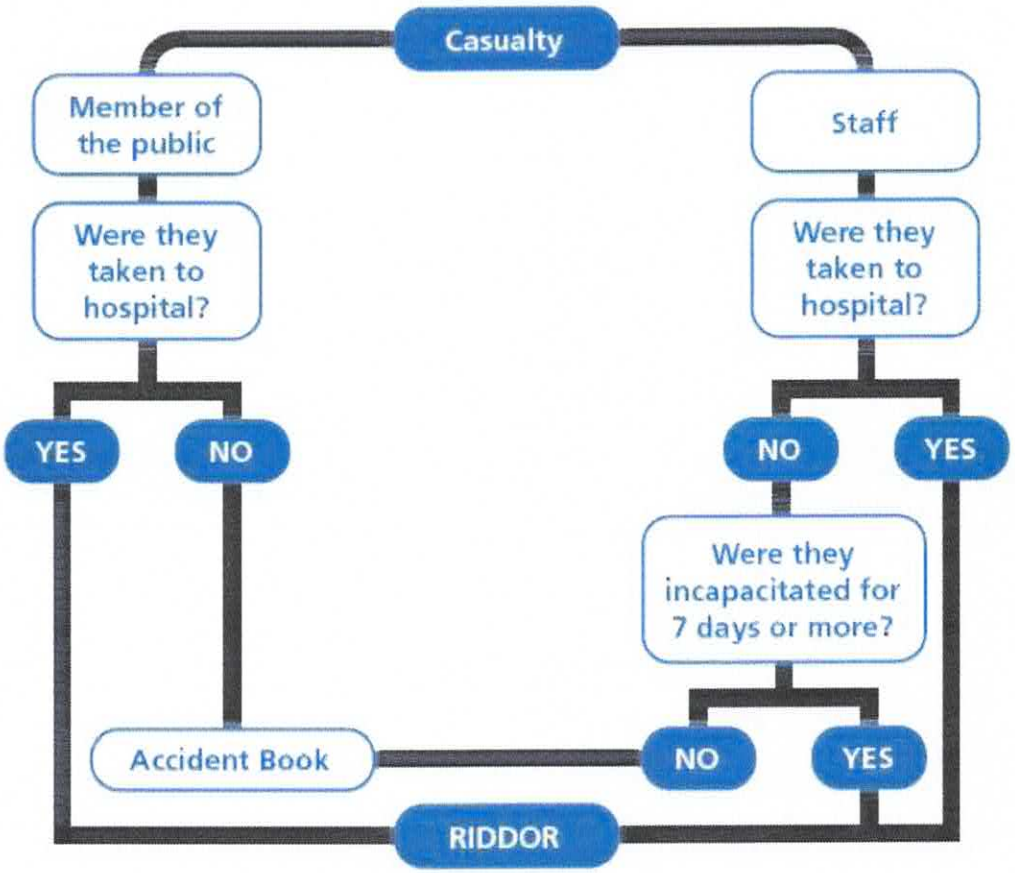
Reporting procedures

All health and safety incidents, accidents and near misses must be reported in line with site policies. Typically, this is to report them to the supervisor or control room, but sometimes other management outside of the immediate team will need to be notified. Incidents where nobody has been injured are logged in the Incident book and injuries must always be recorded in the accident book.

Sometimes when a health and safety related incident is serious enough then the employer has a lawful duty under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (2012) to notify the HSE. Openness and transparency are an excellent way to work with the HSE who are there to support the organisation to ensure the premises is brought back in line to establish a safe working environment. This is far better than the organisation being reported to the HSE by a third party as immediately it demonstrates that the organisation has not fulfilled its requirements.

The HSE have a reporting process called RIDDOR, which is an abbreviation of the above regulations. As security operatives often are the first person on scene, they will have a broader understanding of the situation and therefore are likely to be required to assist with information to the person notifying the HSE. It is recommended that further reading into the requirements is made at this stage: https://www.hse.gov.uk/riddor

A very simplistic overview of the reporting requirements is provided below, but please do take the time to read the full details at the website provided above.



First Aid situations

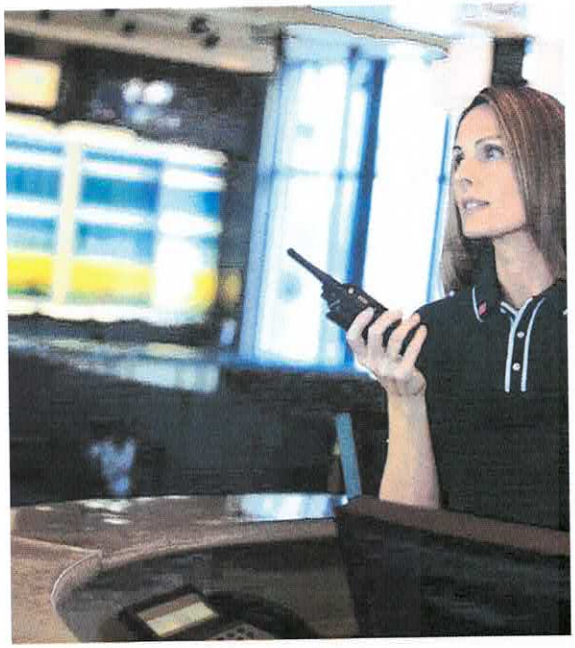
It is likely that a security operative is going to encounter many situations requiring first aid and it is strongly recommended that qualification is sought in this skill set to provide immediate care.
There are many types of situations requiring first aid, some of which might include:

- Bleeding
- Seizures
- Fractures
- Unconsciousness
- Choking
- Shock
- Heart attack
- Stroke

If it is serious (life-threatening), call an ambulance immediately, then the designated first aider.
If the situation is not life-threatening call for the designated first aider.

Lone Working

Lone working is commonplace in the private security industry, especially with the assistance of technical solutions to support the safety of lone working operatives. Historically, lone working was a high risk for workers in the industry if they became injured, ill or victims to assault then there was very little response from the employers as they had no means to check they were okay. Similarly, the employer had difficulties with operatives falling asleep, leaving the site early or failing to conduct their duties.



Modern day lone workers have the benefit of systems such as geo-tagging which tracks their location and movements, which is monitored by Operations Centre staff and often artificial intelligence to recognise if the movements are expected or unexpected. With the evolution of 'smart watches' the health and wellbeing of an operative can also be monitored, for example, an elevated heart rate may be a sign of a physical problem or they are in a situation which has made them adrenalized for some reason, resulting in a mobile patrol visiting the operative. The same systems can alert the operative when patrols are required, a perimeter detection system has identified a potential intruder and provide data to clients regarding the protective activities provided by the operative.

Security Operations Centres (SOC) act as a central hub to many lone workers and often require them to make check calls or respond to timely requests to ensure they are alert, safe and well.

Technology can only go so far in protecting lone workers as ultimately, they will always be vulnerable for a period of time prior to any physical response from a SOC, the following still remain potential risks:

- Injuries/ill-health
- Violence
- Lack of immediate support
- Lack of communication
- Availability of rest breaks

Chapter 5 - Understand fire procedures in the workplace

Many of the continual professional development courses for security operatives focus on dealing with individuals or small groups who have hostile intentions towards people or property and this is clearly an important area to provide protection against. What if you were informed there is an individual who could walk through the property in minutes and take the lives of all the people within and destroy the entire premises? That individual is called 'fire', so it is imperative that a security operative fully understands the basic principles of prevention and action should fire be detected.

The nature of fire

The fire itself can cause burns to varying degrees from superficial to fatal. If a person can move i.e. is not trapped in by the fire, then natural self-preservation instincts will assist to keep the person safe as the heat produces pain and it is an automatic response to move away from this. Greater problems are with the unseen hazards:

- Smoke is not always visible and often contains lethal carcinogenic chemicals within. Some types of smoke can kill a person from just a few inhalations.
- Smoke can travel faster than a person can run in certain conditions via extreme convection currents.
- Flash overs occur when flammable materials in the proximity of the fire get hot enough to produce a flammable gas around them, the gas will ignite (this is known as the flash point). This reaction is highly volatile and can result in an explosion or huge fire ball.
- Structural weakening from heat can cause floors, ceilings, and walls to collapse. Backdraft occurs when a fire within a room has burned most of its available oxygen, this can be seen by partially combusted smoke (often brown) appears to pulse in and out of the edges of a door or window as air gets drawn in, combusts, pushes the smoke out again, then repeat. If the door/window is opened then oxygen surges into the room, suddenly allowing the fire to combust properly, resulting in an explosive fireball

The 5 P's of Fire Prevention

Planning
Preparation
Prevents
Poor
Performance

Prevention duties of a Fire Marshal

This chapter will go into more detail about the nature and components of fire, there are, however some basic 'housekeeping' measures to consider and apply throughout the daily activities as a security operative who will often act in the capacity of a fire marshal.

- Control of fuel and ignition sources - this means keeping flammable items away from sources of heat.
- Safe storage of flammables.
- Regular inspection and maintenance of electrical equipment.
- Ensuring all fire alarms and fire extinguishing equipment are in good order.
- Staff training in basic fire safety measures.
- Avoidance of overloading electrical sockets/extension leads.
- Ensuring all fire doors are being used as they should. • Ensuring all fire exits are clear to access (both sides).
- Fire safety signs are in position.
- Fire alarm call points are unobstructed.
- Fire-resisting doors are closed and functioning properly.
- Any malfunction of the weekly/monthly fire alarm test is reported.

Clearly it is not expected for a security operative to test and certify electrical and fire equipment, but cursory checks should be made i.e., is the item getting hot if switched on/sparking, or are the fire extinguisher inspection labels in date and the pin/contents gauge as they should be? In essence, sensible housekeeping to prevent fire and respond safely if there is an emergency.

The components of fire

For a typical fire to exist, it requires three elements; remove one or more of the three elements and it will cease to exist. By ensuring the three elements do not come together in an uncontrolled way, unwanted fire cannot start.

Employers use the fire triangle as part of the Fire Risk Assessment to identify how to keep all three elements as separate as possible or risk reduction methods to prevent all three elements from occurring at once.

This triangle is also the principles behind tackling fires once they have ignited – fire extinguishers can eliminate one, two or three of the elements to extinguish the fire (depending on the quantity of the three elements).

Examples:

Source of Heat

Sun, electrical faults, sparks, or discarded cigarettes.

Solution

Cooled using water or an appropriate fire extinguisher (depending on nature of thefire). Or simply move the fuel away from the heat source.

Oxygen

21% of the air is oxygen.

Solution

Smother the fire so it runs out of oxygen (think about how home cooking oil fires areput out by smothering them with a wet towel).

Fuel

Fuels are anything that can burn:

Textiles (wood, paper, cloth)
Liquids (petrol, flammable liquids)
Gases (oxygen, propane, butane)
Metals (aluminium, magnesium)
Fats (cooking oil, lard, butter, engine oil)

Fire classification

To bring some order to the seemingly disorderly nature of fire, experts have developed a method of identifying what type of fuel is involved with the fire, to be able to select the correct type of fire extinguisher to put it out. This system enhances the safety for those fighting the fires by providing a simple classification and identification method to avoid scenarios where the incorrect extinguisher is used and the fire gets worse, for example, using a water fire extinguisher on a flammable liquid fire will cause it to spread.

A **Ordinary combustible**: e.g., 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

E **Electrical**: not strictly a classification as electricity is a source of ignition not a fuel, but identified on extinguishers that are safe to use near to electricity

F **Hot oils or fats**

Fire extinguishers

All fire extinguishers within the European Union (and other countries) have labels on them to identify what fire classification they can be used for; the labels look like the image to the right.

These icons and letters mean that this particular extinguisher can be used on flammable liquids and fires near electricity (sockets etc).

During a fire, the operator does not want to be confused as to which extinguisher to use. While the body of the extinguisher may be red, there is a label that takes up approximately 5% of the body. This label is colour coded in accordance with the content of the extinguisher.

Common features on fire extinguishers are:

- Operating handle
- Tamper tag
- Safety pin
- Pressure gauge
- Content label
- Inspection label
- Instruction label
- Hose and/or nozzle

Class A fires involve solid materials that are often organic intheir nature. Examples include coal, paper, wood, cardboard. They also include materials such as soft furnishings and curtains.

Class B fires involve liquids such as petrol, paraffin, paints, whitespirit, varnish, and thinners.

Class C fires involve gases. This can include natural gas or gases such as butane or propane.

Class D fires are fires involving metals. These metals may include sodium, lithium and aluminium swarf or powder.

Electrical fires do not have a classification as there are no fuelsthat can be extinguished.

Class F fires involve fats used in cooking. These can include vegetable and animal fats. These fats retain considerable heat, making them difficult to extinguish.

Water extinguishers

Works best on:

Fires involving materials such aswood, paper, cloth, plastics, coal, etc.

Warnings:

Do not use on burning fat or oil, or on electrical appliances.

How to use:

Point the jet of water at the base of the flames and keep it moving across the fire. Ensure all of the fire is out.

How it works:

Water cools the fire. Some water extinguishers also generate a fine spray, ensuring greater coverage.

CO2 extinguishers

Works best on:

Live electrical equipment. It can also be used on liquids such as paint and petrol.

Warnings:

Do not use on chip or fat pan fires. The pressure may cause solid materials to be blown away, potentially spreading the fire. CO2 can cause asphyxiation if used in small spaces. The horn of the extinguisher becomes very cold during use; therefore, the horn should not be held during use.

How to use:

Direct the horn at the fire, release the horn and operate the extinguisher. Aim at the base and use a sweeping motion.

How it works:

The carbon dioxide extinguisher works by displacing oxygen in the air, preventing the fire from'breathing'. Once the extinguisher is used, the CO2 will dissipate,potentially allowing the fire to 'breathe' again.

Foam extinguishers

Works best on:

Solids such as wood and paper as well as liquids such as paint and petrol.

Warnings:

Do not use on chip or fat pan fires. Do not use on electrical fire unless stated otherwise on the extinguisher label.

How to use:

For fires involving solid materials, aim at the base of the fire and sweep the foam across the fire from side to side. If dealing with a liquid fire, allow the foam to build up and flow across the fire.

How it works:

Foam is water based and therefore sits on top of the flames, smothering them.

Dry powder extinguishers

Works best on:

Wood, paper, cloth, plastic, as well as liquids such as grease, fat, oil, paint, petrol, etc.

Warnings:

Do not use on chip or fat pan fires. Powder does not significantly cool fires and therefore some fires may reignite. Indoors, powder may be inhaled.

How to use:

Aim the nozzle at the base of the fire and with a rapid sweeping motion push the fire towards the far edge until all of the flames are out.

How it works:

Powder covers the fire, smothering it. Some cooling also occurs.

Wet chemical extinguishers

Works best on:

Class F fires involving cooking oils and fats such as lard, olive oil and butter.

Warnings:

Not to be used on other liquid fires such as petrol unless otherwise stated on the label.

How to use:

Using the applicator, a gentle action should be employed to prevent splashes. Apply in a circular motion; a soapy consistency covers the fire. Use the extinguisher's full content to minimise the risk of re-ignition.

How it works:

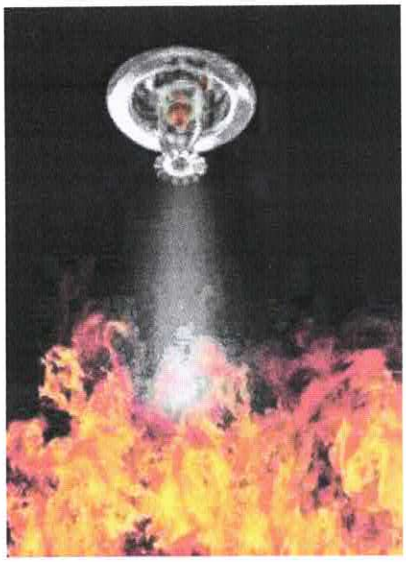
The wet chemical has a cooling effect but, in addition, salts in the solution react with the fat to create a soapy layer, smothering the fire.

Other types of fire equipment

There are many other types of fire equipment within a typical workplace to be aware of and their uses.

Fire blanket

Used to remove the oxygen from the chemical chain reaction.



Sprinkler system

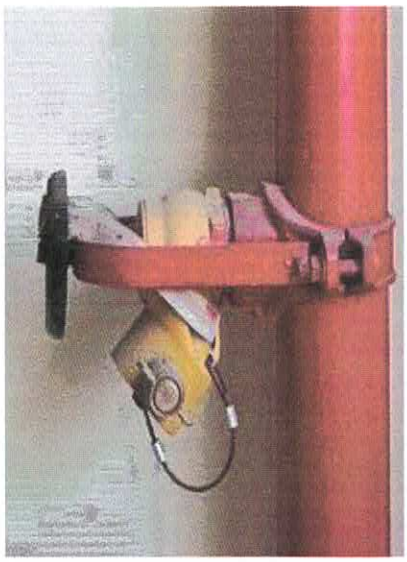
Triggers when the heat of a fire bursts the capsule inside which then releases water from the sprinkler.

Fire hose

Used to provide a continuous flow of water.

Dry riser

This is an empty piping system which the fire service can plug into and supply the outlet (on each floor) with water from the engine. This negates the need to extend hoses from the fire engine all the way to the fire.



Wet riser

This is a 'primed' piping system which the fire service can plug into, similar to a dry riser except there is no need to fill the pipes with water before it reaches the desired floor of the building. Providing an instantly available flow of liquid for the fire fighters from the outlet

Actions upon discovering a fire

When discovering a fire, there are two clear considerations:

1. People first
2. Property second

Property (even entire buildings) can be replaced and are insured, but people's lives and well-being cannot. But in order to keep people safe, the site-specific emergency plans must be followed both in the event of a small fire, keeping people at a safe distance from both flames and smoke, also in the event of an evacuation.

Human nature varies from person to person when a fire alarm sounds:

- Ignore the alarm (thinking it is just a malfunction, test or drill)
- Confusion
- Possessiveness over personal property
- Panic once the alarm is confirmed by either smoke or flames

Another anomaly to note is that people will always leave a building via the route they know best (often the same way they came in), in some situations this is fine, in others they may be heading into significant danger. This behaviour will even occur if they are standing right next to a fire exit, so it is important that those acting as fire marshals (often security staff) act calmly, firmly, and efficiently to communicate and guide people to the correct means.

The following is a useful thought process to maintain a clear and efficient way of managing a fire situation:

Find

Discovery of the fire and analysis of the severity and potential risk

Inform

Notify the control room/supervisor immediately, this is either to prepare colleagues to be in position to evacuate, or for them to assist controlling the situation locally. The supervisor will use the information to decide on partial evacuation, full evacuation and calling the emergency services is required.

Restrict

Immediately moving people out of harm's way (fire itself and smoke)

Evacuate or Extinguish

Proceed to commence either of these options as a joint decision of the security operative on scene and the supervisor/management.

Fire control panels

These are a really useful item of fire safety equipment. All of the fire detectors, sensors and alarms within a building are linked to the control panel. Some will automatically call the fire service; others can send SMS messages to relevant people (or both). It is impossible to provide specific guidance within this workbook, so it is the responsibility of the security operative to understand the use and functions of a fire control panel upon induction to a new premise. There are some common functions of fire control panels which can be highlighted:

- The control panel will identify where the alarm has been activated. Often this information is given directly on the control panel identifying which area/zone detector has triggered but sometimes the light will have a number or code on it which corresponds to a location on a map or index kept nearby.
- Fault indicators, these trigger the same light as the fire alerts but in a different colour when the control panel is receiving no or a strange signal from the detector.

- The detectors are binary, meaning they will always be sending a signal to the control panel which will be either a state of 'normal' or 'activated', so when a fault is alerted it can be for many reasons ranging from power loss to a worn-out component

Modern fire control panels have the ability to send electronic alerts to people remotely. In some cases they will automatically call the emergency services if the initial alarm has not been responded to by the staff on site within a set period of time from activation. Security operatives are often the person responsible for fire alarm responses meaning it is essential that the site assignment instructions are fully read, understood and they are fully aware of how fire control panels operate on each site.

Responding to fire control panels

Faults must always be recorded and reported immediately. Many organisations will keep a fault log which the security operative will be required to complete. They are not asking for complex details just date, time, the zone, and any other information you may have.

All fire alerts must be investigated (ideally via CCTV first if available) to confirm the fire. This must happen immediately and you must not silence the control panel until a physical investigation has happened as others need to know there is an active situation being dealt with. If the CCTV identifies a significant fire then follow evacuation protocols as per the site instructions, if nothing is visible then leave the alarm sounding on the panel and someone physically investigates (follow site protocol).

The investigations need to occur because alarm sensors can trigger from other elements such as dust or a defective sensor, even the control panel itself may have a fault!

The investigation will establish if the fire is able to be extinguished or an evacuation is required. The person investigating must take precautions such as avoiding inhaling smoke, touching doors with the back of their hand first to see if there is heat from the other side and being vigilant for the signs of possible back draft. Common sense prevails that in the situation of excessive smoke, heat or danger signs as discussed, an evacuation is requested, and they do not proceed to the source of the fire.

Fire evacuation procedures

This may sound simple in theory, but there is a well-rehearsed and practiced structure to performing a safe and efficient evacuation of a premises. Notwithstanding the predictable unpredictability of human instincts during these situations, there are a number of additional considerations.

- To keep self and others safe
- To save time in an emergency
- To assist emergency services
- To confirm each part of the evacuation has been completed

Zones = Buildings
Sectors = Floors

Sub-sectors = Rooms

There will often be two stages to the evacuation announcements, the first of which is for the fire marshals (often includes the security team) to prepare. In preparation for an evacuation, the staff involved should collect their required equipment (high visibility vests, clipboard/checklists, radios) and head promptly and calmly to their designated area of responsibility. It is essential that all the actions of these staff are calm and professional as others are likely to panic if they notice uncontrolled behaviour from those who are responsible for their safety.

As discussed previously, people will have a variety of responses to a fire alarm, therefore effective use of non-verbal, clear, and assertive gestures towards the appropriate exit route will be the best form of communication (especially as it is hard to hear over the sound of a fire alarm).

Identify vulnerable people and provide assistance/ask others to assist to facilitate their safe exit, people who may be vulnerable can include:

- Very young
- Very old
- Those under the influence of drink or drugs
- People who do not understand the requirements of them
- Any person who is in shock or state of panic
- People with physical disabilities

It is natural for people to want to take personal belongings, however this should be discouraged as items such as bags can block exit routes and cause trip hazards.

Once the sector is visually clear, begin secondary checks to ensure all people have left (toilets, waiting areas, canteens, changing facilities etc).
Notify the evacuation controller that your areas of responsibility are clear and head towards the muster point or assist others with the evacuation as per instructions.

There may be further duties assigned by the evacuation controller once outside, which could include:

- Meeting the emergency services to direct them to the fire location (externally)
- Providing additional welfare support to evacuees
- Establishing an outer cordon
- Assisting with the business continuity plan

Chapter 6 - Understand emergencies and the importance of emergency procedures

The word 'Emergency' is often used and very often associated with the outcomes of a disastrous situation. Television and film regularly dramatize emergencies with police, fire, and medical teams in attendance, accompanied by general chaos. This is not always the case and early interventions by security operatives can avoid such catastrophic outcomes.

Context and perspective need to be applied as one person's emergency is not necessarily another's. For example, a power outage at one factory would be just an inconvenience, but at another with refrigerated stock, could cause serious disruption and damage the business. An early intervention by a security operative to activate the backup generators (if not automatic) could avert the crisis.

Emergency

A SITUATION THAT IS UNEXPECTED, THREATENS SAFETY OR CAUSES SERIOUS DISRUPTION AND REQUIRES IMMEDIATE ACTION

Types of emergencies

As identified, emergencies can and will vary from premises to premises depending on the hazards, effects and people involved. Below are examples of what these could be:

- Power outage
- System or equipment failure
- Flood
- Actual or threatened serious injury
- Serious illness
- Bomb threat
- Violence
- Public disorder
- Fire
- Entrapment
- Weapons

Very few (if any) situations have been successfully and safely resolved by panicking, therefore the security operative should lead by example by acting swiftly, calmly, and efficiently whilst encouraging others to do similar. This also helps to analyse and prioritise the situation/s, inform the emergency services (if appropriate) and achieve command and control of the situation.

Emergency or incident?

It is useful to understand if the situation is an emergency or incident as it will help the security operative to understand how to respond and the expectations of them. Emergency situations are highly dynamic and often require immediate problem solving, whereas incidents are situations which have been predicted and the expectations are to follow protocol or training.

Emergency

- Power outage
- System or equipment failure
- Flood
- Actual or threatened serious injury
- Serious illness
- Bomb threat

Incident

- Violence
- Public disorder
- Fire
- Entrapment
- Weapons

Common reactions to an emergency situation

People behave in a variety of ways depending on how large the adrenaline surge is within their systems:

- **Freeze** – Do nothing and wait for danger to pass
- **Fight** – Become highly aggressive to fight off the threat
- **Flight** – Do anything physically possible to get away from the threat
- **Panic** – The brain does not want to fight but cannot identify an exit route
- **Default to safety** – Leave via the known entry route (can be unsafe)

With many people trying to escape as fast as they can and others reacting in a variety of ways, chaos or crushing can ensue without strong leadership.

Calling the emergency services

In very serious situations, which are often life-threatening the speed of the emergency service response to the scene can be the difference between safety and fatalities so every second counts.

Before making the call, the security operative should know key information:

- If the telephone being used requires additional numbers to get an outside line (for example some systems require '9' to be dialled first, so the emergency call would be 9999)

- The address of the situation
- What emergency service/s you require
- If anyone's life is in immediate danger (for example someone being or about to be attacked with a weapon or the offenders have left without attacking, or a casualty is injured and breathing or injured and not breathing)
- Scale of the emergency (how many people require medical assistance, the size of the fire, how many people in the mass brawl etc)
- Other immediately relevant information, such as additional hazards the responding services should know about (for example the fire is next to a large quantity of propane bottles)

Not sure of your location?
Consider downloading the 'What 3 Words' app
https://what3words.com

///WHAT3WORDS

From this information, the operator will understand who to send, where to send them, how many, how quickly and alert them to any other hazards whilst on their way.

Safeguarding – a duty of care

Broadly speaking vulnerability is not a label to identify an individual with; it is when a person is in a situation where their ability to proactively manage their own safety is limited due to the circumstances, they find themselves in. For example, a martial arts specialist would not typically be someone who is vulnerable to assault, however, if the same person was intoxicated to the point that their ability to risk assess their surroundings was limited and had very few motor skills available due to the level of intoxication, was to become the target of robbers upon leaving a venue, they would be considered to be a vulnerable individual at that moment in time.

All adults, young people and children can be vulnerable due to a variety of reasons or factors, including:

- 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
- Having a physical or learning disability

Assisting vulnerable individuals

It is the moral and lawful duty of every security operative to assist vulnerable individuals by extending a duty of care to make reasonable efforts to prevent potential harm. There are many options, however it is imperative that the security operative acts within professional boundaries and limitations to ensure they themselves do not become open to vexatious complaints or challenge. Where a situation is distinctly greater than managing the immediate safety of an individual then the relevant authorities should be involved to continue that duty of care.

Some immediate and reasonable interventions may include:

- Seeking help of Street Pastors, Street Marshals, or any other active schemes
- Calling a relative to assist in the case of a younger or vulnerable adult
- Calling for a licensed taxi to take the vulnerable person home
- Using 'safe havens' or other local initiatives run by organisations such as St John Ambulance
- Calling the police
- Notifying local CCTV control rooms to monitor the individual/s

Child Sexual Exploitation

Sadly, within the UK is still occurs where a child is used as a commodity in the sex trade by individual adults or gangs to profit from their vulnerabilities. As security operatives are often in locations where they can observe the 'hand over' taking place then it is imperative they firstly know what the potential indicators (signs) are and, secondly, how to respond according to their suspicions.

Some of the visual clues to raise suspicion are:

- 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
- Visible signs of fear
- Visible signs of drug taking

Some of these on their own may not be attributable to exploitation, however the context and situation will provide a clearer understanding of the situation.

If a security operative is suspicious then contacting the police non- emergency number (101) or Crimestoppers (0800 555111) is an appropriate response. If the situation is urgent and the child is in immediate risk of harm, then the police emergency number (999) should be used.

Chapter 7 - Understand how to communicate effectively as a security operative

Effective communication is the difference between "jacket filler" and a consummate professional. A security operative needs to communicate with colleagues to make operational requirements a success and increase team efficiency. But, possibly more vitally, communication with customers is of paramount importance on all levels; from customer service to conflict management, to potentially saving lives.

Be aware of facial expressions and tone when communicating as these elements can completely change the message given, even if the words remain the same...

Non-verbal communication (NVC)

The actual words we speak accounts for only 7% of face-to-face communication, 55% is body language (also known as NVC) and 38% is the tone of the words. It is entirely possible to communicate fully and effectively without words when a person can see you. Recognising the movements and gestures associated is covered in depth during the conflict management unit.

Communication principles

When communicating in person, there are two types of communication happening. Ideally, to ensure the message is clear, it is appropriate to make sure both verbal communication (the spoken word) and non-verbal communication (gestures, stance, eye contact, facial expressions, physical distance, and hand movements) are commensurate to each other. This is particularly important in noisy environments, or when there may be other blocks to communication, such as alcohol, drugs, emotions, pain, anger etc.

There are two types of customer which a security operative will engage with:

- **Internal customers**: Line managers, colleagues, staff working at or for the premises,

And,

- **External customers**: Visitors, customers, emergency services, trade, deliveries

Both types of customer should be treated equally to establish a positive working relationship. Some customer needs will vary in relation to most effective method of communication for them to understand (see blocks to communication above).

The principles of customer care are as follows:

- Establish a rapport (positive working relationship)
- Empathising (acknowledging and understanding their point of view)
- Polite, helpful, positive, and approachable behaviour

Telephone communication

Security operatives will often be required to make and receive telephone calls. This skill at first view may seem obvious, however corporate communication includes a number of additional requirements than personal communication.

- Polite and professional approach and language to represent the organisation.
- Clear, distinct voice with moderate pitch and volume
- Good use of listening skills
- Appropriate questions to achieve clarity of requirements and understanding
- Knowledge of how the telephone system operates (some are very complex)
- Ability to place calls on hold and transfer
- Appropriate message taking and maintaining confidentiality of the written information.
- Completing phone logs and records
- Use of the NATO phonetic alphabet

Radio communication

A handheld or base station radio is one of the many tools that a security operative will use when working as part of a team. Prior to use (upon collection each shift), check the radio is functioning correctly and the batteries are fully charged. A brief "radio check" message at the start will be enough and at a time when there is doubt, however regular checks are unnecessary and unwelcome, so these are to be used only when absolutely required.

Standard protocol

- Press the transmit button for 1-2 seconds before speaking
- Identify call sign (who is speaking) and the desired call sign (who you wish to speak with)
- Use the word "over" when expecting an answer, use "out" when finished the conversation.
- Do not use "over and out" as it is a confusing message! Be concise and clear.

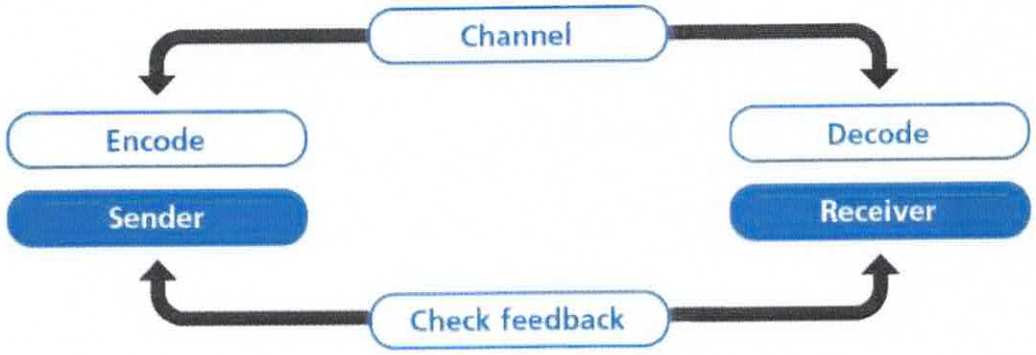
Emergency protocol

- Press the transmit button for 1-2 seconds before speaking
- Identify call sign (who is speaking) and the desired call sign (who you wish to speak with)
- State "urgent message"
- All other non-related communication is ceased to ensure clear communication channel
- Identify location and important details of the situation

Always use the NATO phonetic alphabet to spell words (if required) and communicate key information such as vehicle registrations.

A	Alpha	N	November
B	Bravo	O	Oscar
C	Charlie	P	Papa
D	Delta	Q	Quebec
E	Echo	R	Romeo
F	Foxtrot	S	Sierra
G	Golf	T	Tango
H	Hotel	U	Uniform
I	India	V	Victor
J	Juliet	W	Whiskey
K	Kilo	X	X-Ray
L	Lima	Y	Yankee
M	Mike	Z	Zulu

Communication process



Communication channels

Communication channels is the term given to the method of communication. There are multiple communication channels available, for example face-to- face conversations, telephone calls, text messages, email, the Internet (including social media such as Facebook and Twitter), radio and TV, written letters, brochures, and reports to name just a few.

Choosing an appropriate communication channel is vital for effective communication as each communication channel has different strengths and weaknesses. For example, broadcasting news of an upcoming event via a written letter might convey the message clearly to one or two individuals but will not be a time or cost-effective way to broadcast the message to a large number of people.

On the other hand, conveying complex, technical information is better done via a printed document than via a spoken message since the receiver is able to assimilate the information at their own pace and revisit items that they do not fully understand. Written communication is also useful as a way of recording what has been said, for example taking minutes in a meeting.

Encoding messages

All messages must be encoded into a form that can be conveyed by the communication channel chosen for the message. This is done continually when transferring abstract thoughts into spoken words or a written form. However, other communication channels require different forms of encoding, e.g., text written for a report will not work well if broadcast via a radio programme, and the short, abbreviated text used in text messages would be inappropriate if sent via a letter. Complex data may be best communicated using a graph or chart or another visualisation.

Effective communicators encode their messages with their intended audience in mind as well as the communication channel. This involves an appropriate use of language, conveying the information simply and clearly, anticipating and eliminating likely causes of confusion and misunderstanding, and knowing the receivers' experience in decoding other similar communications. Successful encoding of messages is a vital skill in effective communication.

Decoding messages

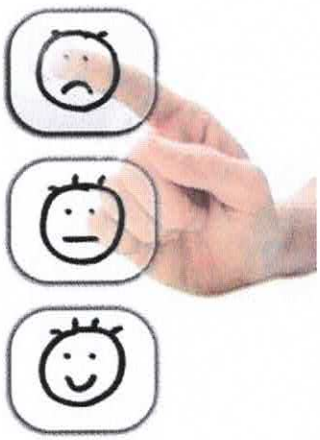
Once received, the receivers need to decode the message, and successful decoding is also a vital skill.

Individuals will decode and understand messages in different ways based upon any barriers to communication which might be present, e.g., their experience and understanding of the context of the message, their psychological state, and the time and place of receipt as well as many other potential factors.

Understanding how the message will be decoded and anticipating as many of the potential sources of misunderstanding as possible, is the art of a successful communicator.

Checking for feedback

Receivers of messages are likely to provide feedback on how they have understood the messages through both verbal and non-verbal reactions. Effective communicators should pay close attention to this feedback as it the only way to assess whether the message has been understood as intended and allows any confusion to be corrected.



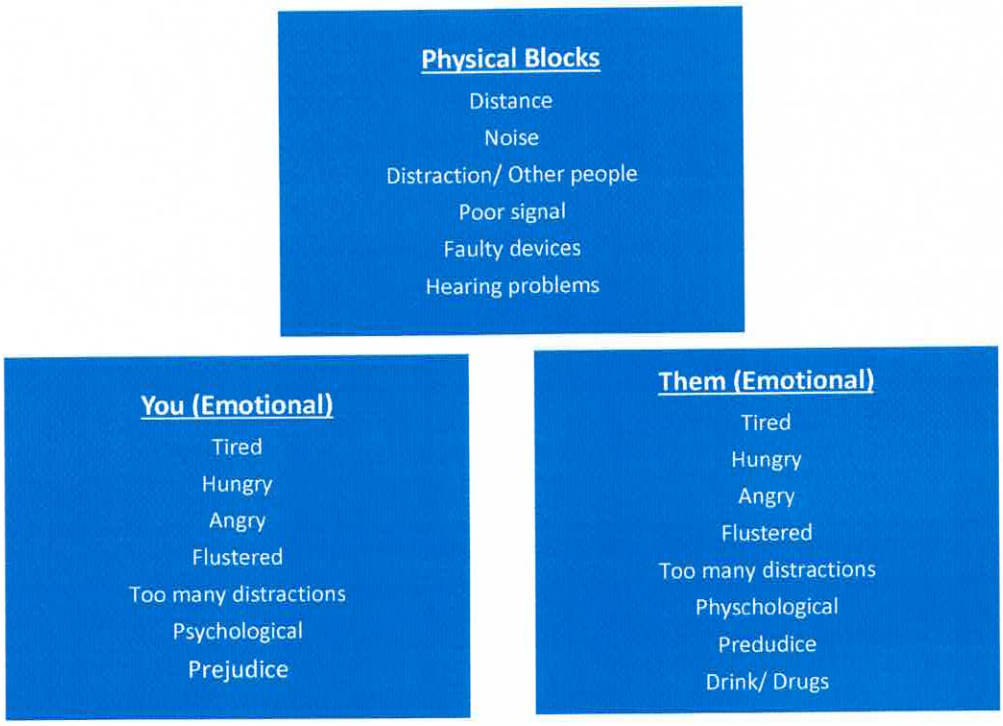
Bear in mind that the extent and form of feedback will vary according to the communication channel used: for example, feedback during a face-to-face or telephone conversation will be immediate and direct, whilst feedback to messages conveyed via TV or radio will be indirect and may be delayed, or even conveyed through other media such as the Internet.

Blocks to communication

There can be many reasons that the message communicated to a person may be misunderstood or misinterpreted, these reasons are known as 'blocks to communication' and, if successfully identified by the sender, can restore the integrity of the message. It is essential that all communication is accurately sent and understood, via any channel, as the consequences may be as slight as frustration to life threatening, depending on the situation. Even frustration can lead to violence, which can have fatal consequences.

Blocks can be categorised in to two types:

- Physical blocks
- Emotional or psychological



Communication and teamwork

Personal communication skills are an essential part of functioning as a team. Without effective communication a team literally cannot function as a team and will default to a collection of individuals. Having good personal communication skills:

- Promotes safety
- Provides a professional and safe service and establishment
- Supports colleagues
- Promotes efficiency
- Greatly enhances speed and efficiency

Chapter 8 - Understand record keeping relevant to the role of the Security Operative

Security operatives are required to complete an array of records to meet the requirements of:

- The law
- The Employer
- The Client

The key purpose of all records is to create an audit trail from a notable situation, which may be relied upon in contracts and criminal law. Records also serve as an accurate reflection of actions taken at a given time, which are likely to be forgotten without the support of complete records. Examples of these include:

- 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

Methods of record keeping

Records need to be the words of the person writing them and leave no chance that another, with corrupted intentions, can alter them in anyway. So, there are some 'golden rules' to follow which include:

Write in pen

Put a single line though mistakes and initial above the incorrect word/s

Print and sign name and date at start of report and end of report

Draw a line though any blank spaces or gap between last word and the final signature

Keep them secure

Follow the 5 'W's' and 1 'H' format

HOW

Attending court

During the career of any security operative, there is a strong possibility that they may be called upon to provide evidence in a courtroom to assist the wider community. This will usually be as a result of being a direct witness to criminal activity or, should an operative become known as an expert in their role, to provide professional opinions to support the prosecution or defence of a case. There is a wide range of crimes which may result in court hearings, from assault to fraud and many inbetween.

Court cases can sometimes take years to be called depending on the nature of the hearing. This reinforces the requirement for accurate record keeping allowing the operative to accurately recall the situation.

Points to remember:

- Arrive early and report to the Court Clerk
- Refresh your memory of the contents in your original statement and incident report
- Enter courtroom and head directly to witness box (as directed by the court usher)
- Swear a religious oath or generic oath
- Listen to questions from Solicitors (Barristers in Crown Court), answer honestly, do not interrupt or argue but politely challenge inaccuracies
- Remain formal; address the judge as 'your honour' or 'sir/ ma'am' and only address the person asking you questions
- Answers should be objective facts not subjective assumptions
- Relax as this is a common function of a Security Operative

Chapter 9 - Understand terror threats and the role of the Security Operative in the event of a threat

There are two distinctive types of terrorism:

1. **Domestic**

Internal within the country in an attempt to make a "statement" to their own government.

2. **International**

Made from outside the country borders from another country.

Terrorism is used to create a climate of fear within a population, with the intent of bringing about a particular change. Some terrorist groups work on an international basis, whereas others fight for domestic issues. Certain terrorists target just one particular organisation or company for a specific reason, while others may be more indiscriminate in their targeting.

Public, commercial and retail premises, as well as places of entertainment, could become targets of either a threat or an actual terrorist attack.

Security operatives should always keep an eye on current affairs locally, nationally, and internationally to ensure their understanding of risk is always maintained. Even if nothing has been reported recently, it is still a strong consideration to be vigilant for:

- What is currently happening around the world and in their particular area
- Any recent terrorist attacks or threats
- The location of their own site in relation to other possible targets nearby
- Whether the site itself is famous or important in its own right
- The vulnerability of the site to attack
- The current level of threat nationally

The Security Service (MI5) is responsible for setting the threat level. The system of threat levels and definitions has been created to keep people informed about the level of threat the UK faces from terrorism at any given time.

Critical
An attack is expected
Severe
An attack is highly likely
Substantial
An attack is a strong possibility
Moderate
An attack is possible but not likely
Low
An attack is unlikely

Counter Terrorism

Key Stages to attack or general pre-meditated crime:	**Noticeable activities:**
1. **Target selection** – Who or what? Value either materialistic or political 2. **Information gathering** – Open-source intelligence (OSINT) such as internet 3. **Hostile reconnaissance** – Direct (in person) intelligence gathering 4. **Planning** - May also require further information via surveillance 5. **Preparation** – This stage is sometimes missed if confident of success, otherwise involved a 'dry run' to physically reach the intended target without the final act of theft or terror 6. **Action** – Implementing the plan 7. **Take credit or profit**	1. None 2. Possible high concentration of same IP address on website statistics 3. Unusual questions, looking at security devices/people, taking photos etc. 4. Potential covert surveillance activities 5. False alarms, broken locks, wedged doors, unauthorised people in restricted areas 6. Genuine emergency situation unfolding 7. Media, social media, unusual acquisition of wealth etc.

Hostile reconnaissance

Hostile reconnaissance is a term used to describe how terrorists gain information on potential targets. They will often visit potential targets a number of times prior to attack.

They will be trying to find out as much as they can about the location itself, discover the best time, method of attack and vulnerabilities. Vulnerabilities in security systems and staff are the commonest cause for successful attacks.

Security Operatives need to be vigilant at all times to try and identify suspicious behaviour that may indicate interest in their site. Suspicious behaviour may include:

- A particular interest in the outside of the site
- An interest in the CCTV system
- Taking pictures of the site (overtly or covertly)
- Making notes or drawing diagrams of the site
- Taking an interest in the timings of activities
- False alarm activations (testing response times)
- Damage to perimeter security
- Attempts to disguise identity (hats and hoods)
- Trespassing with no good reason
- Asking unusual questions about the site or security arrangements
- Nervousness
- Reluctance to be noticed or seen
-

All suspicious behaviour in or around site must be reported immediately to the site supervisor or manager. The police may need to be called to investigate.

Effective deterrents to hostile reconnaissance

- Be vigilant to what is happening in the venue and near the venue
- Search customers and bags on entry
- Regularly patrol concealed areas
- Be suspicious of people taking a significant interest in the security measures (this might
- include takings notes, photographs or footage or asking too many questions)
- Be aware of parked vehicles with occupants as well as unoccupied vehicles that have been
- left unattended for long periods
- Feel confident to report the concerns to management or the counter terrorism hotline
- Ensuring a visible presence of vigilant security staff; frequent patrols but at irregular
- intervals
- Maintaining organised search procedures
- Ensuring emergency exits are secured when not in use to prevent unauthorised entry
- Using your customer service skills to disrupt potential hostile reconnaissance.
- Understanding the importance of showing professional behaviour and visible security as a
- tool to deter hostile reconnaissance.
- Knowing where to report suspicious behaviour including:
    - Internal procedure for site
    - Confidential (Anti-Terrorist) Hotline: 0800 789
    - 321
    - British Transport police (BTP) "See it, Say it,
    - Sorted": text 61016 or call 0800 40 50 40
    - Non-emergency: 101
    - ACT online reporting
    - Life threatening emergency or requiring immediate response: 999

Common attack methods

1. **Marauding Attack** – This is where the terrorist/s indiscriminately attack people on foot using any kind of handheld weapon.

2. **Improvised Explosive Device (IED)** – Often made from domestic and occasionally military grade explosives, the component parts to activate, charge and detonate the device are similarly made from domestic electronic devices.

3. **Person Borne Improvised Explosive Device (PBIED)** – Also known as suicide belts or vests, a terrorist will carry the device on their person and detonate as close to other people as possible.

4. **Vehicle Borne Improvised Explosive Device (VBIED)** – Explosives loaded into a vehicle and located as close to the target as possible.

5. **Leave Behind Explosive Device (LBIED)** – Explosive devices contained in bags, boxes or similar and left at the intended location to allow the terrorist to escape prior to detonation, or to wait for the most effective time to detonate.

6. **Vehicle As A Weapon (VAAW)** – Driving a vehicle at people or buildings to cause harm.

7. **CBRN Attack** – Chemical, biological, radioactive, or nuclear substances released or planted to cause harm.

8. **Cyber Attack** – Using hackers to shut down websites, acquire sensitive information or access bank accounts.

9. **Insider Threat** – Using or becoming an employee at a target location to gain access to the property or assets.

Actions to take in the event of a terrorist attack

- 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 procedures 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 make 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

Sources of counter terrorism advice

Centre for the protection of national infrastructure (CPNI)

CPNI
Centre for the Protection of National Infrastructure

https://www.cpni.gov.uk/

National Counter Terrorism Security Office (NaCTSO)

NaCTSO
National Counter Terrorism Security Office

https://www.gov.uk/government/organisations/national-counter-terrorism-security-office

Dealing with suspicious items

It is difficult to define what is or is not a suspicious item as IEDs can be hidden in all kinds of packages, so it relies on the security operative to recognise something which is out of the ordinary and use a common-sense approach to the situation to understand if the out of place item has a legitimate reason or explanation for being where it is. An example of this might be a security officer working at a train station who identifies an unattended bag. The next step is a consideration as to what is 'normal' in that environment and human behaviour. Most people, if they place their bags down, will keep it in their sight and not leave it unguarded, so a sensible first action would be to ask people nearby if they own the bag or if they can see the person who left it. If not satisfactorily resolved, then it would be appropriate to treat this as a suspicious package and act accordingly.

The Action Counters Terrorism (ACT) eLearning introduces the HOT principles:

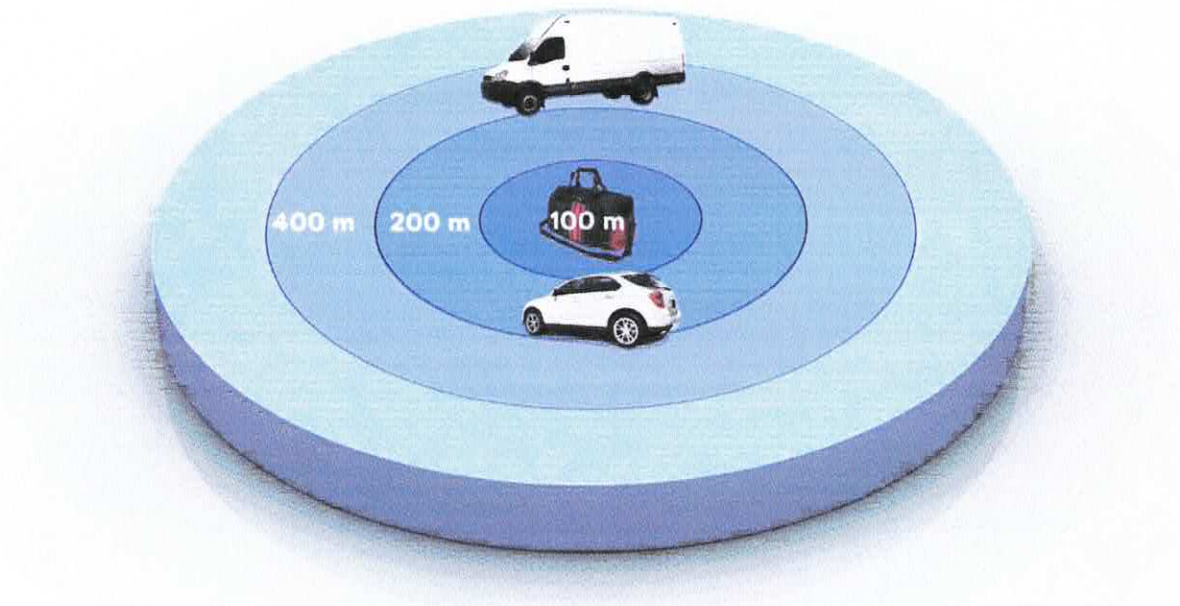
- Is it **Hidden**?
- Is it **Obviously suspicious**?
- And is it a **Typical** item you expect at this location?

After analysing these factors then the security operative should dismiss or confirm it as a suspicious package in a similar manner to the above example. Obviously if there are component parts of an IED visible (wires, batteries etc) then it is immediately a confirmed threat.

Once an item is confirmed as suspicious by a security operative then they should follow the 4 C's approach:

- **Confirm** it is a threat (HOT approach)
- **Clear** the area
- **Communicate** (no less than 15m away) to colleagues, control room or police (as emergency procedures dictate)
- **Control** access by setting up a cordon and letting nobody past unless they are from the emergency services and aware of why the cordon is in place.

How far should a cordon be established from a suspicious package?



No radio or mobile phone use within 15m

Chapter 10 - Understand how to keep vulnerable people safe

As identified previously within this workbook, anyone can become vulnerable at anytime and it is the legal and moral duty of a security operative to do their best to keep them safe.
This short chapter looks at some specific threats to vulnerable people and how to help protect those at risk.

Sexual predators

Sadly, there are people within the public who seek vulnerable targets for their own sexual gratification, it is essential to be able to recognise some of these behaviours in order to prevent a sexual assault from happening.

- Look for individuals making unusual and intense observations of a potentially vulnerable
- person. These observations may include them following their victim for a while to assess
- their level of vulnerability.
- Excessive generosity is another tactic used by potential predators in order to gain trust for
- them to move to a location for the intended assault.
- Suspicious behaviours around certain times and venues. A classic example is at closing time
- at a nightclub, where victims are at their most vulnerable due to alcohol consumption and
- tiredness. Look for someone who moves from one person to the next and aborts if their
- target becomes associated with friends.
- Inappropriate use of technology e.g., up skirting, this is a crime in itself which should be

dealt with immediately and appropriately. It is a precursor to the possibility of further

unwanted behaviours from the stimulus received by the actions of the predator.

Indicators of abuse

Abuse happens to both male and female victims, and there are many types of abuse including physical and mental. Abuse is often carried out by someone close to the victim; a partner, family member or 'friend'. Some of the signs of abuse to look out for are:

- The victim having their freedom restricted e.g., not allowing them to move or talk to
- somebody or aggressively insisting on them doing something that they clearly do not want
- to do.
- Unexplained bruising can occasionally be noticed on a victim. Most bruising can be explained
- by an individual confidently, but when a victim is making up a story, they often show a lack
- of conviction to their explanation, vagueness, or inconsistencies.
- Lack of confidence or insecurity can be noticed in victims of abuse, this often amplifies when
- in the presence of the abuser and may show as nervousness.
- Change in circumstances e.g., cleanliness or appearance. It is not necessarily their appearance which is the issue, when it changes negatively from their usual state that it raises concerns that something is going on.

Security operatives need to use their professional judgement in these situations as to the most appropriate response. If there is an immediate risk to the possible victim's health, then separate them from the abuser and call the police/ make a citizen's arrest. If unsure and non-urgent call crime stoppers or 101 to discuss your concerns.

Be aware of the **'Ask Angela'** campaign

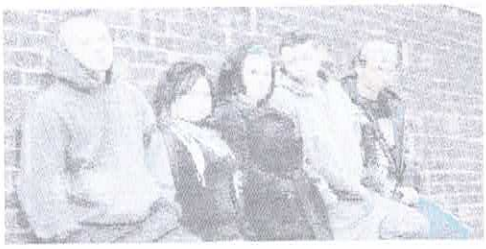
Dealing with anti-social behaviour

Anti-social behaviour is a collective term which includes many public order offences such as breach of the peace, vandalism, intimidation and may other undesirable activities. It is not limited to youth either, consider the scenes in a town centre late on a weekend evening for example.

There is no one particular method of dealing with it without police powers and a security operative must remember that it is often a behaviour associated with tribalistic positioning (being seen to be the 'alpha' in the group they are associated with). Outside of groups, an individual may be displaying anti-social behaviour without the group stimulus and this may be a symptom of drink, drugs, or mental illness. In all of these situations the risk of harm to whoever intervenes directly is increased and direct confrontation is not always the safest option.

Options

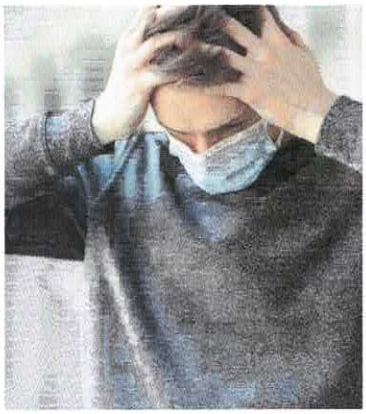
- Follow your organisation's policies and procedures
- Speak to the person/people
- Explain the situation and the risks of the anti-social behaviour
- Explain the consequences if the anti-social behaviour continues
- Remain calm
- Ensure that your colleagues know about the situation and that you have 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.



Chapter 11 - Understand good practice for post incident management

We are always learning from our experiences informally. Following an incident, this is also the case but needs to be done in a **professional** manner as the implications of not getting it right a second

time might have severe consequences. Learning is the second priority as the most important issue is to ensure all those involved are safe and are not suffering from serious mental health issues as a result of the incident they have been involved with. Often overlooked but can lead to **Post Traumatic Stress Disorder (PTSD),** chronic adverse mental health and potentially suicide if not treated as the highest priority, post-incident.



It should also be considered that the incident was merely a trigger to a series of previous experiences that cause the individual to lose the stability they had established prior to the incident occurring. So, it is important that, no matter how insignificant the incident, to recognise that it may have extreme negative effects on those involved.

Sources of support

- Colleagues, management, and counsellors
- Publications, internet
- Help lines (e.g., Samaritans)
- Other support e.g., Citizen's advice/ Trade Unions

Benefits of reflecting on incidents

- 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

Value of a Security Operative's experience

Using shared experiences as a team helps to develop the capability of the organisation in responding to incidents. Increased capability also increases the safety for staff and customers alike.

Never forget the older more experienced staff. Every security company has at least one 'veteran' of the private security industry. With age comes experience and often they will have encountered similar situations and may be able to advise what worked, what went wrong, why it went wrong and many other significant insights to a wealth of experience.

A team which communicates, a team that shares knowledge is a team which grows and a team which will go places!

Further study

At this stage, reading this will be the following types of reader:

1. Those who have now completed the required 8 hours distance learning with this workbook
2. Those who read quickly and are well under the 8 hours
3. Those who have spent longer than 8 hours and read it in small parts over a period of time
4. Those who jump to the back page

Whichever applies, in the security industry especially, knowledge is safety and QNUK always advise you to keep learning at every opportunity.

Spend some time researching to either make up the hours, develop your knowledge or seek clarity for subject areas which were only briefly discussed.

Recommended reading

- 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-madeeasier-for-home-users
- Centre for the Protection of National Infrastructure https://www.cpni.gov.uk/
- National Counter Terrorism Security Office https://www.gov.uk/government/organisations/national-counter-terrorism-security-office
- Resuscitation Council Home | Resuscitation Council UK