

Module 1: Principles of working in the private security industry

Chapter 1: The main characteristics and purposes of the private security industry



The SIA has 3 main aims:

1. The compulsory licensing of individuals undertaking designated activities within the private security industry
2. To recognise quality service by managing the voluntary Approved Contractor Scheme (ACS)
3. Introduction of business licensing for all regulated security companies



The key purposes of the private security industry

Security is a state or feeling of being safe and secure. The UK's private security industry provides manned and technical protection in an effort to prevent and detect crimes and other unauthorised activities and raise standards within the industry.

As well as protecting premises, people and their property, security operatives also help to prevent and detect crime, prevent or reduce loss, waste and damage, as well as monitoring and responding to safety risks.

Security can be provided to clients in 3 main ways:

- **manned security** – where one or more security operatives work on a site, providing both a deterrent against crime and an immediate response to incidents as they occur
- **physical security** – physical deterrents such as locks, alarms, barriers and grilles to help reduce crime
- **systems** – electronic and other technical systems used to monitor premises for crime and other dangers, such as intruder alarms, fire detection systems and closed-circuit television (CCTV) systems

A 'security operative' is the general term used throughout this book to describe any person paid or used to provide any kind of manned security to a client or premises. This term includes door supervisors, uniformed security officers (including key holders), store detectives, CCTV operators, cash and valuables in transit operatives and close protection operatives.

The professionalism within the private security industry, alongside the licencing regime of the security industry authority, are both aimed at raising standards within the sector.

The aims and functions of the Security Industry Authority (SIA)

The organisation responsible for regulating the private security industry is the Security Industry Authority (SIA). The SIA is a non-departmental public body reporting to the Home Secretary, under the terms of the Private Security Industry Act 2001. Its mission is to protect the public by regulating the industry effectively through individual and company licensing, to remove and reduce criminality, to raise standards, to recognise quality of service and to monitor the industry generally.

The SIA's main functions are to:

- protect the public and regulate the security industry through licensing
- raise standards (through the Approved Contractor Scheme)
- introduce business licensing for all regulated security businesses
- monitor the activities and effectiveness of those working in the industry
- set and approve standards of conduct, training and supervision within the industry
- keep under review the private security industry and the operation of the legislative framework
- increase customer confidence



Module 1

Module 1: Principles of working in the private security industry

Chapter 1: The main characteristics and purposes of the private security industry

Licensable roles under the Private Security Act

Door supervisors – those who carry out security duties in or at licensed premises (for example pubs and nightclubs), preventing crime and disorder and keeping staff and customers safe.

Security officers (guarding) – those who guard premises against unauthorised access or occupation, outbreaks of disorder, theft or damage. They may also guard one or more individuals against assault or injuries that occur as the result of the unlawful conduct of others. This protection is given by providing a physical presence or by carrying out a form of patrol or surveillance to deter crime.

Security officers (key holding) – key holding is where a security officer keeps custody of, or controls access to, any key or similar device for operating (whether mechanically, electronically or otherwise) any lock.

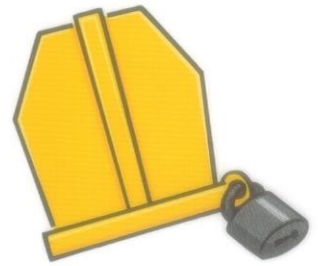
Cash and valuables in transit operatives – those who guard property against destruction or theft while using secure transportation of the property in specially manufactured vehicles.

CCTV operators – those who carry out guarding activities using closed circuit television equipment to either monitor the activities of members of the public in a public or private place or to identify a particular person. This includes the use of CCTV to record images to be viewed on non-CCTV equipment.

Close protection operatives – those who guard one or more individuals against assaults or injuries that might be suffered as a consequence of the unlawful conduct of others.



Vehicle immobilisers are only licensed by the SIA in Northern Ireland. These are security operatives who either remove or relocate vehicles, restrict the movement of vehicles using a device or release vehicles after demanding or collecting a charge.



Other as yet non-regulated sectors of the private security industry include private investigation, event security, electronic security and fire systems.



Module 1: Principles of working in the private security industry

Chapter 1: The main characteristics and purposes of the private security industry



Furthermore, security operatives must always conduct themselves in strict accordance with the SIA's **standards of Behaviour** for their particular role within the industry, as well as their own organisation's values and standards. For further information about the SIA, please visit: www.sia.homeoffice.gov.uk



Individual licensing

SIA licensing currently covers door supervision, security guarding, key holding, CCTV operations, cash and valuables in transit operations and close protection.

Licensing ensures that security operatives are 'fit and proper' persons who are properly trained and qualified to do their jobs. The SIA also sets and approves standards of conduct, training and supervision within the industry.

Anyone wishing to work as a security operative must have an SIA licence before they start work. To work without a licence is a criminal offence, carrying fines of up to £5,000 or up to a 6-month prison sentence.

It is also a criminal offence for an employer to use an unlicensed security operative. To get a licence, you need to apply to the SIA itself. Your identity will be verified, you will be required to undergo the specified training, your criminal record will be checked and you will be required to pay a licence fee. Your licence will last for 3 years, after which time you will need to renew it.

Approved Contractor Scheme

The SIA's Approved Contractor Scheme (ACS) introduced a set of operational and performance standards for private security companies.

Companies that can prove that they can meet these standards can be awarded Approved Contractor status, which provides their customers and clients with independent proof of the company's commitment to quality.

Standards of behaviour

It is very important that all security operatives conduct themselves professionally at all times. Clients and members of the public expect security staff to act in a certain way.

But what qualities should security operatives possess?

Security operatives should be:

- professional
- polite
- sensitive
- honest
- reliable
- responsible
- courteous
- fair
- dedicated
- alert
- observant
- helpful
- approachable
- smart in appearance
- tactful
- self-disciplined
- cooperative
- patient
- loyal
- positive
- good communicators
- effective problem solvers
- team players
- handle sensitive situations

Above all security operatives should have integrity and be prepared to take responsibility for their actions.

Module 1: Principles of working in the private security industry

Chapter 1: The main characteristics and purposes of the private security industry

Community safety initiatives

Working with the various private and community crime reduction initiatives in the area can go a long way towards helping security operatives keep their premises and clients safe.

This is done by helping to reduce the opportunities for crimes to take place. For example, local authorities now use Safer Community Partnerships to help reduce crime and the fear of crime in their areas. They work together with the police, the other emergency services and other relevant public and private organisations to try to reduce crime, public disorder, reoffending, anti-social behaviour, substance misuse and vandalism.

Working with national and local crime reduction initiatives like these can help security operatives to raise levels of security for themselves, the public and for their own clients and customers, as well as helping to reduce crime, disorder and anti-social behaviour in the area generally. Sharing information with these other initiatives and groups can also help to improve a security operative's knowledge of what is happening in the area in which they are working.



Crime reduction initiatives try to do this by:

- improving the physical security of vulnerable areas
- improving the environment itself
- removing the means and opportunities to commit crime
- using extra lighting to improve visibility in an area
- using warning signs
- controlling access to certain areas at specific times
- using CCTV
- using radio communications between various organisations and companies
- making use of local and national Pubwatch and Shopwatch initiatives
- using the yellow and red warning cards in conjunction with the local Pubwatch policy

How assignment instructions support the security operative role

The documents used to describe what the client requires of the security company are known as assignment instructions (A.I.s). They are primarily used for security sites and retail but are not commonly used in licenced premises.

Assignment instructions will state when certain duties, such as a patrol, must be carried out.

They also state the emergency procedures, emergency contact numbers and the numbers of other key individuals that you may need to contact, e.g. maintenance contractors.

Assignment instructions are confidential and should never be discussed with individuals outside of the security team and your management.

Module 1: Principles of working in the private security industry

Chapter 1: The main characteristics and purposes of the private security industry



Benefits of using CCTV

CCTV has become one of the most essential pieces of technology used to monitor sites/premises.

Ideally, CCTV cameras should be monitored at all times while the business is functioning. The CCTV operator can then direct security operatives to points of high risk while monitoring their safety. This is a cost-effective method of deploying security resources while keeping staffing to a minimum level.

Many customers and staff find CCTV reassuring as the presence of CCTV is known to be a deterrent to some criminals. If used correctly, the footage can be used as evidence in court.

CCTV can also be used to assist in investigations, for example for accidents or thefts. This can prevent malicious claims against companies, for example if someone attempts to push a trolley up an unsuitable escalator despite having clearly seen the signage prohibiting this action. CCTV cannot, however, be used to spy on people.



All businesses must register their systems with the Information Commissioner's Office (ICO). The ICO regulate the use of CCTV systems and storage of all personal data via the Data Protection Act 2018.

At each entry point to the premises, there must be signage stating that CCTV is in operation, as well as stating the name and number of the responsible person. Only approved and trained persons can view live footage.

Storage of the footage must be secure and the images must only be retained for the time period stated on the approval. This is usually 28 days, but approved time periods may vary.

CCTV must not be used where people are likely to be in a state of undress, e.g. the toilet cubicle.

Limitations of using CCTV

The use of CCTV can frighten some people, as they may feel that their privacy is being violated. Some people will even avoid certain areas because they do not want their image to be captured.

The cost of CCTV equipment has decreased significantly over the last 10 years, however the initial outlay for good and sufficient equipment can still be cost prohibitive for some businesses.

Poorly positioned cameras are more likely to be damaged prior to the occurrence of an illegal act. A camera cannot prevent crime, and a damaged/vandalised camera cannot do anything.

The capability of the CCTV operator, and their familiarity with blind spots or poor lighting, is key when looking to gain footage that is acceptable for use in court and for maintaining the continuity of evidence.

Although a CCTV system needs a human being in order to be fully effective, sometimes that person may use the cameras for the unauthorised monitoring of friends or even just someone they like to look at. This is misuse of the equipment and is illegal in many cases.

Key tasks



1 What does the abbreviation SIA stand for?

.....

.....

.....

2 Describe the THREE main aims of the SIA.

1

.....

2

.....

3

.....

3 Identify FIVE standards of behaviour expected of a security operative.

1

2

3

4

5

Module 1: Principles of working in the private security industry

Chapter 2: Awareness of the law in the private security industry



Criminal offences include:

- murder
- kidnap (abduction in Scots law)
- rape
- sexual assault
- assault
- drugs offences
- possession of weapons
- theft
- burglary (housebreaking in Scotland)
- fraud
- robbery
- criminal damage
- arson (wilful fire-raising in Scotland)
- firearms offences
- child abuse
- domestic abuse
- driving under the influence

Security operatives and other members of the public have powers of arrest for some of these offences as they are so serious.

The standard of proof in the criminal courts is 'beyond reasonable doubt'.

Civil and criminal law

The role of a security operative in the fight against crime is increasing. Because of this, and so that you can be effective in the workplace, it is important for you to gain a basic working knowledge of the law.

Laws are there to ensure that citizens abide by certain rules that are made to keep everyone safe. Laws tell us what people are and are not allowed to do and allow people to be punished if those laws are breached.

There are 2 main types of law in the UK, **civil law** and **criminal law**.



CIVIL LAW

Civil laws help govern our daily lives. They usually deal with disputes between people, companies or other organisations. They are there to right wrongs, and proceedings are usually started by the person or people who believe they have been wronged in some way.

They deal with things like money owed, family and matrimonial disputes, property disputes, breach of contract, employment law, personal injury cases, custody of children, adoption, libel and slander (known as defamation in Scotland). Cases are often remedied by way of compensation orders for loss or damage.

Civil cases are usually dealt with in the county courts, with more serious cases being heard in the High Court. In Scotland, civil cases are heard by the Sheriff Court with more serious cases being heard at the Court of Session. The standard of proof in the civil court is 'on the balance of probabilities'.

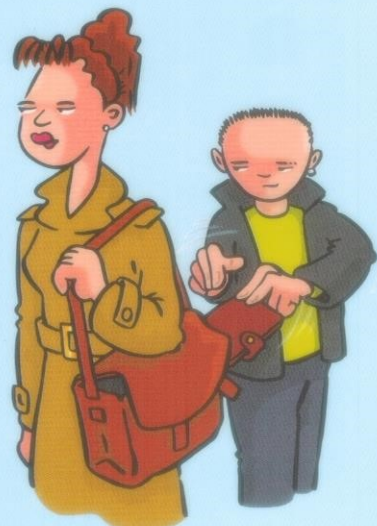


CRIMINAL LAW

Criminal laws, on the other hand, are there to prevent people from committing more serious offences, usually against people or property, and to punish people when those laws are breached.

Criminal laws come from either very old judicial decisions made in courts (common law) or can be found in Acts of Parliament (statute law).

Cases are normally brought by the state, often following an arrest, and prosecution is sought through the criminal courts. Guilty verdicts can result in fines, probation orders and terms of imprisonment.



Module 1: Principles of working in the private security industry

Chapter 2: Awareness of the law in the private security industry

Trespassers

A trespass is committed by a person who is improperly on someone else's property without consent.

One of your duties as a security operative is to ensure that only suitable and authorised people are allowed into the premise. During the course of your duties, you may well have to ask people to leave the premises and as a last resort you may have to physically eject them if they refuse to leave when asked. This section explains the powers you have to deal with these types of situations.

Trespass is not normally a criminal offence. It is, however, an act of interference against the lawful occupier of any specific premises and can be actionable through the civil courts.

A 'lawful occupier' is someone who owns, occupies or has control over the property. In the case of private buildings like factories, shops, pubs or clubs, it means the owner, manager or person in charge of the property and includes any members of staff acting on their behalf, as well as any authorised customers or visitors. This would include security operatives, whose job it is to protect the premise.

Security operatives may ask people to leave a premise if they:

- have no right or reason to be there
- break criminal laws
- break licensing laws
- breach specific premise rules or conditions
- start to display unacceptable behaviour

When asking a member of the public to leave the premises, you should first ask them to leave and explain why, telling them why they are not allowed to be there, what law they have broken, what rule they have breached or how their behaviour has become unacceptable.

If they refuse to leave, you should repeat the request, informing them that if they refuse to leave they will either be physically removed or the police will be called.

If they still refuse to go, you should offer them one more chance to leave peacefully by saying something like, 'Is there anything else I can say to make you leave on your own?'. This gives them one more opportunity to change their mind and is also a good defensible statement that other people will hear that shows that you did everything possible to encourage the person to leave peacefully, before having to resort to the use of force to remove the person from the premises. If you are working with another security operative, it will also warn them that you are about to take action and will allow them to prepare themselves to assist with the ejection. If someone you have ejected from a site becomes violent or attempts to force their way back in, then you should call the police to assist.

It is also within the law that police officers can be called upon to assist with ejecting people who are refusing to leave, having been asked to by a lawful occupier, their employee or agent. They may use such force as may be required to effect their purpose.

If you need to eject someone from the premises you are protecting, then it should be reported to the person in charge of your duty immediately. To safeguard yourself against any subsequent malicious allegations, it should also be recorded as an incident.

It is obviously always better to try to use tact and persuasion to get an unwanted customer to leave the premises, only using force as a last resort. Even then, you must use no more force than is necessary to remove the person.

R.E.A.C.T.

explains the best way to remove a trespasser:

- R** request them to leave
- E** explain the reasons for the request
- A** appeal for them to leave, explaining what will happen if they do not
- C** confirm that they still refuse to leave peacefully
- T** take action (eject)

As a last resort, you may have to physically eject the trespasser from the site. The law allows you to do this, provided that:

no more force is used than is necessary to remove the trespasser from the premises.



Module 1: Principles of working in the private security industry

Chapter 2: Awareness of the law in the private security industry

SCO

The Trespass (Scotland) Act 1865 makes it an offence under Scots law to trespass. The legislation was amended under the Land Reform (Scotland) Act 2003 which established universal access rights to most (but not all) land. These reforms do not apply (hence why trespass remains an offence) to:

houses and gardens and non-residential buildings and associated land, land in which crops are growing, land next to a school and used by the school, sports or playing fields when these are in use and where the exercise rights would interfere with such use, land developed and in use for recreation and where the exercise of access rights would interfere with such use, golf courses (you can cross a golf course provided that you do not interfere with any games of golf), places like airfields, railways, telecommunication sites, military bases and installations, working quarries, construction sites and visitor attractions or other places that charge for entry are exempt and as such unauthorised access would be trespass.



SCO

Trespass in Licensed Premises in Scotland

Under Section 116 of the Licensing (Scotland) Act 2005 it is an offence for any person to refuse to leave licensed premises as follows:

- a person on any relevant premises who behaves in a disorderly manner, and refuses or fails to leave the premises on being asked to do so by a responsible person or a constable, commits an offence
- a person on any relevant premises who, after the end of any period of licensed hours, refuses or fails to leave the premises on being asked to do so by a responsible person or a constable commits an offence

Where a person refuses or fails to leave any relevant premises, then the door supervisor may remove the person from the premises and if necessary for that purpose, use reasonable force.

A constable must, if asked by an authorised person to assist in exercising a power conferred by subsection 3 (above) and if the constable reasonably suspects the person to be removed of having refused or failed to leave as requested, provide the assistance asked for.

A person guilty of an offence under this section is liable on summary conviction to a fine not exceeding £1,000.

NI

In relation to trespass, the new criminal trespass law enacted under s128 of SOCPA, has made it illegal to trespass on certain designated military and nuclear sites in Northern Ireland. There is a common law offence of trespass against property and a criminal law offence of trespass/harassment against the person, including assault.

Module 1: Principles of working in the private security industry

Chapter 2: Awareness of the law in the private security industry

The Private Security Industry Act

The Private Security Industry Act 2001 was brought in specifically to regulate the UK's private security industry and to help raise the standards of the individuals and companies working within it. One of its main aims was to increase the public's confidence in the sector and to increase public safety.

The government formed a new corporate body called the Security Industry Authority (SIA) to do this.

The SIA now licenses security operatives, supervisors, managers, directors and company owners in the areas of door supervision, manned guarding, key holding, cash and valuables in transit, CCTV operations and close protection (and vehicle immobilisation in Northern Ireland).

This is to ensure that people employed within the industry are 'fit and proper' for their job roles.

The SIA also provides a public register of licensed individuals and maintains a list of its approved companies via the Approved Contractor Scheme (ACS).

The Private Security Industry Act also gives the SIA various powers of entry and inspection to ensure compliance, and lists specific offences and subsequent sentences for those caught breaching the act.

Equality and diversity in the workplace

As a security operative, in order to improve your image and level of professionalism, it is important that you are aware of and act correctly in relation to issues concerning diversity and equality. Security operatives provide a service and must provide the same quality of service to everyone. You must not **discriminate** against certain types of people when carrying out your duties. Discrimination is treating a person less favourably than another person.

Prejudice is having a hostile (or sometimes positive) attitude towards someone who belongs to a certain group, simply because they belong to that group and are therefore assumed to have all of the characteristics ascribed to that group.

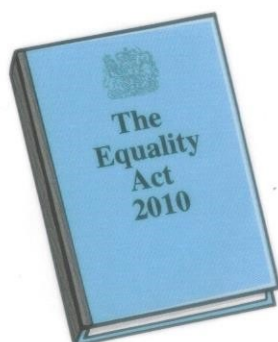
Stereotyping is lumping certain groups of people together, assuming that they are all the same simply because they belong to that group.

Prejudices and stereotyping can be harmful when they are used to openly discriminate against people. As a security operative, you are reliant on the public for support and confidence, so it is important that your conduct is seen to be impartial and reasonable at all times.



Module 1: Principles of working in the private security industry

Chapter 2: Awareness of the law in the private security industry



The Equality Act 2010 (Not applicable in Northern Ireland)

Previously, discrimination, equality and diversity were enforced by numerous separate pieces of legislation. Those laws were often confusing and some were outdated and ineffective.

The Equality Act received Royal Assent on 8 April 2010 and its core provisions came into force on 1 October 2010. The purpose of the Act is to provide a new legislative framework to protect the rights of individuals and to advance equality and opportunity for all. The new Act simplifies 9 pieces of legislation, bringing into existence a singular statute dealing with discrimination. Some of the old laws remain the same, while others have been changed or expanded. Some new elements have appeared for the first time.

The Equality Act prohibits discrimination on the grounds of:

- age
- disability
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity
- race
- religion
- sex
- sexual orientation

These are known as the protected characteristics. It is illegal for employers, for example, to discriminate against any of these groups of people in the areas of recruitment, access to training, pay and benefits, promotion opportunities, terms and conditions, redundancy and dismissal.

Furthermore, employers now have to make reasonable adjustments to cater for the employment of disabled people.

Types of discrimination

Direct discrimination occurs when someone is treated less favourably than another person because of a protected characteristic they have or are thought to have, or because they associate with someone who has a protected characteristic.

Indirect discrimination occurs when a policy or practice that applies to everyone particularly disadvantages people who share a protected characteristic.

People's rights under this legislation can be enforced through the county courts, resulting in fines and/or compensation being awarded.

Discrimination can be hurtful, insulting and demeaning to the recipient, and is not acceptable from security professionals.

It is also made clear under the Human Rights Act that all people have the right to be free from discrimination.



In Northern Ireland, discrimination is illegal under the following laws:

- The Race Relations (Northern Ireland) Order 1997
- The Sex Discrimination (Northern Ireland) Order 1976
- The Disability Discrimination (Northern Ireland) Order 2006

As a security operative, you cannot refuse entry or evict anyone on the grounds of sex, race, colour, disability or physical appearance. Should you refuse entry to or evict an individual for any of these reasons alone then you will be committing an offence. The individual who has been discriminated against has the right to make a formal complaint to the premises management requesting an apology, a commitment that such discrimination does not reoccur or even compensation. If the issue is not dealt with to their satisfaction, they may even take legal action against you and your employer.

Module 1: Principles of working in the private security industry

Chapter 2: Awareness of the law in the private security industry

The Data Protection Act 2018

The Data Protection Act 2018 enabled the General Data Protection Regulation (GDPR). The legislations cover any information related to a person or 'data subject' that can be used to directly or indirectly identify them. It can be anything from a name, a photo and an email address to bank details, social media posts, biometric data and medical information. It will also introduce 'digital rights' for individuals.

The GDPR manages how personal and sensitive information can be used, stored and passed on. These laws give you rights as an employee and also require you to treat individuals' information responsibly.

The regulation ensures that organisations maintain the protection of data. It makes sure that personal data held by organisations is kept confidential, processed lawfully, used only for the purpose it was intended, not kept longer than necessary and is accurate. The regulation gives individuals the right to see the data and information held about them. It also promotes greater accountability and governance by organisations, as evidenced by the 'accountability principle', which requires organisations to demonstrate that they comply with the data protection principles.

The data protection principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. In short, Article 5 (1) of the regulation requires that personal data should be:

- (a) Processed lawfully, fairly and in a transparent manner
- (b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- (d) Accurate and, where necessary, kept up to date
- (e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- (f) Processed in a manner that ensures appropriate security of the personal data

Data protection rules often apply to the use of written records and notebooks, as well as the use of body-worn cameras.

You can find more information about the General Data Protection Regulation 2018 here:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?q=digital>



Key tasks



1 Describe civil law and criminal law.

Civil law

.....

.....

.....

Criminal law

.....

.....

.....

2 Identify the key legislation relating to equality and diversity in the workplace.

.....

.....

.....

.....

3 Explain how the data protection regulation impacts your role as a security operative.

.....

.....

.....

.....

.....

.....



Health and safety in the workplace

Every year, thousands of people in the UK are forced to take time off work due to health and safety-related issues. For some, this may only mean a few days off work, but for others it could mean long-term injuries or even death.

The vast majority of incidents can be avoided through better health and safety procedures. Health and safety procedures in our places of work need to be effective to keep staff, visitors and customers safe. Furthermore, there is specific legislation in place to ensure that proper health and safety procedures are enforced anywhere where people work or come to be served.

The Health and Safety at Work etc. Act 1974

(Health and Safety at Work (Northern Ireland) Order 1978) covers employers, employees, the self-employed, suppliers, people who control premises and visitors/customers who come onto the site. Those failing to comply with health and safety legislation face a range of penalties, and businesses can be closed for serious breaches.

Breaches of the legislation can be dealt with by either the Health and Safety Executive (HSE) or by the local environmental health practitioner (EHP) from the local authority. Breaches can result in:

- improvement notices
- prohibition notices
- criminal proceedings

Duty of care

Employers have a moral and legal duty of care to protect the health, safety and well-being of their employees and others, including customers and members of the public who might be affected by their business. Employers must do whatever is reasonably practicable to achieve this. Serious breaches of health and safety legislation can result in penalties of up to 2 years' imprisonment and/or unlimited fines.

Health and safety responsibilities

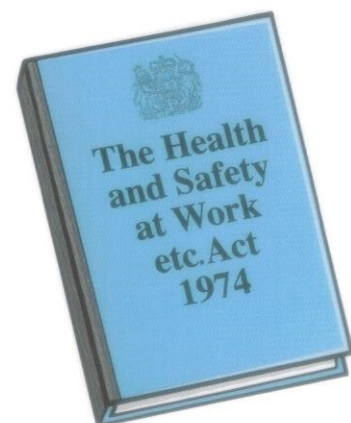
Employers must carry out a proper risk assessment of any possible risks to employees and other people visiting the site. Then they must do what they reasonably can to either remove or reduce those risks. They can do this by providing proper safety equipment, relevant warning signs, putting safe working practices in place, providing any relevant training or instruction and by supplying staff with any suitable personal protective clothing or equipment (PPE). They must provide safe access and egress as well as providing proper first-aid facilities, and ensuring that there are proper reporting procedures in place in case of incidents.

Depending on the size of the site and the number of people working there, they may have to also provide a written health and safety policy.

Employees and the self-employed

Employees and the self-employed working on the site, be they full-time or part-time, have a duty to take care of their own health and safety, and must make sure that they do not do anything that puts someone else's health and safety at risk.

Employees must follow the site's health and safety policy at all times if there is one in place, they should obey all safety instructions and should use safety and personal protective equipment properly. If serious incidents occur, they must follow the site's emergency procedures to help protect themselves, other staff and any visitors/customers. They must then follow the site's reporting procedures to inform the employer of any accidents and/or injuries.



Chapter 4: The importance of safe working practices

Workplace hazards and risks

Good health and safety practices in the workplace are all about reducing hazards and risks.

Definition

Hazard

Potential source of harm or adverse health effect on a person or persons.

Typical hazards in the workplace include:

- factors that cause slips, trips (e.g. unsuitable footwear), flooring, steps, uneven surfaces, spillages for example cleaning fluids and contamination, poor lighting

Risk

Likelihood that a person may be harmed or suffer adverse health effects if exposed to a hazard. Levels of risk may be, high, medium or low impact.

Typical risks in the workplace include:

- accidents due to poor lighting, uneven surfaces, steps etc.
- infection from body fluids
- dealing with aggressive or violent behaviour
- injuries from poor manual handling
- misuse/abuse of machinery
- sharp objects (needles/knives)
- diseases
- hazardous chemicals
- noise pollution
- moving vehicles
- obstructions
- fire/floods and other emergencies
- unsuitable footwear
- spillages, for example cleaning chemicals
- global or critical incidents

In relation to global (or critical) incidents such as pandemics, epidemics, acts of terrorism, etc. you must ensure that you follow all relevant health and safety policies and organisational procedures. In the case of a pandemic, you may find that you are required to work from home where possible, if this is not possible then you may be asked to wear additional PPE such as face masks when in the workplace. You can find further information on the .gov website and the World Health Organization website <https://www.who.int/> about current global incidents.

Minimising risks to personal safety and security

Once a hazard or risk has been identified, you need to follow the **hierarchy of control** to work out the best ways to deal with the potential problem. This is done by asking yourself:

- can the hazards be eliminated?
- can the hazard be substituted with a reduced risk?
- can the hazard be isolated or enclosed?
- would the introduction of a safe system of work reduce the risk? For example, new procedures and routines.
- would information, training or supervision reduce this risk?
- would PPE help?

Examples of personal protective equipment (PPE) for security operatives include:

- waterproof clothing
- high-visibility clothing
- headwear
- gloves (needle/slash resistant)
- rubber gloves and face shields (body fluids)
- stab-resistant vests
- ear defenders
- eye protection
- safety footwear
- face masks/coverings (infectious diseases)

There are **5** steps to carrying out a risk assessment

Step 1

Identify the hazards

Step 2

Identify who may be harmed and how

Step 3

Evaluate the risk and introduce further controls

Step 4

Record the findings and implement them

Step 5

Review and revise and update if necessary

The **6** safe lifting techniques are:

1 Stop and think

2 Position the feet

3 Bend the knees

4 Get a firm grip, keep the back slightly flexed

5 Raise with the legs

6 Keep the load close to the body

Definition

Risk assessment

The identification of hazards, the calculation of risk, the reduction of that risk, either completely or to an acceptable level.

Equipment:

- metal detectors and/or mirrors for searching
- body-worn CCTV
- radios
- mobile phones
- personal alarms
- torches
- equipment as it applies to the incident e.g. to help control infections

Safe manual handling

Manual handling is the movement or support of any load by physical effort, including lifting, moving, carrying, pushing and pulling.

If you lift or move heavy objects without using the recognised procedures, you run the risk of sustaining the following injuries:

- fractures
- spinal disc injuries
- trapped nerves
- friction burns
- damage to muscles
- damaged ligaments and tendons
- abrasions and cuts
- hernias

It is important to follow safe routines and be systematic before attempting to lift a load, use

L I T E

to evaluate the risk.

L LOAD

Look at the load. If it is too heavy, can it be lightened or split? If it is unstable, can handles be fitted or the load be reapportioned?

I INDIVIDUAL

Consider the capability of the person. Are they strong or fit enough? Are they adequately trained for the task?

T TASK

Evaluate the job to be done. Does the task involve stretching, twisting or bending? Can machinery be used or can team handling be used?

E ENVIRONMENT

Control the environment where the task takes place. Is the floor slippery or uneven? Can the layout or floor condition be improved?

Lone working

Security operatives who work alone can be at particular risk in the workplace. They may feel isolated if they only have technological means with which to communicate with colleagues or call for assistance, technology can often fail to work in the manner intended.

Security officers could particularly be susceptible to:

- violence
- injury
- ill health
- lack of support/communication
- lack of welfare facilities for rest

Module 1: Principles of working in the private security industry

Chapter 4: The importance of safe working practices

Safety signs and signals

Safety signs are used to communicate health and safety instructions. They must be kept clean, in good condition and must be displayed where they can be easily seen.

Security operatives must be aware of the colours and shapes of the 6 different types of signs.



Signs & Signals

PROHIBITION 1

Prohibition signs mean that you are prohibited from doing something.

MANDATORY 2

Mandatory signs mean that you must do something.

SAFE CONDITION 3

Safe condition signs indicate where to go to for safety.

WARNING 4

Warning signs indicate a specific danger.

FIRE SAFETY 5

Fire safety signs indicate firefighting equipment.

HAZARDOUS SUBSTANCE 6

Hazardous substances signs warn you about dangerous chemicals.

Module 1: Principles of working in the private security industry

Chapter 4: The importance of safe working practices

Reporting health and safety accidents and incidents

Following any accident or medical incident it is important to record all of the details relating to the situation. The information contained in the accident or incident book can help employers to identify accident trends, so they can then improve practices and procedures on the site to prevent further similar incidents.

These records may also be required for insurance and/or investigative purposes.

Reporting procedures

Accident and incident reports need to include at least the following information:

- day, date and time of incident
- location of incident
- how you were alerted to it
- what you saw
- what you were told
- what happened
- what action you took
- whether first aid was required
- whether the emergency services were called
- what the result was
- details of any injuries
- details of any witnesses
- any descriptions of property or people

These reports need to be made as soon as possible after the incident has finished, while the events are still fresh in your mind.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013

For serious accidents, incidents and near misses at work, **the employer** or the designated 'responsible person' is required by law to notify their local authority, the Health and Safety Executive (HSE) or the Incident Contact Centre. This can now be done online.

The first person on the scene assisting a casualty may not be directly responsible for completing the RIDDOR report, but they must ensure that their supervisor, manager or the health and safety officer within the company receives the correct information contained within the accident or incident report. Security operatives need to know the site's procedures for reporting medical incidents and must adhere to them.



RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (Northern Ireland) 1997.



Chapter 4: The importance of safe working practices

Keeping personal information safe

The Data Protection Act/GDPR, covers any information related to a person or 'data subject' that can be used to directly or indirectly identify them. It can be anything from a name, a photo and an email address to bank details, social media posts, biometric data and medical information. It will also introduce 'digital rights' for individuals. As a security operative, it is vital that you keep all personal information safe. This can be done by:

- following all organisational procedures
- following assignment instructions
- maintaining confidentiality of information
- using social media in a responsible way; this includes having the highest levels of security settings on your accounts

- not wearing anything identifiable outside the workplace
- demonstrating personal vigilance, e.g. not completing surveys
- not discussing work issues outside the workplace
- not discussing work information with colleagues

Personal Information



Key tasks



1 Identify the responsibilities of employees and employers under the Health and Safety at Work Act.

Employees	Employers

2 Identify FOUR risks associated with lone working.

- 1
- 2
- 3
- 4

3 State the procedures that should be followed for recording and reporting accidents and health and safety incidents.

Accidents	Health and safety incidents

Chapter 5: Fire procedures in the workplace

Fire safety measures

As you saw in the health and safety section, both employers and all members of staff have a legal duty to do what they can to help keep everyone safe.

Fire safety on the premises or site is important for both staff and any visitors or customers. If a fire occurs in the workplace, it could result in the disruption of the normal business activities and can affect profitability. More importantly, staff and/or customers could be injured or even lose their lives.

Good fire safety is, therefore, everyone's responsibility. Basic fire prevention measures can go a long way towards helping to prevent the chances of a fire starting in the first place, for example:

- all non-essential electrical appliances should be switched off
- electrical points should not be overloaded
- all electrical equipment should be inspected regularly and maintained properly
- flammables must be stored safely
- ashtrays should be emptied regularly
- rubbish should be stored away from the building
- electric and gas fires must be kept well away from furniture

Under the **Regulatory Reform (Fire Safety) Order of 2005**, (*Fire (Scotland) Act 2005*) employers must nominate a competent person to carry out a full fire risk assessment for the site, which must be documented.

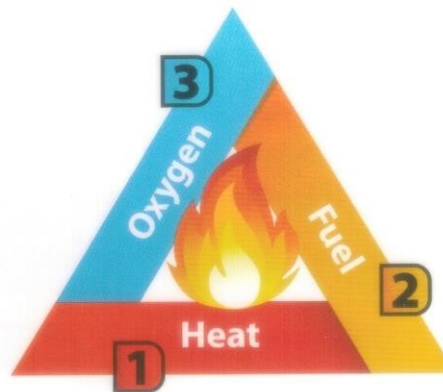
They must also provide their employees with any relevant information, instruction and training to ensure their safety while working on the site.

Employees such as security operatives must take responsibility for their own health and safety, and for that of others. They must be observant, vigilant and also cooperate with their employers in all matters relating to fire safety. This includes following any training and adhering to the fire plan.

Elements needed for a fire to exist

Fire needs 3 elements to start and survive. They are heat, fuel and oxygen. If any of these 3 elements are greatly reduced or removed, then the fire itself will be reduced or extinguished.







The fire triangle



This is known as the fire triangle. All 3 elements need to be present for a fire to start and continue. If any 1 or more of these elements are taken away, then the triangle is broken and the fire will die out.

Classifications of fire

Fires are divided into types or classifications. Each class requires a different method of extinguishing and so it is important that we understand the differences.

	CLASS A	Ordinary combustibles, i.e. paper, wood, textiles, rubber, plastic, fabrics
	CLASS B	Flammable liquids, i.e. petrol, oil, paints and solvents
	CLASS C	Flammable gases, i.e. butane, propane
	CLASS D	Metal fires, i.e. magnesium, sodium
	CLASS F	Cooking oils and fats
		Fires involving electricity



Fire needs 3 elements:

1
HEAT - a minimum temperature is needed to start a fire, and for it to continue.

2
FUEL - fire needs something to burn, like solid fuel, oil or gas.

3
OXYGEN - fire needs oxygen to burn, as it supports the combustion process.

Module 1: Principles of working in the private security industry

Chapter 5: Fire procedures in the workplace

Information on fire extinguishers

- Contents gauge
- Type of extinguisher
- Method of operation
- Class of fire suitable for use
- Service maintenance date*



*All extinguishers should be inspected annually by a competent person, e.g. an extinguisher engineer.

Actions on discovering a fire

It is important that all security operatives take the correct actions on discovering a fire. You will need to:

- follow the organisation's policies and procedures
- sound the alarm and inform emergency services
- follow the acronym of FIRE:
 - Find – you discover a fire
 - Inform – raise the fire alarm
 - Restrict – restrict access to the area of the fire
 - Evacuate – evacuate the building or extinguish (extinguish the fire if safe to do so).
- control panel: Important to ensure full understanding of the extent of the area of the incident, to pass on correct message to emergency services e.g. with regard to materials or chemicals stored in the affected area

Fire-fighting equipment

Fire extinguishers are generally used to fight small fires, to prevent them spreading and causing large-scale damage.

They have a limited capacity, but they can be easily carried to the fire and quickly put to work.

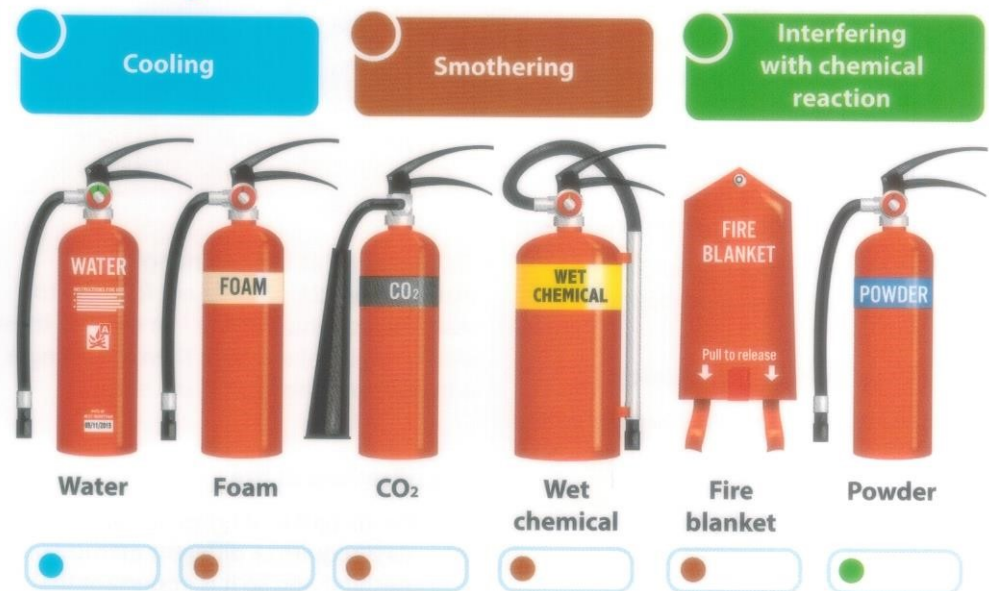
They are intended to be used by anyone who needs them, so it is important that all members of staff learn of their uses, locations and methods of operation.

Fire extinguishers should be sited in conspicuous locations on escape routes, such as next to exits and in corridors, and should be mounted on wall brackets.

Different types of extinguishers are designed to fight different classes of fire, so it can be useless or even dangerous to use the wrong type of extinguisher at the scene of a fire.

We need to understand, then, how the different types of extinguishers work and how they put out fires.

Fire extinguishers



Only attempt to fight a fire if:

- the alarm has been raised
- the emergency services have been contacted
- the fire is not spreading and has been confined
- you have a clear escape route not threatened by fire
- you have selected the correct extinguisher

Do not attempt to fight a fire if:

- it is bigger than a wastepaper bin (rule of thumb)
- you need more than 1 extinguisher
- the room is filling with smoke
- you do not have a clear escape route
- gas cylinders or chemicals are involved
- your efforts are not reducing the size of the fire
- you do not have the correct extinguisher

To operate an extinguisher:

- select the correct extinguisher
- check the contents gauge
- pull the pin to break the seal
- holding the extinguisher upright and squeeze the trigger
- test the range and content (away from the fire)
- extinguish the fire using the correct technique for that type of extinguisher and the nature of the fire

Module 1: Principles of working in the private security industry

Chapter 5: Fire procedures in the workplace

Other firefighting equipment

Apart from fire extinguishers, there are several other types of equipment used to put fires out or to reduce their effects.

Fire blankets

Fire blankets can be used to extinguish fires by smothering them. They are often found in kitchens as they are very useful for extinguishing fat fires in pans.



Sprinklers

Some fire alarm systems are connected to sprinklers which spray water on to the fire from outlets in the ceiling, holding back the fire until the arrival of the fire brigade.

Hose reels

Hose reels are long lengths of rubber hose on large drums positioned strategically around the site. The hoses are permanently connected to the mains water supply and are started by opening a valve before use. They can be quite heavy to unreel when needed but are very effective when used as they provide a limitless supply of water.



Dry and wet risers

Some buildings, particularly multi-storey ones, have riser systems built in. These systems consist of long water pipes running along the outside of the building and across the ceilings on each floor, allowing water to be dispensed via sprinklers to each floor in the event of a fire.

Wet riser systems have water in the pipes all the time, whereas dry riser systems need to be activated manually to send the water into the pipes.

Flooding systems

Flooding systems are designed to be used in unoccupied rooms where there are high value contents or areas where a fire may cause major disruption to the activities of the organisation. Examples might be archives, electrical equipment or switchgear.

On detection of the fire, a fire extinguishing medium (most commonly CO₂) will be discharged into the room to replace the air and extinguish the fire by smothering.



Fire doors and fire exits

Internal fire doors are used to help prevent or reduce the spread of smoke and flames from one room to another. They should be closed at all times, unless they can be closed electronically if the fire alarm activates.

They should not be obstructed. Fire exits are vital as a means of escape in the event of a fire. They should be clearly marked, must be unlocked when anyone is in the building, and should not be obstructed on the inside or the outside.

Fire alarm control panels

These are the warning and controlling units within a fire alarm system. Once a possible fire emergency is detected within the building or somewhere on the site, usually as the result of a signal from a smoke or heat detector, the control panel alerts those monitoring it via various lights and audible alarms.

Module 1: Principles of working in the private security industry

Chapter 5: Fire procedures in the workplace

Risk assessments will prescribe the site's own specific procedures for the action to be taken in the event of a fire.

Typical actions would include:

- raising the alarm - yelling fire to warn others
- operating the nearest manual call point (if fitted)



- calling the fire service (999)
- evacuating the area
- restricting access and isolating the fire
- reporting to the assembly point

By understanding the layout of the control panel, security operatives can work out what type of an emergency it is, exactly where it is occurring and over what extent of an area.

A decision can then be made as to what appropriate action to take, be it to inform a supervisor and then search the area concerned, or to call the fire brigade immediately, and provide information about the incident itself and any secondary dangers there might be.

Some of the more sophisticated systems actually call the fire brigade, sound the fire alarm, unlock doors, cut off electricity and set off sprinkler systems automatically.

If you are required to monitor a fire alarm control system as part of your role as a security operative, then you need to properly understand how it works and what actions you personally need to take in an emergency.

Fire evacuation procedures

One of the most important roles for security operatives in the event of a fire will be ensuring that the site is evacuated quickly and safely.

Hopefully, both staff and visitors/customers will know to leave the building when they hear the fire alarm sounding. As a security operative, you must be available to encourage people to leave via the safest exit, and to assist anyone who does not seem to know what to do. Particular care needs to be taken to look after any vulnerable people like children, the elderly or those with physical or mental difficulties. It is also important to try to avoid causing unnecessary panic.

Security operatives need to take control of fire incidents in an assertive but calm manner. You need to show decisiveness, leadership and use clear, effective communication skills so that others understand how serious the situation is.

Security operatives also need to know where the fire assembly points are and what needs to be done once the building or site has been evacuated.

Evacuation procedures need to be practised.



- only attempting to fight fire if it is safe to do so and you have been trained



Remember the 5 P's:

P PLANNING and

P PREPARATION

P PREVENTS

P POOR

P PERFORMANCE

As a security operative, if you act promptly and correctly in times of emergency, you can help save time in the evacuation, keep yourself and others safe, assist the emergency services, prevent injuries and save lives.

Chapter 5: Fire procedures in the workplace

Fire wardens/marshals

Fire wardens (sometimes called fire marshals) are members of staff that are nominated to take responsibility for a particular area with regards to fire safety. The numbers of nominated wardens/marshals will vary depending on the size of the site and the numbers of people involved.

Under the Regulatory Reform (Fire Safety) Order of 2005, (*Fire (Scotland) Act 2005*) they are there to assist the designated person responsible for fire safety generally.

The actions to be taken by fire wardens/marshals in the event of a fire are detailed in the evacuation plan. Those duties will usually include:

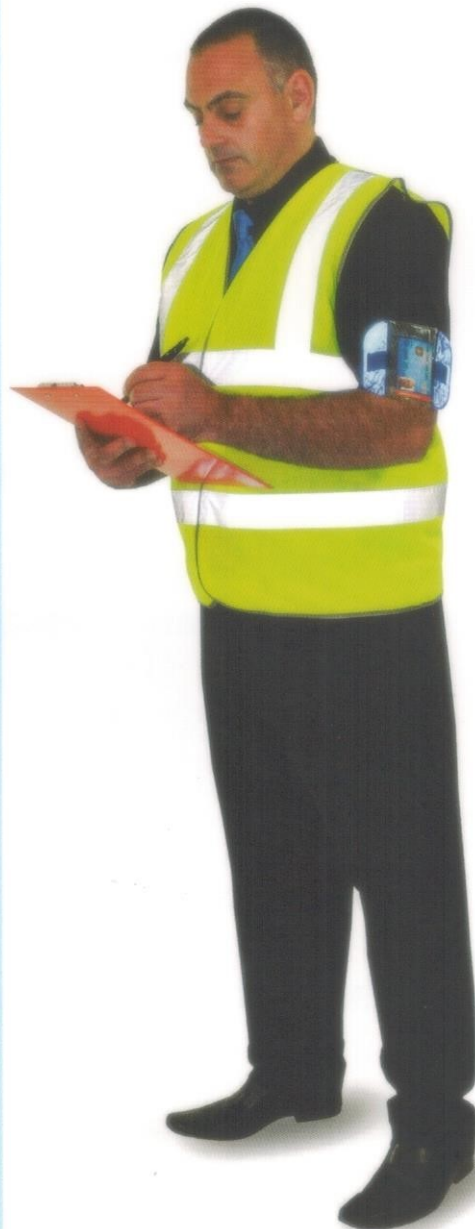
- sounding the alarm/calling the fire service
- checking the allocated area to ensure that everybody has left
- taking control of the evacuation and ensuring that anybody with evacuation difficulties is aided
- proceeding to the assembly area and reporting to the fire officer in charge

The following list, although not exhaustive, details some of the specific roles usually given to fire wardens/marshals:

- assisting with fire risk assessments
- checking that all exit doors and escape routes are unlocked and unobstructed



- ensuring that all fire extinguishers are in the correct position with seals in place
- checking that all safety signs are clearly visible and in the correct place.
- making sure that all alarm call points are unobstructed and working correctly
- checking that all fire doors are closed and functioning properly
- ensuring that corridors and walkways are kept clear
- ensuring that assembly points are clearly marked and easily accessible
- reporting any equipment faults



Taking or assisting with the roll call.

Key tasks



1 State the **THREE** elements needed for a fire to start and survive.

- 1** _____
- 2** _____
- 3** _____

2 List **FOUR** tasks a fire warden/marshal may be required to carry out.

- 1** _____
- 2** _____
- 3** _____
- 4** _____

3 List **FOUR** classes of fire and their meaning.

- 1** _____
- 2** _____
- 3** _____
- 4** _____

Module 1: Principles of working in the private security industry

Chapter 11: Good practice for post incident management

Accessing help and support

Because of their varying degrees of experience and exposure to conflict, people cope with assaults and incidents in different ways.

Incidents where you are abused, threatened or even assaulted in the workplace can have various different impacts on everyone and so you need to be aware of what is available out there to help you if you need assistance or support following a traumatic incident.

It is important, therefore, that businesses and organisations are able to help staff after an incident of workplace violence, particularly in relation to:

- providing immediate and ongoing support
- helping all members of staff to learn from the incident
- updating policies and procedures to improve safety
- sharing good practice

Responses to incidents

Typical symptoms are how the brain and body react to abnormal situations or incidents. The severity of the symptoms will usually depend on the severity of the incident, although something that might not affect you could well affect one of your colleagues and vice versa.

Certainly, in the time directly following an incident, anyone could start to feel shock, anger, embarrassment and disbelief that this has actually happened to them at all.

Typical effects

Anyone could show any or even all of the following short-term or long-term symptoms following exposure to workplace violence:

- sickness
- insomnia
- behavioural changes
- becoming withdrawn
- anxiety
- intolerance
- hypersensitivity
- fear
- depression
- loss of confidence
- stress
- post-traumatic stress disorder (PTSD)

Post-incident support

It is vital that if a member of staff starts to show any signs that they may be suffering from any of these symptoms, support must be given immediately to reduce the changes of long term effects. Support can be provided by:

- colleagues
- management
- counsellors
- helplines (such as the Samaritans)
- citizens advice
- trade unions
- trade publications such as victim support: (www.victimsupport.org.uk/)
- the internet

Professional medical help may be even required for serious problems.



Module 1: Principles of working in the private security industry

Chapter 11: Good practice for post incident management

Reflecting on and learning from conflict

Dealing with people, particularly within the private security industry, is a large ongoing learning curve. You never stop learning, and there is always room for improvement in everything you do. This is especially true when it comes to how you deal with conflict, anger, aggression and violence.



There are 6 basic steps to take following an incident.

1 STEP 1 - Reflect on what happened

Consider: *What happened?*
Why did it happen?

What went wrong?
What could we have done better?

2 STEP 2 - Recognise trends and any poor practice

Consider: *Does this problem occur regularly?*
At any particular place or time?

Can we reduce or stop these types of incidents?
Is there something we are doing wrong?

3 STEP 3 - Share good practice

Consider: *Did we do something well?*
Does everyone know how to do it?

Is extra training required?
Does it need to be a policy?

4 STEP 4 - Learn from what happened

Consider: *How do we make sure this doesn't happen again?*
Can we improve something for next time?

5 STEP 5 - Update policies, practices and procedures

Consider: *Are our policies, practices and procedures up to date?*
Can anything be added or improved?

6 STEP 6 - Monitor progress

Consider: *How can we record future incidents better?*
How can we monitor the effectiveness of any changes made?

When and how do we re-evaluate our future performance?

The proper debriefing of these types of incidents can help you to improve how you deal with similar problems in the future. Organisations can use data that has been collected for licensing hearings and they may even be able to reduce the

chances of them happening in the first place, or even stop them from happening at all. And if they do occur, you should be able to provide an agreed, common positive response each time, automatically improving your own safety, as well as the

Module 1: Principles of working in the private security industry

Chapter 11: Good practice for post incident management

safety of customers, colleagues, other members of staff and the public. All members of the security team, particularly those involved in the original incident, should take part in this process so that they can help to make the changes required to deal with future conflict situations more effectively.

Improving practice

Like all industries, the security industry needs to continue to evolve and progress. As a security operative you have the responsibility to ensure that you continually contribute to improving practices within the industry.

Improved practices help to:

- promote a professional service
- increase safety for staff
- promote teamwork
- increase safety for customers
- identifies procedures or methods to better deal with situations effectively



Key tasks



1 Explain where post-incident support or resources can be found.

A large rectangular box with a light blue border, containing horizontal dashed lines for writing.

2 Explain why it is important to access support following an incident.

A large rectangular box with a light blue border, containing horizontal dashed lines for writing.

Key tasks



3 Identify FIVE benefits of reflecting on an incident.

1	
2	
3	
4	
5	