



PSA TRAINING REQUIREMENTS

Security Guard (Monitoring Centre)
(PSA 70:2018)

Training Requirements For The Licensing Of
Monitoring Centre Employees

August 2018

Contents

Forward	2
A.1 Describe the private security industry.....	3
A.2 Explain the role of government and state bodies in private security	6
A.3 Explain the term security in the context of private security	11
A.4 Describe the role and duties of the Monitoring Centre Controller	13
A.5 Outline the principles of crime prevention.....	24
A.6 Describe the structure and operation of a typical security monitoring company	26
A.7 Outline the principles and benefits of quality management systems	32
A.8 Describe the range and application of security hardware products	36
A.9 Outline the main provisions of the relevant standards applicable to licensed Monitoring Centres	39
B.1 Outline the relevant aspects of Irish Law	47
B.2 Outline the relevant aspects of Irish health & safety law and environmental law...50	
B.3 Outline the relevant aspects of Irish equality law.....	69
B.4 Explain private security industry regulations and legislation.....	74
B.5 Outline responsibilities and obligations under Irish Data Protection legislation	78
C.1 Outline the role of a monitoring centre	88
C.2 Outline the general procedures in a monitoring centre.....	91
C.3 CTV Systems and Operating Procedures	94
C.4 Alarm Systems and Operating Procedures	98
C.5 How to deal with incidents in the context of monitoring centre employees.....	104
C.6 Outline the range of documentation relevant to monitoring centres	107
C.7 Explain the range of on-site safety and fire equipment	111
D.1 Outline the constituent elements and contributing factors of an emergency.....	119
D.2 State the procedures for immediate action on finding a range of emergencies. .126	
D.3 Outline, basic first aid principles and procedures for response to an injured person	132
D.4 Outline the procedures for emergency evacuation of people.....	134
E.1 Outline the principles of effective communications and customer service.	139
E.2 Describe the methods of effective verbal communications	146
E.3 Outline how to interpret written documents and communicate effectively in writing	152
E.4 Explain the importance of observation skills in the performance of duties	155
E.5 Explain how to compile reports for a range of incidents	160
E.6 Outline the range and uses of communications equipment.....	168
E.7 Explain the importance of interpersonal skills in dealing with people.....	173
E.8 Explain the benefits of teamwork.....	175

Forward

The Government of Ireland through the Private Security Services Act, 2004, established the Private Security Authority (PSA) as the national regulatory and licensing body for the private security industry. Amongst the functions of the PSA are:

- The controlling and supervising of persons providing security services and maintaining and improving standards in the provision of those services.
- Specifying standards to be observed in the provision of security services.
- Specifying qualifications or requirements, including requirements as to training, for the granting of licences.

This document sets out the requirements, which apply, to training of employees in the Security Guarding (Alarm Monitoring) or Security Guarding (CCTV Monitoring) sectors. Employees licensed by the PSA and those seeking a licence from the PSA must comply with this requirements document. The training requirements of this document must be provided through PSA licensed contractors in the Security Guarding (Alarm Monitoring) or Security Guarding (CCTV Monitoring) sectors.

By applying for and holding a licence, employees agree to the sharing of information relating to this document and the contents herein between the PSA and their employer. Where an employee fails to comply with the requirements of this document, the employer is obliged to notify the PSA.

Only the most recent edition of the Requirements Document specified by the PSA shall apply for licensing purposes. To ascertain the edition applicable visit the PSA website, www.psa.gov.ie.

A.1 Describe the private security industry

Learning outcomes are designed to enable candidates understand the private security industry, its role and its sectors and range of services. By the end of this section you should be able to:

- Describe how private security responds to public needs and describe its benefits
- Explain what is meant by private security and outline its role in society
- List the sectors within the private security industry and the services they provide

Response to Public Needs

All people in a society have a right to protect themselves, their family and their property. Their use of private security satisfies that need and gives the security company client influence over the services provided which they do not have over statutory agencies. The substantial role therefore of private security in society is loss prevention. A critical feature of this is the prevention of crimes against property and safeguarding people.

Private security works closely with statutory agencies as there is no real crossover or competition. They complement each other and generally work together very well. In the vast majority of societies state services do not have the resources to address prevention as a priority.

Private security fills this need as it incorporates organisations or individuals privately employed or contracted to carry out security duties or services and provide equipment. This can include people such as security staff. Statutory agencies do not provide equipment to members of the public. Organisations and individuals must purchase equipment such as CCTV, intruder alarm system or a safe. These are all available from private security companies.

However, security within the context of private security, while it does include crime prevention, is described as loss prevention giving a greater coverage.

Private security personnel do not investigate, convict and sentence criminals. They do deal with crime prevention and loss reduction principles. Once a crime has been committed private security are responsible for handing those suspected of the crime over to State police.

Role of Private Security

The main function of the private security industry is loss prevention with all other elements being handled by the State. Crime prevention in the context of the private security industry is a critical part of its overall role in loss prevention generally. Crimes such as theft from a house, shop or factory are examples, and while these acts can have very serious consequences for individuals, they are not the highest priority for a police force. These agencies tend substantially to respond or react to incidents, with limited resources being applied to practical prevention measures. Prevention is left to individual members of the public such as householders and the business community by use of private security. The role of private security in society is to respond to this need.

Sectors and Services Summary

The private security industry encompasses a wide range of sectors and services. To more clearly define the industry and to assist with clarifying the duties and responsibilities of individuals working within the industry it is best to break the industry down into sectors and services.

The range of services and products generally classed under the headings of loss prevention and security is vast, with up to one hundred loosely linked to the broader industry. The main services typically provided within the private security industry can be broken down into four main sectors:

- Guarding Security Services Sector
- Technology Sector
- Hardware Sector
- Specialist Sector

The following are examples of the services and products available within these sectors.

Guarding Security Services

Examples of the main services provided within this sector are:

- Static guard (Retail outlets, Industrial, Commercial etc.)
- Door supervisor (Licensed premises, Bars, Nightclubs etc.)
- Event security (Concerts, Sporting Events, Parades etc.)
- Mobile patrols, Key holding / emergency response
- Close Protection/Bodyguards
- Alarm/CCTV Monitoring centres
- Cash in transit, cash and valuables handling

Technology

Examples of the main services provided within this sector are:

- Intruder alarms
- Access control
- CCTV
- Security lighting
- Installation of fire detection systems
- Safety and emergency systems
- Fogging systems

Hardware Sector

Examples of the main services provided within this sector are:

- Locks and locking devices
- Safes and strong rooms
- Fencing and gates
- Security seals, tags and marking systems
- Glass, plastics and laminates for security and safety
- Crowd and traffic control barriers

Specialist Sector

Examples of the main services provided within this sector are:

- Training and Supply of Guard dogs
- Security consultants
- Staff and Management Training
- Fire suppression systems
- Supply and maintenance of fire extinguishers
- Private investigators
- Covert security
- Computer and information security
- Identification card systems
- Equipment suppliers e.g. radio, uniforms, proof of service systems

Evolving technology particularly digital electronics and computerisation, has brought about a merging of various products and a change in the way some products work. Locks are no longer exclusively manual and keys may be obsolete in some cases, having been replaced by an electronic card.

A.2 Explain the role of government and state bodies in private security

Learning outcomes are designed to enable candidates understand private security industry regulations and legislation, including the role of the industry regulator and the impact of regulations on the public, the industry and end users. The learning outcomes in this section are as follows:

- Explain the involvement of government in the private security industry
- State who the private security regulator is in the Republic of Ireland and list its main statutory functions
- Explain the importance and benefits of regulation and licensing
- Outline the difference between security provided by the State and security provided by the private security industry
- Outline the enforcement powers of the State's private security regulator

Government Involvement

The role of government generally is to establish laws in the public interest. The involvement of government in private security is through the establishment of an industry regulator. Through the Private Security Services Act, 2004, the Government of Ireland established the Private Security Authority.

The Private Security Authority is the national regulatory and licensing body for the private security industry in Ireland.

Act Preamble

"An Act to provide for the establishment of a body, to be known as the Private Security Authority, to control and supervise individuals and firms providing private security services and to investigate and adjudicate on any complaints against them; for the establishment of a body, to be known as the Private Security Appeal Board, to hear and determine appeals against decisions of that Authority; and related matters". (4th May, 2004)

For clarity Legislation means laws made by the legislature (Parliament / Oireachtas). Within most pieces of legislation passed by the Oireachtas there is a section giving the responsible Minister the power to add regulations or bye-laws by the use Statutory Instruments (SI) giving individual Ministers the power to create laws within the confines of the primary Act as approved by the Oireachtas. It can be described as a delegation of powers (within the confines of the relevant Act) to reduce the workload.

Private Security Services Act

The Government of Ireland through the Private Security Services Act, 2004, established the Private Security Authority (PSA), which took up office in that year.

The Act established the Private Security Authority (PSA) and sets out the functions of the Authority as follows:

- Grant and renew licences
- Issue identity cards to licensees
- Where appropriate, suspend or revoke licences
- Establish and maintain a register of licensees
- Specify standards to be observed in the provision of security services by licensees or particular categories of licensees
- Specify qualifications or any other requirements (including requirements as to training) for the grant of licences
- Undertake or commission, or collaborate or assist in, research projects and activities relating to the provision of security services, including the compilation of statistical information and other records necessary for the proper planning, development and provision of those services
- Investigate any security service being provided by any person
- Establish and administer a system of investigation and adjudication of complaints against licensees
- Monitor the provision of private security services generally
- Liaise with licensees with a view to keeping itself informed of any matters requiring its attention
- Advise the Minister on any matters relating to its functions
- Keep the Minister informed of developments in relation to the provision of security services by licensees or particular categories of licensees and assist him or her in coordinating and developing policy in that regard

A number of other State bodies play a role in assisting the Authority carry out its functions. In particular An Garda Síochána carry out vetting on behalf of the authority and the national education awarding body Quality and Qualifications Ireland certify some entry level mandatory courses for licensing. The PSA have also signed memorandum of understanding with other State bodies such as the Revenue Commissioners, the Department of Social Protection and the Workplace Relations Commission.

Purpose of Licensing

Legislators when considering drafting and enacting laws of this nature consider the primary purpose to be “in the public interest”.

The PSA on establishment expanded on this by stating:

“Our purpose is to instil customer and public confidence in this multi-stranded, multi-faceted business with the introduction, control and management of a comprehensive, standard driven, licensing system for all individuals and companies involved in the industry and to do so in a manner that is sensitive to the needs of the market”

It is the aim of the Authority to use the statutory regulation and enforcement powers provided to it to introduce positive, fundamental change to the industry.

Section 2 of Private Security Services Act sets out the activities which are licensable by the PSA, these are:

- Door Supervisor
- Installer of Security Equipment
- Locksmith
- Private Investigator
- Provider of Protected forms of Transport
- Security Consultants
- Security Guard
- Supplier and Installer of Safes

Definitions of what is licensable for each sector are prescribed by regulations signed by the Minister for Justice and Equality.

Importance and Benefits of Regulation and Licensing

The original legislation and subsequent regulations are designed to ensure that companies and individuals providing services in the private security industry operate to standards and comply with legislation generally.

A feature of this is the setting of mandatory standards. The Authority has prescribed certified quality management system standards for contractors and accredited training standards for individuals. A criminal record check is also carried out before a licence is issued and as part of this process applicants are assessed against the Authority's Fit and Proper Guidelines.

The impact of the licensing regime has brought change to the industry which previously adopted a voluntary system where some companies operated to a standard and some training took place. All licensees must now operate to same standards as a minimum. Audits by approved certification bodies and visits by PSA inspectors help ensure that the requirements are maintained.

The public benefit by having access to a regulatory authority. The regulator can investigate and adjudicate on any complaints made, for example, on the performance or behaviour of individual licence holders. Security officers must display identification while on duty, adding confidence to the public and end users.

End users or clients of the industry also have access and may complain or comment on the nature or quality of the service provided to them.

End users or clients of the industry must use PSA Licensed Contractors and or licensed individuals to provide security services to them. It is an offence under the Private Security Services Act to use unlicensed contractors or individuals.

The PSA publish a register of all licence holders and provide information of suspensions and revocations. This information is beneficial to end users and the public.

The licensing regime has more clearly defined the known industry and has created barriers to undesirables who may have previously entered the industry unchallenged.

Fit and Proper Guidelines

The PSA have published suitability criteria guidelines on “fit and proper person” for both contractors and individuals applying for a licence. The following are the headings under which the assessment will be applied:

- Criminal convictions and cases pending a court hearing
- Person subject to an investigation by An Garda Síochána, Health Service Executive, Criminal Assets Bureau or any Government Body or Agency with the authority to carry out investigations
- Person subject to an investigation by a relevant authority in another Member State of the European Union in circumstances where the person seeks to provide a security service in the State in accordance with Part 7 of the Act
- compliance with the various companies Acts and any other statutory provisions of being a body corporate
- Compliance with Revenue and Social Welfare provisions
- Compliance with the Joint Labour Committee Employment Regulation legislation
- Compliance with the Private Security Services Acts, licensing regulations and any standards or qualifications relating to licensing
- Any previous Private Security Services Licence held, applications made for a licence or investigations conducted by the Authority’s Enforcement Division
- Any actions, suspensions or revocations issued by the Authority
- Compliance with the provisions of any regulatory body or subject to a current investigation by such a body
- Any matter where in the view of the Authority the issuing of a licence would pose a risk to the safety and welfare of the public
- Any other such matter which the Authority deems relevant to the issuance of a licence

The above is a summary; the complete document extends to twenty pages and is available from the PSA website.

State Security Comparison

The overall responsibility for security within a State usually rests with the Government of the day. There are a number of differences between State and private security, the main difference being the concept of loss prevention. State criminal justice systems generally deal with crime prevention, investigations, and sentencing of individuals who are found guilty in a court of law of committing a crime, which is punished by the State. State security has a much broader context and can be described as national security, involving for example, military forces and border security and intelligence services.

Crime is a natural feature in all societies and dedicated statutory agencies are established to enforce these laws and norms. This includes national police forces, a courts system and a prisons system. These can be viewed as deterrents put in place by society. These statutory agencies are responsible for enforcing all criminal laws, from murder and rape to minor traffic offences.

Enforcement Powers of the PSA

The Private Security Authority as a statutory body has responsibility for licensing and regulating the private security industry. Legislation bestows extensive powers to the Authority, including, but not limited to investigating security services being provided by any person, investigating complaints and taking action.

Warranted¹ PSA Inspectors have substantial powers. They may enter, inspect, examine and search anywhere the inspector has reasonable cause to believe that a security service is being provided. This includes unannounced visits to premises to ensure the security staff members are licensed and are wearing and displaying their PSA licence in the prescribed manner. Inspectors are entitled to inspect licences during these visits.

PSA inspectors also carry out audits on licensed contractors to confirm compliance with standards and licensing requirements. These audits are normally arranged by appointment and take place at the contractor's place of business. The inspector may review documentation; such as service contracts, personnel files etc. and can take away copies of documents related to the provision of security services if required.

A report will be provided to the contractor and where required non-compliances must be resolved within the timeframe determined by the inspector.

A.3 Explain the term security in the context of private security

Learning outcomes are designed to enable candidates understand the meaning of security and the terms prevention, protection and detection. At the end of this section you should be able to:

- Explain the term security
- Explain the principles of prevention, protection and detection
- Provide examples of prevention, protection and detection

Security

A brief description of security is the state of being free from danger or threat. This state of being free from danger or threat is considered a personal need of people within society, and in some jurisdictions a constitutional right.

Society can be defined as a group of people who live together in an organised way. A critical feature of societies are laws and accepted norms of behaviour.

The term "Security" has to be applied in context. For example, it can be "State Security", "National Security", "Job Security" or "Social Security".

A Definition of Security

There is no single agreed definition of the term security; various jurisdictions seek to capture the one that best suits their interpretation. In this context the Private Security Authority have published the following:

"Security is the safeguarding of life, the taking of measures to prevent unauthorised entry or attempted unauthorised entry into premises, the provision of a secure environment where the physical person or persons is/are protected from criminal action or the effects of criminal action, or the protection of property of all kinds from loss through accident, theft, fraud, fire, explosion, damage or waste".

For the purpose of this document, the context in which security is discussed is that of the "private security industry" as opposed to a police force or state security context.

Prevention

The common definition of prevention means to stop something happening. In the context of security these are any measures put in place to prevent loss or minimise the amount lost, through for example theft, accident, weather or waste.

Prevention is the overall or big picture and involves, for example conducting risk assessments, removing the risk or threat altogether, having policy and procedures in place, encouraging awareness and training staff, putting in place physical or other protective measures.

Protection

The common definition of protection means measures that keep a person or thing from being harmed or lost, to defend or guard against something, the state of being protected. In the context of security protection means the protective measures utilised to address the risks identified.

Protection becomes relevant when the risks associated with safeguarding goods or people cannot be eliminated or reduced to an acceptable level. As discussed in the prevention section, removing the risk or threat is the first step; protective measures are then considered where these cannot be eliminated.

Distinction can be drawn between protective measures which offer resistance to attack and those which deter, delay or detect, which are covered further on.

Practical examples of physical protective measures which offer resistance can include:

- Quality walls, fencing and gates
- Solid doors
- High security locks
- Safe or security cabinet

Detection

The common definition of detection means to discover or uncover something, being noticed. In the context of security detection means an alert or warning of a security breach. To be effective detection requires follow up action.

Examples of detection can include:

- A security officer on patrol discovers a break-in
- An intruder alarm activates
- A controller monitoring a CCTV system reports unusual activity

A.4 Describe the role and duties of the Monitoring Centre Controller

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- State the functions of an Monitoring Centre Operator
- Explain the general importance of confidentiality in private security
- State the importance of absolute confidentiality within an Monitoring Centre
- State the positive characteristics and skills required of a monitoring centre employee
- What skills are required by Monitoring Centre personnel
- Outline the importance of personal appearance, customer care, communications, attitude and behaviour in the performance of duties
- Outline the importance of customer care, communication skills, disposition, an ability to remain calm and coherent in a crisis for Monitoring Centre personnel
- Explain the importance of training in the performance of Monitoring Centre duties
- List the types of equipment and documentation monitoring centre employees may use
- Explain the duties and responsibilities of each member of the CCTV and ALARM monitoring team
- Identify appropriate reporting procedures and explain the importance, in both directions of the reporting chain, of the conveyance of accurate and timely information

What is a Monitoring Centre

Monitoring Centre or Alarm Receiving Centres are dedicated protected centres from which controllers (Monitoring Centre operational staff or operators) monitor signals received from a client security system, such as an alarm system or CCTV system. All Monitoring Centre's are permanently staffed, providing a 24 hour, seven day service. In PSA documentation, Monitoring Centres are referred to as Monitoring Centres.

Control Room Operators or "Controllers" respond as appropriate informing emergency services and other designated contacts as per established, agreed protocols. A critical feature of the work is the analysing and filtering of information received to reduce interventions in response to "false activations". This work substantially assists the emergency services by having processes in place to verify signals received, reducing the burden on the emergency services.

Verification technology on the protected premises is a contributor to this also.

These centres were historically known as Alarm Monitoring Centres or Central Stations and also use the acronym Monitoring Centre (Monitoring and Alarm Receiving Centres).

Domestic and commercial monitoring services available include:

- Intruder Alarm
- Panic Alarm
- Fire Alarm
- Remote CCTV
- Remote Access Control
- Medical Alert
- Man Down
- Person and Vehicle Tracking

There are additional or ancillary services such as command and control support for security companies also provided.

Under Private Security Services legislation CCTV Monitoring Centre and Alarm Monitoring Centre contractors must be licensed by the Private Security Authority.

Defining a Monitoring Centre Operator

The PSA Standard for the Licensing of CCTV Monitoring Centre and Alarm Monitoring Centre defines operators as:

CCTV Monitoring - a person who as a security guard monitors security equipment which consists of a continuously manned remote centre to which information concerning the status of one or more CCTV systems is reported.

Alarm Monitoring - a person who as a security guard monitors security equipment which consists of a continuously manned remote centre to which information concerning the status of one or more intruder alarm systems is reported.

State the functions of an Monitoring Centre Operator

The nature of the services available can be very diverse depending upon the particular contractor, some offer an extensive range while others may specialise in a certain field. The list below looks at the “typical” contractor as one providing CCTV and Alarm Monitoring services.

In this context the primary functions of controllers in a Monitoring Centre would include:

- Responding to alarm signals
- Responding to CCTV data received
- Handling incoming and outgoing telephone calls
- Handling two-way radio traffic
- Handling text and e-mail traffic
- Supporting clients and installers
- Maintaining accurate records and reports
- Entering client data accurately

- Retrieving information
- Safeguarding evidence
- Passing on information to emergency services and emergency contacts
- Keeping management informed generally
- Testing equipment, logging and reporting any deficiencies and faults
- Interacting efficiently and professionally with clients
- Updating records
- Implementing centre access control protocols
- Maintaining security of information, including passwords and code words
- Playing an active and positive role in workplace safety health and welfare
- Implementing emergency action, contingency and disaster recovery plans
- Taking part in training, refresher, upskilling, drills and rehearsals.

Each organisation must clearly identify the functions, role and responsibilities of each relevant member of staff. This will help initially with defining the type of person suitable for employment and will also identify the core tasks, leading to relevant training and familiarisation. A procedures manual is necessary to document all requirements. Terms and conditions of employment should include an undertaking to follow all reasonable instructions and procedures.

The controller works in a secure environment, interpreting and responding to PA, Intruder, fire alarms and CCTV alerts. The role is substantially computer and telephone based. It can involve dealing with people who sometimes may be distressed offering assurance and clarity.

Explain the general importance of confidentiality in private security

Trust and integrity are expected of all those engaged in the security industry, honesty and truthfulness are features of this. Besides legal obligations to the client and the requirements under data protection legislation, inherent critical characteristics of discretion and the ability to exercise good judgement in the use of information is essential in security generally.

State the importance of absolute confidentiality within a Monitoring Centre

Those employed in a Monitoring Centre are put in positions where there is access to a substantial body of information which can be economically sensitive, personal and private. This information is entrusted to management who then allow operators access under certain conditions, such as dealing with alerts. The information is essential to the functions of the centre and must never be misused or abused as this can impact on the security of the client.

Data protection is covered in-depth in **Section B.5** and the general requirements under the PSA fit and proper person guidelines and licensing requirements are also relevant.

Positive characteristics and skills required of a monitoring centre employee

Characteristics

Characteristics are qualities or distinguishing features as opposed to skills which are linked to abilities. Characteristics of controllers therefore are those beneficial qualities which are brought to the Monitoring Centre environment.

Characteristics would include being:

- Adaptable
- Assertive
- Competent
- Confident
- Cooperative
- Disciplined
- Diplomatic
- Decisive
- Dependable
- Diligent
- Discreet
- Honest
- Loyal
- Methodical
- Observant
- Positive
- Practical
- Reliable
- Resourceful
- Responsible

Skills required by Monitoring Centre personnel

A skill is defined as ability, talent or proficiency. Skill is the ability to do something well. Skills are acquired typically through training or experience.

Unique skills required in an Monitoring Centre are linked to the tasks to be performed and the equipment to be used. These are based on an individual needs analysis as they may vary depending upon the nature of the work to be carried out and the type of equipment used in different centres. Even when the nature of the business is similar, organisations can have differing rules and protocols and equipment design can also vary from centre to centre.

General Skills

General skills which are beneficial to the Monitoring Centre environment include:

- Being PC literate
- Having an understanding of the World Wide Web and the Internet
- Being proficient in e-mail use
- Typing skills
- Communications including reading, writing and English language skills
- Supporting Knowledge:
 - To be most effective, skills will require supporting knowledge, this will include:
 - Organisation structure
 - Organisation protocols
 - Criminal Law
 - Civil Law
 - Licensing and the Private Security authority
 - Data Protection
 - Knowledge of security and loss prevention in particular

Within the Monitoring Centre environment communication skills may be considered the most relevant. While the ability to read and write is important the modern Monitoring Centre environment requires computer keyboard skills for example. Those with responsibility for CCTV monitoring will need observation skills and decision making abilities. In all situations, particularly emergencies, the ability to speak clearly is a vital asset.

Teamwork is also a feature of communications. This is the ability to interact well with others, bringing different characteristics and skills together in a coordinated way, to achieve common goals.

The importance of personal appearance, customer care, communications, attitude and behaviour in the performance of duties

Personal Appearance

While the quality of work may be the most important quality in a workplace, personal appearance at work can play an important part in gaining the respect of work colleagues and managers. Being appropriately dressed and groomed increases self-confidence and creates a good impression with other people.

Customer Care

Each connection to an Monitoring Centre represents a customer. It is important to provide excellent customer care to potential, new and existing customers. Each Monitoring Centre will have their own customer care policy and it is important that all customers, no matter how difficult, are treated with the same respect and offered the best service.

Communications

Controllers will need to demonstrate good communication skills, including listening, speaking and writing. They will be called upon to answer phones, call emergency services and contact persons, provide reports to supervisors and managers and give statements to An Garda Síochána.

Attitude and Behaviour

A positive attitude and good behaviour are essential qualities of a controller. Monitoring Centre's will have a code of conduct which will set out which behaviours are acceptable and which are not. Displaying the correct attitude and behaviour is evidence of a high level of professionalism and pride in ones work.

The importance of training in the performance of Monitoring Centre duties

The purpose of training is to help people acquire skills and knowledge or the process of learning the skills needed for a particular job. The primary functions of controllers mentioned earlier, the skills and knowledge required to carry out those functions can be substantial. The uniqueness of the role, responsibilities and nature of the Monitoring Centre environment means that training is a very important feature. For example, use of CCTV receiving equipment requires physical familiarisation and practice and knowledge of data protection legislation as well as an understanding as to why it is being done, which is knowledge of security and loss prevention.

Organisation familiarisation and centre induction is the first step in internal training. This covers an understanding of the organisation, its people, equipment, clients and business as well as knowledge of the physical environment.

Organisation familiarisation and training are not once off activities all controllers should actively participate in ongoing refresher training and upskilling to remain up to date with changes in procedures, legislation and equipment.

Controllers should always endeavour to keep themselves informed of developments within their sector and the industry generally.

When the appropriate skills and knowledge have been acquired, controllers may be deemed competent. Experience is then the application of skills and knowledge applied over time.

Types of equipment and documentation monitoring centre employees may use

Each Monitoring Centre will operate differently and may classify or describe and use equipment and documentation differently. The following list therefore is general or typical.

Equipment

Monitoring Centre equipment would include primarily:

- Operator PC (Alarm and CCTV monitoring software)
- Telephone equipment
- Access control system
- Multi-function printer/scanner/copier
- Emergency and first aid equipment
- Safety equipment
- Two way radio

Documentation

The range of documentation used in a typical Monitoring Centre includes:

- Work Instructions:
 - Access to Monitoring Centre procedures
 - Control of CCTV images
 - Counter duress
 - Evacuation
 - CCTV system commissioning
 - Telephone call handling
 - Approved supplier list
 - Fault reporting
- Monitoring Centre Contingency plan
- Safety Statement
- VDU policy and procedures
- Manufacturer technical manuals
- Alarm monitoring policy
- Garda policy on monitored intruder alarms
- Monitoring Centre quality manual
- Monitoring Centre approved staff list
- Data protection policy and procedures
- Employee handbook
- Visitor authorisation log
- Manual or electronic report book or daily occurrence book / telephone log may also feature.

Forms

The range of forms (soft or hard copy) used in a typical Monitoring Centre can include:

- Shift handover
- Garda forms (RC1A, RC1B, RC1C)
- New customer record
- Customer details change
- Verbal instructions
- Customer complaint registration
- Visitor non-disclosure agreement

Duties and responsibilities of each member of the CCTV and ALARM monitoring team

The range of duties can vary from Monitoring Centre to Monitoring Centre and it is not uncommon for both CCTV and Alarm monitoring controllers to be trained in both areas.

CCTV Duties

CCTV controllers are mainly responsible for operating and maintaining surveillance equipment, watching both live and recorded video surveillance footage, reporting incidents or suspicious behaviour and contacting the authorities when necessary.

Regardless of the type of environment they work in, the role of a CCTV controller is relatively uniform across the board. They are charged with maintaining control centre equipment, watching multiple monitors at once, making note of any unusual occurrences and interacting with the Garda. Typically, CCTV controllers will report to a higher-level member of staff such as a CCTV supervisor or CCTV manager and will be expected to maintain a high level of professionalism, care and integrity at all times.

To do their job effectively, CCTV controllers must have a thorough understanding of the equipment they are working with. They may be tasked with deleting or archiving old footage as needed, organising old footage in an orderly fashion, and switching out memory cards, hard drives or servers.

CCTV controllers do not simply watch a series of monitors (screens) all day. Rather, they must be unwaveringly focused and observant so that whenever they witness something unusual, suspicious or questionable they are able to make a detailed note of it. If a CCTV controller sees something suspicious on one of their monitors, it is up to them to contact the appropriate authorities in a timely manner. In serious situations, for example, CCTV controllers can also save vital Garda time by immediately reporting a suspect's registration plate number, clothing, tattoos or other identifying features.

CCTV controller skills

From an employer perspective, successful CCTV controllers are mindful, alert and scrupulous individuals who are highly dedicated to protecting others. In addition to having a talent for all things technical, they also have the ability to quickly identify patterns and abnormalities. In addition to these general personality traits and abilities, employers are looking for CCTV controllers with the following skills:

Surveillance System Knowledge

Because extensive knowledge of video surveillance systems is crucial to the job of a CCTV controller, many employers require CCTV controllers to have video surveillance certification of some kind

Attention to Detail

CCTV controllers must be able to identify small, seemingly insignificant details that most people would overlook. This ability allows them to keep the area as safe as possible

Ability to Multitask

Even when a CCTV controller receives a telephone call, has to speak to a colleague or any other interaction or distraction, they must always be observing their monitors

Ability to Work Independently

For the most part, CCTV controllers will not be required to interact with very many people. The typical Monitoring Centre will have a small number of staff on duty at any one time. Because of this, it is important that they are able to work and stay alert without constant supervision

Communication Skills

Besides normal customer interactions, CCTV controllers will occasionally have to give statements to the Garda, communicate with emergency services or even give evidence in court. They need to have good written and verbal communication skills

Alarm Monitoring Duties

Alarm monitoring controllers are mainly responsible for monitoring alarms and verifying and responding to intruder alarm signals received by an Monitoring Centre. The interpreting of alarm signals is a key responsibility of controllers.

Regardless of the type of environment they work in, the role of an alarm monitoring controller is relatively uniform across the board. They are charged with maintaining control centre equipment, responding to alarm activations at once and interacting with contact persons and emergency services. Typically, alarm monitoring controllers will act as part of a team and report to a supervisor or member of management. They are expected to maintain a high level of professionalism, care and integrity at all times.

To do their job effectively, alarm monitoring controllers must have a thorough understanding of the equipment they are working with. They may be tasked with completing daily, weekly and monthly tests of equipment, noting the results, and reporting faults.

Appropriate reporting procedures, in both directions of the reporting chain, of the conveyance of accurate and timely information

In a security context a report means an incident report. This means to give a personal account or statement of an event or situation witnessed or observed. A good report provides an accurate, detailed and chronological account of what you seen, heard and done.

An incident reporting process

While procedures may differ from company to company, the following are the essential features:

- Use a quick reference heading e.g. client name or building name
- Insert the date the report is been written or submitted
- Indicate who the report is for e.g. named manager or client contact
- Makes rough notes during an incident or call where possible
- Write / type the report as soon as possible after the incident or event
- Ensure accurate dates of the incident
- Ensure accurate timings of the incident
- Be clear on the details of the incident
- Structure the report chronologically, as events evolve
- Record names of witness or other controllers with supporting information
- Secure any evidence such as video related to the report
- Sign the report
- Maintain confidentiality of report, notes and evidence.

Reporting in the broader sense can mean any transfer of information within the organisation. This means customers, managers, authorities and team members. The nature of the incident will determine how and to whom it is reported.

The reporting chain is linked to the chain of command, typically detailed in an organisation chart. Each controller working in an Monitoring Centre must know to whom they report. A reporting procedure may not be absolutely rigid. While under normal circumstances a controller may report to a named individual on a day to day basis, the process should not be unduly militaristic. It must be possible, in certain

circumstances such as an emergency to “jump” the chain of command or reporting chain and take the information to a higher level directly, as this leads to faster decision making. An unduly militaristic process can stifle thinking and decision making at subordinate levels, this is particularly relevant when controllers may have to make instant decisions in response to alerts received.

Reporting can be done verbally or in writing, in writing can mean e-mail or texting. Urgent or not important matters can be verbal. The priority in all cases is that the information is accurate and truthful. While an informed opinion may be offered undue speculation or guesswork should be avoided.

It is also important that reporting is timely; this gives an opportunity for a more efficient decision or other response and also ensures that the details are more reliable. Rough notes, no matter how brief taken at the time of an incident are useful reporting resources.

Is it very important in the Monitoring Centre environment that there is efficient upwards and downwards communications. When information is passed up the chain acknowledgement and relevant and timely responses back down the chain must also feature. This reduces the risk of controllers feeling isolated and unsupported. It is the responsibility of management to provide clear unambiguous instructions and to manage communications within the Monitoring Centre.

Organisation charts are covered in more detail in **Section A.6**.

A.5 Outline the principles of crime prevention

Learning outcomes are designed to provide candidates with an understanding of crime prevention principles. The learning outcomes of this section are:

- Define the term crime prevention and explain the principles of prevention measures
- Summarise the principles of crime prevention and reduction
- Provide examples of crime prevention measures

Defining Crime Prevention

Crime prevention is a part of overall loss prevention. The most concise and accurate definition of crime prevention is:

“The anticipation, recognition and appraisal of a crime risk and the initiation of action to remove or reduce it”

Crime prevention generally and loss prevention in particular follow the same broad principles, assess the risk and put in place measures to mitigate those risks.

Practical examples of prevention can include:

- Reduce the amount of cash kept in a till
- Keep high value goods away from doors and windows
- Vet staff
- Effective management and control of stock and materials
- Use of the three D's (explained further on)

Crime Prevention Measures

In **Section A.3** we learned that the common definition of prevention is to stop something happening and that in terms of security this involved measures to prevent or minimise loss.

Prevention measures may involve;

- conducting risk assessments
- removing the risk or threat altogether
- having policy and procedures in place to address risk or threat
- encouraging staff awareness and providing staff training
- putting in place physical or other protective measures

The principles of the three D's, Deter, Delay, Detect are explained below:

Deter

To deter is to discourage therefore deterrents within security generally, and loss prevention in particular, are measures put in place to discourage.

The broader definition is to deter by instilling fear or doubt. This is satisfied by the potential offender being aware of the risk of capture and its consequences by the use of Human Resource services or CCTV.

Doubts will also be raised when the potential offender considers the obstacles put in place and matches them against the possible rewards from the act.

Delay

Where measures cannot be applied that deter absolutely or remove completely the risk of loss for example as the result of a break-in or robbery, then physical obstacles must be in place that will offer resistance to attack relative to the value of the potential loss.

These barriers include strong perimeter fencing, doors, locking devices, safes, shutters and grills etc. as well as internal layout and storage of goods to reduce access and ease of egress. Any system that delays will reduce the levels of loss.

Detect

The common definition is to notice or discover the existence or presence of something. The most common forms of detection are by the use of intruder alarms to detect when a door or window has been opened and patrolling by security staff to detect damage to locks, doors, windows perimeter etc.

Detection also includes procedures for stock checks and stock control to detect shortages and highlight risk areas. Covert security systems are also used to detect however, these are not generally installed as deterrents but specific purpose systems to gather information and evidence. Integration or merging of protective and preventative measures also feature.

A.6 Describe the structure and operation of a typical security monitoring company

Learning outcomes are designed to provide candidates with an understanding of companies providing monitoring services. The learning outcomes identified for this section are:

- Provide an example of a company structure
- Explain what an organisation chart is and state typical roles and responsibilities
- Outline management and supervisory functions in a typical security company
- Explain what is meant by company ethos and culture
- Understand and explain company standards and licensing
- Explain what is meant by policy and give examples of types of company policy
- Explain the legal and licensing requirements under which a security company operates

Provide an example of a company structure

There are a number of different types of company structure, depending upon the size and the nature of its business. Companies can range from small with one director to large multinationals whose directors may be based in a foreign country.

Large organisations will have a number of senior directors in charge of aspects of the business such as finance director or marketing director. These could then have managers working within each department.

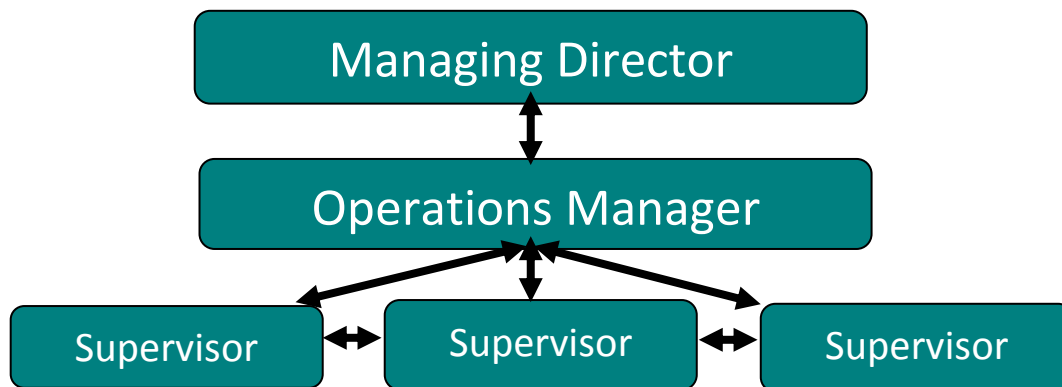
Small companies will typically see one or two directors and a small management team multitasking with each taking on a number of administrative and operational roles. In some instances, the directory may also be the management team.

Sole traders such as a locksmith or consultant can literally mean one person carrying out almost every function.

Organisation chart and typical roles and responsibilities

An organisation chart describes in a diagram the hierarchy of the organisation. A company structure is ideally presented in an organisation chart indicating a clear hierarchy or chain of command. Starting with the most senior or executive level at the top and working downwards, stating positions or job titles within the organisation. Names are not normally stated in an organisation chart as they may change regularly, titles however such as operations manager are less likely to change. Company induction will include an overview of the positions and the people who currently hold the position.

A simple organisation chart would be structured as follows:



The managing director may also be known as the chief executive. He is at the most senior level of management in the organisation. If he is not the owner he will be reporting to a chairman or board of directors.

The operations manager may be also known as a general manager. Supervisors can be broken down as a night supervisor or shift supervisor depending upon the organisation. Team leaders and operational staff will then come under supervisors.

Understanding the company structure is important as all operators should know who to report too and take instructions from; this must be clearly outlined by management. The arrows are very important as they indicate in the sample provided, the direction of communications which are very important in a company. The upward, downward and sideward flow of communications ensures the efficient and effective operation of a company.

Management and supervisory functions in a typical security company

Managing Director

The managing director or chief executive is at the most senior management level in an organisation. He may be supported by a senior management team which could include a finance director, operations director, sales directors and human resources director. Different organisations may use different management titles and those titles can have different connotations from one organisation to another.

This senior management level sets policy and determines the culture and ethos of an organisation. They are responsible for providing direction, leadership and guidance to their employees

The following is a summary of the five generally accepted main functions of senior management.

- Plan
To think ahead and forecast what might happen or what the company might like to happen, then consider how best to deal with the situation or achieve the objective.
Planning can be both in response to the positive such as new developments or the negatives such as market downturn.
- Organise
This means how to use and/or apply the company's resources properly. Organising ensures the right people are placed in the positions most beneficial to the company aims. Other resources such as equipment, machinery, suppliers, buildings, facilities etc. are organised as part of an overall process linked directly to the aims and objectives of the company.
Organising is having everything in place.
- Direct
Delegate and instruct employees in the context of the overall aims and objectives of the organisation. Managers have responsibility for sections, divisions or departments. There is a common purpose within divisions, for example the HR Department or the Finance department. While individual managers or separate departments can work effectively on their own, overall direction or attention to the big picture is a critical senior management function.
- Coordinate
This is the next logical step, which brings together the work and efforts of the various departments or divisions or people. Senior management coordinate the activity of all of those involved in the business and ensure that the ultimate objectives of the organisation as a whole are met.
- Control
All the activities, which take place within an organisation, happen as part of an overall planned purpose. Organisations always have objectives or a particular ethos. This is captured in mission statements and policy documents. A critical management function is to safeguard and maintain the mission and policies of the organisation, this is control.

Managers

Depending on the size of the organisation, there may be further levels of management below senior management. These are commonly known as Middle Managers. Those who come under Middle Managers are commonly known as Junior Management. Junior management can be duty manager, shift manager, assistant manager or supervisor.

The decision-making authority of these managers is governed by the parameters set by senior management. While they may contribute or advise, they do not have the final say on policy or procedures.

Company organisation charts ideally clarify these structures.

Supervisor

The supervisor is the first line or first layer of management, a junior manager responsible for the performance of individuals, a group or team. A supervisor is one given authority by management to direct work, taking responsibility for implementing decisions made by management. This means assigning work and coordinating work by instructing subordinates and ensuring that work directed by management is carried out. The duties and responsibilities of the supervisor are determined by management.

Company ethos and culture

Defining Ethos

An organisations ethos drives its mission statements, objectives and policies. Ethos is described as “the distinguishing character of an organisation”. Each organisation is unique in that its founders or owners look to instil a certain personality. An ethos can also be described as the vision that the organisation wishes to portray.

Defining Culture

Culture is described as “the way we do things around here”. Culture is what happens in reality on a day-to-day basis within an organisation. Culture is what the organisation does or what an organisation really is, as opposed to ethos, which is more a vision such as that captured in a mission statement.

Mission Statements

Some organisations may reflect their ethos and culture in a mission statement. A mission statement may be to provide the best service, to be the biggest or to offer the best value. Mission statements therefore tend to be broad bold statements designed to inform customers or the public of the organisations ethos.

Company standards and licensing

In the context of PSA licensing, standards are the required way of doing things against which a contractor is audited. The PSA as the industry regulator determines under what conditions a company or contractor licence is issued. An essential feature of licensing is compliance with a standard. The standard sets out how the contractor manages its business. These standards are developed in consultation with the relevant sector of the industry as well as approved auditing bodies. An auditing body will visit the contractor's place of business and inspect work practices against the agreed standard. Auditing bodies, when satisfied, provide evidence of compliance by way of a letter or certificate. The organisation provides this evidence to the PSA when applying for a licence. Certificates of compliance and subsequent licenses have expiry dates and require ongoing compliance and continuous inspections.

PSA 33:2014 is the PSA standard specific to the CCTV Monitoring and Intruder Alarm Monitoring sectors. Other sectors of the security industry will have different PSA standards to comply with. PSA 33:2014 references a suite of other standards that monitoring contractors must comply with. These are:

- I.S. EN 50518-1 (Construction Requirements)
- I.S. EN 50518-2 (Technical Requirements)
- I.S. EN 50518-3 (Operational Procedures)
- S.R. 25 (PSA Licensing Standard for Alarm Monitoring)
- S.R. 45 (PSA Licensing Standard for CCTV Monitoring)
- I.S. 228 (Original 1997 Irish Standard for Monitoring Centres)

Examples of types of company policy

Policies can be described as statements of intent within an organisation. Their aim is to influence the actions of the organisation and its employees. They should avoid being vague or unduly general and can provide an insight into the organisations ethos and culture. Policy statements are formal documents which are agreed at senior management level, then signed and dated by management.

Typical examples of policies in a Monitoring Centre environment could include:

- Customer Care
- Data Protection
- Quality Service
- Discrimination
- Internet Use
- Smoking/Substance Abuse

Legal and licensing requirements under which a security company operates

Under the Private Security Services Acts 2004 and 2011, the licensing of companies (contractors) engaged in CCTV Monitoring and Alarm Monitoring is the responsibility of the industry regulator the Private Security Authority (PSA). It is against the law to provide these services in Ireland without a current PSA licence.

Contractors seeking a licence from the PSA must comply with the PSA licensing standard for monitoring centres known as PSA 33:2014. PSA 33:2014 sets out requirements in the areas of organisation ownership, finances, staffing, training, structure of the Monitoring Centre and Monitoring Centre operations. Compliance with PSA33:2014 must be continuously maintained and companies are subject to inspection by the PSA at any time.

Contractors seeking a licence or renewing a licence must provide the PSA with:

- The licence fee based on the turnover of the contractor
- A tax clearance certificate
- Certification showing compliance with PSA 33:2014
- Garda vetting application for directors and shareholders.

A.7 Outline the principles and benefits of quality management systems particularly in relation to:

- The customer
- Applicable and relevant standards
- Frontline staff

Learning outcomes are designed to provide candidates with an understanding of the importance of quality management systems. By the end of this section you should be able to:

- Explain what is meant by quality service in the context of quality management standards
- List the relevant quality management standards and give examples of their requirements
- Explain the importance of ongoing review
- Be able to identify roles which have responsibility for quality management
- Explain quality service principles
- Outline the most common issues covered in a typical customer care policy

Quality service in the context of quality management standards

Quality service is the process by which the contracted or agreed service delivered is measured against the expectations of the customer. In the context of an Monitoring Centre this would include the level and quality of the response when an activation occurs.

Service delivery can be measured by feedback using customer surveys or questionnaires. It can also be more immediate resulting from customer complaints. Frontline staff can also play a role by reporting on system failures or their own independent observations. All these are important and should be used as part of ongoing internal responses and improvement processes.

Most organisations will have a quality management system in place. This system aims to achieve or improve the level of customer service provided by the organisation. The system is usually supported by a customer care procedures manual. The quality of customer service can be measured against a quality management standard. The standard will provide a template for the implementation of a quality management system.

Quality management standards and examples of their requirements

An example of a quality management standard is ISO 9001 Quality Management Systems a widely used internationally recognised standard. The standards required by the PSA for licensing can be considered as quality management standards as they incorporate the main principles of quality management.

As already mentioned in **Section A.6**, PSA 33:2014 is the PSA standard specific to the CCTV Monitoring and Intruder Alarm Monitoring sectors. Other PSA standards include:

- PSA 28:2013 – Door Supervisor and Security Guarding (Static) sectors
- PSA 39:2014 – Event Security
- PSA 42:2015 – Private Investigators
- PSA 55:2016 – Locksmiths

For a company to be certified as operating to a recognised quality standard requires a substantial commitment. Certification requirements include auditing of the companies processes to ensure they meet the stated requirements. While there are some variations between standards the main principles are summarised below.

The PSA use an established system for presenting their standards as follows:

- Scope
An outline of the extent of the standard and an explanation of relevant definitions are included at the start.
- Organisation
This includes identifying who owns the company, company finances, insurance and premises.
- Staffing
This includes staff screening, terms of employment and code of conduct.
- Training
This includes a training policy and aspects of operational staff, supervisor and management training.
- Operations
This includes security of information and general operational matters.
- Compliance
This section set out the compliance requirements set by the PSA.
- Specific Provisions
Some standards will have a section for special provisions.

The importance of ongoing review

A vital part of any quality standard is a review process which preferably should be directed from the highest level in the organisation. A review of this nature is conducted as a formal structured process and meetings with a detailed agenda and the topics discussed and results documented.

Scheduled at least once a year the review will look at results of audits and reports. This includes surveys, customer feedback and input from management at all levels and frontline staff. Any interventions which took place during the year will also feature. These inputs will include both positive and negative, identifying what is working well and what needs to be improved.

A review will also look at changes to legislation or standards, technological advances and the business environment generally. The results of a review may lead to changes to policies and procedures, changes to practises and the application of resources such as updating equipment or training of staff in new practices.

Roles which have responsibility for quality management

The previous sections make it clear that quality management is driven from the very top in all organisations. Senior management designate or delegate others then to take responsibility for aspects of service delivery. This may be department heads, managers or supervisors. In larger organisations, there may be a specific quality management officer. Quality management roles should be captured in an organisation chart and the details included in company induction. Frontline staff members are an important part of quality service and customer care and as such they should ensure that they know who in the organisation is responsible for these areas.

Common issues covered in a typical customer care policy

A typical customer care policy will state the organisations commitment to customer care principles. The policy can be presented in a number of short paragraphs or in a series of direct statements which will fit on one page. These statements are designed to capture the main issues as approved by senior management. Some of the common issues covered in a policy would be:

- The type and level of monitoring service customers can expect
- All interactions whether face to face, by telephone, post or e-mail will be dealt with in a professional and timely manner
- Treating customers with courtesy and respect
- Responding to customer complaints efficiently
- The quality of services offered are designed to meet customer needs and are continuously monitored
- Staff commitment to service delivery and customer service

Benefits of quality management systems in relation to the customer

The benefits to the customer are that a quality management system is designed to:

- Identify customer needs
- Meet those customer needs
- Monitor customer satisfaction levels
- Improve customer satisfaction
- Include frontline staff in the process
- Work to documented policies and procedures
- Review the systems effectiveness continuously

Benefits of quality management systems in relation to Applicable and relevant standards

Quality management systems support and enhance both technical standards and operational standards.

Benefits of quality management systems in relation to frontline staff

Frontline staff will see benefits as standards generally and QMS in particular will:

- Define an organisation
- Identify those responsible
- Document procedures
- Clearly define tasks
- Involve staff in implementation
- Involve staff in improvement processes

A.8 Describe the range and application of security hardware products

Learning outcomes are designed to provide candidates with a knowledge of basic security products. The learning outcomes of this section are:

- Define security hardware products
- List sample hardware products
- Explain the terms perimeter protection and give examples of types of perimeter protection
- Explain the terms physical protection

Security hardware products

Security hardware products are best described as security products which offer physical resistance to attacks requiring force. It has also been described as physical security equipment. Security hardware products are largely tangible, incorporating a visual deterrent aspect. Security safes and secure cabinets for example are tested, rated and certified based on the level of resistance they offer to attack. Safes are also designed to look imposing.

Distinction should also be drawn between privacy and security. A small sliding bolt on a bathroom door is for privacy, a five lever mortice deadbolt lock on a front or back door is for security. A low picket fence around a property is to define a boundary, a two metre wall, topped with razor ribbon is for security.

Sample hardware products

Hardware security products include:

- perimeter fencing, gates, doors, shutters and grills are used to prevent access
- Padlocks, deadbolts, mortice and euro-profile are all types of locks. These can be keyed or keyless.
- Intruder alarms, CCTV and access control while electronic in operation all have hardware components such as bell boxes and cameras
- Safes, cabinets and secure containers are used to secure smaller valuables such as cash or jewellery or documents
- Strong rooms are used to secure larger valuables or documents

Perimeter protection and examples of types of perimeter protection

A perimeter is a boundary or line, the outer edge or border. In a security context, the perimeter can be defined as both the boundary line of a property and the external aspects of buildings.

In the context of loss prevention, the focus on perimeter protection is keeping people out as opposed to for example a prison, designed to keep people in. Perimeter protection in a military context may involve a body of manpower as opposed to any fixed permanent protection. This method is also applied in certain security settings such as a temporary or occasional event held in an open space.

Perimeter protection therefore means those measures taken to secure that boundary or border against breaches from outside. This is described as safeguarding the first line of defence and protection takes the form substantially of the use of hardware products.

These products include security fencing such as chain link, palisade, railings or a wall. Appropriate security grade gates and control barriers are used at openings.

External building security is next and includes doors, windows, shutters, grilles and grids. Security glass including laminates and polycarbonates are used in windows and screens.

A perimeter can be monitored by CCTV or protected by an electronic system. These are an alerting or warning system and while acting as a deterrent they cannot be described as offering physical resistance.

Natural perimeter protection is another aspect. Some examples of this would be a river or ditch, tight hedging or shrubbery and thorn bushes.

Lighting can also feature as a deterrent as part of perimeter protection.

Physical protection

Physical protection or physical security is a broad term used to describe physical measures designed to safeguard people and property from damage and theft. Perimeter protection is a part of physical security, focusing on the outer layer of a property or building.

Physical protection extends to all other measures such as use of security staff, internal protection controlling access to goods or equipment and includes an IT system. Staff, authorised visitors, contractors and customers in a shop will not feature in perimeter protection. Further internal controls and restrictions, including physical security may be required.

Access control is separate to perimeter protection and is about controlling access of people or vehicles entering or leaving premises or buildings. Access control measures are a form of physical protection and follow on from perimeter protection. Access control can be manually operated, such as a key or bolt. Doors, gates and control barriers can be supported by CCTV monitoring and electronic and remote access control. Turnstiles while offering a physical barrier of sorts are better described as access control measures. All of these measures can be described as offering physical protection.

A.9 Outline the main provisions of the relevant standards applicable to licensed Monitoring Centres

Learning outcomes are designed to provide candidates with an understanding of how standards impact on the daily operations of the monitoring centre. At the end of this section you should be able to:

- Outline the impact regulatory standards and operational procedures have on CCTV and ALARM monitoring operations
- Outline the main contents of the Garda Síochána Policy on Monitored Intruder Alarms
- Outline the main requirements contained in SR25 (*Alarm Receiving Centres Alarm Handling Procedures*)
- Outline the main requirements contained in SR45 (*Remote Monitoring of CCTV systems*)
- Explain the role these documents play in:
 - Helping to protect the CCTV and ALARM systems staff from complaints of malpractice and negligence
 - Reassuring the public about CCTV and ALARM operations

The impact regulatory standards and operational procedures have on CCTV and ALARM monitoring operations

The original legislation and subsequent regulations are designed to ensure that companies and individuals providing services in the private security industry operate to standards and comply with legislation generally.

A feature of this is the setting of mandatory standards. The PSA has prescribed certified quality management system standards for contractors and accredited training standards for individuals. The PSA also publishes auditing guidelines which provide details on how the standards are to be audited. A criminal record check is also carried out before a licence is issued. The PSA has also published fit and proper person guidelines. These state clearly a number of other requirements of the licensing process, with particular emphasis on compliance with other relevant legislation.

All licensees must now operate to same standards as a minimum. Audits by approved certification bodies and visits by PSA inspectors help ensure that the requirements are maintained.

The implementation of mandatory standards required for licensing place an onus on management and staff of the organisation to maintain a consistent level of quality service. Regulatory standards which are consistent and applied in all organisations bring clarity to the way an Monitoring Centre provides its services. The services themselves are defined and the way the services are delivered is clearly documented which means everyone involved knows what is required and who is responsible. Those who have implemented standards report that it can increase efficiency. There can be a positive impact in the public eye on a company's image when certified to a standard and when licensed.

The main contents of the Garda Síochána Policy on Monitored Intruder Alarms

The purpose of the policy is to keep to a minimum the number of false alarm calls passed on to the Garda. This leaves the force more operationally effective in dealing with genuine activations.

A Garda response to an activation from a monitored alarm system requires a Garda issued Unique Reference Number (URN). This is used to identify each individual protected premises. The premises occupier applies in writing for this number using a specific Garda issued application form. The form requires details of the premises, including directions and a comment on any risks and hazards to which attending Garda may be exposed. Where a change in risk or hazard takes place, the occupier must inform the Garda. Sections of the form must also be completed by the installer and the Monitoring Centre. Notification to the Garda, by the occupier is also required where a change of Monitoring Centre takes place.

The URN once issued is the main identification used by Monitoring Centre controllers when passing on activations to the Garda. The URN is issued by the Garda based on an address. It is issued entirely at the discretion of the Garda and is not the property of the occupier, the installer or the Monitoring Centre.

The current policy came into force in January 2008 and the main provisions are as follows:

- The Garda will respond to a verified alarm activation only. Verified is defined as the activation of a secondary detection device as a sequential verified alarm, or by visual or audible inspection (including remote camera or microphone).
- For a verified activation, a key holder must be notified first and an estimated time of arrival given to the Garda.
- The notified key holder is expected to attend the premises at the shortest time possible. Failure of key holder to attend will result in the activation being recorded as a false alarm.
- The Monitoring Centre must be licensed by the PSA.
- Installation companies and alarm systems installed must be certified to relevant standards.
- A Garda issued Unique Reference Number must be quoted for all activations notified.
- Testing of alarm system operation shall not involve Garda notification or participation.
- The Garda will only accept alarms cancelled by the Monitoring Centre and not an occupier or key holder.
- No installer or Monitoring Centre may make reference to the Garda in any stationery or advertising material or infer that Garda response will result from all alarm activations.
- When three false alarms are recorded against a premises in a three month period, Garda response will be suspended. A reinstatement process is in place requiring a period free from false alarms.
- The Garda will always respond to personal attack activations unless there is evidence of abuse of the purpose of a personal attack alarm.

- Failure to comply with the policy will result in the Monitoring Centre no longer being recognised.
- It is a condition of PSA licensing that the Monitoring Centre complies with the Garda policy.

**The main requirements contained in SR25
(Alarm Receiving Centres Alarm Handling Procedures)**

SR25 is one of the standards required by the PSA for licensing of alarm monitoring centres. SR refers to Standard Recommendation. SR25 details how Monitoring Centres should respond to signalled alarm conditions from intruder alarm systems. The standard should be read in conjunction with the requirements of the Garda Síochána Policy on Monitored Intruder Alarm Systems.

A substantial body of the standard relates to alarm verification and alarm filtering as set out below:

Alarm Verification Techniques

- Verified Alarm Condition
If alarm verification is not used, it is possible that Garda Síochána response will not be provided. Reference should be made to the Garda Síochána Policy on Monitored Intruder Alarm Systems.

The purpose of using alarm verification is to provide high confidence that an alarm signal has been caused by genuine intrusion or genuine attempted intrusion. It is also important therefore to recognise that those alarm systems that are capable of providing verification can also in certain circumstances generate an alarm condition (which can indeed represent genuine intrusion) but without the alarm receiving centre receiving any verification of activity within the premises.

- Authorization
The alarm company (the installer) shall ensure that the signalling protocols, alarm verification procedures and alarm filtering techniques are compatible for use with the alarm receiving centre. Also, that they are clearly and unambiguously communicated to the subscriber (client).

Note. Where communication or transmission faults are to be signalled, the alarm company should notify the subscriber in writing at the time the alarm monitoring agreement is being set up of the actions that will be taken by the alarm receiving centre upon its receiving a signal indicating that a communication or transmission fault has occurred.

- Audible Verification
When, using audio technology, the operator at the alarm receiving centre reaches a decision, acting within agreed procedures, that the sounds emanating from the protected premises are such that they verify activity at the protected premises, the alarm signal shall be designated as being an audibly verified alarm signal.

- Visual Verification
When, using video technology, the operator at the alarm receiving centre reaches a decision, acting within agreed procedures, that the images emanating from the protected premises are such that they verify activity at the protected premises, the alarm signal shall be designated as being a visually verified alarm signal.
- Sequential Verification
When, using sequential technology, the operator at the alarm receiving centre reaches a decision, acting within agreed procedures, that the signals emanating from the protected premises are such that they verify activity at the protected premises, the alarm signal shall be designated as being a sequentially verified alarm signal.
- Verification Time
When the verification time for verified alarm conditions is to be managed by the alarm receiving centre or by the alarm system, this time shall be agreed between the parties.

Alarm Signals Associated with Communications or Transmission Faults - if an unverified alarm signal be received from the premises from which an uncleared communication or transmission fault signal has been previously received, the unverified alarm signal may now be deemed as a verified alarm.

Note. Where the alarm signalling and monitoring arrangements are such that a communication or transmission fault might possibly give rise to Garda Síochána call-out, the alarm company should advise the subscriber in writing at the time the alarm monitoring agreement is being set up that communication or transmission faults that result in Garda Síochána call-out can adversely affect future Garda Síochána response to the alarm system.

Alarm Filtering

General

Alarm Filtering involves the delaying of alarm signals at the Monitoring Centre which allows their status to be reviewed in order to prevent unnecessary call outs of An Garda Síochána or keyholder. Filtering is applied to all alarms signals with the exception of signals which have been accepted as being verified.

Authorization of Alarm Filtering

Cancellation of an alarm signal following an agreed procedure may be authorized by the subscriber. This may be:

- (a) On a case-by case basis in accordance with a defined alarm filtering routing operated by the alarm receiving centre whereby the subscriber or his alarm system communicates with the alarm receiving centre, using suitable code words or numbers or abort signal, affirming that Garda Síochána or key holder call-out is not required, or
- (b) By prior written agreement, whereby the subscriber has given authority that some alarm signals may be regarded as cancelled

Application of Alarm Filtering

Following receipt of an alarm signal, the alarm receiving centre shall apply alarm filtering.

Alarm filtering may be applied to exempt alarm signals, by agreement between the parties.

Note. For example, it can be appropriate to apply alarm filtering to exempt alarm signals where the alarm receiving centre is certain that the alarm system is being unset or if alternative actions have been agreed between the parties.

Verified Alarm Signals

Alarm filtering need not be applied to alarm signals that have been designated as being verified.

Note. An exception can be appropriate where an alarm receiving centre is aware that the alarm system is being unset or if alternative actions have been agreed between the parties.

Alarm Filtering Delays

Where alarm filtering delays are applied, the duration of such delays shall be agreed between the parties.

Method of Alarm Filtering

If prior to the Garda Síochána or the key holder being informed, the alarm receiving centre receives a signal that is identifiable to the alarm receiving centre as being an abort signal or a signal that is identifiable to the alarm receiving centre as indicating that the alarm system is unset, then the alarm receiving centre may designate the alarm condition as being a false alert, and regard the alarm condition as cancelled, without extending any alarm message to the subscriber, Garda Síochána or key holder.

Note. It is a matter between the parties whether or not key holders are to be called in the event of a false alert.

During alarm filtering the alarm receiving centre may attempt to contact or be contacted by the subscriber and / or key holder with a view to obtaining authorization using suitable code to cancel the signalled alarm condition.

The main requirements contained in SR45 (*Remote Monitoring of CCTV systems*)

SR45 provides guidelines for the connection and monitoring of remotely monitored CCTV systems, primarily where the system is to trigger alarms through some type of detection system, and send those alarms to a Monitoring Centre for processing and response. The alarm footage is reviewed at the Monitoring Centre and a decision made as to whether to obtain a Garda response for the incident. The main requirements of the document are listed below.

CCTV System Design and Installation

Includes details on camera positioning and configuration, lighting, control equipment and system performance requirements.

Risk Assessment and Commissioning

This section is mostly site specific and includes requirements relating to the risk assessment and the testing and commissioning of the system. There is also a requirement for the installer to provide a copy of the risk assessment and a commissioning certificate to the Monitoring Centre

Client Responsibilities

This section requires that the Monitoring Centre have a protocol agreement in place outlining the response times and actions for various site scenarios, information on the site and key holders is also included here.

Monitoring Centre Specification

This section requires the Monitoring Centre to have the following additional facilities for remote CCTV monitoring:

- Sufficient alarm receiving workstations to meet the normal level of demand
- Sufficient staff numbers to handle all activity
- Sufficient communication paths to ensure that the paths never exceed maximum
- Adequate facilities to handle alarm activity in line with client expectations

Monitoring Centre Procedures

This following procedures shall be undertaken by the Monitoring Centre.

- The Monitoring Centre shall receive from the client, the installer or his own designated personnel the following information pertaining to the site before or at the final commissioning;
 - Site address
 - Installer details
 - Site map, including camera numbers / names
 - Site operation – arming and disarming times etc.
 - Agreed response plan
 - Key holders and local emergency contacts
 - Directions to the site
 - Fault reporting procedures
- All communications with the site, including alarm and non-alarm video, text information, fault reporting shall be stored at the Marc. All operator actions in relation to electronic communication with the site shall be automatically logged in a database and be easily searchable.
- Monitoring Centre operators shall follow documented procedures in all aspects of their alarm receiving responsibilities.
- Monitoring Centre operators shall be trained in the actions involved in producing evidential images.
- If a Monitoring Centre operator or supervisor forms the opinion that the visual or other information coming from the site is not of sufficient quality to enable the alarm events to be properly determined, then the Monitoring Centre shall issue the client and installer with a technical update notice. The notice shall outline the nature of the problem identified at the Monitoring Centre, its likely effect in the quality of the monitoring service, and a period in which the problem shall be resolved.
- Every effort shall be undertaken by the alarm installer and the client to minimize the number of false or nuisance alarms. The client and the Monitoring Centre shall agree that in the event of a previously specified number of activations of which the cause cannot be determined, or can be determined to be of a non-critical nature (e.g. wildlife or foliage), the detection system relating to this cause may be disabled. The client shall then agree on the remedial action before the detection system may be reactivated.
- The evaluation of images received at the Monitoring Centre as a result of each initial activation shall commence within 90 seconds of their arrival on the operators screen for 80% of the activations, and 180 seconds for 98.50% of initial activations.
- In the event of an alarm event requiring incident reporting to the client, the incident report shall be sent to the client within a two hour start of the following day or sooner if agreed with the Monitoring Centre.
- Loss of video signal on the site shall generate an alarm event at the Monitoring Centre within 10 seconds. Loss of power to any element of the system shall cause an alarm event at the Monitoring Centre.

The role these documents play in helping to protect the CCTV and ALARM systems staff from complaints of malpractice and negligence

The documents referenced have a common theme. They all refer to having in place transparent, consistent and documented methods of carrying out CCTV and alarm monitoring services. All standards place an onus on management at the highest level to ensure that the requirements are known and complied with.

This means that controllers working in any Monitoring Centre have systems and procedures in place describing how they carry out the tasks required. Provided controllers are competent, follow instructions, understand and implement the requirements the likelihood of any allegations being made against them will be reduced.

The role these documents play in reassuring the public about CCTV and ALARM operations

The public benefit by having access to a regulatory authority who can investigate and adjudicate on any complaints made, for example, on the performance or behaviour of individual licence holders.

The PSA sets and enforces comprehensive standards which the Monitoring Centre must operate under. This reassures the public that quality and professional services are expected. End users or clients of the industry also have access and may complain or comment on the nature or quality of the service provided to them.

End users or clients of the industry must use PSA Licensed Contractors to provide security services to them. It is an offence under the Private Security Services Act to use unlicensed contractors. The PSA publish a register of all licence holders and provide information of suspensions and revocations. This information is beneficial to end users and the public.

The licensing regime has more clearly defined the known industry and has created barriers to undesirables who here-to-fore may have entered the industry unchallenged.

B.1 Outline the relevant aspects of Irish Law

Learning outcomes are designed to enable candidates understand the private security industry, its role and its sectors and range of services. By the end of this section you should be able to:

- Describe the Judicial system
- Explain the purpose of criminal law
- Explain what is meant by civil law
- Explain the term trespass

Describe the Judicial system

The Judicial System or Judicial Branch of Government is the Courts System, described as the branch of Government with the authority to interpret and apply the law in the public interest. Courts in this context are considered as entities made up of people and processes and not merely buildings or places; in fact since 2006 it is accepted practice to address the sitting judge as “the court”. Judges are appointed by the President of Ireland on the advice of the Government.

While there are a number of specialist courts such as The Children Court, The Drug Treatment Court, Juvenile Court, Special Criminal Court and the Central Criminal Court, generally speaking there are five distinctive types of court in Ireland. The following briefly describes these in hierarchal order:

District Court

The District Court is lowest level of court and can be described as a local court. It can deal with claims up the value of €15,000, family law cases and criminal cases such as road traffic offences, assaults and criminal damage. The district court sits with one judge and no jury.

Circuit Court

The circuit Court is also a local, although a more regional based court established in main centres throughout the country and hearing cases relevant to that region. It can deal with claims up to the value of €75,000. The court deals with family law matters and criminal cases excluding the most serious offences such as murder. In criminal matters the judge sits with a jury. The Circuit Court hears appeals from the District Courts within its region.

High Court

The High Court can hear all criminal, civil and family law cases and has power to determine all matters whether law or fact including the validity of any law having regard to the Constitution. It can deal with claims exceeding €75,000. The High Court can hear appeals from the Circuit Court in civil matters and rule on questions of law raised in the District Court. The Central Criminal Court is at the same level at the High Court but deal with criminal matters only. The Central Criminal Court sits with a judge and jury.

Court of Appeal

The Court of Appeal hears appeals in civil cases from the High Court and appeals in criminal cases from the Circuit Court, the Central Criminal Court or the Special Criminal Court.

Supreme Court

The Supreme Court is the highest court. Describes as the court of final appeal it sits normally with three or five judges and hears appeals from the Court of Appeal and the High Court. Certain determinations can be made by a sole judge or in exceptional circumstances seven judges may sit.

The purpose of criminal law

Criminal Law is a means for protecting society and allowing it to develop by providing a code of conduct, which may only be breached at the risk of sanction.

Laws reflect society and change as society changes; however, the purpose has remained consistent. Societies decide what constitutes a crime such as robbery or murder; then determine how an offender should be punished, if found guilty, such as imprisonment. Criminal prosecutions are conducted on behalf of the people as criminal acts are described as acts against the community at large. Laws make a statement as to what is unacceptable to that particular society at that time, ideally to prevent occurrence by acting as a deterrent. The purpose in its broadest sense is to “protect society”.

Examples of crimes include murder, rape, robbery, assault and burglary.

What is meant by civil law

While criminal law determines acts deemed to be against the community as a whole, civil law is described as a private wrong or private matter. Common definitions include “private law” or “the regulating of ordinary private matters”.

The Law Library of Ireland describes it as “cases involving disputes between individuals, organisations or the State”. In civil cases people sue for compensation, usually money, for a wrong caused. The amounts have been referred to earlier under the courts section.

Civil actions due to negligence are very common cases; this typically involves an employee suing an employer as the result of a workplace accident, or a customer suing a supplier for a defective product. Defamation is a common action against security companies and the retail trade; this typically happens when a visitor to shop is denied access, falsely accused of something or removed from premises without just cause. When this action takes place in front of witnesses it can result in embarrassment and loss of reputation.

Physical injuries, loss of earnings or loss of reputation are reasons why people sue, this can include traffic accidents, assault, spoken or printed words, trespass and contract disputes may result in civil actions.

Criminal law and civil law can be described as the two main branches of the legal system in Ireland. Certain criminal actions can also lead to civil actions; assault for example may lead to a criminal prosecution as well as the victim suing for compensation.

Trespass

Trespass is a very broad subject; it can lead to a civil action and a criminal prosecution or both depending on the circumstances. It can be intentional or unintentional. It includes trespass to the person and trespass of animals. The context of this section is the security industry and as such the focus is on trespass to land or property. For convenience the term premises (land or buildings owned by someone) is used.

In this context trespass is defined as intentionally or negligently entering on a property in the possession of another. If a person has lawfully entered property in the possession of another and is then refused permission to stay on the property, they may be regarded as a trespasser.

A visitor may enter a shop and under normal circumstances they have been invited to be there, however in an emergency, a breach of conditions or when the shop is closing the person can be asked to leave, if they fail to do so, their status as a visitor is changed, they are trespassing as the right to remain has been withdrawn.

If a person enters premises by any means other than the official or designated entry point, they may be treated as trespassers and asked to leave. If a person enters without complying with the stated entry criteria or conditions such as payment of a fee, they may be treated as a trespasser.

It is important that the entrant is asked to leave, and asked by a person acting on behalf of and with the authority of the occupier. Thereafter a reasonable opportunity must be given to allow the entrant leave. Due consideration must be afforded to those who entered accidentally or unintentionally. In extreme circumstances reasonable force may be used to remove a person. In all cases exiting must take place safely through the normal designated entry / exit point.

Where a person enters premises in good faith such as to rescue another or extinguish a fire, this is not generally considered an offence by the courts.

B.2 Outline the relevant aspects of Irish health & safety law and environmental law

Learning outcomes are designed to enable candidates understand the private security industry, its role and its sectors and range of services. By the end of this section you should be able to:

- Summarise Safety, Health, and Welfare at Work legislation in respect of:
Duties of employers to include:
 - Safe place to work
 - Safe systems of work
 - Safe access and egress
 - Welfare facilities
 - Personal Protective Equipment
 - Information, training and supervision
 - Control any article or substance
 - Responsibilities of employees
 - Risk assessment
 - Safety statement
 - Consultation and representation
 - Lone workers
- State the principal points of prevention in relation to controlling workplace hazards
- Explain who the Health and Safety Authority is and state its principal functions
- List the actions the Health and Safety Authority can take if it finds an unsafe workplace
- Outline the guidelines for CCTV operators under the HSA guidelines on the aspects of the Safety, Health and Welfare at Work (General Application) Regulations 2007 as they relate to Display Screen Equipment (Chapter 5 of Part 2)
- List the key indicators of workplace stress and how to remediate or help reduce the impact of those factors

Safety, Health, and Welfare at Work legislation in respect of the duties of employers to include:

Safe place of work

Under the Act employers are primarily responsible for creating and maintaining a safe and healthy workplace, employees and visitors also have a part to play. The Act specifically references the following as duties of the employer as published by the Health and Safety Authority:

- Managing and conducting all work activities so as to ensure the safety, health and welfare of people at work (including the prevention of improper conduct or behaviour likely to put employees at risk) horseplay and bullying would come within these categories.
- Designing, providing and maintaining a safe place of work that has safe access and egress, and uses plant and equipment that is safe and without risk to health.
- Prevention of risks from the use of any article or substance, or from exposure to physical agents, noise, vibration and ionising or other radiations.
- Planning, organising, performing, maintaining and, where appropriate, revising systems of work that are safe and without risk to health.
- Providing and maintaining welfare facilities for employees at the workplace.
- Providing information, instruction, training and supervision regarding safety and health to employees, which must be in a form, manner, and language that they are likely to understand.
- Cooperating with other employers who share the workplace so as to ensure that safety and health measures apply to all employees (including fixed-term and temporary workers) and providing employees with all relevant safety and health information.
- Providing appropriate protective equipment and clothing to the employees (and at no cost to the employees).
- Appointing one or more competent persons to specifically advise the employer on compliance with the safety and health laws.
- Preventing risks to other people at the place of work.
- Ensuring that reportable accidents and dangerous occurrences are reported to the Health and Safety Authority.

Safe systems of work

Safe systems of work are directly linked to tasks performed. This is a formal systematic process where tasks are identified first, followed by associated hazards and risks; then safe methods of work are designed to carry out that task. The focus is on firstly to eliminate where possible or minimise risks to safety and health. A safe system of work is essential when hazards cannot be eliminated and a risk remains.

The main headings under which a safe system of work can be approached are as follows:

- Assess the task
- Identify the hazards
- Define safe methods
- Implement the system
- Monitor the system

The system must be communicated properly, understood by employees and applied correctly and monitored on an ongoing basis.

As with all safety management processes, this system is reviewed on a regular basis and whenever there are changes to work practices or processes.

Safe access and egress

It is the responsibility of management to ensure that safe means of access and egress are in place in all workplaces. The focus of this section is on access and egress generally as well as the ability for people to move about safely in normal or non-emergency situations.

Typically this includes level surfaces such as, for example:

- Floors
- Corridors
- Footpaths
- Walkways
- Doorways

Changing levels in particular may present a higher risk than level surfaces, these include, for example:

- Stairs
- Steps
- Escalators
- Landings
- Ramps
- Balconies

A third aspect is hazards associated with vehicles and machinery. Cars, trucks, cranes and forklifts are typical features in a lot of premises. Machinery can generate heat and noise as well as risks associated with moving parts. Precautions must be taken where people come into close proximity with vehicles and machinery. Correct parking of vehicles in designated areas is also a feature.

These precautions can include clearly designated and marked walkways for example through a production or vehicular traffic area. Warning signs, railings, kerbs and barriers will assist with keeping people within designated safe travel areas.

All routes should be of a suitable width to accommodate the anticipated flow of people.

Surfaces must be protected against slipping hazards caused by leaks or spillages, specialist covering can be provided where hazards are prevalent.

Suitable handrails are required on both sides of stairs, steps and ramps.

All surfaces must be maintained in good condition, avoiding cracks and defects in floors for example.

Appropriate lighting is essential, including emergency lighting.

Warning signs, markings and notices are required to guide people safely around all premises. This includes directional signs, maps and diagrams, in complex or large workplaces familiarisation exercises or tours are beneficial.

Doorways should not hamper the flow of people. For example a large busy corridor should not lead to a small locked door. Door design should be consistent with the anticipated volume of traffic.

Avoiding hazards associated with slipping, tripping and falling are priority features; therefore good housekeeping is essential, in particular:

- Regular checking of all areas and recording of checking
- Cleaning spillages efficiently
- Removing debris
- Kept free from obstruction – not used as a storage area for machinery, supplies or equipment
- Awareness - employees and visitors are aware of the requirements needed to ensure safe access and egress

Additional precautions may be required for people of limited mobility.

Welfare facilities

Employers are required to ensure that there are welfare facilities provided at each place of work. Welfare facilities in this context are:

General welfare requirements

- The place of work is kept clean and tidy
- A standard of hygiene is maintained
- Appropriate seating is provided. To avoid standing for long periods every opportunity should be provided for seating with sitting breaks accommodated where possible.
- Supply of wholesome drinking water is provided
- The means to boil water
- Comfortable facilities for meal taking, including tables, chairs, heat and light

Rest rooms and rest areas

Certain types of work such as physical activity or dirty, noisy, hot or cold environments will require a separate rest area away from the hostile work environment for employees to have a break. A canteen type area which is shared by others may be used, provided employees from these hostile areas do not contaminate the canteen with any odours, dirt or fumes. A separate place is preferred.

Sanitary and washing facilities

- Adequate number of lavatories with washing and toilet facilities
- Separate lavatories for non-staff members
- Shower facilities where the nature of work dictates
- Hot and cold running water
- Protection of privacy
- Ideally separate facilities for men and women

Provision of adequate toilet paper, soap and drying facilities are essential, as well as a sanitary disposal receptacle for women. All facilities should be ventilated, well lit, kept clean and comfortable.

Changing rooms and lockers

These are required generally in workplaces if employees have to wear special work clothes such as overalls or aprons which are likely to become soiled or contaminated. These are clothes not worn to and from work requiring employees to change. Lockers are required to keep employees clothes clean and safe and to store personal effects.

Comfortable surroundings are essential as well adequate hooks, pegs, seating and clothes drying facilities (where required). A separate facility is required for men and women unless usage is low volume, then one lockable room can be adequate.

Accommodation area

On rare occasions employees may live on a work premises or site. Where this is the case the employer is responsible for the accommodation provided. This responsibility extends to fully equipping the accommodation with all equipment and facilities appropriate to any other living space.

Personal Protective Equipment

Section 8 of the 2005 Act places a duty on employers to provide personal protective equipment. A critical feature of PPE is that it is provided “where risks at a place of work to the safety or health of employees cannot be avoided or sufficiently limited”. This means that PPE is a last resort when all other measures have been implemented and a risk still exists, the first duty of the employer is to avoid or limit risks. The Act also places a duty on employees to use the PPE provided properly whenever it is required to be used.

The Health and Safety Authority Guidelines outlines ten categories of PPE as follows:

Head Protection

This includes helmets, hairnets or caps to protect the head and skull

Hearing Protection

This includes earplugs and earmuffs

Eye and Face Protection

This includes spectacles, masks and goggles

Respiratory Protection

This includes dust and gas filters

Hand and Protection

This includes gloves and oversleeves

Foot and Leg Protection

This includes safety boots, shoes and kneepads

Skin Protection

This includes barrier creams and ointments

Whole Body Protection

This is equipment designed to prevent falls such as braking equipment, safety ropes and harnesses

This includes overalls, weatherproofs and reflective clothing

The above is a brief summary, PPE is designed to protect against particular risk, based on a risk assessment. A huge variety of boots and gloves for example are available and manufactured to protect against specific events, the type selected must be appropriate to risk and individual user.

PPE must be provided without charge to the employee, the employer is responsible for maintaining and replacing the equipment and must also provide training and afford employees the opportunity to practice its use and become familiar with the equipment if required.

Information, training and supervision

Employers have a duty to provide the level of information, instruction, training and supervision necessary to ensure, so far as reasonably practicable, the safety, health and welfare of employees.

Information must be provided in respect of the hazards to safety, health and welfare at work and the risks identified by the risk assessment and the protective and preventive measures to be taken concerning safety, health and welfare at work under the relevant statutory provisions in respect of the place of work and each specific task to be performed at the place of work.

Instruction and training must directly relate to the specific tasks to be performed and the associated hazards. These hazards and associated risks will already form part of the safety statement and previous risk assessment. Thereafter employees must know of the control measures put in place and critically, their role as part of these control measures. Instruction and training focuses on how to perform the tasks required and how to do so in a safe manner. Critically, measures to be taken in an emergency must be included. Information includes providing the names of emergency staff and safety representatives.

All information instruction, training and supervision provided must be in a form, manner and, as appropriate, language that is reasonably likely to be understood by the employee concerned. As a part of this employers must consider for example literacy difficulties when providing information. The duty of employers includes not just full time employees but part time and temporary employees as well, including agency staff. Employees of another employer working in the place of work must also be informed. A critical feature is induction; all new employees or visiting employees must be provided with the information also.

Ongoing training may be required in the event of transfer of employees or changes to the tasks. The introduction of new work equipment, new technology or changes to systems of work will also require refresher training or upskilling.

The employer must be clear as to the competency requirements of employees, where certain skills and qualifications are required to perform tasks; the employee must have these skills or be provided with the necessary training to be deemed competent. No employee can be put at risk by been given work that they do not have the competence to do. Risk assessments must always consider the competence of employees. This is relevant in particular to employees who may be disabled, equally young workers and pregnant workers and other groups are considered based on the ability to carry out the task and do so in a safe manner.

All aspects of the task, the competency of the employee and the safety procedures put in place must be monitored, reviewed regularly and changed when required.

There can be no financial cost to the employee or loss of earnings in respect of these requirements.

Control any article or substance

The Act includes a section titled “General Duties of Other Persons”; this relates to those who design, manufacturer, import or supply articles or substances for use at work. A duty ensuring the safe use of these materials is placed on the producers or suppliers.

An article can be defined as any plant, machine, machinery, appliance, tool or any other work equipment or any other product used by persons at work.

A substance can be defined as any natural or artificial substance, preparation, or agent in solid or liquid form or in the form of a gas, vapour or micro-organism. Information must be supplied with regard to the identification of the substance, any risk arising from its inherent properties, any relevant test results and any condition necessary to ensure its safe use, handling, processing, storing, transportation or disposal.

Responsibilities of employees

Under Section 13 of the Safety, Health and Welfare at Work Act, 2005, each employee is reminded that they have specific statutory responsibilities as follows:

- Comply with health and safety legislation
- Protect his or her own safety, health and welfare and that of any other person who may be affected by their acts or omissions
- Not to be under the influence of any intoxicant to the extent that they could be a danger to themselves or others while at work
- Cooperate with their employer on safety, health and welfare at work
- Not engage in any improper conduct which could endanger their safety, or health or that of anyone else
- Participate in safety and health training offered by their employer
- Correctly use any article or substance and personal protective equipment provided for use at work or for their own protection
- Report any defects in the place of work such as equipment etc. which might endanger safety and health

The above are self-explanatory and mean that employees must share some responsibility for safety at work.

Risk assessment

Risk assessment is one of the most important aspects of the duties of employers under the legislation. Every employer must identify the hazards at the place of work, assess the risks and have a written risk assessment of those risks as they apply to all employees. The risk assessment process can be carried out using five broad headings or steps, as follows:

- Identify the Hazards
- Assess the Risks
- Control Measures
- Safety Statement
- Review and Record

Each is described in more detail as follows:

Identify the Hazards

A hazard can be described as any substance, material, piece of equipment or activity that can cause harm. For example working with chemicals, lifting loads or using a ladder, fire and electricity are also examples of hazards. Hazards can exist in all workplaces; the purpose of risk assessment is to identify all hazards, putting in place control measures for those hazards which may adversely impact on employees in the workplace.

The fact that a hazard exists is one stage of risk assessment, to progress to rating the risk, employees must be exposed to the hazard. The prolonged use of visual display units such as computer screens is a common workplace hazard, if employees do not use visual display screens there is no risk to them.

Assess the Risks

Risk in this context can be described as the likelihood that an employee may be harmed or suffer adverse health effects if exposed to a hazard. Assessing risk means determining if a hazard, such as fire exists, then forming a view based on the tasks carried out if employees are exposed to that hazard. If there is a fire, is there a risk that employees may be harmed in any way.

Effective risk assessments will look at the likelihood and severity of events as well the potential for a hazard to cause harm to more than one person. These determinations lead to the implementation of control measures appropriate to the risks.

Control Measures

Control measures are the most significant part of risk assessment. Having documented the task, identified the hazards and assessed the risks associated with those hazards, control measures are required. Control measures can be described as actions that can be taken to reduce the potential of exposure to the hazard.

A control measure could be to remove the hazard or reduce the likelihood of the risk. Control measures can also include providing training, changing the way a task is performed or as a last resort providing personal protective equipment.

Control measures should be described in a way that is understood by those affected, proper choice of language and avoiding undue technical terminology is recommended.

Safety statement

Each place of work must have its own individual safety statement. The safety statement documents the hazards identified and sets out how the safety of employees is managed.

The safety statement must include:

- The hazards identified and the risks assessed
- The protective and preventive measures taken and the resources allocated
- The plans and procedures for dealing with emergencies or any serious or imminent risk
- The duties of employees including sub-contractors as regards health and safety
- The names and job titles of persons with responsibility for implementing and maintaining the measures
- The arrangements for appointment of safety representatives and safety consultation at the place of work and the names of any safety representative and/or safety committee members

The employer is required to bring the safety statement to the attention of employees, and as stated previously, in a manner that can be understood by employees. This should be done at induction stage initially and thereafter annually or when it has been reviewed and amended.

Review and Record

Workplaces activity and staff change, new processes or new products may see the risk assessment and controls no longer valid or appropriate. The employer must monitor and manage safety on a continuous basis and any changes in the workplace must lead to a review and possibly amendments to the safety statement. Even where no changes have taken place the safety statement must be reviewed regularly, at least annually.

Consultation and representation

Consultation and participation are vital elements of the risk assessment process and workplace safety generally. Employers must consult with employees or their safety representative on:

- Any proposed measure that is likely to substantially affect their safety, health or welfare at work
- The designation of employees having duties under the Act in relation to emergency, or serious and imminent danger planning and preparation
- Any matters arising from measures related to the protection from and prevention of risks
- Hazard identification and any risk assessment carried out
- The preparation of safety statements
- The information to be given to employees
- Information on reportable accidents and dangerous occurrences
- The appointment of competent persons
- The planning and organisation of training
- The planning and introduction of new technologies and the implications for the safety, health and welfare of employees

Employers must refrain from penalising any employee for acting in accordance with safety and health laws or for reporting complaints regarding safety and health matters at work.

Representation

The Act provides for employees to appoint a safety representative from amongst their number to represent them at the place of work in consultation with their employer on matters related to safety, health and welfare at the place of work.

The appointed safety representative can play a very active role including investigate accidents, investigate complaints, accompany an inspector carrying out an inspection, make representations to the employer on safety matters, consult and liaise on relevant matters with other safety representatives.

The employer must give the safety representative reasonable time off without loss of earnings to perform the functions, attend meetings and undergo training.

Certain workplaces may, due to their size or nature of work have a safety committee in place. A safety committee is a group made up of employer and employees representatives carrying out the same functions described above.

A section of the Act covers protection for representatives, as the following extract makes clear by prohibiting:

“Any act or omission by an employer or a person acting on behalf of an employer that affects, to his or her detriment, an employee with respect to any term or condition of his or her employment”.

Lone workers

Lone workers are defined as those who work by themselves without close or direct supervision. Anybody who works alone, including contractors, self-employed people and employee, is classed as a lone worker.

The Health and Safety Authority provides the following examples of lone workers:

- People in fixed establishments where only one person works on the premises, e.g. in small workshops, kiosks, petrol stations, shops and home-workers
- People who work separately from others, e.g. in factories, warehouses, some research and training establishments, leisure centres or fairgrounds
- People who work outside normal hours, e.g. cleaners, security, special production, maintenance or repair staff, etc.
- People working away from their fixed base e.g. on construction, plant installation, maintenance and cleaning work, electrical repairs, lift repairs, painting and decorating, vehicle recovery, etc.
- Agricultural and forestry workers
- Service workers, e.g. rent collectors, postal staff, social workers, home helps, district nurses, pest control workers, drivers, engineers, architects, estate agents, sales representatives and similar professionals visiting domestic and commercial premises

Lone workers can encounter problems not typical to other workers such as:

- An accident on site
- A sudden illness
- Fatigue
- An attack or assault
- A fire or similar emergency

Where there is no immediate support the lone workers is at a higher level of risk.

A risk assessment should determine if is possible for work to be done safely by a lone worker. Lone working should not take place where for example no support, reliable communications or back-up is immediately available. The risk assessment must consider the worker e.g. young workers or woman, the processes or nature of the work and risks such as violence.

The risk assessment must specify the detailed control measures put in place to eliminate or minimise the risks identified, these can include measures such as:

- Telephone or radio communication
- Periodic physical checks such as supervisory visits
- Panic alarms
- Instruction and training
- Use of personal protective equipment
- Health surveillance
- First aid kits and training
- Standard operating procedures
- Secure place of work

Legislation does not prohibit lone working but places a duty of both the employer and employee to be aware of the risks involved and put in place measures to ensure that all that is reasonably practicable has been done to ensure the safety, health and welfare of the worker. This duty extends to those in charge of away work sites also as they must ensure that lone workers on their premises, irrespective of who they work for, are safe.

Principle points of prevention in relation to controlling workplace hazards.

On completion of a risk assessment it will be necessary to put in place control measures. Control measures in the first place seek to eliminate the hazard and where this is not possible, to reduce the risk. As part of this process, employers must take into account the general principles of prevention, which are as follows:

- The avoidance of risk
- The evaluation of unavoidable risks
- The combating of risks at source
- The adoption of work to the individual, especially as regards the design of places of work, the choice of work equipment and the choice of systems of work, with a view, in particular, to alleviating monotonous work and work at a predetermined work rate and to reducing the effect of this work on health
- The adaptation of the place of work to technical progress
- The replacement of dangerous articles, substances or systems of work by safe or less dangerous articles, substances or systems of work
- The giving of priority to collective measures over individual protective measures
- The development of an adequate prevention policy in relation to safety, health and welfare at work, which takes accounts of technology, organisation of work, working conditions, social factors and the influence of factors related to the working environment
- The giving of appropriate training and instruction to employees

In general terms the above means that the work space, the tools or equipment, the nature of the work and materials used should be adapted to suit the worker in the first instance.

Health and Safety Authority and its principal functions.

The Health and Safety Authority was established in 1989 under the Safety, Health and Welfare at Work Act, 1989. It is the national statutory body with responsibility for ensuring that workers and those affected by work activity are protected from work related injury and ill-health.

Its principal functions are:

- Enforcing occupational health and safety law
- Promoting accident prevention
- Providing information and advice

Its activities include;

- Promotion of good standards of health and safety at work
- Inspection of all places of work and monitoring of compliance with health and safety laws
- Investigation of serious accidents, causes of ill health and complaints
- Undertaking and sponsoring research on health and safety at work
- Developing and publishing codes of practice, guidance and information documents
- Providing an information service during office hours
- Developing new laws and standards on health and safety at work

The Authority now operates under the Safety, Health and Welfare Act, 2005.

Actions the Health and Safety Authority can take if it finds an unsafe workplace.

Inspections are carried out by authorised inspectors appointed by the Health and Safety Authority. Inspectors have substantial powers under the Act including:

- Visiting any premises without notice
- Entering any premises believed to be a place of work
- Entering any place where articles, substances or records are kept
- Requiring the production of records
- Inspecting records and take copies of same
- Examining and testing

These inspectors compile written reports on observed activity in the workplace and where they feel it necessary can take the following actions:

Verbal Advice

An inspector may during an inspection comment verbally on activity observed which may, if not monitored lead to minor breaches of the Act.

Report of Inspection Letter

An inspector may issue a Report of Inspection Letter detailing minor breaches of the law observed during an inspection and stating where improvements can be made. The occupier of the premises must undertake to remedy the items.

Improvement Direction

An Improvement Direction is a legal directive from an inspector requiring that certain improvements be carried out in a specified time frame. An Improvement Direction is issued where the inspector considers there may be a risk to the safety and health of persons. The premises occupier must submit an improvement plan setting out how the matters raised are to be remedied and when. If not satisfied the inspector may seek amendments to the plan.

Improvement Notice

An Improvement Notice is served when an inspector considers that the law has been contravened. The specified contravention must be remedied by the occupier within the time frame specified by the inspector.

Prohibition Notice

A prohibition notice is a legal instruction directing that a specified work activity be stopped immediately due to the level of danger.

Interlocutory Order

At a serious level the Authority may seek an Interlocutory Order from the High Court to restrict or prohibit a work activity.

Prosecute

The Authority can initiate criminal proceedings against directors and senior managers responsible for premises where they feel the individuals may have acted irresponsibly. Courts may impose fines or prison sentences on conviction of offences

Guidelines for CCTV operators under the HSA guidelines on the aspects of the Safety, Health and Welfare at Work (General Application) Regulations 2007 as they relate to Display Screen Equipment (Chapter 5 of Part 2)

Under legislation there are provisions which relate to the safety and health requirements for employees who habitually use display screen equipment as a significant part of their work. The acronym VDU (visual display unit) is used in this section to describe display screen equipment, typically a computer screen or monitor. This legislation is relevant to CCTV operators and others who work in a control room or alarm receiving centre type environments using VDU's as defined below.

The legislation requires the employer to:

“Ensure that the general use of the equipment is not a source of risk for the employee, perform an analysis of the workstation in order to evaluate the safety and health conditions to which it gives rise for the employees, particularly as regards possible risks to eyesight, physical problems and problems of mental stress, and, on the basis of that evaluation, take appropriate measures to remedy any risks found”

Employee covered are those who:

- Have no choice but to use the VDU to carry out his or her work
- Normally uses the VDU for continuous periods of more than one hour
- Use the VDU on a daily basis

Those employees:

- Are entitled to have their workstation assessed
- Must be trained in the use of the workstation and be given information about health and safety factors
- Must also have periodic breaks or changes of routine, away from VDU's
- Must be informed by their employer that they are entitled to an appropriate eye and eyesight test (or may opt for either) before working with VDU's and at regular intervals
- Are entitled to an appropriate eye and eyesight test (or may opt for either) before working with VDU's and at regular intervals. If at any time working with VDU's an employee experiences visual difficulties he or she has a similar entitlement

The definition of "workstation" is all-encompassing and includes VDU's and all the individual pieces of equipment, chair, desk and immediate work environment, which can constitute a workstation. A VDU includes a keyboard (which must be separate and tiltable) and / or any other accessories and peripherals. One of the most critical factors affecting the health of employees working at VDU's is the design and layout of the workstation.

In general terms there are three risk areas, as follows:

Eyesight

Using VDU's is not known to cause eye or eyesight damage, nor is there any evidence to suggest that existing eye defects are made worse. Use of VDU's however can lead to eye fatigue, sore eyes and headaches. Those with existing eye or eyesight defects, which may not have been apparent or corrected may find working with VDU's more tiring or stressful.

Causes of eye problems can include:

- Rigid posture
- Intensive concentration
- Poor positioning of VDU
- Fixed VDU or fixed control equipment
- Glare
- Poor lighting
- Flickering or other movement on the screen
- A failure to correct existing eye defects

Physical Problems

Work related upper limb disorders affecting the back, neck, arm, hand and shoulder areas are possible affects, causing discomfort, pain, fatigue or soreness. Repetitive strain injury, which is pain in the muscles, tendons or other soft tissue, is caused by the repetitive use of a part of the body, for example the hands, while performing tasks. General muscle and joint pain are common place due to poor posture or rigid posture; there can be long term effects, particularly with the back.

Causes of physical problems can include:

- Poor layout of workstation
- Unsuitable chair or other furniture
- Repetitive tasks
- Poor space and general work environment
- Poor lighting
- Screen typeface / screen size and image size

Other general issues leading to physical problems include risk of electric shock due to unsafe or faulty equipment or tripping due to poor housekeeping.

Workplace Mental Stress

Stress, particularly mental stress, also described as pressure or anxiety can have both physical and psychological effects on workers. Any job with responsibility can involve a level of stress. Not all levels of stress are considered harmful, each individual deals with stress differently, some perform poorly and others, with high levels of job satisfaction for example, may be driven to perform better. The negative effects of stress can be difficult to measure, however it can lead to mental and emotional problems inside and outside of the workplace. Stress can lead to fatigue, which is extreme tiredness or a feeling of weariness. This results in reduced efficiency, lack of concentration and can lead to mistakes.

Causes of workplace mental stress can include:

- Work overload
- Poor organisation of work
- Complex work involving a high level of concentration
- High speed / intensive work
- Work involving deadlines
- Uncertainty in how to do the job
- Uncertainty in employment
- Lack of support
- Lack of appreciation
- Work scheduling impacting on work life balance

Control Measures Summary

A competent person must carry out a risk assessment of the workstation and document the findings; this assessment includes an analysis of the tasks performed. Employees using the workstation should be given the opportunity to comment.

A general guideline for working continuously at a screen is one hour, a short break or change of activity is recommended after this period. Employers must take account of the nature of the work as concentrated or high intensity work in front of a screen presents a higher risk.

General precautions or typical actions in all workplaces will apply and the risk assessment will take all hazards for each workplace into account, the following is a list of general precautions:

- Workstations and surrounds must be kept clean and tidy
- Task management
- Safe equipment
- Suitable adjustable furniture
- Information and training
- Comfortable environment include lighting, ventilation and heat
- Taking regular breaks away from the workstation
- Taking regular exercise, organisation of work including breaks and changing activity, time management

Monitoring worker performance and engaging with workers will help employers determine problems and solutions.

Laptops

Laptops are not specifically covered in the legislation as a laptop does not have a separate keyboard. Laptops should not be used for long periods of time and where they are in regular use they are subject to a separate risk assessment.

Indicators of workplace stress and how to remediate or help reduce the impact of those factors.

Defining Stress

Stress is a complex topic and not easily defined precisely. The Health and Safety Authority provides a definition or description as follows:

“A negative experience / feeling, associated with new physical symptoms. These including increased heartbeat, swiftness of breath, dry mouth, upset stomach and sweaty palms and over the longer term, more serious digestive upset, cramp and raised blood pressure / cardiovascular disease”.

Psychological symptoms range from racing thoughts and speech, lack of impulse control, and feelings of being overpowered, losing control and fearfulness generally. People behave differently to their “normal” behaviour when under stress. They may be angrier, more confrontational, show less time for others and impose an urgency on situations which is unrealistic for those around them.

Stress will cause a change in behaviour and everyone will react differently to a stressful situation. Levels of stress escalate from slight pressure which can be coped with; higher levels which while challenging may be acceptable to some individuals and ultimately excessive pressure which causes stress. At its most serious; stress can ultimately lead to depression and heart disease.

Where the task, working environment, management or indeed other workers cause stress, these can be defined as hazards, potentially leading to ill-health these cannot be disregarded and may feature in a risk assessment.

Best practice safety and wellbeing responses focus on removing or reducing the cause of stress at source, looking at areas such as the particular tasks, the workload, the work system or the broader working environment as well as the abilities of the individual.

Each individual must, in the first instance, try to determine as clearly as possible what factors lead to stress in their lives. Individuals should not look to compare themselves directly with others and how others cope, stress is individual.

Stress Management

Modern living and working makes stress difficult to avoid completely and when stress is a factor which leads to a negative impact on an individual's wellbeing then stress management techniques may be required.

Linked to the previous sections, each individual must first determine the causes of stress and when they cannot be eliminated or reduced sufficiently then stress management techniques will be considered relevant to the individual and the environment. Self-awareness is very important for early intervention.

The following points will help with more effectively dealing with the demands of the job or life generally:

Identify Stressors

Stress is individual and awareness of what causes it is essential, identify the stressors or stress triggers and work to reduce those causes. An important part of this is when to say yes to the things that help and saying no to the things that don't.

Time Management

Working to deadlines and missing important deadlines may require time management awareness, information and training. Rostering of employees, shift duration and scheduling of work must be considered.

Adapting the Work System

Changing the way work is done, redesigning tasks, changing equipment and monitoring the workload feature. The working environment and working culture should seek opportunities for more fulfilling interactions with colleagues. Lone working for example can increase the perception of responsibility and lead to higher levels of stress.

Training

Where the task may be complex, additional or different training may assist, providing information to employees is a feature here also. It is important that those carrying out the task are afforded the opportunity to comment.

Breaks

Additional breaks away from the workstation, varying breaks or longer breaks may assist.

Support

Through supervision and management the employer should seek to show respect as well as to motivate and encourage. Regular contact will assist the employer with recognising the symptoms of stress. The employer representatives must be approachable and open to feedback from employees on problems.

Equipment

Incorrect equipment and lack of equipment to do the job properly leads to stress. This is particularly relevant where employees are held accountable for failings beyond their control.

Talking

Having a conversation with a colleague, friend or family member can help by making the situation clearer and putting the cause into perspective. Understanding the situation better and isolating it can help in managing it.

Working Environment

A comfortable environment with access to adequate facilities is essential to help counterbalance stressful workplace situations. Ventilation, lighting and heat are also features.

Managing Change

Change and particularly uncertainty can have a very negative impact on individuals, the employer has a responsibility to manage change effectively and reduce the likelihood of causing stress.

Exercise and relaxation are very successful stress management techniques, either within or external to the workplace. A stressful job combined with a stressful private life increases the risk of problems, a healthy lifestyle generally and a good work life balance helps.

Finally, even with individual techniques and employer responses, it may not always be possible to cope effectively with stress, ultimately it may be necessary to seek professional help either through the employer or external to the workplace.

B.3 Outline the relevant aspects of Irish equality law

Learning outcomes are designed to enable candidates understand the private security industry, its role and its sectors and range of services. By the end of this section you should be able to:

- Explain the term discrimination
- List all the legal grounds covering discrimination and explain their meaning
- Explain the terms direct and indirect discrimination
- Explain the term discrimination by association
- Explain the terms harassment and sexual harassment and describe the related behaviours
- Explain what is meant by disability, bullying and racism in a legal context
- Explain the importance of prohibiting behaviour covered by equality legislation

Discrimination

The Irish Human Rights and Equality Commission (IHREC) are Ireland's national human rights and equality institution. The commission was established under the IHREC Act 2014, this was effectively a merger of the Irish Human Rights Commission and the Equality Authority. Its purpose is to protect and promote human rights and equality in Ireland and build a culture of respect for human rights, equality and intercultural understanding across Irish society.

Legal grounds covering discrimination

The Equal Status Acts 2000-2015, prohibit discrimination in the provision of goods and services, the provision of accommodation and access to education, on any of the nine grounds set out below. The Equality (Miscellaneous Provisions) Act 2015 has inserted a tenth ground in the provision of accommodation only; the "housing assistance" ground. The Acts outlaw discrimination in all services that are generally available to the public whether provided by the state or the private sector.

The Nine Grounds

Discrimination is the treatment of a person in a less favourable way than another person is, has been or would be treated in a comparable situation on any of the following nine grounds:

Gender Ground

There can be no discrimination between a man, a woman or a transsexual.

Civil Status Ground

There can be no discrimination between a single, married, separated, divorced or widowed person.

Family Status Ground

There can be no discrimination due to pregnancy, being a parent, guardian or carer.

Sexual Orientation Ground

There can be no discrimination against a person who is heterosexual, gay, lesbian or bisexual.

Religion Ground

There can be no discrimination where a person has a different religious belief, background, outlook or none.

Age Ground

There can be no discrimination due to a person's age (does not cover people under 18 unless it relates to vocational training).

Disability Ground

There can be no discrimination due to physical, intellectual, learning, cognitive, emotional or medical disability.

The Ground of Race

There can be no discrimination due to race, skin colour, nationality or ethnic origin.

Traveller Community Ground

There can be no discrimination against people who are identified as travellers.

The Acts also prohibit discrimination against a person on the basis of association with another person, acting as a witness on behalf of that other person, giving evidence on their behalf, legally opposing an act which is unlawful under the Acts, or who has given notice of an intention to take any such actions.

Terms direct and indirect discrimination

Direct Discrimination

Direct Discrimination is where a person is treated less favourably than another in the same situation or circumstances. The thrust of the legislation is that decisions cannot be made, or actions taken against a person because of, for example, their skin colour or because they are gay. While there may be various forms of discrimination in society generally, the legislation specifically sets out to protect those who can be identified under the nine grounds.

Indirect Discrimination

Indirect Discrimination is where a person is treated less favourably as a result of requirements that they may find hard to satisfy. An historical example is where a height requirement may be specified in a job application, the requirement may automatically exclude the vast majority of woman from the position and in reality the job does not require this condition. While there may be occasions where certain criteria can be set, it must be justified and proven to be relevant.

Discrimination by association

Where a person is treated less favourably because they are associated with or connected to another person who comes under the nine grounds. This is where, for example, a friend or relative of a person who falls under one of the grounds may be victimised due to that relationship or association.

Harassment and sexual harassment and the related behaviours

Harassment is defined as any act or conduct that is unwelcome and offensive, humiliating or intimidating on a discriminatory ground. Another definition used is “unwanted conduct that has the purpose or effect of violating a person’s dignity and creating an intimidating, hostile, degrading, humiliating or offence environment for the person”.

As a general rule harassment is decided upon by the victim or target of the behaviour. If a person feels harassed then the actions are unwelcome and unwanted and must cease, the opinions of the perpetrator or any third party is less relevant.

Behaviour that is unintentional or misinterpreted such as a once off remark or ill thought out gesture, once corrected may not be considered to be harassment as long as it is not repeated.

Unwanted physical contact, verbal abuse, intimidation, offensive language, abuse of position and bullying can all be forms of harassment, also behaviour such as making fun of someone, name calling or placing people in embarrassing situations can be harassment.

Sexual harassment

Sexual Harassment is any unwanted physical intimacy, requests for sexual favours, spoken words and gestures and the display or circulation of written words, pictures or other materials.

Besides the obvious forms of unacceptable behaviour such as inappropriate physical contact, for example touching or making suggestive sexual comments or propositions, other behaviour such as jokes of a sexual nature or circulating questionable images can be viewed as sexual harassment.

Equally, the fact that the behaviour may be inoffensive to one person does not justify the behaviour.

Perhaps the worst form of harassment generally and sexual harassment in particular is when it is carried out by anyone in a position of authority against someone in a lesser position.

Social media has added a new dimension to area, it must be clear that harassment, bullying and intimidation will still be deemed to have taken place and social media is not excluded, nor are text or e-mail messages or images.

The Equal Status Acts falls under the category of civil law and provides for redress in the form of compensation or specifying that a certain course of action be taken.

Criminal Considerations

Some of the actions and behaviour described may also lead to a criminal prosecution. For example, the Non-Fatal Offences against the Person Act 1997 creates an offence of “harassment” where a person causes alarm, distress or harm to others by following, watching pestering or communicating with them. The more serious offences can, on conviction lead to up to 7 years in prison. Other behaviour or actions may constitute an assault in criminal law.

Disability

The term “Disability” is defined in the Disability Act, 2005 as:

“In relation to a person, means a substantial restriction in the capacity of the person to carry on a profession, business or occupation in the State or to participate in social or cultural life in the State by reason of an enduring physical, sensory, mental health or intellectual impairment”. This act is only relevant to Public Service bodies.

The vast majority of protection in law for those with disabilities falls under the Equal Status Acts 2000-2015 as described in the previous section.

Bullying

In Ireland there is no criminal offence of “Bullying” and legislation that refers to bullying as an action is related to the workplace, coming under health and safety regulations. The Health and Safety Authority defines bullying as:

“Repeated inappropriate behaviour, direct or indirect, whether verbal, physical or otherwise, conducted by one or more persons against another or others, at the place of work and / or in the course of employment, which could reasonably be regarded as undermining the individual’s right to dignity at work”.

Bullying is described in a previous section as a form of harassment, which is covered under Equal Status legislation, and the behaviours can be similar such as the use of aggressive or obscene language and intimidation. Both bullying and harassment can have very serious negative impacts on the victim; it is common for victims to become isolated and withdrawn sometimes leading to long term psychological damage.

An isolated incident of the behaviour described in this definition may be an affront to dignity at work but as a once off incident is not considered to be bullying.

Racism

There are numerous definitions of the term “Racism”. Prejudice or discrimination against someone of a different race or a belief that each race possesses inherently different characteristics are examples of some wording. All definitions however agree that racism is based on a fundamental belief that one’s own race is superior. Racism by definition is not always a simple person to person individual belief but can be a societal and institutional level issue.

As with civil law under the Equal Status Acts, Racism as an offence does not feature in Irish criminal law directly. A number of pieces of legislation reference “Race” and in particular racially motivated crime which is considered by courts as a more serious offence. The following legislation does seek to address some of the issues associated with racism under a broader category of hate crime.

Prohibition of Incitement to Hatred Act, 1989

Hatred means hatred against a group of persons in the state or elsewhere on account of their race, colour, nationality, religion, ethnic or national origins, and membership of the travelling community or sexual orientation.

While not directly a piece of legislation covering racism, the Act covers broadcast, distributing, publishing, recording and written material deemed to threatening, abusive or insulting and intended to or likely to stir up hatred against the categories mentioned above which includes Race. These are criminal offences and on conviction can lead to fines and imprisonment of up to two years.

Prohibiting behaviour covered by equality legislation

Changing the beliefs of individuals; and the culture of communities and broader society is not easy and may not always be possible. Negative attitudes to travellers or foreigners, for example, can be difficult to change at an individual or community level. This means that Governments internationally feel it necessary to address the growing problems under equality generally through legislation. In Ireland the legislation is mainly civil and based on the nine grounds mentioned previously.

This legislation makes it clear that certain behaviour and actions against certain people is unacceptable and not tolerated in this society. While individuals and indeed communities have a responsibility to abide by the laws of the land, it is also important that employers and managers of businesses and premises ensure that the legislation is understood and enforced. This is particularly relevant to those front line employees dealing directly at service delivery level. It is the ultimate responsibility of management to ensure that all those under their control understand what levels of behaviour are unacceptable and take appropriate action when necessary.

B.4 Explain private security industry regulations and legislation

Learning outcomes are designed to enable candidates understand the private security industry, its role and its sectors and range of services. By the end of this section you should be able to:

- Describe the impact of private security regulation
- State the aim and purpose of licensing
- Explain the different types of licences
- Explain the powers of a PSA inspector and outline the statutory powers they have
- Describe the actions the PSA can take when non-compliance is found
- Summarise the main elements of private security licensing legislation

Impact of Regulations

The original legislation and subsequent regulations are designed to ensure that companies and individuals providing services in the private security industry operate to standards and comply with legislation generally.

A feature of this is the setting of mandatory standards; the Authority has prescribed certified quality management system standards for contractors and accredited training standards for individuals. A criminal record check is also carried out before a licence is issued. The fit and proper person guidelines summarised further on in this section states clearly a number of other requirements of the licensing process, with particular emphasis on compliance with other relevant legislation.

The impact of the licensing regime has brought change to the industry which previously adopted a voluntary system where some companies operated to a standard and some training took place. All licensees must now operate to same standards as a minimum. Audits by approved certification bodies and visits by PSA inspectors help ensure that the requirements are maintained.

The public benefit by having access to a regulatory authority that can investigate and adjudicate on any complaints made, for example, on the performance or behaviour of individual licence holders. Security officers must display identification while on duty, adding confidence to the public and end users.

End users or clients of the industry also have access and may complain or comment on the nature or quality of the service provided to them.

End users or clients of the industry must use PSA Licensed Contractors and or licensed individuals to provide security services to them. It is an offence under the Private Security Services Act to use unlicensed contractors or individuals.

The PSA publish a register of all licence holders and provide information of suspensions and revocations, this information is beneficial to end users and the public.

The licensing regime and has more clearly defined the known industry and has created barriers to undesirables who here-to-fore may have entered the industry unchallenged.

Purpose of Licensing

Legislators when considering drafting and enacting laws of this nature consider the primary purpose to be “in the public interest”.

The PSA on establishment expanded on this by stating:

“Our purpose is to instil customer and public confidence in this multi-stranded, multi-faceted business with the introduction, control and management of a comprehensive, standard driven, licensing system for all individuals and companies involved in the industry and to do so in a manner that is sensitive to the needs of the market”

It is the aim of the Authority to use the statutory regulation and enforcement powers provided to it to introduce positive, fundamental change to the industry.

Section 2 of Private Security Services Act sets out the activities which are licensable by the PSA, these are:

- Door Supervisor
- Installer of Security Equipment
- Locksmith
- Private Investigator
- Provider of Protected forms of Transport
- Security Consultants
- Security Guard
- Supplier and Installer of Safes

Definitions of what is licensable for each sector are prescribed by regulations signed by the Minister for Justice and Equality.

Individual Licensing

Individuals working within the industry are the frontline staff dealing on a day to day basis with the client, customers of the client and the general public.

Because of this individuals have tended to be a priority for licensing in most jurisdictions, Ireland is no different. The PSA determined that licensing of individuals, particularly in the guarding services would be a priority.

This was addressed at the early stages of the introduction of licensing in Ireland to ensure that frontline staff were trained to a recognised standard and had to undergo a screening and vetting process performed by their employer.

There are three categories of licenses available for individuals working in the Guarding Services sector.

- Door Supervisor (Licensed Premises) Licence (An individual who provides security services as a door supervisor at or in the vicinity of a licensed premises)
- Security Guard (Static) Licence (An individual who as a security guard guards property for the purposes of preventing loss, damage or waste by crime, fire, carelessness or flood)

- Providers of Protected Forms of Transport (Cash-in-Transit) Licence (An individual who carries out vehicular transportation of cash, processes cash, handles cash in a secure vault and related activity)

Each licence is specific to the category above; for example, individuals cannot work as Door Supervisors if they only hold a Security Guard licence.

Individuals can apply for a licence for more than one category.

Licensing is applicable to those active in the private security industry, members of the Garda, military and state or semi employees generally are exempt from these requirements.

Powers of a PSA Inspector

The Private Security Authority as a statutory body has responsibility for licensing and regulating the private security industry. Legislation bestows extensive powers to the Authority, including, but not limited to investigating security services being provided by any person, investigating complaints and taking action.

Warranted* PSA Inspectors have substantial powers. They may enter, inspect, examine and search anywhere the inspector has reasonable cause to believe that a security service is being provided. This includes unannounced visits to premises to ensure the security staff members are licensed, are wearing and displaying their PSA licence in the prescribed manner. Inspectors are entitled to inspect licences during these visits.

*Warranted means an officer with the legal authority to carry out certain functions.

PSA inspectors also carry out audits on licensed contractors to confirm compliance with standards and licensing requirements. These audits are normally arranged by appointment and take place at the contractor's place of business. The inspector may review documentation; such as service contracts, personnel files etc. and can take away copies of documents related to the provision of security services if required.

A report will be provided to the contractor and where required non-compliances must be resolved within the timeframe determined by the inspector.

¹ *Warranted means an officer with the legal authority to carry out certain functions.

PSA Sanctions

Following upon the results of investigations or inspections, The PSA have a range of sanctions which can be used for both individuals and contractors when non-compliance is found, as follows:

- Issuing reprimands, caution or advice
- Refusing, suspending or revoking licences
- Refusing renewal of licences
- Instigating prosecutions of alleged offences under the Act (Prosecutions can lead to substantial fines and ultimately imprisonment on conviction)

B.5 Outline responsibilities and obligations under Irish Data Protection legislation

Learning outcomes are designed to enable candidates understand the private security industry, its role and its sectors and range of services. By the end of this section you should be able to:

- Explain the role of the Data Protection Commission
- Outline the relevant main provisions of the Data Protection Acts
- List all the rules for Data Protection
- Outline the interaction between Data Protection requirements and use of CCTV and other technology
- Explain the importance of an awareness of security, confidentiality and data protection issues when using communications and computer equipment
- Explain the importance of treating information received with discretion and the responsibilities in maintaining security of information

Role of the Data Protection Commission

The role of the Data Protection Commission is to ensure that those who keep personal data comply with the provisions of the Acts.

The Commission describes its mission as:

“Protecting data privacy rights by driving compliance through guidance, supervision and enforcement.”

The Data Protection Commission does this by:

Conducting Investigations

The Commission may investigate complaints from individuals or may instigate an investigation whenever it is considered appropriate.

The Commission is obliged to seek an amicable resolution to complaints. Investigations usually take the form of privacy audits. Notice of audits is typically given as the Commission’s initial focus is to assist with improvements in practices.

The Commission does have further sanctions available in the event of serious breaches or failure to implement recommendations.

Obtaining Information

The Commission can require any person to provide information deemed necessary. The Commission exercises this power by providing a written notice, called an “Information Notice” to the person. The Acts provides for offences in the event of failure to comply with the notice or providing false or misleading information.

Issuing Enforcement Notices

The Commission may issue an “Enforcement Notice” to a data controller or data processor directing them to take whatever steps the Commission considers appropriate to comply with the Acts.

Prohibiting Overseas Transferring

The Commission has the power to prohibit the transfer of personal data from the State to a place outside the State. This power is exercised by providing a written notice called a “Prohibition Notice” to the data controller or data processor.

Powers of Authorised Officers

The Commission may appoint “Authorised Officers” to enter and examine the premises of a data controller or data processor, in the course of, for example, an investigation. The Authorised Officer has the power to:

- Enter the premises and inspect any data equipment there
- Require the Data Controller, Data Processor or staff to assist in obtaining access to data, and to provide any related information
- Inspect and copy any information
- Require the Data Controller, Data Processor or staff to provide information about procedures on complying with the Acts, sources of data, purposes for which personal data are kept, persons to whom data are disclosed, and data equipment on the premises.

Appeals processes are in place.

Sanctions

Penalties apply to both controllers and processors found to be in breach of the GDPR. There are different penalties, depending on the importance of the breach.

Serious infringements

For the most serious infringements (for example, not having sufficient customer consent to process data or violating the core of privacy by design concepts) organisations can be fined up to 4% of their annual global turnover or €20 million, whichever is greater.

Member states may introduce further fines legislation, which will be enforceable within that state only.

Lesser breaches

Under the GDPR, organisations in breach of the Regulation can be fined up to 2% of their annual global turnover or €10 million, whichever is greater, for lesser breaches. Some examples of lesser breaches include: not having records in order, not notifying the supervisory authority and data subject about a breach or not conducting impact assessment.

Data Protection Legislation

The office of the Data Protection Commission was established by the Data Protection Acts 1988 to 2018 (“the Data Protection Acts”).

Under the GDPR and the Data Protection Acts, the Commission is responsible for monitoring the application of the GDPR in order to protect the rights and freedoms of individuals in relation to processing.

The Acts set out the law in relation to:

- Collection, processing, keeping, use and disclosure of personal data
- Processing of personal data
- Processing of sensitive personal data
- Security measures for personal data
- Fair processing of personal data
- Right to establish existence of personal data
- Right of access
- Restriction of right of access
- Right of rectification or erasure
- Right of data subject to object to processing likely to cause damage or distress
- Rights in relation to automated decision making
- Duty of care owed by data controllers and data processors
- Disclosure of personal data in certain cases

The Acts established the Office of the Data Protection Commission

The Data Protection Commission states that the Acts:

“Set out the general principle that individuals should be in a position to control how data relating to them is used”

The Eight Rules for Data Protection

There are eight rules for Data Protection; the following is a brief summary of some of the main requirements of each rule.

1. Obtain and process information fairly

Individuals who are asked to provide information should know; who is collecting it, why is it being collected, what is it being collected for and who else may be given access to the information.

2. Keep it only for one or more specified, explicit and lawful purposes

The purpose for each set of data must be precise, specified and must be lawful, the purpose must be known to each data subject. Data Controllers and Data Processors are required to register with the Data Protection Commission

3. Use and disclose it only in ways compatible with these purposes

Do not use the data for any other purpose, the conditions under which the data subject provided the information must be respected, particularly with regard to disclosing the information to anyone else.

4. Keep it safe and secure

High levels of security are essential for all personal information and in particular information that is regarded as sensitive. Security procedures are covered in other sections of this document.

5. Keep it accurate, complete and up-to-date

Procedures must be in place to ensure that data held remains accurate, this requires a periodic review and audit of all personal information held.

6. Ensure that it is adequate, relevant and not excessive

Data is collected and held for a specific purpose, it must be justified as necessary. This means no information is held that is not needed for that purpose at that time. This is particularly relevant when dealing with sensitive or personal information.

7. Retain it for no longer than is necessary for the purpose or purposes

The information cannot be kept for longer than is absolutely necessary, there must be a good reason for retaining personal information and reviews or audits should indicate when certain information is no longer necessary. This information is then deleted from computer files. In the case of paper records these are destroyed.

8. Give a copy of his/her personal data to an individual, on request

Any individual is entitled to know what data relating to them is held. This right to access involves an individual writing to a data controller and requesting a copy of the data held. The applicant will have to provide sufficient details to allow a data controller source information held, if any. The results of a request for information may lead to the applicant demanding that inaccurate information be rectified or erased. In certain circumstances the applicant has the right to have all data removed. There are some exceptions such as criminal investigations or certain medical data.

Data Protection and CCTV

Closed Circuit Television or CCTV systems involve the processing of personal data and therefore must operate in compliance with the Acts.

The use of CCTV systems has greatly expanded in recent years. So has the sophistication of such systems. Systems now on the market have the capacity to recognise faces. They may also be capable of recording both images and sounds.

The expanded use of CCTV systems has society-wide implications. Unless such systems are used with proper care and consideration, they can give rise to concern that the individual's "private space" is being unreasonably invaded.

The Commission states that a data controller needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The terms used are adequate, relevant and not excessive. The data controller must question what the system is used for and determine if this is reasonable under the circumstances.

The Commission expects that a data controller would have carried out detailed assessments as to how the use of such equipment meets requirements. It is expected that the following steps have been carried out and documented:

- A risk assessment
- A privacy impact assessment

- A specific data protection policy drawn up for use of the devices in a limited and defined set of circumstances only (this policy should include documented data retention and disposal policy for the footage)
- Documentary evidence of previous incidents giving rise to security / health and safety concerns
- Clear signage indicating image recording in operation

The Acts also requires that certain essential information is supplied to a data subject before any personal data is recorded. A written CCTV policy must be in place and should include the following information:

- The identity of the data controller
- The purpose for which data are processed
- Any third parties to whom the data may be supplied
- How to make an access request
- Retention period for CCTV
- Security arrangements for CCTV

Historically CCTV was primarily used for clear security purpose, simply monitoring a fence, gate or door for unauthorised access. While this remains the most popular use of CCTV, it no longer is the only use. The quality, scope and versatility has led to use which can be described as intrusive. A common example is the excessive monitoring of employees, including data controllers attempting to justify its use in toilets, smoking areas and rest rooms where people can have an expectation of privacy.

Furthermore, systems have had the original purpose extended as a cost cutting measure to replace the traditional forms of supervision and management of staff, leading to continuous permanent and invasive monitoring of staff activity.

The Data Protection Commission uses the term “proportionality” in the context of data collection and the Acts uses the terms “adequate, relevant and not excessive”. This places the onus on data controllers to justify the reasons for the use of equipment that captures images or records voices.

Justification must be evidence based. Where a system is installed for security or safety reasons there should be a history of incidents or an independent review and recommendation. Once installed for that purpose the data collected cannot be used for other reasons without a review and justification for the extended purpose. Equally, where a camera is positioned for a specific purpose, it should not be placed in such a way as to capture a large volume of other data not relevant to that purpose.

The previous section relates to internal justification. Collecting large volumes of data is particularly a concern when dealing with members of the public who also have a right to privacy. CCTV is used more and more as a security tool and the quality, functionality and recording capabilities of modern systems can easily either innocently or purposely cause data protection concerns.

Headsets or other body worn cameras, including the additional feature of a microphone can be particularly invasive. By their nature these devices are flexible and

mobile and sometimes discreet. It is essential that the need for the use of these devices is justified and that potential data subjects are made aware through, for example, clear signage. Data collected must be relevant to the purpose and data must be kept only for as long as necessary.

Voice recording is considered particularly intrusive and data subjects are entitled to clear warning in these environments. The traditional notice informing of CCTV in operation is not sufficient as any reasonable person would consider this to relate to images only.

The additional feature of compatibility with the Internet increases these concerns, due to the risk of hacking data bases. The responsibilities of the data controller are therefore intensified to ensure the protection of privacy.

Data controllers must avoid the collection of large volumes of data from members of the public going about their normal business including shopping or social activities. This is particularly important when the public may not be aware of the presence of cameras or microphones.

Consideration must be given to privacy issues when deciding on the installation of systems at design stage. These considerations include the reasons for the type of equipment and the locating of equipment.

A breach of the Data Protection Acts may take place where the collection of data cannot be justified.

Before proceeding with such a system, it should also be certain that it can meet its obligations to provide data subjects, on request, with copies of images captured by the system.

The use of covert systems is generally unlawful unless the purpose is related to criminal or civil proceedings. This is regarded as a once off matter based on evidence and subject to a specific written policy. Permanent covert surveillance is unacceptable.

Security companies who operate cameras on behalf of clients are considered to be data processors. As data processor they operate under the instructions of data controllers (their clients).

Rights also apply to photographs and voice recordings.

Data processors must have security measures in place to prevent access to, or unauthorised alteration, disclosure or destruction of the data.

Measures must be in place to protect data that is transmitted over a network. Collecting data is only one aspect, as with staff of the data controller mentioned in an earlier section, staff of data processors must be made aware of their obligations in regards to safeguarding and disseminating data held.

While other privacy legislation may be relevant, as a general rule these Acts do not apply in a domestic environment. Equally, community CCTV schemes are the authority of the Garda Commissioner, under different legislation.

Retention periods are not specified; however the Acts state that data shall not be kept for longer than is necessary for the purpose for which they were obtained. While a general convention for security systems is one month retention, a data controller must justify any period of retention.

Relevant data subject of an investigation may be kept for the period of that investigation.

Any person whose image is recorded on a CCTV system has a right to seek and be supplied with a copy of their personal data from the footage. Where images of parties other than the requesting data subject appear on the footage, the data controller must pixelate or otherwise redact or darken out the images of others before releasing the data.

Requests for access to certain specified data by the Garda is a common feature. There are two aspects to this:

- There are no specific data protection concerns where a Garda visits the premises of a data controller to view footage without taking anything away.
- A Garda taking footage away is more serious and should, except in an emergency, be subject to a written request. It is the responsibility of the data controller to verify that the request is genuine and the transaction is recorded.

As with previous sections, the data must always be kept secure.

Security and Confidentiality Issues

Security and confidentiality are important features of the Acts; this is reflected also within the eight rules for data protection. The Acts states that where the processing involves the transmission of data over a network, the Data Controller can be regarded as the person in charge and shall ensure that the measures provide a level of security appropriate to:

“The harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, the data concerned, and the nature of the data concerned”

The type, volume and nature of the data are features, appropriate measures means that security levels must be commensurate with the risk. A large volume of data classed as sensitive is naturally a higher risk.

The next section will provide more in-depth information on discretion and security.

Security Guidelines

While no particular measures are prescribed, the Data Protection Commission has published security guidelines for electronic storage and processing of data, which are summarised as follows:

The Law

Those handling data should understand the legal requirements.

Policies

The organisation should have policies in place, starting with data collection and retention to ensure only what is necessary is collected and held. Further policies thereafter are required for all other activity.

Access Control

Access is granted only to those who “need to know” the information. Policies and procedures must include the decision process used to grant access to the data.

Access Authentication

This is the second step in access control; those who are entitled to have access must have a unique identifier such as a token or password. Levels of access may feature also depending on the nature of the data. Access control logs or records should be capable of identifying individual users who access data.

Automatic Screen Savers

Where screens are left unattended screen savers should be activated, automatic locking or closing down may be necessary depending on the working environment and the nature of the data on view.

Encryption

This is a higher level of protection where plain text is converted to cipher text requiring a password to decrypt it.

Anti-virus Software

Software used to prevent infection from files downloaded through e-mails or websites or memory sticks. Ideally procedures should be in place to limit downloading of external files due to the risks involved.

Firewalls

This is software that prevents or blocks unauthorised traffic accessing a network.

Software Patching

These are updates installed to fix potential security concerns.

Remote Access

Where staff have access to data from a remote location the risks can be increased, where remote access is unavoidable additional measures will be necessary to manage access to the data.

Wireless Networks

As with remote access, wireless networks, particularly unsecured WiFi networks are more vulnerable and require protection.

Portable Devices

Due to the portability this equipment is more vulnerable to theft and accidental loss, encryption is very important to protect data held on portable devices. The use of portable devices in the first place must be deemed essential.

Logs and Audit Trails

This means having in place processes to identify those who gain access to data. It includes a detailed record of changes made.

Back-up Systems

These are systems which copy or archive data, should any or all of the original data be lost a duplicate or secondary record is available, ideally kept in a separate location.

Incident Response Plans

Organisations are expected to anticipate something going wrong and have a plan in place. The Commission has published a code of practice for a security breach which provides information and guidelines on dealing with an incident. All incidences and complaints should be thoroughly investigated and the results used to prevent reoccurrence and improve processes.

Disposal of Equipment

Levels of technology beyond desktop and portable computers, in particular the increasing use of devices such as smart phones and indeed modern photocopiers all of which can store data creates problems when these devices are deemed obsolete or redundant. While reuse and recycling, particularly for charitable purposes, is encouraged, extreme caution must be taken to ensure that all data is removed from all devices. A destruction policy is necessary where there is any risk of the data being vulnerable.

Physical Security

While the emphasis on protection measures described above is centred on the physical equipment, basic security safeguards are also essential to assist with access to equipment and also hardcopy or paper files held in manual systems. Physical security measures are ideally for the entire facility, but as a minimum the areas where data is processed or stored. This includes:

- Perimeter protection, secure doors and windows, quality locking devices
- Control of access of people coming into and moving around a facility, including contractors
- Monitoring and managing staff movement
- Use of security technology such as access control, CCTV and intruder alarm systems
- Lockable secure cabinets for paper and other physical records
- Shredding and other destruction processes

The Human Factor

Basic security safeguards include the human factor, this includes:

- Safeguarding passwords
- Precautions before opening up unscreened attachments
- Precautions when connecting to, or inserting personal devices including memory sticks to reduce the risks of hacking or other forms of attack
- Discussing or sharing confidential information or processes with unauthorised persons or anyone outside of the organisation, staff integrity and discretion is essential
- Ensure that those with access to data have no vested interest

- Controls must be in place, they must be known and enforced; clear instructions, written procedures, training and familiarisation are critical features of this as is clear lines of authority
- Restrict the use of personal devices such as smart phones; ideally the only equipment used for storage of data remains the property of the organisation.
- Ensure, as highlighted at the start of this section that staff understand the law and their personal obligations.
- Monitor and control the use of photocopiers and scanning equipment, this includes restrictions on personal cameras.

Pre-employment vetting of staff and disciplinary procedures also feature.

Discretion

Discretion or exercising good judgement are important attributes of those who handle data and particularly sensitive information. This is more relevant to those within the security industry, as there is an expectation that information is handled with tact and discretion. Sharing information internally or in particular externally are serious breaches of the Acts and the responsibilities and ethical standards of security personnel.

Sharing information in this context is not limited to paperwork, video images or voice recordings but also includes any discussions in any forum on the nature of personal information covered under the Acts.

C.1 Outline the role of a monitoring centre

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Describe the physical characteristics of a monitoring centre
- List the different types of monitoring activities that can occur, and identify which activities are licensable
- Outline the functions of a monitoring centre

Characteristics of a monitoring centre

A monitoring centre is a secure facility from which monitoring can take place. Its principle role is that it can remotely monitor, store and respond to incidents on a client's premises. To do this, the centre itself must be physically and operationally secure. The monitoring facility should have:

- Physical access control systems to prevent intrusion or unauthorised access
- Robust data storage and security systems
- Backup and contingency facility for a range of emergencies, from a physical and information security perspective.

In practical terms this means the monitoring centre should be covered by:

- Intruder alarms
- Electronic and manual access control
- Fire alarm systems
- Fire suppression systems
- CCTV
- Electronic security measures
- IT security measures
- Backup power and network infrastructure
- Remote monitoring capability.

Ideally, the monitoring facility should be a standalone and not a shared facility, accessible only by the security firm and its employees.

Monitoring activities

Various types of monitoring activity can take place in a monitoring centre, including:

- Fire alarm monitoring (domestic and commercial)
- Intruder alarm monitoring (domestic and commercial)
- CCTV monitoring (domestic and commercial)
- Personal alarm monitoring
- Electronic access control
- Petrol pump monitoring.

Under the Private Security Authority (PSA) standards, certain monitoring activities are licensable under PSA 33: 2013. Monitoring of any CCTV or alarm system – including fire, intruder or personal – is a licensable activity. Ancillary activities such as providing remote access or petrol pump sale approval are not licensable (unless CCTV monitoring is used), but these are rarely the main activity of a security firm. The licensing standard also applies specifically to remote monitoring centres. Using an on-site security control room to monitor CCTV or alarms is not a licensable activity.

Functions of a monitoring centre

Because of the diverse range of monitoring activity that can be provided, a monitoring station can serve a variety of functions, including:

- Provide remote monitoring of CCTV. CCTV can be monitored safely from a secure off-site location. This provides peace of mind to clients, who can be assured that their site is being monitored but at no risk to staff who otherwise would be on site.
- Provide remote monitoring of alarms. A variety of alarms can be monitored and responded to. This provides clients with an intermediary who can receive and assess alarms on their behalf. The client can be kept informed of alarms at multiple premises, with designated responses for different types of alarms and premises.
- Provide a communications system to on-site personnel. On-site security operatives or lone workers can be protected through regular communications and check-ins. This ensures both the safety of staff and an emergency response to potential issues.
- Reassure vulnerable clients that they have help at the end of a phone line if they need it.
- Liaise with emergency services in the event of incidents or alarms.
- Provide a secure method of access control to buildings that are unoccupied or require remote access management.

Monitoring centre guidelines

The appearance, contents and effectiveness of a monitoring centre control room reflect the security team. It is a professional space and should be treated and appear as such. This means there should be a clear desk policy, and it should be acknowledged as a work area. A few general guidelines are outlined below.

- The clock in the control room is the time the security operation uses. This is the time that all incidents and communications are recorded at. This ensures a consistent approach to recordings of incidents, CCTV footage, alarm signals, etc. With automatic date and time stamping on electronic systems, it is important that all manual entries correspond to this time.
- All signing in/out to be done at the control room. This includes attendance sheets, equipment registers, keys and vehicles. This means there is a single control point for all equipment and operatives, where the status and location of all security assets is readily available.
- No eating or drinking. The security control room is a professional space – not a canteen. It should not be used for welfare breaks or lunch breaks. These affect the professional appearance of the control room and distract the control room operator from their duties. However, the security control room is often also the designated staff welfare point, where meal-making and toilet facilities are provided. Where this is the case, it should be done in a designated area away from the work space.
- Condition of control room should be part of the handover if multiple shifts are operating. The handover should include a detailed report on all operatives on site, incidents to report, and the status and condition of equipment.

C.2 Outline the general procedures in a monitoring centre

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Outline the reasons the control room is regarded as a secure environment, and outline the operation of access control systems in that context.
- Explain the procedures for dealing with authorised visitors to the control room.
- Outline the actions to be taken if unauthorised access to the control room is attempted.
- Demonstrate how to carry out functional checks.
- Demonstrate the use of keypads and joysticks to operate the cameras, monitors and associated equipment.

The control room

The security and integrity of the control room and its processes are vital elements of any monitoring centre. Clients need to be assured that their security systems are themselves being monitored securely and are receiving the quality of service they are paying for. Also, the nature of work in a control room could make it a target for criminal acts, so the work there must be done in a secure manner.

The security of the control room and the entire monitoring centre starts at the perimeter. The building itself will have good physical access-control facilities in place, including:

- Fencing
- Barriers
- CCTV
- Passive intrusion detection
- Electronic or biometric access control.

Employees will be issued with appropriate access-control methods, such as swipe cards, or set up on biometric systems such as thumb scans or retina scans. Vehicles will be stopped at automatic barriers, and only authorised vehicles should be allowed access to the area. Layers of access control will be in place to ensure that unauthorised visitors are stopped at a number of points.

Visitors

Authorised visitors should only be attending the control room by pre-arranged appointment. Visitors and contractors should be in the habit of calling the control room in advance of a service visit and confirming the names of the people attending and the make, model and registration numbers of any vehicles. Guests of employees and management should also be noted in advance, with the same details, in an expected visitor log.

When a visitor arrives at the first access control point, they should identify themselves via intercom or telephone to the control room. The control room can then cross-reference them against the expected visitor log. If they are not listed on the log, the control room may try to contact their employer or contact person to verify their identity before allowing them access to the premises. Once a visitor arrives at the main door, they should be met by a member of staff – preferably in a secure area segregated from the main control room.

The visitor should be signed in a visitor log and briefed on site safety. The briefing should include safety topics such as evacuation, and security topics such as the prohibition of phones and recording equipment in the control room. All visitors should be given a visitor's badge that clearly identifies them. Visitors should have a place to put belongings such as coats and bags outside of the control room. Visitors should be escorted by a staff member at all times while in the control room. When the visitor is finished, they should be escorted back to the entrance point, where they can collect their belongings and sign out. Some control rooms may have a search clause in their visitor procedures which allows security operatives to search the belongings of visitors as a condition of entry.

Unauthorised visitors

If a visitor is not expected, and their identity or reason for visiting cannot be verified, they should be politely refused access to the premises at the entrance gate or main entrance via intercom. Security staff should avoid physically going to meet the visitor. If the visitor persists in wishing to enter, or tries to force entry to the control room, then the situation should be escalated to management. The control room may initiate lockdown procedure, locking all access points and returning staff to their desks. The visitor should be instructed firmly to leave or the Gardaí will be called. If the visitor still refuses to leave, then the Gardaí are called. Security operatives should never put themselves at risk by trying to physically prevent an unauthorised visitor from gaining access.

Functional checks

Functional checks are conducted at the start of shift to ensure that all the equipment the security operative will be using is working and that all paperwork is up to date and completed. On arrival, the security operative will complete the handover documentation with the previous shift, and note any issues or equipment failures from the previous shift. The operative should check that each monitor and camera is working and complete the CCTV functional checklist. They should ensure that all recording equipment is working and note the condition of the workstation. Any issues should be noted and brought to the attention of management.

The function of the joystick or keyboard should also be checked, and each operation should be tested to ensure it works. All required documentation should be checked as present, and the logs should be checked as up to date.

It is important to carry out these functional checks at the beginning of each shift, so the security operative can be sure that all equipment is operational, and so the company and clients can be made aware of faults as soon as possible.

Joypads and keypads

CCTV systems are controlled by joypads and keypads, which allow users to interact with the system in a simple and effective way. The joystick usually allows the user to select and observe a set of cameras from a particular site, then an individual camera from that site. It also allows the user to switch between multiple monitors and sites on the same system. Where the system contains PTZ (pan, tilt, zoom), these can be moved as required, using the joystick, to track and observe incidents. The security operative must be fully aware of the functionality of the joystick or keypad they are using. Many systems will have additional advanced functions to help the security operative in complex monitoring tasks.

Electronic aids to monitoring personnel

Advances in security technology are occurring every day to help security operatives perform their duties. These complement existing CCTV systems and give operatives additional support to make them effective in their role. These technologies include:

- Automatic number plate recognition (ANPR)
- Biometric recordings, such as facial recognition
- Thermal scanning
- Intercom systems.

C.3 CTV Systems and Operating Procedures

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Describe the purposes of a CCTV system.
- Summarise how the components of a CCTV system works.
- Discuss how weather, lighting and poor positioning can affect camera images, and outline possible solutions to these problems.
- Demonstrate how to record images onto storage media.
- Demonstrate how to produce images for purposes of evidence and how to ensure their secure management.
- Outline how CCTV connects to the Alarm Receiving Centre.

CCTV system

A Closed-Circuit Television (CCTV) system allows video cameras to transmit images to a limited number of monitors in a closed circuit. With a CCTV system, a single person can monitor a large or complex area, both indoors and outdoors. The benefits of a CCTV system include:

- Deterring criminal activity
- Detection tool for early identification of criminal activity
- Evidence for the prosecution of criminal activity
- Identifying patterns of habitual incidents.

Components of a CCTV system

The components of a CCTV system include:

- Camera – CCTV cameras come in various shapes and sizes and have many different uses. They can be static cameras or PTZ cameras, bullet or dome design, overt or covert. Each has its own design features and uses, but its function is to gather and transmit visual images. The camera is the input for visual data.
- Monitor – The function of the monitor is to display the visual images in the monitoring station. It is the output stage for the images.
- Digital Video Recorder (DVR) / Network Video Recorder (NVR) – The function of the DVR is to process the images from the camera to the monitor. It also stores the images in a recorded drive for future access or downloading. The DVR/NVR software allows the cameras to be configured, named and set up. It can be connected to the internet to allow for remote access. The difference between DVR and NVR is that the DVR records wired or analogue cameras, while NVR works with wireless or IP cameras.

CCTV issues

CCTV cameras are a great security solution, but they can experience some issues which, if not anticipated, can reduce their effectiveness. Examples of this are:

- Poor lighting – If a CCTV camera is positioned in an area with no or poor lighting, it may not pick up effective images. Also, if a CCTV camera is positioned with a light shining directly at the lens, this can effectively “blind” the camera. Solutions include using CCTV cameras with night vision, or installing more lighting next to the CCTV camera, to light the area.
- Adverse weather – Heavy rain can cover the camera lens with water and obscure the image. It can also damage the camera in the long term. A solution is to install weatherproof housing around the camera with a non-smear glass lens to ensure that rain does not obscure the camera’s images.
- Poor positioning – If a camera is positioned incorrectly, the image may be obscured or blocked by debris or other items in the environment. This can be resolved by doing a thorough risk assessment before installation and removing potential blockages. The CCTV may also need to be repositioned, or mounted on its own standalone pole mounting.

Recording images to storage media

When a security operative is recording material to storage media, it is essential that they store it securely and maintain an access log to it. Where possible, data should be stored to a secure, password-protected drive – not to portable storage media unless necessary. When recording to storage media, the security operative should:

- Identify the correct dates, times and cameras required. No more than is necessary should be recorded.
- Select the relevant footage and save it to the storage media.
- Mark the file with a reference number, and record this number in a log.
- Create an access log to the file.
- Password protect or encrypt the file if necessary.
- If a copy must be created on portable storage media, the “master copy” should be kept on the drive, the “working copy” put on the portable media.
- Mark all copies of the recording with the date, time, and reference number.
- Make a written report of the recording being downloaded.

Producing footage for evidence

All information captured and downloaded will be retained on a secure drive, which will be password-protected as above. Any material required to support potential criminal investigation or prosecution will be retained until passed to the Gardaí via secure transfer.

Secure transfer involves copying the footage – both master and working copy – onto a disc and taking the following steps:

- This is signed for with an evidence release form and is passed into the data control protocol of the Gardaí. Where possible, the monitoring centre will request that the Gardaí submit a request in writing for download and transfer of CCTV and audio evidence (if applicable). Alternatively, the Gardaí can complete and sign the evidence release form with the required details, and the local manager can make an on-the-ground decision about the request.
- The original digital copy of the footage is held until the outcome of Garda actions or for two years, whichever is longer.
- A written record of the handover should be kept, detailing its date and time, the reference number of the data, and the Garda's details.
- An access log is kept of the footage until the footage is securely destroyed.

Transmitting CCTV to the monitoring station

Traditionally, CCTV on local sites would have been transmitted through coaxial cable or CAT 5/6 cable to the DVR on site, and recorded there. Modern systems, however, use the internet and wireless CCTV cameras to transmit signals off site to the monitoring centre. There are many video transmission methods, such as fibre optic, coaxial cable, microwave, phone lines, and radio frequency. The choice of depends mainly on factors such as distance, environments, cost and facility layout.

The CCTV in the monitoring centre itself will sometimes be traditional coaxial- connected analogue cameras, but off-site cameras will be some or all of:

- Co-axial
- Fibre optic
- PTSN
- ISDN.

PTSN and ISDN use telephone and internet lines to transmit signals over the net to the monitoring station. They are much quicker, better-quality and more cost-effective than the traditional options.

Modems

Modem stands for modulator and demodulator. This device helps a computer to transfer data over telephone lines. This is done by changing the digital data into an analogue signal that can be transferred over the phone lines (modulator function). At the receiver end, it converts the analogue signal back to digital data (demodulator).

Most monitoring stations have high-speed internet and secure modems, but the sites from which the CCTV signal is being transmitted will have a variety of modems installed. Generally speaking there are a small number of modem types:

- Cable/DSL modem
- ISDN

Modems will also be connected to routers, which allow multiple devices to be connected to the network and route all the data together back to the monitoring station.

C.4 Alarm Systems and Operating Procedures

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Explain the term “protected premises”
- Explain the term “verified alarm”
- Describe the purposes of an intruder alarm system
- Summarise how the components of an alarm system work
- Explain the term “perimeter protection” and give examples of types of perimeter protection
- Explain the term “physical protection”
- Explain the techniques used to verify alarms
- Outline what alarm filtering is, and explain alarm filtering procedures
- Outline the potential risks when responding to alarms, and state the general response required
- Explain procedures for dealing with false alarms
- Outline the benefits of prompt response
- Outline the various communication protocols for sending alarms
- Outline the various types of modems for transmission
- Explain how I.T. contributes to the functions of an alarm receiving centre

Protected premises

A protected premises is any premises protected by an alarm system. It can be a fire alarm detection system, with or without fire extinguishing, or intruder alarm protection.

Verified alarm

A verified alarm is an alarm activation verified by the activation of a secondary detection device as a sequential verified alarm, or by visual or audible inspection. The Gardaí have a policy of responding only to verified alarm calls from alarm monitoring centres.

Purpose of an intruder alarm system

The purpose of an intruder alarm is to deter unauthorised entry to a protected premises. If deterrence does not work and unauthorised entry is attempted, then the purpose of the alarm is to detect the intrusion at the earliest stage and alert the appropriate people. Alarms are used in commercial and domestic settings to protect against burglary, theft, trespass or criminal damage.

Components of an intruder alarm

Like any system, an intruder alarm has 3 phases. It has inputs which detect intrusion, a processor which processes the signal, and outputs in the forms of alerts. We will look at each separately:

Control panel: This is the brain of the intruder alarm. It takes the detection input and decides on the best output based on its programming. The control panel can also be addressed and configured to a user's needs. Modern alarm panels are addressable, which means that each unit on the system has a separate designation and the source of the detection can be narrowed to this single detector. It also means that the system sends a signal on a constant loop through all of the inputs to make sure they are working correctly. If a unit is not working correctly, it registers as a fault.

Inputs: Inputs are the detectors for the system. They detect intrusion and they input a signal to the panel. Inputs come in a variety of forms, including:

- Motion detectors
- Door/window contacts
- Vibration detectors
- Break-glass detectors
- Pressure sensors.

Based on the input received, the panel will decide on the next course of action.

Outputs: Alarm outputs are the signals sent from the panel to the most appropriate parties. They are designed as a means of alert, both locally and remotely.

- Bells or sirens
- Lighting
- Communications to alarm monitoring centre.

Perimeter protection

Perimeter protection uses detection inputs such as motion detectors to form a security perimeter around a premises. It is designed to alert the intruder alarm if a person enters the perimeter of the property, and it provides advance warning of intrusion. Perimeter protection can come in a variety of forms, including:

- Fence alarms
- Option detection alarms
- Pressure sensors
- Thermal alarms
- Links to CCTV system
- Vehicle sensors.

Physical protection

Physical protection comprises the physical barriers that prevent access to a premises and the supplementary detection systems that support them. Examples of access points to the premises include doors, windows and roof lights. Physical protection in an alarm context is the detection inputs that protect the physical barriers. These include:

- Door and window contacts
- Broken-glass detectors
- Vibration detectors.

Verifying alarms

An alarm must be verified by the alarm receiving centre before notifying the Gardaí. This can be done in a number of ways:

- When a secondary device is triggered on the same premises within a minimum timescale. For example, a motion detector on the grounds of the premises is activated, then a door contact detector is activated.
- The monitoring centre may use CCTV to verify the presence of an intrusion on the site.
- A call to an on-site keyholder who verifies verbally that there is a genuine alarm.

Gardaí require the presence of a keyholder to attend the premises in a reasonable time before attending an alarm call-out. If an alarm cannot be verified by a secondary device or CCTV, or a key holder cannot be contacted, then the Gardaí will not attend.

Alarm filtering

Alarm filtering is the process employed by an alarm monitoring station to reduce false alarms and ensure that the escalation of alarms is performed correctly. Many monitoring centres will have a minimum time for activation of an alarm for the site to acknowledge a false alarm or test and reset the alarm. This will vary with each site and is designed to ensure the site has enough time to deal with an accidental alarm before involving the monitoring centre. Alarm monitoring centres may have a 120- second filter on intruder alarms. This means that monitoring centre operatives will not know about the alarm unless it has not been aborted or reset within 120 seconds. This reduces false alarms to emergency services.

Alarm monitoring centres will have slightly different protocols for open and closed sites or when the system is set or unset. To do this, the monitoring centre must be aware of the opening and closing times for the site. Relevant parties who may need to be contacted about an alarm include the site, keyholders and Gardaí. Since the monitoring centre cannot pass an unverified alarm to Gardaí, they must filter the alarm through channels depending on the situation and the type of alarm.

An example of an alarm filtering plan is set out below:

Activation type	Response
Panic alarm	Site and immediate Garda
Verified intruder	Keyholder and immediate Garda
Unconfirmed intruder	Keyholder and site
Fire alarm	Site, keyholder and fire brigade
Systems fail / Mains fail	Site and service engineer
Open/Close signal	No response

False alarms

False alarms can occur in a number of ways. The main way is through faulty detection equipment on site. If a monitoring centre becomes aware of faulty equipment on site causing excessive signals that are identified as false alarms, it will take the following actions:

1. If more than 4 activations are received from a single specified piece of equipment, and no cause of activation is seen, then the monitoring centre will try to relieve the issue first. First the monitoring centre will suspend the site for 30 minutes. If the false activations continue after the site returns from suspension, then the monitoring centre will put the affected equipment onto test for no more than 2 hours.
2. Following the 2-hour test period, if the affected equipment returns with 4 or more false alarms again, then the equipment will be placed onto permanent test.
3. Once the faulty equipment is on permanent test, the monitoring centre will notify the installer or engineer or keyholder as required, via email, specifying the name of the site(s) and the affected equipment.
4. Once the engineer has received the email, they are expected to reply with a resolution as soon as possible. Once an acknowledgment has been received, advising that they have visited the site and rectified the faults, the monitoring centre will place the affected equipment onto 7-day monitoring to evaluate the level of alarms following the resolution.
5. If the level of activations decrease to an acceptable level over the 7-day period, then the equipment will be reinstated and the client will be informed. If however the level of activations are still beyond the acceptable level for monitoring, then the affected equipment will remain on permanent test until the level of activations is resolved.

The second reason for false alarms is through human error on sites. In this case the reason will be passed to the keyholder and site management for review. General Gardaí will not attend false alarms, as they would only receive a call from the monitoring centre once the alarm is verified. If Gardaí do attend to an alarm which turns out to be false, they may after a number of occasions remove response to the premises.

The security operative should take note of all false alarms and make a report detailing the date, time and cause. Persistent false alarms should be escalated to management for review.

Prompt response

Whether an alarm has been verified or not, it is essential that the monitoring centre respond promptly to all alarms. This is for a variety of reasons, including:

- Potentially saving lives in the event of a fire or personal alarm
- Reducing loss or damage to client's premises
- Providing a high-quality service to clients
- Working relationship with third parties, including keyholders and emergency services.

Modems

Most intruder alarms use high-quality modems to send their signals over multiple channels for redundancy. Most alarms systems send a signal down a primary fixed phone line to the monitoring centre. However, phone lines can be cut by intruders, which will only register as a fault with the alarm monitoring station. For this reason, the phone line is usually supported by a GSM dialler, which uses a mobile SIM card type arrangement to send a backup signal wirelessly from the site to the monitoring station. The GSM dialler can also be set to send a text message alert to the monitoring centre or keyholder. This redundancy ensures that the monitoring centre can respond promptly to alarms.

IT in monitoring centres

Internet technology is essential to the working of an alarm receiving centre. All of the modern systems we have discussed in this document rely on the internet and technology in general to function. The work of the remote monitoring station would not be possible without the benefit of :

- Remote alarms
- Wireless CCTV
- GSM diallers
- IT systems and software.

...and many other systems. Anyone hoping to pursue a career as a security operative in a monitoring centre must be proficient in all aspects of IT technology and must keep up to date with its progress.

C.5 How to deal with incidents in the context of monitoring centre employees.

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Define an incident in the context of CCTV and alarm operations.
- Explain how CCTV and alarm operations interact with the work of the Gardaí.
- Outline the range of actions to be carried out when suspected criminal activity is detected by a CCTV operator.
- Discuss the actions to be carried out on receiving a request for assistance from the Gardaí.
- Explain how to deal with two or more incidents simultaneously.
- Describe non-crime incidents and how the operator should deal with them.

Definition of an incident

In the context of a CCTV monitoring and alarm response, an incident can be defined as any occurrence viewed on the screen. It could be anything outside of the ordinary that occurs on or near a protected site and require the attention of the operator. It may be criminal or non-criminal, but either way it requires the attention and sometimes the interaction of security operatives to resolve. Examples are:

- anti-social behaviour
- civil negligence or malpractice
- criminal activity (theft, burglary, criminal damage, assault, drug-taking)
- non-crime incidents.

Non-crime incidents

Non-crime incidents that require the attention of the security operative, but do not constitute a criminal offence, may include:

- arguments
- spillages
- intoxicated person(s)
- lost property
- situations requiring first aid
- unsecure areas
- crowd management
- missing person(s)
- accidents
- traffic monitoring
- emergencies (fire, flood).

Upon witnessing a non-crime incident, the security operative should begin real-time monitoring and inform a supervisor. If emergency services such as fire or ambulance are required, the security operative should contact them and give them real-time updates until they arrive. If emergency services are not required, and the client has staff on site, the operative may be required to contact the staff on site and observe while they resolve the situation. Once the situation is resolved, the security operative must make a note of the incident and preserve relevant recordings.

Identifying criminal activity

While monitoring CCTV and alarm sites, the security operative may observe potential criminal behaviour. This could be in the form of nervous or suspicious body language, repeated movement patterns or unusual routes being taken. Or it could be items the person is carrying or the way a vehicle is being driven. Once the security operative observes behaviour that they feel is potentially criminal, they should treat it as though it is a criminal act until it can be verified otherwise.

Criminal acts

Once a criminal act has been confirmed, the security operative should immediately contact their supervisor and the Gardaí. They should then use all the tools at their disposal to gather evidence of the act, including real-time viewing from as many cameras as possible. The operative should get close-up images for recognition purposes, and wide-angle images to show the complete act. If the person begins to move or leave the area, the security operative should track their movement and liaise with the responding Gardaí until the person is detained or leaves the CCTV coverage.

Dealing with multiple incidents

When dealing with multiple incidents simultaneously, a security operative should use other operatives to help or supervise if possible. The incidents should be prioritised and the highest-risk incident dealt with first. The security operative should try to use all camera angles to get the best images of the high-priority incident, while still using general monitoring to observe the other incidents if possible, or have a colleague observe them.

If one incident requires the emergency services, the security operative should contact them and liaise while a colleague observes the others. If two incidents require the emergency services, then two security operatives should make simultaneous calls and deal separately with the emergency services.

After the incidents, detailed reports of both should be written outlining the reasons why one was prioritised over the other, and the events that unfolded.

Working with emergency services

The work of the CCTV and alarm monitoring centre can involve a good deal of liaison with Gardaí and other emergency services. Often, when responding to alarms and CCTV incidents, the emergency services will be reliant on the information they get from the security operative. Operatives must therefore ensure that this information is factual and accurate. Failure to do so could damage the monitoring centre's reputation and its working relationship with emergency services.

Monitoring centres often also give proactive information to Gardaí about potential incidents around protected sites that do not affect the site itself, such as anti-social behaviour or traffic accidents observed on CCTV. Monitoring centres may also need to work closely with Gardaí and other emergency services to provide evidence for prosecutions – Gardaí often rely on the chain of evidence produced by the monitoring centre.

Responding to requests for assistance

When a security operative receives a request for assistance from a Garda, they should first make a record of this and communicate it to their supervisor. Once the request has been approved, the operative must ensure they can find the correct information and communicate it accurately to the Garda. They should be aware of any potential risks to confidentiality or privacy, and tell the Garda of any limitations on what can be provided with a written request or warrant. Once the information has been passed to the Gardaí, they will take control of the incident. They may make a written request for information to be downloaded or for a witness statement from the security operative.

Response to a verified alarm

When a verified alarm is received, the security operative will follow the alarm filter procedure for the site. The keyholder may be notified, and in most cases the Gardaí. When calling the Gardaí, the security operative should convey that it is a verified alarm, the location of the alarm, any CCTV evidence, and the expected meeting point for the keyholder. The operative may also need to remain in contact with the keyholder until Gardaí arrival. Once Gardaí arrive, they will investigate, and if they find no reason for the alarm, they will declare a false alarm. The security operative must make note of this, prepare a report, and retain records of the alarm.

C.6 Outline the range of documentation relevant to monitoring centres

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- List sample site documentation relevant to monitoring centre employees and explain their purpose
- Explain the purpose of standard operating procedures
- Summarise the contents of a general set of site assignment instructions
- Explain the importance of site maps
- Outline documentation requirements for safety and environmental procedures
- Outline documentation relevant to access and egress control

Monitoring centre documentation

A monitoring centre must keep and maintain a range of on-site documentation to fulfil its obligations to clients and meet regulatory standards. Some documents will be created and maintained in paper format, others electronically. General requirements for all monitoring centre documentation are that they be completed accurately and professionally and stored securely, regardless of the format. Examples of on-site documents include:

- Security occurrence log
- Incident report form
- Accident report form
- Fire safety audit checklist
- Key and access control log
- Visitor log
- Telephone message book
- Sign in/out attendance log
- Equipment records
- Lost and found property log
- Patrol check-in log
- Handover sheet.

Standard operating procedures

Standard operating procedures (SOPs) are detailed instructions on how to deal with a particular issue. A monitoring centre will have a range of SOPs for the centre itself as well as individual SOPs for each of a client's sites. The SOP should give enough detail so that anyone in the monitoring centre can follow it. SOPs serve as a guide to security operatives, providing a process that can be followed based on management and client wishes. SOPs should contain, at a minimum:

- The purpose and scope of the procedure
- The people who are involved in or affected by the procedure
- Any equipment or resources required for the procedure, including PPE
- The process to be followed when carrying out the procedure
- Contingency plans in case the procedure fails or there is an issue with it
- A chain of escalation for the issue, detailing who should know about the procedure and at what stage they should be informed
- A list of documents and reports generated by the procedure, plus where they will be retained and for how long.

Assignment instruction

An assignment instruction is a document containing all the SOPs, which is site-specific and designed for every site. It is maintained and updated on site and is available to all staff. It should contain all the command and control instructions for that site and describe how the tasks required of security operatives are to be done. It should also contain, at a minimum:

- Working hours and handover requirements
- Emergency procedures
- Communications procedures
- Specifically requested services
- Clients' facilities, vehicles or equipment
- Welfare facilities for staff
- Access control and searching facilities
- Accountability for employees, and any restrictions concerning them
- Safety statement
- Risk assessment
- Confirmation of on-site training and familiarisation for each officer. Level of supervision on site and role of supervisor(s). Implementation of PSA ID requirements
- Sign-off on assignment instructions by both a senior officer of the organisation and relevant operational staff.

Site map

A site map is an illustrative guide to a site. It will contain the locations of all essential equipment and areas of note on the site, including emergency escape routes. The map provides an easy reference point for security operatives to locate important information quickly. It may be produced on paper or electronically, displayed on screens.

The monitoring centre will have site maps of the centre itself, showing all the essential information for the location. There will also be site maps for all protected premises, showing vital data relevant to the security function. For example, if a site is having its fire and intruder alarm monitored as well as CCTV, the map would contain:

- Location of all access points to the premises
- Location of the alarm panels
- Location of the CCTV server or DVR
- Location of cameras
- Location of input detectors for fire and intruder systems
- Fire escape routes
- Location of emergency equipment
- Power and water shut-off points (if applicable).

Safety and environmental documents

The monitoring centre will retain a number of safety documents on site for regularity, training and reference purposes. These are required to ensure that staff are familiar with the safe conditions of work provided for them, and the company's expectation of employees with regard to safety and emergencies. These documents will include:

- Safety statement – This document will contain the organisation's safety policy, as well as safety arrangements with regard to fire, first aid and other emergency procedures. It will contain risk assessments for each task and location in the monitoring centre.
- Fire Register – The fire register will contain all the ongoing inspection and maintenance records for the monitoring centre's fire equipment and infrastructure. It will contain the service records for fire equipment, such as extinguisher and fire alarm systems. It will contain the daily, weekly and monthly inspections of fire doors, escape routes, etc. carried out by security operatives.
- Environmental control logs – A monitoring station will contain a range of servers and storage devices to service its networks and equipment. This equipment must be maintained to ensure it does not negatively affect the internal or external environment. Environmental control logs will be maintained to show regular monitoring of the temperature, humidity and air quality in the monitoring centre.

Access and egress logs

For a secure environment, access and egress will be closely monitored and measured in the monitoring centre. Access to and from work for employees will be logged and maintained. This may be in several formats, including:

- Biometric data
- Electronic sign-in (swipe cards/codes)
- Manual (sign-in sheets)

Audit logs of sign-in and usage of workstations will also be retained electronically to control access levels and periods.

Visitor controls will be strictly managed, using a form of visitor registration and accreditation. Records of all visitors' access and egress will be maintained.

C.7 Explain the range of on-site safety and fire equipment

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Define what constitutes fire equipment
- List range of fire extinguishers
- Explain extinguisher colour coding
- Outline how to check fire extinguisher service records
- List the names and functions of fire alarm and suppression systems
- Explain the purpose of emergency lighting in the context of fire-based emergencies
- Outline the range of safety equipment used by a security officer
- Define PPE and list samples and their uses
- Explain safety and fire signage
- Outline the actions to be taken in the event of fire
- List emergency equipment available on site
- State who should operate this equipment
- Explain why it is important to know the location of all emergency equipment
- Explain why equipment should be in its correct place
- Outline procedures for reporting damaged equipment

Fire equipment

Fire equipment can be described as any technical equipment designed to rescue people and protect goods and natural resources from fire. Firefighting equipment includes fixed fire-extinguishing and fire-alarm systems, fire extinguishers, fire hydrants, and other means for conveying fire-extinguishing agents to the scene of a fire. At a more advanced level, fire equipment can include fire trucks and other firefighting vehicles.

Fire extinguishers

The most common type of firefighting equipment is fire extinguishers. These are colour-coded depending on their contents. Colour-coded labels on fire extinguishers explain the extinguisher's contents and the types of fire for which it is suitable:

1. Water extinguishers (RED) – class A: used on organic combustibles such as paper, plastic, cloth and wood.
2. Foam extinguishers (CREAM) – class A & B: used on flammable liquids involving oil, petrol and paint thinners.
3. Powder extinguishers (BLUE) – class C & A/B: used on electrical hazards and blazes involving liquids and flammable gases.
4. Carbon dioxide extinguishers (BLACK) – class B: used on electrical fires and flammable liquids.
5. Wet chemical extinguishers (YELLOW) – class A & F: used on cooking oils or fats, usually in kitchens.

Water fire extinguishers

Water fire extinguishers are the cheapest and most common fire extinguishers available. They are used on solids such as paper, wood and plastics (class A) but are not suitable for use on liquids, i.e. petrol, oil, paraffin, etc.

Water fire extinguishers are easy to clean up after and don't usually cause long-term damage to curtains, furnishings, etc. (also known as class B fires). But they are highly unsuitable in an electric fire, due to risk of electrocution. They are less effective than foam but continue to be used in some offices, retail, shops, homes and areas of low risk.

Foam fire extinguishers

Foam fire extinguishers are usually more expensive than water but also more adapted to different functions. They can be used on class A and B fires. They are not recommended for use on electrical fires but are safer in the necessity of an emergency situation. Foam extinguishers are often used in offices, retail, shops, pubs, restaurants, apartments, farms, petrol stations and companies of any kind.

Dry powder fire extinguishers

Dry powder extinguishers are one of the most versatile fire safety products and are safe for use on class A, B and C (flammable gas) fires. They should be used only in emergencies and when the gas supply has been cut off at source. Otherwise they will not completely extinguish the flame and may cause gas poisoning. Some special dry powder fire extinguishers are also available, for use on magnesium, aluminium and titanium (class D) fires, but these are limited to specialist industries.

Dry powder extinguishers are messy to clean up and can cause damage to curtains and other soft indoor furnishings. They can be an irritant to people if used in a busy or crowded space, such as a bar, restaurant or hotel. Dry powder extinguishers are versatile and can be used in almost all environments. They are mainly found in cars, boats, offices, commercial buildings, petrol stations, factories, warehouses and large premises of any kind.

CO₂ fire extinguishers

Carbon dioxide fire extinguishers are best used for electrical fires, as they cut off the fire's fuel supply (air) without using water or other electricity-conducting material. They can also be used on flammable liquids. However, they offer no after-fire protection and can lead to either electrocution or post-fire heat burn. With electrical fires it is very important to cut off electricity at the source – this includes the mains.

CO₂ extinguishers are often used in offices, shops, server rooms and data centres, retail outlets and most commercial buildings of any kind. They are even found in the home.

Wet chemical fire extinguishers

These are specialised fire extinguishers for use on cooking oils and burning fats (class F). They are often found in kitchens and should be considered for anywhere around kitchens or cooking activity, including in private homes. Wet chemical fire extinguishers are often used in commercial kitchens such as in bars, restaurants and hotels.

Service records

On the side of each fire extinguisher will be a sticker containing its service records. Fire extinguishers should be serviced annually by a professional fire safety company. The service record sticker will contain the date of last service, engineer's signature and due date of next service. Security operatives, as part of their role, must periodically check the service record on the fire extinguishers, to ensure they are in date. Extinguishers that are out of date should be reported to management.

Fire alarms

Fire alarm systems form an integral part of any building's overall protection and security systems. They are designed to detect, alert and in some cases create automatic responses to fires or potential fires. Fire alarm systems consist of three parts:

- Inputs – Smoke detectors, heat detectors, fire call points
- Processor – Fire alarm panel
- Outputs – Bells, sirens, relays to suppression systems.

The fire alarm control panel is the brains of the system. It receives signals from the input devices and generates the most appropriate output based on its programming. The control panel is addressable, which means it displays the exact location of the input signal and allows the user to control or address the system's outputs. The system can be manually activated, silenced or reset by the user, depending on the situation. A building will usually be divided into zones, with each input given a number. For example, a smoke detector in zone A on the first floor might appear as "Zone A Det 11: First floor stockroom". This allows the user to dispatch an immediate response to the exact area of the alarm.

Addressable systems will also continually monitor the performance of the system by checking individual devices on a loop basis for faults. The unit will then display a "fault" signal which will usually beep continually at the alarm panel to let the users know there is an issue. A fault signal will not activate the output means of alert unless it is critical. Fire alarm systems run on mains power supply but will also be connected to a backup battery power supply in case of electrical failure. Electrical failure of the mains power supply will also cause a "fault" alert on the panel.

Inputs

When a fire starts, a person may not be present, may not raise an alarm in an effective manner, or may not be able to recognise fire signs. Automatic fire detectors have therefore been developed. These are meant to mimic one or more of the human senses of touch, smell or sight. Thermal detectors are similar to our ability to identify high temperatures, smoke detectors replicate the sense of smell, and flame detectors are electronic eyes that detect the light emitted from flames.

Manual fire alarm call points in a building will also activate the alarm. The principle is to place manual call points along paths of escape, so they can usually be found near exit doors in corridors and large rooms. The advantage of manual call points is that, upon discovering a fire, occupants have a readily identifiable means to activate the building's fire alarm system.

Outputs

Outputs from a fire alarm system generally consist of audio and visual alerts to make occupants aware there is a fire and to signal an evacuation. Audio alerts can be in the form of bells, horns, sirens or voice messages, which are repeated until the alarm is silenced. Visual alerts can be in the form of lights or message boards containing evacuation instructions.

Other output functions include shutting down electrical equipment such as computers, shutting off air-handling fans to prevent smoke migration, automatically cancelling door hold open devices, grounding elevators and shutting down operations such as chemical movement through piping in the applicable area. They may also activate fans to extract smoke – a common function in large spaces. These systems can also activate gaseous fire extinguisher or pre-action sprinkler systems.

Fire suppression systems

There are various types of fire suppression systems in operation in buildings. These include:

- Fire sprinkler systems (wet, dry, pre-action and deluge)
- Gaseous agents
- Wet and dry chemical agents.

Sprinklers

Security operatives should be aware of several types of sprinkler systems:

Wet Pipe – Wet pipe fire sprinklers constantly have water in them. This allows a quick reaction to fire and is the most common type of sprinkler installed in buildings. A typical building that uses the wet pipe sprinkler system is a high-rise or office building with a few floors. This system is cost-efficient and low-maintenance, but there is a risk of accidental activation, causing damage.

Pre-action – Pre-action fire sprinkler systems are filled with air and allow water to pass through when the smoke alarm or detector goes off. This type of system requires two triggers to start water flow, and is set to prevent water from releasing in case of a false alarm or system failure. The pre-action system is used where sprinklers are only necessary when there is an actual fire, so other items in the building do not get water damage. Such buildings include libraries, museums and data centres.

Dry Pipe – Dry pipe sprinklers are similar to pre-action systems, as they use pressurised air in the pipe which exits before water escapes. This causes a minute's delay in water discharge but is ideal for buildings with low temperatures so the pipes do not freeze. These systems have a fast opening tool to get rid of the air and speed up the flow of water. Unoccupied buildings with no heating or outdoor loading bay canopy are good examples of where dry pipe sprinklers are used.

Deluge – Deluge fire sprinkler systems also need a smoke or heat detector to activate. They have open nozzles that can be used when a hazard is present. When flammable liquids are spread across a floor, deluge fire sprinklers are good to have, hence their installation in industrial parks and buildings with many tanks. They are designed to stop the fire spreading to further combustible material in the area.

Other suppression systems

Other suppression systems include gaseous agents or wet/dry chemical suppression where water is not an appropriate extinguishing agent. These work on a similar extinguishing principle as powder, CO₂ and wet chemical fire extinguishers as a replacement for water. The sprinkler system remains largely the same, but the extinguishing material is changed to a more appropriate type.

Emergency lighting

Emergency lighting is installed in buildings to help occupants leave in low light or where the power has failed due to fire or electrical issues. The function of an emergency lighting system is to ensure that in the event of a fire or other emergency the occupants of the building will be able to clearly locate and follow escape routes out of the building. Emergency lighting is connected to both the mains power and a backup supply. If the mains power fails, the emergency light either remains on (if already lit) or turns on (if it's a dedicated emergency light). Emergency lighting in buildings is tested periodically by engineers turning off the mains water and checking the activation of the lights.

Security operative equipment

In the event of an emergency, a security operative may be required to deploy a range of personal equipment. This includes:

- Torches: All security operatives are advised to carry a small torch while on duty. A torch has multiple uses, including patrolling for fire, searching, lockdown procedures, evacuation in low light, signalling and first aid.
- Two-Way Radio: The standard two-way radio is widely used across the security industry as the primary method of communication between security operatives. If available at your work location, it should be used. It is an effective method of summoning support and help in the event of an incident.
- Loudhailer: When evacuating a large building, it may be necessary for security operatives to use a loudhailer to give clear instructions to others.

Personal protective equipment

Personal protective equipment (PPE) is any equipment or clothing used or worn for safety reasons. A security operative may have to wear or use a variety of PPE depending on the situation. This includes:

- Disposable gloves: No matter what area of the security industry you work in, disposable gloves are essential equipment. In the course of your role you may come into contact with bodily fluids, hazardous materials, first aid incidents or dirty environments. Any of these can be harmful to your health and safety, and disposable gloves should be used in all such circumstances.
- Safety shoes: Depending on your work environment, safety shoes may be mandatory. Even where they are not, many employers will require safety shoes to be worn on duty. In industrial environments such as construction sites or factories, the benefit of safety shoes to reduce the risk of injury is obvious, and their use will probably be mandatory. This may not be the case in a monitoring centre, but there may be times when a security operative has to carry out checks in generator, plant or building management system rooms where safety shoes are advisable.

- High-visibility clothing: Any workplace where security operatives work near moving vehicles or machinery will require high-visibility clothing to be worn. The most common item is the high-visibility vest. This should be kept on every work site regardless of the role. It should be worn any time the security operative goes outside of the building for identification and safety reasons. High-visibility clothing should be worn to attract attention in all emergency situations, such as evacuations or crowd management after incidents, as it makes the security operative easy for both the public and the emergency services to identify from a distance.
- Wet weather clothing: An evacuation or drill may involve a prolonged period spent outside, in which case wet weather clothing should be provided. This can include waterproof jackets or trousers to keep the security operative dry while working outside.
- Safety ties: Where ties are worn as part of the uniform, they should be safety clip-on ties. This is especially important when the security operative works near machinery such as generators.
- Hearing protection: When carrying out inspections of generator and plant rooms, or when testing alarms, hearing protection may be required.

Safety signage

The Health, Safety and Welfare at Work (Signs) Regulations 1995 provide employers with guidelines for placing and using safety signage in the workplace. Signage should be used where hazards cannot be avoided or reduced. Signs are generally categorised in the workplace and colour-coded for ease of reference:

- Red: Red signs represent danger or prohibition, e.g., No parking, No smoking, and Stop signs. Red signs also identify firefighting equipment.
- Yellow or amber: These signs represent areas where caution is needed or where there are hazardous conditions or exits, e.g., wet floor signs, electrical rooms.
- Green: Green safety signs indicate safety or safe areas in the event of emergencies, e.g., fire exit signage, first aid points, assembly points.
- Blue: Blue safety signs are used to indicate mandatory information or instructions to be followed, e.g., wearing PPE, or fire doors to be kept shut.

Fire equipment signs are also found in the workplace. These signs are red and rectangular, with white text or images depicting the location and identification of fire equipment.

Action on discovering a fire

On discovery of a fire, security operatives should use the “RIEFA” method of dealing with the situation:

- Raise the alarm: This can be done by breaking the activation point nearest to your location. Do not rely on the alarm being automatically raised by the fire detection system, as every second can count in a fire situation.
- Inform the emergency services: Call 999 or 112 as soon as it's safe to do so, and ask for the fire services. Don't assume that somebody else will or that it will be done automatically. The emergency services operator will talk you through the information they need and dispatch the fire service to your location. Always hang up last when talking to emergency services.
- Evacuate: Begin a quick and orderly evacuation of the area towards the nearest available fire exit, and direct occupants to the assembly point. When evacuating, check all rooms on your route and ensure they are empty.
- Fight the fire: Once the area is evacuated, you may decide whether to attempt to fight the fire. This is only advisable if you are fully trained and feel confident in trying to extinguish the fire. If you are not 100% sure you can safely extinguish it, then evacuate and await the emergency services.
- Assemble/Assist: You can assist the emergency services from the assembly point before they arrive by keeping the access route clear and keeping bystanders clear of the area. When the emergency services arrive, you can help by providing key information, such as the status of all occupants, type of fire, size and location of fire, and presence of electricity, gas or other hazardous materials.

Other emergency equipment

There may be other emergency equipment on site that security operatives need to be aware of:

- First aid kits
- Artificial External Defibrillators (AED)
- Evacuation chairs
- Emergency grab bag.

Security operatives should be familiar with the location and function of all emergency equipment on site, so they can find it and bring it to the scene of an emergency if required. However, items such as AEDs and evacuation chairs are specialist equipment and require training to operate. Security staff not trained in first aid or AED should try to summon a qualified person and not attempt to perform these duties unless it is critical and no other help can be found. Evacuation chairs should not be used by untrained parties, as they may cause further injury to an occupant.

Emergency equipment should always remain in its designated location, so that everyone knows where it is and so it is near its dedicated signage. If security operatives see that any safety or emergency equipment has been moved, they should replace the item and make a written report of the issue.

Lost or damaged equipment

Lost or damaged safety equipment must be immediately reported in writing to management. The report should contain the security operative's name, the date and time of the occurrence and the type of damage. If the equipment is no longer usable due to damage, it should be removed along with the signage until it can be replaced. Replacing lost or damaged safety and emergency equipment is a high priority for monitoring centre management.

D.1 Outline the constituent elements and contributing factors of an emergency

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Define the term “emergency”
- Explain what constitutes an accident
- Explain what is meant by an incident
- List a range of emergencies
- Outline the importance of the security officer identifying and communicating with appropriate personnel in an emergency
- Outline causes of fire
- Explain how fire spreads
- Provide examples of procedures for safe systems of work
- Define potential major incidents

Emergencies

An emergency can be defined as: a serious, unexpected, and often dangerous situation requiring immediate action. In the security industry, training and planning for emergencies is standard practice. Security forms will develop emergency plans for a variety of potential emergencies, so that if the situation arises, the employees have guidance on how to deal with them. Accidents and incidents can potentially be or lead to emergencies, due to the severity of the damage or harm done, or to the poor management of the initial incident.

Accident

An accident can be defined as: an unfortunate incident that happens unexpectedly and unintentionally, typically resulting in damage or injury. An accident that doesn't cause injury or damage is often referred to as a 'near miss' for reporting purposes and is treated just as seriously.

Incident

An incident can be defined as: an instance of something happening; an event or occurrence. It is different from an accident in that it tends to refer to intentional acts. An incident may or may not result in damage or injury.

Types of emergency

A security operative working in a monitoring centre may encounter a range of emergencies during their work. These emergencies may include:

- Fire
- Flooding
- Bomb threat
- Power failure
- Break-in
- Access breach to the monitoring centre
- Network failure.

Communicating emergencies

For a security operative dealing with an emergency, there will be many tasks which have to be done simultaneously. Communicating the right information to the right people about the emergency is essential. Security firms will have escalation plans in place for incidents and emergencies. These should detail who must be informed about the incident, and when. The people who must be informed may include:

- Emergency services
- Clients
- Property management agencies
- Other security providers

The security operative will have to communicate the information to those people. When communicating with emergency services, it is important to:

- Know the emergency services number (112 or 999)
- Request the appropriate emergency service
- Listen to the dispatcher – they will ask the relevant questions
- Know the exact location of the incident, including the Eircode
- Stay on the phone until the dispatcher says to hang up.

When informing clients or property managers of an incident:

- Identify yourself and verify the identity of the other person
- Speak slowly, clearly and professionally
- Explain the incident clearly
- Inform them of the steps that have been taken
- List any emergency services response
- Take note of any requests or questions the client may have
- Make a written record of the conversation as soon as possible

Fire safety

Fire Services Act 1981

The Fire Services Act 1981 is the primary piece of fire safety legislation in Ireland. It forms the framework for numerous sets of regulations and standards in this country. The Act places substantial responsibility on owners, occupiers and employers in public buildings. It states:

“It shall be the duty of every person having control over premises to which this section applies to take all reasonable measures to guard against the outbreak of fire on such premises, and to ensure as far as is reasonably practicable the safety of persons on the premises in the event of an outbreak of fire.”

The Act also places a certain amount of responsibility for fire safety on all persons within a building:

“It shall be the duty of every person, being on premises to which this section applies, to conduct himself in such a way as to ensure that as far as is reasonably practicable any person on the premises is not exposed to danger from fire as a consequence of any act or omission of his.”

Since the enactment of the Fire Services Act 1981, numerous pieces of regulation have been drafted to supplement it, in both fire safety and health and safety. We will aim to explain these when discussing safe systems of work later in this section.

What is fire?

The technical definition for a fire is:

“a chemical reaction involving oxygen and an oxidisable substance resulting in the release of energy in the form of light.”

That is a technical explanation of what is commonly known as burning. This occurs when a source of heat is introduced to any fuel, causing it to give off vapours. When those vapours are heated to a high enough temperature, they ignite in any environment where oxygen is present. The ignition then heats the fuel continuously, causing it to give off further vapours, and the burning process continues. The burning only ceases when the fuel is exhausted, the heat is reduced, or the oxygen is used up.

The fire triangle

The fire triangle is a simple way of describing the three ingredients required to cause a fire:

- Fuel: A fuel is any combustible or oxidisable substance and is required to sustain any fire. Fuels can come in three forms, solid, liquid or gas, and can become a combination of all three throughout the burning process.
- Heat: Heat or a source of ignition is required to heat a fuel enough that it begins to give off its own vapour. Once a fuel reaches a high enough temperature, it will ignite, causing fire. The point of ignition of any substance is known as its flashpoint, and it varies by material.
- Oxygen: The burning process requires oxygen to continue. A fire will consume all of the oxygen in its proximity and seek further oxygen to continue. Where sufficient oxygen is not available, a fire will not continue. However, adding oxygen suddenly to any fire can cause it to escalate quickly.



Causes of fire

In public buildings throughout the country, the three ingredients required in the fire triangle – fuel, heat and oxygen – can be present to varying degrees. When all three are brought together, the risk of fire increases. Common causes of this include:

- Electrical issues: The presence of electricity is an everyday and ever-present fact of life. But it also poses a great risk when not respected or treated with due care. Overloaded power sockets, poor wiring, replacement of fuses and poor ventilation in electrical installations are all common fire risks in buildings.
- Poor housekeeping: This occurs through complacency or lack of knowledge in fire safety. Fires can result from smoking in restricted areas, poor maintenance of machinery or plant, not adhering to safety precautions, and poor storage of flammable materials. Information training and proactive policy when patrolling can mitigate the chances of careless activity causing fire.
- Heating appliances: By their very nature, heating appliances provide one of the ingredients needed to cause a fire, and oxygen is omnipresent. All that is required in these instances is for a fuel to be added to the equation, and a fire can occur. Simple actions can easily lead to combustion, such as aerosol use or electrical equipment left on a heat source such as radiator, or paper stacked on a heater.
- Kitchen environments: Cooking rings or toasters in restaurants or staff canteens may come in contact with fuels accidentally. Possibly the biggest risk in kitchen environments is deep fat cookers, which we will discuss later.
- Arson: Arson may be committed for many reasons, such as vandalism, insurance fraud, revenge, psychological reasons or terrorism. Whatever the reasoning, proactive security measures are one of the greatest deterrents to arson.

Fire spread

Fire can spread in a number of ways. Heat can travel from one place to another in three ways: conduction, convection and radiation. Both conduction and convection require matter to transfer heat, while radiation does not.

If there is a temperature difference between two systems, heat will always find a way to transfer from the higher to the lower system.

- Conduction: This is the transfer of heat between substances that are in direct contact with each other. The better the conductor, the more rapidly heat will be transferred. Metal is a good conductor of heat. Conduction occurs when a substance is heated. Particles gain energy and vibrate more, then bump into nearby particles and transfer some of their energy to them. This continues and passes the energy from the hot end to the colder end of the substance.
- Convection: Thermal energy is transferred from hot places to cold places by convection. Convection occurs when warmer areas of a liquid or gas rise to cooler areas in the liquid or gas. Cooler liquid or gas then takes the place of the warmer areas which have risen. This results in a continuous circulation pattern. Water boiling in a pan is a good example of these convection currents. Another good example is in the atmosphere. The earth's surface is warmed by the sun, the warm air rises and cool air moves in.

- **Radiation:** This method of heat transfer does not rely on contact between the heat source and the heated object, as is the case with conduction and convection. Heat can be transmitted through empty space by thermal radiation, often called infrared radiation. This is a type of electromagnetic radiation. No mass is exchanged, and no medium is required. Examples of radiation include heat from the sun, and heat released from the filament of a light bulb.

Safe systems of work

When it comes to fire safety, the safe systems of work required by occupiers of buildings are set out in the Fire Services Act 1881 and associated regulations. These safe systems of work include:

- **Fire exits:** There must be a sufficient number of fire escape routes in a building to ensure the safe evacuation of all occupants in an emergency. This is calculated based on the size of the building, the activities taking place in it, and the number of persons who may be occupying the building at any time. The fire exits must be unlocked at all times, be clear of obstruction inside and outside, and be clearly signed.
- **Fire detection equipment:** All public buildings must contain a fire alarm system able to detect an outbreak of fire at the earliest possible stage. The most commonly used equipment is smoke detection units, heat detection units and carbon monoxide detection units.
- **Exit signage and emergency lighting:** There should be adequate signage in place to ensure that people unfamiliar with a building's layout can easily be directed to a place of safety or a fire escape route. Emergency lighting should be provided to help people leave a building even in darkness, during a power cut or in the presence of smoke. Emergency lighting should have a battery back-up power so that it still functions correctly in the event of a power cut.
- **Means of alerting people of an emergency:** All fire alarm systems must have an audible signal to alert people to the outbreak of a fire and to signal an evacuation. Newer fire alarm systems have both audible and visual means of alert. Audible alarms can be in the form of bells, klaxons or voice messages broadcast throughout the entire building. Visual alarms may be in the form of flashing lights, strobes or visual displays throughout the building. The alarm system should be capable of being activated from anywhere in the building, usually through a break-glass unit. Means of alerting also include having a suitable way of contacting the emergency and medical services, whether via telephone or remote monitoring.
- **Firefighting equipment:** Following a risk assessment, a suitable level of firefighting equipment for each building must be provided. The level and type of equipment will be specific to each building and its activities. Common firefighting methods include: sprinkler systems, fire extinguishers, fire hose reels and fire blankets. Firefighting equipment should be suitable for its role and serviced annually.

- Evacuation procedures: An orderly and controlled pre-planned evacuation procedure must be designed for safely evacuating all occupants from a building in an emergency. The evacuation procedure should be notified to all occupants in the building, and help must be provided in the form of trained staff in the event of an evacuation. Once the evacuation is complete, there should be a pre-arranged meeting or assembly point for all staff and occupants of a building where the emergency services can attend and be briefed on the situation.
- Fire safety training: All employees in a building should be given fire safety training. In its most basic form, this could include the action to be taken on hearing an alarm, the evacuation procedure, and their expected duties and actions to be taken on finding a fire. Certain staff with additional duties, such as security operatives or fire wardens, should be given additional training in line with their responsibilities.
- Fire drills and training records: Fire drills should be carried out regularly to ensure that all employees know what to expect in an actual event. These drills should involve complete practice evacuations and simulated fire outbreaks. They should be recorded, along with any issues experienced, to enable these issues to be rectified for future drills.

Major incidents

Fire is only one type of occurrence that monitoring centres should plan for. Any of the emergencies listed earlier in the section has the potential to turn into a major incident. A major incident is defined as follows:

A major incident can be defined as any emergency that requires the implementation of special arrangements by one or more of the emergency services, the NHS or the local authority for the initial treatment, rescue and transport of a large number of casualties.

All monitoring centres will have plans in place for major incidents, as will many of the larger client sites being monitored. Local authorities and emergency services will also have their own major incident plans. Once the emergency services are involved in a situation, they will decide whether to declare a major incident.

D.2 State the procedures for immediate action on finding a range of emergencies.

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Outline the general response to a range of emergencies
- Outline the general response to discovery of fire
- List the general actions taken on discovery of fire
- Explain how to prioritise for life, injury, damage in an emergency
- State what bodies comprise the emergency services
- Explain the importance of knowing and following policy and procedures in emergencies
- Explain when written reports should be made
- Outline actions to be taken in the event of a threat to the control room

Emergencies

In emergency situations, it is critical for security operatives to remain calm and in control and have measures in place to reduce the risk and impact of any emergency. In an emergency, people will inevitably look to a security operative or security firm for help and at the very least guidance. The uniform and logo represent authority to the public. Emergencies can range from minor accidents to major incidents such as fires or bomb threats. In this section we will look at a range of responses to emergencies which enable a security operative to return the situation to normal.

Responding to emergencies

In general, when responding to emergencies we use the control–cordon–clear system. It is an efficient method for responding to a variety of emergency situations. This model prioritises the saving of lives followed by the treatment of injured and the control of damage. The security operative working in a monitoring centre may have to respond to emergencies either in the monitoring centre or on a client’s site.

Control	Cordon	Clear
<ul style="list-style-type: none">• Raise the alarm• Clear the area• PPE• Treat critical injuries	<ul style="list-style-type: none">• Establish safe area• Secure perimeter• Secure access route	<ul style="list-style-type: none">• Treat other injuries and clear• Preserve the scene• Hand over to authorities• Withdraw cordon

Flooding

Water can cause just as much damage and devastation as fire and is present in all of our homes and businesses every day. Common causes of flooding include:

- Burst pipes
- Frozen pipes
- Sprinkler systems
- Vandalism

Dealing with flooding will involve at least a partial evacuation. The primary goal is to ensure the building occupants are safe. Unless there is a safety risk, the fire brigade will generally not be called. Once the area is clear, the security operative can obtain suitable PPE and investigate the source of the water if safe to do so. Turn off the mains water if possible.

Set up a perimeter around the flooded area and keep bystanders out. Contact the cleaning staff or company once the area is safe and clear to begin cleaning up. If the area is severely flooded, it may be necessary to contact contractors to pump the water clear. Once the area is cleaned and clear, it can be opened again and a detailed report can be compiled.

Bomb threats

Bomb threats are an unfortunate reality in today's world. Although the vast majority are hoaxes, each one must be treated as real until it can be confirmed as otherwise. Once a bomb threat is received, it should be treated as real and an evacuation should take place.

The emergency services should be called immediately. It is good practice to use a landline to contact the emergency services, or to go outside of the building to use a mobile phone, because explosive devices often use mobile phone or radio signal to activate the device. All mobile phones and two-way radios should therefore be turned off as soon as possible.

It is not advisable to begin a building search to locate a potential bomb, as this places people's lives unnecessarily at risk. Wait for the emergency services and allow them to make the decision to search.

If a suspicious device is found:

- Do not touch the item
- Don't shout "BOMB"
- Do not move the item
- Never attempt to defuse the device
- Follow the bomb threat procedures

Power failure

A power failure is probably the most likely of these emergencies to occur. While it may seem low-risk, it can pose unforeseen emergencies. All modern alarm and CCTV monitoring stations will have back-up generators in the event of a power failure. But these generators are only designed to run essential systems for limited periods of time. Some things which may not work during a power failure include:

- CCTV systems
- Perimeter alarm systems
- Escalators and lifts
- Display lighting
- Certain cash tills in retail outlets
- Sound systems and PA systems

Nothing here may seem critical, but sudden stoppage of lifts and escalators along with the loss of lighting can cause accidents or lift entrapment. It is also important to shut these systems down completely once the power goes, because restarting them suddenly can also cause accidents.

Actions to be taken:

- Guide all visitors and contractors towards the exits
- Once building is cleared, control the access points
- Secure all keys and valuables to a safe location
- Maintain vigilance for potential robbery, intrusion or decoy attempts
- Once power is restored, carry out a full search of the property for safety issues.

All receiving centres must also have an arrangement in place to move to a back-up facility from where they can operate. Security operatives should know the specific process for their facility.

Major accident or incident

Accidents can happen regularly in the workplace. The vast majority will pass with a simple first aid treatment and reporting procedures. But from time to time there will be more serious accidents or incidents that may require more attention from the security operative. This may be due to the severity of the injuries involved, damage to plant or machinery, or even potential serious crimes.

The following process should be followed for responding to accidents:

- Ensure the scene is safe to enter. Has the person been injured by anything in the environment that may be a risk of injuring the security operative?
- Put on gloves. There may be blood or other biohazards present that could harm the security operative.
- Summon assistance. This may be in the form of another security operative, a first aid person or an emergency responder.
- If the security operative is trained in first aid, they can begin treatment. If they are not trained, they can reassure and monitor the casualty until a trained first aider has arrived.

- The security operative can then support and assist the first aider while liaising with emergency services if necessary.
- A cordon or barrier should be established around the area of the accident while treatment is happening. This provides privacy for the casualty as well as protecting others from potential harm.
- The security operative should begin recording details from witnesses to the accident. These could include contact details as well as statements of what they saw, which may be required later.
- Once the casualty has been removed from the area, the security operative should begin scene preservation procedures.

Scene preservation procedures

If a criminal or civil investigation is to be carried out following a serious incident, then the security operative may have to carry out scene preservation measures in order to preserve the integrity of the area.

This would already have started during the incident, by establishing a secure cordon and recording basic witness details, but it may need to be expanded to include preserving the scene to allow evidence to be collected for civil or criminal reasons.

The following scene preservation procedure should be followed.

- Nobody aside from emergency personnel should be allowed inside the perimeter of the incident area.
- Nothing should be brought into or out of the incident area.
- The area should be manned constantly by security until emergency services arrive or the scene is complete.
- The security operative should wear PPE at all times within the incident scene.
- If possible, the security operative should take as many photographs of the scene as possible, without moving or touching anything.
- Once the emergency services arrive, the security operative should hand over control to the most senior person who arrives and note this person's name in their notebook.
- Once the emergency services are finished and authorisation is given, the perimeter cordon can be removed and the area cleaned.
- The security operative can then begin to compile a detailed report on the incident.

Action on discovering a fire

On discovery of a fire, security operatives should use the “RIEFA” method of dealing with the situation:

- Raise the alarm: This can be done by breaking the activation point nearest to your location. Do not rely on the alarm being automatically raised by the fire detection system, as every second can count in a fire situation.
- Inform the emergency services: Call 999 or 112 as soon as it's safe to do so, and ask for the fire services. Don't assume that somebody else will or that it will be done automatically. The emergency services operator will talk you through the information they need and dispatch the fire service to your location. Always hang up last when talking to emergency services.
- Evacuate: Begin a quick and orderly evacuation of the area towards the nearest available fire exit, and direct occupants to the assembly point. When evacuating, check all rooms on your route and ensure they are empty.
- Fight the fire: Once the area is evacuated, you may decide whether to attempt to fight the fire. This is only advisable if you are fully trained and feel confident in trying to extinguish the fire. If you are not 100% sure you can safely extinguish it, then evacuate and await the emergency services.
- Assemble/Assist: You can assist the emergency services from the assembly point before they arrive by keeping the access route clear and keeping bystanders clear of the area. When the emergency services arrive, you can help by providing key information, such as the status of all occupants, type of fire, size and location of fire, and presence of electricity, gas or other hazardous materials.

Emergency services in Ireland

The emergency services in Ireland are on call 24 hours a day, 365 days a year. They provide an emergency response to any situation that may occur. They can be contacted at any time by calling 112 or 999, free of charge. The call is routed to the National Emergency Operations Centre. The call taker will ask which emergency service you need. The emergency services are made up of:

- Gardaí
- Fire service
- Ambulance service
- Coast Guard

The call taker may dispatch numerous emergency services simultaneously. They may also connect the caller directly to the relevant emergency service for guidance and advice while awaiting their arrival.

Emergency procedures

All alarm and CCTV receiving centres will have emergency policies and procedures in place to cover the incidents described above and many more. These procedures will have been designed by management in conjunction with sector specialists and regulators to ensure they meet the exact needs of the site. Many client sites will also have specific emergency procedures based on their particular requirements. It is essential that security operatives have access to and are aware of all of these emergency procedures.

Following procedures in an emergency is important. It ensures consistency in response to an emergency and provides reassurance to staff. Site-specific procedures are often written based on unique issues in a particular site, and the security operative may not be aware of the technical issue. This is why the procedure must be adhered to. Failure to follow emergency procedures may put lives at risk and increase the likelihood of injury or of damage to the property. It could also have disciplinary implications for the security operative or insurance implications for management.

Written reports

Written reports must be completed as soon as it is safe and practical to do so after an emergency situation. Once the initial phase of protecting life, managing injury and controlling damage are complete, the next step is to write detailed reports of the emergency which will be circulated to all stakeholders. While initial communication of an incident will usually be verbal, the follow-up written reports should follow as soon as possible.

Completing reports will be covered in a later section, but the security operative must be aware that reports following emergencies must be comprehensive and cover all of the security operative's actions and the actions of others throughout the event.

Threats to the control room

When an emergency or threat to the control room occurs, security operatives must always prioritise their own safety first. The emergency services should be notified as per the site emergency SOP. Depending on the type of emergency present, there may be two responses. In the first instance, such as a fire or bomb threat, evacuation of the control room may be necessary. This will involve the switchover of essential systems so that the control room can be set up remotely and other systems can be shut down. The site evacuation procedure will then begin.

If the threat is an external one, such as adverse weather or civil disorder outside the control room, then the safest option may be an evacuation or lockdown. Specific control rooms will have their own lockdown procedures. This involves securing all access points to the premises and notifying management and emergency services that the control room is in lockdown and security operatives are still inside. Once the emergency has passed, management will lift the lockdown and the reporting phase can begin. Security operatives must make themselves aware of both the evacuation and the lockdown procedures for their site. Security firms will have welfare provisions in place for staff for both eventualities.

D.3 Outline, basic first aid principles and procedures for response to an injured person

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- State the principles of administering first aid
- List any six items contained in a typical first aid kit as recommended by the Health and Safety Authority

First aid in Ireland

The regulation of first aid training in Ireland is the role of the Pre-Hospital Emergency Care Council (PHECC). They set the training and standards for first aid in Ireland. The current level of training required to do first aid activities in the workplace is First Aid Responder (FAR). Any security operative who is required to do first aid duty as part of their role should have completed this training. The management of first aid provisions in workplaces is overseen by the Health and Safety Authority (HSA). Although this text is not designed as a first aid guidance document, it is important that all security operatives know the general principles of first aid and the contents of a first aid kit.

Principles of first aid

First aid is the initial help or treatment given to someone who is injured or suddenly taken ill. First aid means either:

- Treatment in a life-threatening situation (e.g., heart stoppage or severe bleeding) pending medical help, or
- Treatment for minor injury (e.g., cuts or bruises).

In emergency first aid with the immediate goal of preserving life, the “chain of survival” concept is recognised. This is based on four vital links to save a life:

- (i) Early access
- (ii) Early cardiopulmonary resuscitation (CPR)
- (iii) Early defibrillation
- (iv) Early advanced care. First-aid does not include the administration of drugs or medication.

For less serious situations, key concepts include the principle of not doing any further harm to the casualty, and prompting recovery.

First aid priorities

The following priorities apply in first aid situations:

- Assess the situation quickly and calmly
- Protect yourself and the casualties from danger
- Assess the condition of casualties
- Call emergency services if required
- Deal with any life-threatening conditions
- Comfort and reassure the casualties

First aid kits

Different locations will need different levels of first aid provision, based on their size and other site-specific risks. The Health and Safety Authority sets out the contents of a first aid kit in Ireland, which should include the following (the volume of each item will depend on size):

- Adhesive plasters
- Sterile eye dressing
- Triangular bandage
- Individually wrapped wound dressings (various sizes)
- Disinfectant wipes
- Paramedic shears
- Examination gloves
- Sterile water (where no running water is present)
- Burns dressing
- Crepe bandage

Some sites may also have an Automatic External Defibrillator (AED). While this is not legally required, it is encouraged by the HSA, as early defibrillation forms an important part of the chain of survival.

D.4 Outline the procedures for emergency evacuation of people

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Outline why and when evacuation is necessary
- List the first steps for evacuation
- State the standard procedures to be followed in the event of an evacuation
- State how to raise the alarm and inform the emergency services
- Identify escape routes and outline their characteristics
- Define an assembly area
- List the reasons for keeping a checklist of staff
- Outline the characteristics and purpose of fire doors and exits
- Identify relevant signage and lighting
- Outline the importance of personal safety during an evacuation.
- Explain the liaison and hand-over procedures in relation to the emergency services
- Describe the procedures to be carried out if an evacuation of the control room is ordered
- Outline the procedures to be followed on resuming occupation of the control room after an evacuation.

Raising the alarm

The fire alarm may be raised in a number of ways. It can be activated automatically by the fire detection system, where an input such as a smoke or heat detector is triggered by smoke or heat. It can be activated manually at a fire call point – a red square box sometimes called a break glass unit. This contains a central panel made from glass or plastic, which the security operative should break to activate the fire alarm. Finally, the alarm can be raised manually by pushing the evacuate button on the main fire alarm panel, which will send the alarm system into full operation. This may be required for an evacuation which is not a result of fire, such as flooding or structural damage.

Types of alarms

The type of fire alarm fitted in a building will affect the first steps to be taken in reacting to an activation. A single-stage alarm system has only one alarm mode, and sends the system into full evacuation mode once any detectors or call points are activated. The bells or sirens will ring on full alarm throughout, and the building will be evacuated immediately upon alarm.

A two-stage alarm system has a tiered activation system. On receipt of a signal from a single detector, the alarm will go into stage 1 alert. This will activate intermittent bells or sirens and show the location of the activation on the fire panel. This allows quick investigation of the cause of the alarm. If the security operative investigating the activation confirms a false alarm, then it can be silenced or reset. The alarm will go into stage 2 alert under a number of conditions:

- If a second detector is activated
- If the alarm is not silenced or reset within a defined time period
- If the security operative activates a call point to fully activate the alarm.

Once stage 2 is activated, the bells or sirens will go into full activation, and the evacuation procedure will begin

Evacuation

Evacuation will be necessary during any incident where there is a danger to life or risk of serious injury in the occupied building. The general response to a fire will be to evacuate the building following the immediate actions described earlier. It is important that evacuations are practised and that all staff – security operatives in particular – are familiar with the process.

- Fire action notices will be posted around the building, with instructions on the actions to be taken in an alarm situation. These contain all the information any person would need in case of an evacuation. Security operatives should be familiar with the contents of these notices and the actions they list.
- Security operatives should know at least two emergency exit routes from whatever location they are responsible for in a building.
- Occupants should be directed to emergency exits in an orderly fashion.

Crowd movements should be monitored for pushing or running during the evacuation.

- In some buildings, employees may be used as door attendants to ensure that the public do not re-enter a building.
- Security operatives may be part of the search team who will go through a building and confirm that all areas are clear of people. This should only be done if it is safe to do so.
- When moving through a building, close all doors and windows as you go, and if time permits, switch off electrical appliances.
- When the building search is complete, proceed to the assembly point and prepare for the emergency services.

Calling emergency services

Some fire alarm systems automatically notify the emergency services of an alarm and dispatch them to the address. Others require a manual phone call to 999 or 112. When you call the emergency services, they will want to know:

- Phone number you are calling from
- Address of fire
- The Eircode (if available)
- Location in building
- Whether people are still inside
- Gas or hazardous materials inside

Fire escape routes

A fire escape route or fire exit is a means of escape which can be used to leave a building in the event of a fire evacuation. Because the length of time taken to leave a building can exceed the time it takes for a fire to spread, a protected and dedicated escape route must be put in place.

The fire escape route should be constructed of fire-resistant materials to provide additional protection. Escape routes should be kept clear of all obstructions and should generally be at least one metre wide. The escape route should lead to a place of safety, normally outside and away from the building. The safe escape of occupants should always take priority over security considerations. Occupiers of a building should ensure that the exit route to and from fire doors is clear throughout the journey and that directional signage is in place.

Fire doors

Doors on escape routes must always be available for use without needing a key. Depending on the risk, push pads or panic bar devices should be used. Where possible, fire escape doors should open outwards to facilitate the flow of people leaving the building. They should also close automatically after people have left, to reduce oxygen from outside feeding the fire. Exit routes should be lit with regular and emergency lighting, and final exit doors should be fitted with green emergency exit lights connected to the emergency power supply.

Assembly area

An assembly area is a designated place where people wait after evacuating a building in the event of a fire or other emergency. It will be situated outside of the building and be clearly marked with a green assembly area sign. Larger buildings may have multiple assembly areas. They should be located a safe distance from the building and provide enough space to gather and check off staff and visitors safely.

Checklists

At the assembly area, staff will generally be checked off using some form of checklist. This may be a sign-in sheet used by staff or an automated printout. A checklist is an important tool because:

- It is an accurate record of the people occupying the building
- It provides a reference for management of how many people remain inside
- It can alert the emergency services to the potential areas of occupation for those who remain inside.

Once the checklist is complete, management can confirm that the building is fully evacuated or give the emergency services an accurate number for people who remain inside.

Fire safety signage

Fire point signage will be posted throughout the building at fire points, which are generally points adjacent to or near a fire exit. A fire point usually comprises a fire action notice and a fire call point sign. An example of a fire action notice is shown below. It contains information for staff on what they should do in the event of a fire. A call point sign gives instructions on how to activate the call point.



Fire exit doors will also be marked using a green exit sign. This shows the direction of travel and a picture of a person proceeding through the door.



Emergency lighting

Emergency lighting will be used throughout the means of escape to ensure adequate light for escape. The function and context of this lighting have been discussed earlier. Emergency lighting must provide enough light so the route is visible even in dark or smoke-affected areas.

Personal safety

During an evacuation, the security operative must ensure that their own personal safety is their priority. While they may have specific duties in an evacuation, such as turning off essential systems, enabling back-ups or searching a building, they should regard these as secondary to ensuring they can safely evacuate. A security operative who does not do this can put search-team colleagues and emergency services in further danger, if they need to enter the building to effect a rescue. If the security operative has any doubt about their ability to escape safely, they should forget all other duties and leave the building.

Liaison with emergency services

When emergency services arrive, they will wish to speak to a single point of contact

– usually be the most senior person on site. The liaison person will need to have collected all the checklists and be able to say accurately if people remain in the building and how many. They will also have to say, to the best of their knowledge, where the fire is and whether any hazardous materials are inside. The senior fire service representative on site will then take control of the situation. Once the fire services have taken control, they may still require security operatives to perform certain tasks, such as clearing the access route, moving bystanders back or managing traffic until the Gardaí arrive.

Evacuating the control room

In the event of an evacuation of the control room, similar procedures are undertaken to any other building. There may be additional duties to be considered, such as:

- Fuel cut off to generators
- Mains power supply cut off
- Telephone divert
- Remote access switch

One security operative will generally be tasked to take the emergency grab bag to the assembly area. Some security operatives may be used as fire wardens to search and clear areas of the building. There may also be a need to post door wardens at exit points to direct people to the assembly area and prevent re-entry. Any person who does not have a specific duty in the evacuation should proceed through their nearest available exit to the assembly area.

After evacuation

Once the emergency services have given the all-clear, the control room can be re-occupied and operations begin to resume. Areas of the control room may have suffered fire or smoke damage and may need to be cordoned off. The first priority is to restore power and network supply to the control room. Individual electrical items should be turned off and the mains power restored. These items can then be turned on in sequence in case of any electrical issues.

The building should be searched for any signs of damage. Once it is ready to be fully operational again, the security operatives can take full local control from the backup control room. Once operations are back, the reporting stage can begin, and the incident can be escalated through the correct channels.

E.1 Outline the principles of effective communications and customer service.

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Define communications and outline the importance of communication in the workplace
- List the five senses and outline how they are used in communications and customer care
- Explain how information is received and processed
- Explain sender and receiver
- Explain the two-way process
- List methods of communication
- List the most important communication skills required of a monitoring centre employee
- Summarise the principles of customer care
- Define who the customer is
- Explain why the customer is important
- Outline how security and safety benefit customer care
- Summarise the contents of a typical customer care policy, and summarise where security staff can assist in its implementation
 - Outline how interpersonal skills can assist with customer care

Communication in the workplace

Communication is defined by Oxford Dictionaries as “the imparting or exchanging of information by speaking, writing, or using some other medium”. It is the conveying of information from one person or party to another across a range of means. Put simply, it is the process of getting an idea from one person’s mind into another’s. It can be a simple or a complex process, depending on the number and type of media used by the sender and receiver.

Communication in the workplace is a critical part of any security operation. Effective communication must exist between all parties in the workplace to ensure that messages are spread to the people who need them in the format they need them in.

The security function is based on processes and procedures and the flow of information. When communications break down in the workplace, processes stop working and information stops flowing.

Human senses

Human beings are communicative creatures. Our brains have advanced far beyond those of animals, and our senses have developed to a level where complex communication is second nature. The five senses work together to form the basis of all communication. They are the input signals to the brain which enable it to process the information it is given. The five senses are:

- Sight
- Hearing
- Touch
- Taste
- Smell

Many people view communication methods as simply seeing and hearing information

– but this is not the case. The senses of smell and taste form part of the complex system which allows us to form speech. The articulation between breath, lips and tongue to form words and language is a by-product of our taste and smell sensations.

Tactile communication through touch occurs every time someone shakes hands with another person or references their tactile memory when reading body language.

The shape and make-up of the human ear enable us to decode sophisticated acoustic signals into sound and language and to replicate those sounds through speech. The brain's ability to decode these sounds in microseconds and to format them when inferring the speaker's tone, volume and meaning is a key part of communication.

Vision is complementary to all the other senses. It works with the tactile sense to read and decipher body language, and with the ears to decode the meaning of words and phrases. Vision reads the expressions and micro-expressions of the human face to discover the intent of the message.

Information processing

People send and receive information by combining the five senses and devising a message based on that combination. When we receive information, we combine all the senses. The human brain must receive each of these signals and process them separately before putting them together and getting the whole message. The brain can see, hear, feel, remember and contextualise information in microseconds to form a coherent message, before beginning a second process of deciding what to do with the information.

Sender and receiver

If a person has information to send, they must first encode that message. The encoding can be in the form of words, body language, pictures or text. The person who wishes to pass the information is the *sender*. The sender sends the information to another person, known as the *receiver*. The receiver must then decode the message and work out what the original information was. This may seem straightforward, but there are various barriers which can mean the receiver decodes the message incorrectly or not at all, resulting in miscommunication. The graphic below shows the process of one-way communication:



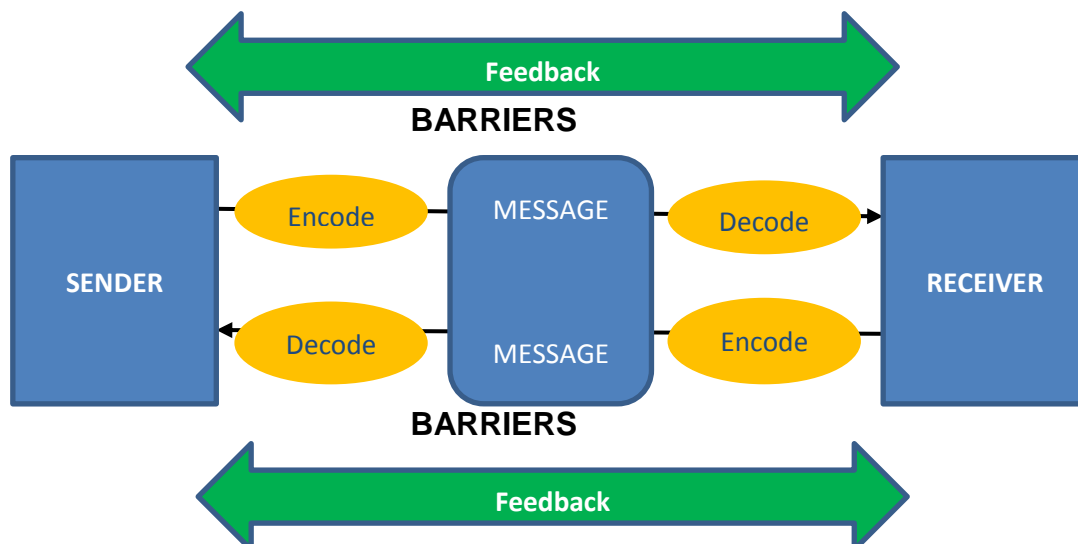
Two-way communication

The process described above is fine for a simple piece of information. But the process must be expanded when more complicated information is required. How do we ensure that a person has understood the message we sent? How do we know that no barriers reduced or stopped the message being processed correctly?

The answer is by seeking clarification and feedback on our message. Effective communication involves minimising potential misunderstanding and overcoming any barriers to communication at each stage. An effective communicator understands the need to alter the channel of communication based on their audience and environment. This reduces the chance of miscommunication. They will also use feedback to clarify the message.

When communication is two-way, feedback and clarification are even more important

– because there are more opportunities for each party to misunderstand the other. Each party takes their turn to be sender and receiver, and to use feedback to ensure the message is clear. Two-way communication looks like this:



Methods of communication

There are many ways for information to be communicated. Throughout a shift, a security operative may use a variety of methods to communicate within the team, to customers and to members of the public. Security operatives working in alarm monitoring centres must be proficient at all the methods. These include:

- Talking – Communicating verbally face to face in a clear and consistent manner is a key skill when dealing with team members and management.
- Listening – The ability to listen actively and take in communication clearly is essential for security operatives. This could be in the form of instruction from an employer or a request from a client.
- Body language – Body language makes up a significant proportion of the communication we send and receive. While we have certain instinctual ability to read body language, a security operative's ability must be excellent. They may need to read the body language of someone trying to be deceptive. There may also be times when a person's intent must be judged based on their actions on CCTV.
- Writing – Security operatives must be able to take clear, detailed notes of incidents and turn those notes into professionally presented reports. These tasks require the security operative to have a high level of writing ability.
- Reading – Detailed site notes and assignment instructions form part of the service of an alarm receiving centre. Security operatives must be able to read and comprehend detailed reports and standard operating procedures to be proficient in their role.
- Electronically – Technology has become an integral part of the security industry. Security operatives must be proficient at using email and other software in combination with the basic human communications skills.
- Telephone – Much of the work of an alarm receiving centre operative will involve using the telephone. This skill set will be discussed in detail later. Telephone skills require a security operative to be able to communicate verbally without the benefit of reading the caller's body language. It also requires specific etiquette, which will be discussed later.
- Two-way radio – Two-way radios are used widely in the security industry.

When communicating with operatives on sites, alarm receiving centre security staff must be proficient in the use and etiquette of two-way radios.

Customer care

Customer care is an integral part of the security operative's role. Much of their time on duty will be in a customer care capacity, regardless of where they work. We often hear the phrase "the customer is always right", and in general this is how businesses like their security teams to operate. Security teams sometimes tend to view themselves in an enforcement role, not a service role, and carry out their duties with this mind-set. But the modern professional security industry is a service industry and as such is designed to serve its customers' needs. In this section we will look at who these customers are and how the security operative can best serve their needs.

Customer care is:

- Creating and maintaining a safe environment where employees, customers and the public can have a safe and enjoyable experience.
- Creating and implementing policies and procedures to ensure that customers' needs and expectations can be met.
- Implementing the 3P's model in every customer interaction.
- Managing and resolving customer issues efficiently.

Principles of customer care

The principles of customer care are best described as treating every interaction using the 3P's model:

- Polite – Every customer interaction should be dealt with politely. This starts with a greeting as soon as the initial contact is made and extends through the conversation.
- Professional – The conversation should be kept professional. Building rapport with the customer is always good, but this should be done without the use of bad language or slang. Remember, you are communicating not just with an individual but to other customers in the vicinity, who may not see the entire context of the situation you are dealing with.
- Positive – The last part of this model is positivity. A positive attitude is key to customer care. Even if you can't fully resolve a customer's issue to their level of expectation, a positive attitude shows that you are trying to help. It also puts the security operative into the correct mind-set to help. If you are convinced there is a solution, then you will find that solution.

Identifying the Customer

Customers are generally regarded as the people who buy your product or service. In the security industry, though, they can be defined more broadly and can include:

- Client – When you work for a contract security company, the client is generally the customer. The client has paid your employer for a service and is therefore a customer. Meeting this customer's expectation now becomes an integral part of your role.
- Employer – Your own employer is your customer. They pay you to provide a service at a high level. When you meet that level, you meet their expectation and are providing good customer service.
- Service users – Employees and contractors of the client who interact with the ARC staff are also customers. Although they are not paying directly for the service, their employers have paid for a service to be provided on their behalf. How security operatives treat the employees who interact with them will reflect directly on the opinion of the paying client on the security operation.
- The public – While the public may not be a paying customer, they are potential future customers. Every interaction with the public should be treated as if the security operative were speaking to a paying customer. It is this overall commitment to customer care that generates new customers.

Importance of customer care

Customer care is important for several reasons:

- The primary reason is to protect the image of the company brand. Due to the nature of contract security work, you may be involved in protecting not only your employer's image and reputation but also the client's. Modern companies are acutely aware that brand damage can be just as harmful as physical or financial damage and can have longer-term effects than either.
- Good customer care generates repeat business, which generates additional work. Repeat business is what guarantees repeat income that a company can rely on. This allows them to look ahead and provide additional resources, including security for busy periods. So by helping to generate repeat business for the employer and possibly their clients, the security operative is increasing their own job security and their potential to increase earnings over time.
- Numerous studies have found that one of the greatest deterrents to losses in business is good customer care. This is true across all sectors of the industry. Security operatives who are proactive in approaching and making positive contacts in their work reduce the risk of loss or damage in that area through target hardening. This is where you make somebody with criminal intent think there is an easier target than yours to exploit. Good relationships with people in your work area can also lead to information that you may not be aware of, and can expose security risks before they cause damage.
- The final benefit of good customer care is the image of the security operative. Projecting a professional image, including good customer care skills, ensures that you are remembered by your customers for all the right reasons. When somebody thinks of security, they automatically think of you. This can make the security operative an integral part of the team. The security industry is acutely aware that in times of financial difficulties, one of the first areas to be targeted for cutbacks and reduction is security. But a security operative or company who is integral to the team is difficult to dispense with.

Benefits of safety and security in customer care

Safety and security are among the most basic human needs. If a person is working somewhere where they don't feel safe and secure, they will not be productive. This is one of the main reasons why clients engage security companies to monitor their premises. Safety and security provide peace of mind for clients whether they are at the location or not. This peace of mind is part of customer care. The security industry monitors the premises so that the client doesn't need to. This serves the client's needs and provides employment for the security sector.

Making the public feel safe is also good customer service. When a member of the public can feel safe in an area because of monitoring by or contact with a security company, then we are serving that person's needs and providing customer service.

Customer care policy

Most organisations have a customer care policy in place which guides the company and its employees in how they are expected to treat customers. A customer care policy will generally include:

- Purpose – the reason why the organisation has the policy in place.
- Scope – who the policy covers, and who must adhere to the policy.
- Vision and values – what does the organisation stand for? What are its core beliefs and values for customer care? This would usually include values such as transparency, integrity, honesty and communication as examples.
- Responsibilities – This section details each of the roles affected by the policy and what their responsibilities are for customer care. Roles include:
 - Senior management
 - Supervisors
 - Security operatives
- Feedback – A facility for customers or the public to provide input and feedback on customer services.
- References to procedures – a range of procedures may be attached to the customer care policy, including:
 - Complaints procedure
 - Communication procedure
 - Investigation procedure
 - Recognition scheme

A security operative's duties in implementing the customer care policy will generally be detailed in the responsibilities section and may include:

- Treat all customers within the core vision and values of the policy.
- Take all training offered regarding this policy, and keep up to date with any new policies and procedures.
- Report any disruption in service to supervisors, human resources and senior management, as appropriate.
- Keep informed of any modifications made to the policy and the changes in training that may result.

Interpersonal skills in customer care

A security operative's interpersonal skills form an important part of customer care. One of the central values of good customer care is communication – the process was discussed earlier. Being able to communicate clearly is essential to providing good customer care. A company policy will provide guidance to security operatives, but they must use their own interpersonal skills to interpret and implement that guidance to the customer.

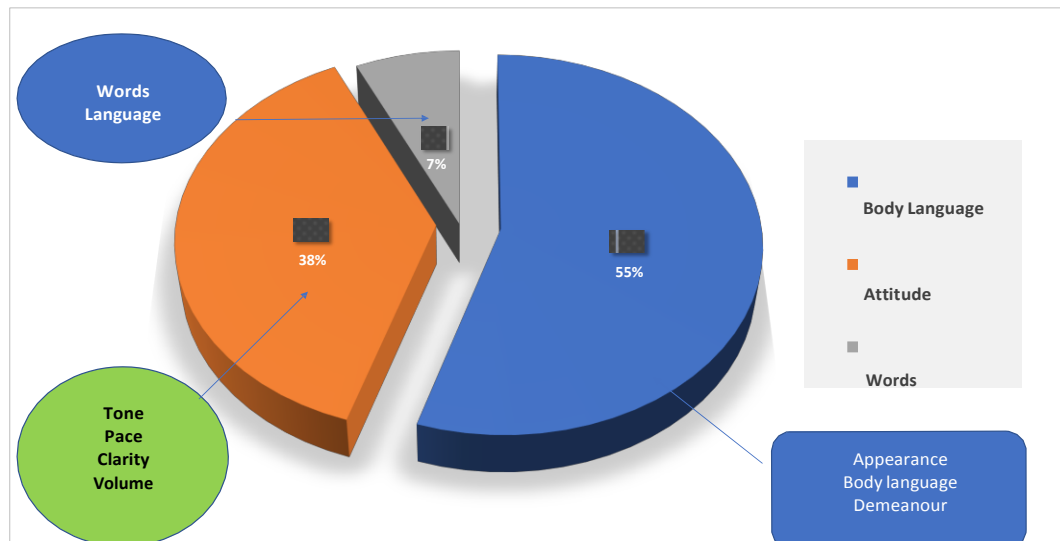
E.2 Describe the methods of effective verbal communications

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Outline the importance of tone and pace in verbal communication
- Outline the importance of clarity and projection
- Explain the benefit of using words with which you are comfortable
- Outline the importance of using suitable and appropriate language
- Outline the importance of clarity when giving instructions
- Outline the importance of listening
- Understand and demonstrate the principles of active listening
- Explain why one should ask different types of questions for clarification
- Summarise the potential effects of not listening
- Outline the risks of being overheard when speaking

Verbal Communication

The graphic below shows a basic illustration of how we communicate as humans. Over 55% of communication is done via body language. The remaining 45% is delivered verbally.



For a security operative working in an alarm receiving centre, much of the communication will not be face to face. Their verbal communication skills must therefore adapt, as they cannot read body language (unless via CCTV) or have their body language read by the respondent. In these circumstances, the security operative must have full control of the tone, pitch, clarity and volume of their voice.

As the graphic above shows, these elements are more important to communication than the wording or language used.

Tone

Tone of voice expresses your way of thinking and your attitude towards the other person. When body language is not available, tone forms a significant part of communication. Your tone of voice can promote a positive relationship with the other person in the conversation, or it can affect it negatively. There are various positive tones that a security operative may choose to use. These include:

- Helpful
- Interested
- Assertive
- Polite
- Confident.

There are also some negative tones that security operatives should avoid. These include:

- Anger
- Sarcasm
- Indifference
- Frustration
- Disinterest
- Rude.

An important point to note is that we can choose our tone of voice. This requires a security operative to be self-aware and to choose a positive tone before communicating with others.

Pace

In stressful conditions, our communication skills can suffer. When the body is under stress, and adrenaline is being produced, the pace of our voice can quicken. This can lead to messages becoming rushed and confusing. This is particularly important if the other person in the conversation is also under stress. Their ability to understand complex language may be inhibited, and the rate at which they understand what is being said may be affected. The security operative must be self-aware and calm themselves sufficiently to control the pace of their communication.

It is also important not to slow the pace too much, as the other person may lose interest in the conversation. The pace should be controlled to ensure that both parties can remain engaged and interested in the conversation.

Clarity

Clear lines of communication are essential. Many factors can affect this, including language difficulties, accents, the medium being used, and environmental noise. The security operative should always try to remove any external interference from the environment, such as background noise or a poor telephone connection, to increase the clarity of a conversation. If language or accent are an issue, the security operative may have to adjust the pace or tone of the conversation.

Projection

Projection of the voice is closely related to the volume. When communicating, the security operative must judge the projection of their voice based on the distance the message needs to travel, the medium being used and external factors such as noise. Common mistakes include speaking too loudly so that others overhear, speaking so loudly that the other person cannot clearly understand, or speaking so quietly that the other person cannot hear you. The message should be projected towards the other person at an appropriate volume given the other voice elements of clarity, pitch and tone. Often the projection can be closely related to the tone used, and both may need to be balanced to ensure a consistent message is delivered.

Appropriate words and language

While words make up only a small part of the overall communication process, they are still important. If we consider talking over the phone, where we do not have the benefit of body language, then using correct wording and language becomes even more important.

The security operative should avoid using words and language that are complex or open to misunderstanding unless it is essential. They should use language that is formal enough to appear professional but also at a level they are comfortable with. Using slang and technical jargon will affect both the clarity and the professional appearance of the security operative. Using overly technical or complicated language also puts more pressure on the security operative and may lead to complications in the communication. Using language that is clear, concise and familiar to the security operative benefits both parties in the conversation.

The security operative should also be aware of using language with negative connotations, such as:

- Don't
- Can't
- Shouldn't
- Wouldn't.

These may give the listener the impression that the security operative is approaching the conversation with a negative attitude. The use of foul or derogatory language by a security operative can never be condoned in any circumstance. Even if the other person uses this type of language, the security operative should refrain from it, as it adds nothing positive to the outcome. The security operative must remember that they are a professional and must use language that is appropriate to their role.

Instructions

When giving instructions to another party, the security operative must ensure they use the correct blend of verbal communication tools to ensure that a clear and appropriate message is sent. This is especially important when giving instructions in an emergency. The security operative should adopt a confident and assertive tone, and project the message towards the person for whom it is intended. They may need to deliberately slow the pace of the instruction and raise the volume of their voice to ensure the message is clear. Clarity and understanding of the instruction should be checked and never assumed. This can be done by using feedback and asking the listener to repeat back the instruction.

Listening

Listening is the process of taking auditory information and forming messages from it. While our eyes are responsible for reading body language signals to the brain, we know this only makes up 55% of the message. The rest, from verbal communication, is delivered through listening. If the security operative is communicating with a person who isn't in the same room, then listening skills are even more important. When we listen correctly we gain information on both the message being delivered and the intent of the person delivering it. There are two types of listening:

- Active listening
- Passive listening.

Security operatives should always seek to listen actively. Active listening will be discussed in detail below, but it is a skill which requires practice. Passive listening is not a professional approach to communication and should be avoided. It reflects poorly on a security operative and has a negative impact on the conversation.

Passive listening

Passive listening is listening without reacting. While the listener may hear what is being said, they are not taking any of the important information from the conversation and are not showing the speaker the attention needed to generate good communication. Passive listening can give the speaker an impression that they are not being listened to. This not only shows a negative attitude from the security operative but can also lead to important information being misinterpreted or missed altogether. It can also evoke negative emotions in the speaker, who feels they are not being listened to. And someone who feels they are not being listened to is more likely to escalate a conversation into a conflict situation.

Active listening

Active listening is the process of listening with intent and listening for resolution. When listening to another party, we need to have an open mind and listen constantly for potential clues to the root of the problem and for a solution to it. Using empathy to establish rapport and show the person you understand their issue is a key part of active listening. Often people in an emotional state just want to be listened to. When we listen actively, we obtain the correct information and form a clear understanding of the issues.

Active listening is a skill which must be practised to develop. Security operatives must make a conscious decision to listen actively. An important part of active listening is acknowledgement. Showing interest in a speaker's body language and acknowledging key pieces of information are important to show them we are listening actively. This can be done with a simple nod of the head or by repeating back important phrases to show understanding. Asking follow-on questions can also signal active listening and show the person that we are interested.

Once the speaker has finished, it may be appropriate to offer them several options to solve their problem. This shows that we have listened to them and understood their issue. Giving the person options often allows them the freedom to choose their own solution. Even if the solution they choose is not ideal for them, they know that we have listened, and they have the freedom to make that choice themselves.

Feedback and clarification

Feedback and clarification are both good tools to help the security operative communicate effectively. When we speak, it is important that we ask questions to generate feedback. This ensures the listener has understood the message correctly before proceeding. When we listen, it is also important that we ask questions, to clarify what the speaker is saying and to ensure we have understood the issue.

When asking questions for either feedback or clarification, the security operative must choose the type of question carefully to get the correct response. There are two types of question:

- Closed questions: these can be answered with yes, no or another single-word response. They are not very good for clarification or feedback, as a person doesn't have to understand the issue to answer. An example of a closed question could be: "Do you understand what I just said?"
- Open questions: these are designed to encourage a full, meaningful answer using the subject's own knowledge or feelings. They require the listener to understand the issue before responding. The response required is more detailed than one word or sentence. Open questions often start with "Why" or "How", which prompt a descriptive response. They are good for gaining clarification and feedback, as they require detail from the original conversation.

Discretion in verbal communication

An important skill in verbal communication is discretion. While clarity and projection are important, they must be balanced with discretion in professional conversations. Confidentiality is a key aspect of the security operative's role in an alarm receiving centre. Security operatives must be very aware of the risks of being overheard when communicating verbally. These risks include:

- Releasing confidential information to unauthorised parties
- Damage to the client's reputation
- Damage to the employer's or the security operative's reputation
- Potential security risks caused by the above.

Security operatives must be aware of their surroundings and mindful of the surroundings that the other person may be in. Confidential information should never be given out unless the security operative is sure it will not be overheard. This may need to be clarified with the listener before delivering such information. Having confidential or personal information overheard may lead to any of the above-mentioned risks and may even breach data protection legislation or be defamatory.

E.3 Outline how to interpret written documents and communicate effectively in writing

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Explain the importance of reading and interpreting site and SOP instructions
- State typical occasions when writing skills are required
- Explain the importance of using appropriate language
- Describe guidelines for clear and accurate writing
- Explain why you consider the reader when writing
- Explain the importance of written presentation

Written communication skills are required for any role in the security industry. Traditionally in the industry, many documents were written by hand. But with the growth of technology, computer-typed documents have become common. In most alarm receiving centres, the security operative will complete both handwritten and computer-written records.

Regardless of whether written records are typed or handwritten, it is important that the content be correct, concise and professionally presented. Your written information reflects directly on your professionalism, no matter what the format. Some examples of where written communication skills are important to the security operative include:

- Taking notes and messages
- Writing reports
- Logging incidents
- Writing requests
- Completing logs and records
- Completing training records

This list is not exhaustive, and security operatives will find themselves creating written records daily.

Interpreting written records

Creating written records is only one part of written communication. The other side of the equation is the ability to interpret written records correctly. An alarm receiving centre will have many types of written record, both paper and electronic. These may include various reports and documents, the most important of which will be the alarm receiving centre assignment instruction and the standard operating procedures (SOP) for the client sites.

Upon starting employment in the alarm receiving centre, the security operative will be given access to the assignment instructions for the site, and must read this document thoroughly. It is not enough to simply skim the text, as it will contain detailed information essential for the operative to be aware of. The security operative must read it carefully and take notes. These notes should include important points from the document as well as questions about its contents for follow-up with a supervisor or management.

Reading and taking notes will help the security operative to interpret the document correctly. This means not just reading and understanding the document but being able to deploy its information in a live situation.

This process should be repeated with each of the client site's SOPs for which the security operative is responsible. The operative must become comfortable with their responsibilities as contained in the SOP before having to use them in a live situation. This will not happen immediately upon reading the SOP, and it may need to be re-read several times before it can be fully interpreted.

Written communication guidelines

When writing, security operatives should seek to achieve four key principles: that written records should be:

- Consistent
- Professional
- Concise
- Factual.

Consistent: Written records should be of a high standard, and that standard must be maintained across all days, shift and security operatives. Each written record of the same type should have a familiar layout, content and structure. Inconsistencies can cause issues with clients who notice differing standards in their records.

Changes in the level of detail or content in written records can cause issues if the records are ever required for court or other legal areas.

Professional: All written records should be presented professionally. If it is handwritten, it should be written clearly and legibly so it can be understood. It should be worded correctly, using appropriate professional language and proper punctuation. It should not contain any slang, abbreviations or technical jargon unless necessary. If the security operative has a concern about their handwriting, then BLOCK CAPITALS should be used.

Concise: The record should have enough detail to cover all the facts and no more. The structure of a record form should support this and leave sufficient space. The security operative must acquire the skill of using only the required information to complete the record. Anything else is wasted.

Factual: All records created by the security operative should be completely factual. The operative is not expected to make records based on opinion or conjecture. The facts are all that matter, and every part of the record must be stood behind as fact. It is fine for the security operative to say they did not see something or cannot remember something, if this is the case. It is better to say this openly than to complete a record using a guess or an opinion which cannot be supported.

Written presentation

When using written communication, it is important to be aware of the quality of the presentation. The content itself may be excellent, but if the presentation is sloppy or unprofessional in appearance, this can detract from the reader's overall impression of the document. Presentation includes the layout, writing style and format of the record. When writing a formal record, the security operative should ensure:

- The writing style is formal and professional. This means there should be no slang terms or abbreviations.
- If the document is handwritten, the writing should be clear and legible. If a security operative is unsure about the legibility of their handwriting, they should consider using block capitals for clarity.
- Where the document is typed, the font should be a clear, basic font style.
- The written record should be properly laid out, using paragraphs.

When completing any written record, the security operative must take the reader into consideration. The reader could come from a wide range of stakeholders and may not have a security background. If the report contains technical terms known only in the security sector, this may be confusing for the reader.

It is also important to note that the reader will form an impression of the security operative and the security firm based on the written presentation. The operative should try to present themselves and their company in a positive light in the document by following the guidelines above and by maintaining high levels of professionalism throughout the writing.

Privacy may also have to be considered. There may be people to whom the document will be circulated who may not be directly involved in the incident or occurrence being documented. In such cases it may be necessary to omit certain personal details for privacy or data protection reasons. In some cases, written records may also need to be redacted before being sent to readers.

E.4 Explain the importance of observation skills in the performance of duties

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- What is meant by observe and observation?
- Outline the importance of accurate memory recall in the performance of security duties
- Outline what senses are most beneficial for effective observation skills
- Explain what is a mental note
- Outline how to describe a person and a vehicle
- Outline the skills needed to interpret an image

Observation

Oxford Dictionaries Online has several meanings for the word 'observe'. In a security industry context, the more relevant meanings include:

1. To notice or perceive (something) and register it as being significant.
'she observed that all the chairs were already occupied'
2. To watch (someone or something) carefully and attentively.
'Rob stood in the hallway, from where he could observe the happenings on the street'
3. Take note of or detect (something) in the course of a scientific study.

'the behaviour observed in groups of chimpanzees'

All the above meanings would involve the security operative noting something out of the ordinary and deciding to pay more attention to it. The ability to observe rather than just watch when involved in a security task is an important skill. The ability to observe something or someone – observation – is different from watching in that it involves a detailed viewing of the object and its actions rather than just seeing.

When observing a person or situation, the most obvious sense used is our sight. Our eyes form a picture of the scene and send a signal to the brain of what it sees. The secondary senses of hearing and touch support sight in giving an overall situational impression of the scene if the security operative is physically there. But if the scene is being viewed remotely on CCTV, the security operative will only have sight at their disposal.

Memory and recall

In a dynamic situation, the security operative will most likely not have the opportunity to immediately record in writing all the details as they happen. Other, more pressing matters will most likely require the operative's attention when dealing with an incident. It is therefore important that a security operative possess sufficient memory recall to ensure they can accurately remember detailed information about an incident some time afterwards.

Memory recall can be influenced by a range of factors, including but not limited to:

- Fatigue
- Stress
- Illness
- Environmental issues (noise, distractions, etc.).

The security operative should be aware of these and try to minimise their impact. Memory recall can be increased by working in a calm, controlled environment and by remaining calm under stress. The use of acronyms can help in memory recall, and will be discussed later when detailing persons and vehicles. Accurate memory recall is a vital skill that security operatives must develop from an early stage. Testing this skill may be appropriate in roles where it is a common part of the security operative's function. It may also be prudent for a security operative to make quick written notes of an incident to assist with memory recall later.

Mental notes

During routine daily occurrences or other incidents, security operatives may make a 'mental note' of an issue. This involves noting an occurrence that requires further detail or explanation, either verbally or in writing, and making an internal note in their mind to give it more attention later.

In a fast-paced environment, mental notes can be important, as not all occurrences will be discussed or recorded in detail at the time. An important aspect of making a mental note is the ability to recall it later. This links closely with the skill of memory recall. A mental note is useless if the security operative does not recall it later and give the issue the attention it requires.

Descriptions

To provide an effective security service, the security operative must be able to provide accurate records of events they have witnessed. One of the most important parts of any written record is the description of the parties. This enables the reader to clearly visualise or identify the people involved in an incident. When describing a person, it is important to give accurate physical details in a structured manner.

When giving a description of a person, we first use what is known as an identity classification (IC). This describes the part of the world a person's appearance looks closest to. There are six categories of IC descriptors, and they are used to indicate a person's general appearance and skin tone. They are not binding to a country but reflect various skin tones and regions of the world.

Following an IC descriptor, seven other details are required to give an accurate description of a person. These are known as the SABHHIC details and are widely used in the security industry, as they give structure and accuracy to a physical description.

Identity Classification	
IC 1	White
IC 2	Mediterranean
IC 3	Black
IC 4	Asian
IC 5	Arabic
IC 6	Indian

Descriptions		
S	Sex	Male Female
A	Age	Approximate age
B	Build	Thin Medium Heavy
H	Height	Approximate height Imperial: 6 feet Metric: 1.7 metres
I	Identifying features	Scars Tattoos Accent
C	Clothes	Top down Colour Brand Names

Description example: IC1 male, approximately 20 to 25 years old, medium build, 5 feet 9", short brown hair, rose tattoo on lower left forearm, wearing a blue Nike hooded top, black jeans and black Reebok running shoes.

Give only the details that can be factually supported. Where estimations are given always use the word 'approximately'. Don't give opinions of the person in the description which cannot be supported, and don't try to fill in the blanks in your memory with guesses. If a security operative did not recall the brand of hooded top being worn, that is fine, but they should not guess.

Vehicle descriptions

Like with a person, a vehicle should be described in an accurate and consistent format. The following is a good format for describing a vehicle:

- Colour
- Make
- Model
- Registration (or partial)
- Identifying features
- Actions

Example vehicle description: Black Ford Focus, 10 D 1234, broken rear left light, driven erratically.

Interpreting images

Interpreting images is a key part of the security operative's role, and it merges several skills we have discussed above. These include the ability to observe an incident, the capability to use memory recall, and the experience to put the incident into context. For example, a car observed driving slowly past a perimeter fence may not be immediately suspicious. But if the security operative recalls the same car driving past multiple times, due to its broken rear light or part of the registration, then it may require further investigation.

All the skills mentioned above work together in this example to interpret the image. First, the initial observation of the car and recording of a mental note of its description in a structured format. Then the memory recall required to bring the second sighting into context, and the ability to accurately recollect the identifying features of the vehicle. All these skills were used to interpret an otherwise innocuous image and make it relevant to the security operative.

E.5 Explain how to compile reports for a range of incidents

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Define the term record
- State the reasons why a monitoring centre employee should record details in writing as soon as possible after an incident
- Outline the potential dangers of just relying on memory rather than a written record
- Outline the range of persons who might use the written report details after it has been put on record
- Explain the term pro-forma
- Provide examples of a typical report format
- Explain what is meant by chronological order
- Outline details that may be required in a typical report
- Outline the range of incidents which may require a written report
- Give examples of the 24 hour clock

Records

A record can be defined as: a thing constituting a piece of evidence about the past, especially an account kept in writing or some other permanent form.

Once we commit information to writing, electronically or on paper, it becomes a record in permanent form. Written records are an important part of the service provided by security firms to their clients and are an integral part of a security operative's duties.

Importance of written records

While we have already discussed the important ability to make a mental note of incidents, it is equally important that these mental notes be committed to written record as soon as is practicable after an event. There are several reasons for this:

- The limitations of human memory may lead to the accuracy of the mental note reducing over time.
- Written records form an important part of the document audit trail provided to clients by the security firm.
- A written record will be required for any follow-up legal or insurance proceedings relating to the incident.

There is a need to retain mental notes during an ongoing incident, but it is also important that we do not rely on them completely. Committing short written notes to paper or electronic form during an incident can help stimulate memory recall. The longer after an incident we rely on memory recall, the less accurate the memory will be. Early written records also ensure that the security firm can provide up-to-date information and guidance to their clients on incidents occurring at their property.

Failure to produce written records in a timely manner could result in:

- Inaccurate records being made
- Damage to the security firm and security operative's reputation
- Important information being missed or omitted from reports to clients
- Written records being deemed inadmissible in legal proceedings.

Written record circulation

Each written record could have a different number of people to whom it will be circulated, depending on the nature of the record and the client's requests. The readers may include people such as:

- Other security employees of the monitoring centre
- Monitoring centre management
- Clients
- Property management companies
- Insurance providers
- Statutory bodies such as Gardaí or Health and Safety Authority officials.

Security operatives, when compiling any report, must be aware of the potential number of people who may be reading their written records.

Pro forma

A pro forma record is any standard document or form designed to be filled out in a certain way. In the security industry many companies use pro forma forms to ensure a consistent approach to completing company records. These may come in paper or digital form and have pre-prepared spaces for the security operative to add specific information about events. Examples of pro forma records can include:

- Daily occurrence logs
- Incident reports
- Accident reports
- Visitor logs
- Fire safety checklists
- Key control logs
- Equipment checklists.

Report Format

A report should be compiled for any incident that requires the attention of management or supervisors. It should be written as soon as is practical after an incident occurs, and should be a concise and factual account of what happened. General guidelines for writing incident reports are:










- Reports should have a proper structure and be professionally presented.
- They should be written in black ink for clarity and ease of photocopying or scanning, or in electronic format.
- They should be clear to the reader and contain the facts of the incident.
- Avoid using slang or abbreviations.
- Don't give opinions or perceptions, as these are open to interpretation.
- When giving times, use the 24-hour clock.
- Write clearly and legibly. The report will be completed after an incident, so there will be time to write the report out properly.
- Always remember to sign and date your report if writing by hand.
- Cross out any space left on the paper following your signature and date.

The report format is:

- I AM – Name and role
- ON – Day and date
- AT – Approximate time
- IN – Place of work and position
- I WAS – What you were doing prior to the incident
- I SAW – Who you saw, descriptions of people, what you saw them do
- I DID – What you did, your actions and words
- THEY DID – How the other person reacted. Did they comply, run, etc. Their personal details if required.
- IT ENDED – How the situation ended. Were emergency services called?

Identity of emergency services workers who attended? Which managers were present, or who was told? Was the client informed?

Incident Report Format

<ul style="list-style-type: none">Your nameYour job role	<ul style="list-style-type: none">DayDate	<ul style="list-style-type: none">Time24 hr clock	<ul style="list-style-type: none">Place of workPosition	<ul style="list-style-type: none">What you were doing
I am 	On 	At 	In 	I was 
<ul style="list-style-type: none">Who you sawDescriptionsWhat you saw them do	<ul style="list-style-type: none">What you did about itType and level	<ul style="list-style-type: none">How the other person respondedWhat they did	<ul style="list-style-type: none">How did the incident endOfficials presentManagement aware	<i>Always sign and date your report</i> <i>J.Smith</i>
I saw 	I did 	They did 	It ended 	

A pro forma document will usually be used to complete an incident report. Its use ensures that the client sees the information in a consistent format after each event and that the security firm always receives the information in a set format.

A standard report format is set out below:

Accident & Incident Report Form

Site:		Reference:	
--------------	--	-------------------	--

Incident Type		Date:		Time:	
----------------------	--	--------------	--	--------------	--

Security Operative 1		Security Operative 2	
Security Operative 3		Security Operative 4	
Manager on Duty		Garda/EMT:	

Customer Details

Surname:		First Name:	
Address:			

Date of Birth:		Telephone:	

Accident/Incident Details

Accident/Incident Summary	
Injury Details	

Treatment Details (if applicable)

First Aider:		Role:	
Treatment Given			
Further Advice			

Times and Dates

When noting times and dates in a report, the format should always be the same. Reports should be in chronological order. This means their content should run in the order that things happened, to give a true reflection of events. Dates should be given fully, using the day, month and year in full, for example "12 April 2018".

Times should always be given in 24-hour clock, and local time included if monitoring premises in another time zone. For instance, if an incident occurred at 5 minutes to midnight in Ireland, the time is recorded as 23.55. But if it occurred on a client's property in Spain, it may be recorded as 23.55 GMT (00.55 CET).

Types of incidents

Reports are required for any incident that requires attention from management or the client. This could include:

- Alarm activations
- Trespassers
- Visitors
- Equipment failures
- Fire
- Flooding
- Criminal actions
- Statutory body visits
- Damage to property
- Any other event which the client requests to be informed about.

E.6 Outline the range and uses of communications equipment

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Understand and demonstrate the use of the phonetic alphabet
- Understand and give examples of codes and code words
- List communication equipment and state their benefits
- Outline correct telephone and radio procedures

Communications equipment

The security industry uses various forms of communication equipment, including:

- Telephone
- Two-way radio.

Telephone procedures

Security operatives often have to use the telephone to send and receive messages. The benefits of these devices include the relative security of communication, ease of use, and widespread availability. It is important that security operatives handle these communications in a professional and efficient manner:

- Security operatives should always clearly identify themselves when answering the telephone.
- The first priority is to take the name and position of the caller, the reason for the call, and the account verification details.
- Bad language or derogatory terms should never be used on the telephone.
- Details of the call should be written down and recorded for passing on to the relevant person or for accurate recording in the occurrence book.
- If you can resolve the person's query immediately, do so.
- Do not offer any additional information or gossip to the caller, and do not engage in non-work conversations or speculation.

Two-way radio procedures

Two-way radios are often used by security operatives to communicate over a distance further than a voice can travel. Their benefits include the ability to send a message quickly to a large number of people and the ability to communicate as a group. They are standard equipment in the security industry.

There are generally two types of unit used in the security industry:

- Base station: A fixed unit kept at the control room or communications centre.
- Handheld unit: A mobile unit carried by security operatives throughout a site.

Two-way radio guidelines

- Security operatives should know how to correctly operate the radio assigned to them.
- If using an earpiece, ensure it is firmly attached before turning the radio on.
- Memorise all the emergency codes in use.
- Keep all conversations brief and to the point. (Think before talking.)
- Never use radios for non-work conversations.
- Remember that even though some radios operate on a secure frequency, there is always the possibility that somebody is listening in.
- If a radio fails, the security operative should inform control via phone ASAP.
- Radios are location-specific. Security operatives must not bring their radio off the premises where they work.
- Listen on the air before transmitting, to avoid interrupting or cutting off other units.
- Use a call sign to identify each party before each transmission, and wait for the other party to acknowledge before proceeding.
- Learn the standardised pro-word (procedure word) codes used for all radio transmissions.
- Learn the phonetic alphabet. Read back numbers and letters to confirm accuracy.
- Do not shout into the radio. Speak in a normal voice.
- Hold the PTT (Push to Talk) button for 1–2 seconds to establish contact before speaking.
- End each transmission with “Over” and end the final transmission with “Out”.
- Never transmit names or places of work over the radio – especially when announcing breaks or off-duty times.

Phonetic alphabet

The phonetic alphabet is an important element of radio transmissions. It is used to clearly spell important words over the radio. It is also often used to make up call signs.

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

Call Signs

A call sign is a unique identifier used on two-way radios to clearly identify the caller before sending a message. Sometimes the call sign will be specific to a security operative, or it may be specific to the location they are working in. Before beginning any message, security operatives should use their call sign to identify themselves and the person they are calling.

Pro-words

Pro-words are a set of key terms and phrases used in two-way radio messages to clarify and standardise radio communications. All security operatives need to learn the pro-words and their applications, as they are common throughout the security industry. Pro-words, sometimes called code words, are simply shortened versions of common phrases. The table below sets out common pro-words:

Pro-word	Meaning
Stand by	Remain silent and in position to receive further information
Ignore last	Last transmission was in error. Please disregard.
Figures	Numbers
I repeat	I am repeating my last transmission
I spell	I will spell phonetically
I confirm / Please confirm	I am confirming / Please confirm that the last transmission was correct
Over	End of my transmission, I expect a reply
Out	End of my transmission, I do not expect a reply
Go ahead	Ready and waiting to receive your message
Relay to	Please pass this message to
Roger	I have received and understood your message
Time	Time to follow (24-hour clock)
Wait out	I can receive/reply to your message. Wait a short time.
Location	My location is / What is your location?
ETA	Estimated Time of Arrival
Radio check	Confirm that your radio is working
RTC/RTB	Return to Control/Base

Radio check

A radio check is a standard initial message sent by every security operative on receiving a radio. It is used to ensure that the radio unit can send and receive a message.

The security operative sends a message to a monitoring centre, seeking a radio check. The centre replies, confirming receipt of the message. The operative confirms they have received the reply and are ready to start their duty. Example:

Security operative: *“Sierra Oscar to Control, radio check, over.”*

Control: *“Control to Sierra Oscar, receiving your signal loud and clear, over.”*

Security operative: *“Sierra Oscar to Control, roger, out.”*

Priority transmissions

In general there are two different levels of transmission:

- Medium priority
- High priority.

Medium-priority messages make up the vast majority of radio communications and always begin with the call sign. High-priority messages are reserved for serious incidents, and when these are used the standard transmission rules are broken. When sending a high-priority message, an emergency code word is placed before the message to ensure that everybody is aware that this message takes precedence over other radio messages. Example:

“Code Black, code black, Sierra Oscar to control, assistance required at the main door, over.”

E.7 Explain the importance of interpersonal skills in dealing with people

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Explain the importance of understanding others' point of view
- List interpersonal skills and reasons they are important to a monitoring centre employee
- Explain how to give constructive feedback
- Outline the main differences between assertiveness and aggressiveness

Interpersonal skills

Interpersonal skills are the skills people use to interact with each other in a group. Security operatives in a monitoring centre have to show their interpersonal skills daily with colleagues, clients and the public. Some important interpersonal skills were discussed in earlier sections. Key interpersonal skills required by security operatives include:

- Verbal communication – The ability to speak clearly, calmly and professionally to others using appropriate tone and body language. This is often the only asset a monitoring centre operative has when taking telephone or radio calls.
- Non-verbal communication – The ability to use appropriate body language when communicating with others. Presenting a professional appearance through presentation, posture and stance.
- Listening skills – The ability to hear attentively and process information correctly. This is essential when dealing with issues on the telephone or in person, so that the security operative gathers the correct information and interprets the problem correctly.
- Empathy – Understanding people's problems and showing that understanding in a positive way, so the other person feels understood and listened to. It is also important to use empathy to show the other person that we understand and value their point of view.
- Negotiation/conflict management – This means being able to discuss and reach an agreement in a professional manner. Negotiating and managing conflict are key interpersonal skills in the security profession. People often contact a monitoring station because of an issue or problem. We can't begin to solve it when the person is being adversarial to the security operative. The ability to negotiate conflict successfully leads into problem-solving skills.
- Problem-solving – The ability to effectively resolve issues – technical or behavioural – that are presented to the security operative. The operative must be able to analyse, prioritise and solve common problems that arise.

- Decision-making – Making effective decisions is important in a monitoring centre environment, as these decisions could have many knock-on consequences for the security firm and the client. Monitoring centres will have policies and procedures in place to guide the security operative in making decisions and escalating decisions to management, but the operative still needs to make the basic decisions correctly.
- Assertiveness – From time to time, security operatives will encounter challenging situations. In these situations, assertiveness is an important interpersonal skill. You must be able to support your point with rational argument and not be bullied or intimidated.

Points of view

Everyone the security operative encounters will have their own perspective and point of view. Sometimes these won't align with those of the operative, the security firm or the client. The client's point of view may also not agree with the security operative's. It is important that the security operative does not take this personally and remains professional.

Understanding that other people's points of view will not always be the same allows security to better manage incidences of conflict and show empathy. Even though a security operative may not agree with the other person's point of view, they must respect it and try to understand it. When the security operative can empathise and show understanding of the other person's perspective, it becomes much easier to use problem-solving skills to resolve the issue.

Assertiveness v. aggression

Assertiveness is a key interpersonal skill for security operatives – aggression is not. The two behaviours are often confused, which can lead to further conflict. An assertive person can assert a rational opinion respectfully to others. They speak clearly and openly while displaying positive body language and a conversational tone of voice. An aggressive person attacks people who do not share the same viewpoint.

Their tone is adversarial, and their body language is intimidating. They show a lack of respect to the other person.

Security operatives must remain in control of their emotions and be self-aware so that their actions are not perceived as aggressive. Assertive behaviour is a positive trait, but it can easily be clouded by emotions and turn to aggression.

E.8 Explain the benefits of teamwork

Learning outcomes are designed to enable candidates understand the responsibilities of persons working in the Monitoring Centre. By the end of this section you should be able to:

- Define teamwork and provide examples
- List the benefits of teamwork
- Outline the various roles in a team
- Explain who makes decision in teams
- Explain why respect is important

Teamwork

Teamwork is the concept of a group of people working together towards shared values and goals. In a monitoring centre there may be one overall team which consists of smaller teams all working towards the security firm's overall goals. Teamwork is not a simple concept, and it requires a number of ingredients working together to be effective. These ingredients include:

- Co-operation
- Relationships
- Leadership
- Respect.

Co-operation

Teamwork requires the co-operation of all elements of the team to work. If one area is not co-operating, then the team fails, because all the parts depend on each other to succeed in the overall goal. An example of this in a monitoring centre is the co-operation between shifts. If the day shift leaves work undone for the night shift, this affects the night shift's ability to do their job, which in turn adds to the day shift's workload the next day. The initial lack of co-operation caused the breakdown in workload, leading to further lack of co-operation which could harm the efficiency of the entire team.

Relationship

There must be positive working relationships for a team to exist. The relationships must be professional and courteous. The people on a team do not need to have any positive *personal* feelings towards the other team members, but the *professional* relationship must remain positive. For example, two people with different social interests, backgrounds and beliefs may come together on a project and complement each other's skills to make a good team. They may disagree on many things outside of work, but in work they can co-exist professionally.

Leadership

Good teams have leadership throughout. In any team there will always be stronger personalities who will take a leading role, but it is important that others' views are also heard. Leadership can come from rank (managers, supervisors, etc.), level of experience, or personality. The best teams have leaders spread throughout and don't rely on one person's leadership to function. This means that even if one or several key people leave, the team can still function efficiently.

Respect

Respect is a key value in any organisation and especially in teams. Respect means showing consideration of other people's values, beliefs and ideas. It requires all members of the team to be aware of the values of others and to adhere to the other three ingredients discussed above. Respect should be present in all dealings with team members and with people outside the team. It is a two-way process. If respect is not given, then over time it will not be received either. An example of this may be asking for input from all team members in decision-making, or recognising that a team member needs support in a particular area and helping them.

Benefits of teamwork

The benefits of teamwork can include:

- Foster creativity and learning – People can come up with ideas and solutions and have team members evaluate those ideas. This allows people to be creative with ideas without worrying about having sole responsibility for the decision.
- Complementary Skills – Teamwork allows people with skills in certain areas to support others who don't. It also allows people to be supported with their weaknesses. Teams bring together people with different skills and personalities which can be merged to form a team with a complete skill set.
- Trust – Teamwork allows a bond of trust to develop between team members over time. When people are supported and helped by team members, they begin to trust them. They also begin to trust more in their own ability, safe in the knowledge that the team can support them.
- Negotiation skills – Teamwork helps people to develop their negotiation skills.

People in teams will have different ideas and viewpoints. A person must be able to put forward their ideas and support them through negotiations and conflict. They must also learn to accept that their ideas will sometimes not be retained. These negotiation skills have a wider benefit for the person and the organisation.

- Ownership – Being part of a team promotes a sense of ownership. A person is responsible for a certain part of a project or role, and they must manage it effectively or the entire team suffers. The resulting sense of buy-in, of not wanting to let colleagues down, can be a powerful motivator.

Roles in teams

Dr Meredith Belbin, a famous researcher on the roles of teams, studied people's interpersonal performance as they worked together over many years. His Nine Team Roles model is used worldwide to help people understand own role and function in a team. Belbin suggests that by understanding your role in a team, you can develop your strengths and manage your weaknesses as a team member, and so improve how you contribute to the team.

Belbin identified nine team roles and placed them into three groups: Action-Oriented, People-Oriented, and Thought-Oriented. Each team role is associated with typical behavioural and interpersonal strengths. Belbin also defined weaknesses that tend to accompany each team role. He called these the "allowable" weaknesses; as with any behavioural weakness, they are areas to be aware of and potentially improve. Having a balanced team with a distribution of roles is important.

Action-Oriented Roles

Shaper (SH)

Shapers are people who challenge the team to improve. They are dynamic and usually extroverted people who enjoy stimulating others and finding the best approaches for solving problems. The Shaper is the one who shakes things up to make sure that all possibilities are considered and that the team does not become complacent. Shapers often see obstacles as exciting challenges, and they tend to have the courage to push on when others feel like quitting. Their potential weaknesses are that they may be argumentative and may offend people's feelings.

Implementer (IMP)

Implementers are people who get things done. They turn the team's ideas into practical actions and plans. They are typically conservative, disciplined people who work systematically and efficiently and are very well organised. These are the people you can count on to get the job done. On the downside, Implementers may be inflexible and can be resistant to change.

Completer-Finisher (CF)

Completer-Finishers are the people who see that projects are completed thoroughly. They ensure there have been no errors or omissions, and they pay attention to the smallest of details. They are very concerned with deadlines and will push the team to make sure the job is completed on time. They are perfectionists who are orderly, conscientious and anxious. Completer-Finishers may worry unnecessarily, and may find it hard to delegate.

People-Oriented Roles

Coordinator (CO)

Coordinators are people who take on the traditional team-leader role; they are also referred to as the chairmen. They guide the team to what they perceive are the objectives. They are often excellent listeners and are naturally able to recognise the value of each team member. They are calm and good-natured, and they delegate tasks very effectively. Their potential weaknesses are that they may delegate away too much personal responsibility and may tend to be manipulative.

Team Worker (TW)

Team Workers are people who provide support and make sure that team members are working together effectively. They have the role of negotiators in the team and are flexible, diplomatic and perceptive. Team Workers tend to be popular people who are very capable in their own right, but who prioritise team cohesion and helping people get along. Their weaknesses may be a tendency to be indecisive, and to be uncommitted during discussions and decision-making.

Resource Investigator (RI)

Resource Investigators are innovative and curious. They explore available options, develop contacts, and negotiate for resources on behalf of the team. They are enthusiastic team members, who identify and work with external stakeholders to help the team accomplish its objective. They are outgoing and often extroverted, so others are often receptive to them and their ideas. On the downside, they may lose enthusiasm quickly, and are often overly optimistic.

Thought-Oriented Roles

Plant (PL)

The Plant is the creative innovator who comes up with new ideas and approaches. They thrive on praise but find it hard to deal with criticism. Plants are often introverted and prefer to work apart from the team. Because their ideas are so novel, they can be impractical at times. They may also be poor communicators and can tend to ignore given parameters and constraints.

Monitor-Evaluator (ME)

Monitor-Evaluators are best at analysing and evaluating ideas from other people (often Plants). They are shrewd and objective, and they carefully weigh the pros and cons of all the options before coming to a decision. Monitor-Evaluators are critical thinkers and strategic. They are often perceived as detached or unemotional. Sometimes they are poor motivators who react to events rather than instigating them.

Specialist (SP)

Specialists are people who have specialised knowledge that is needed to get the job done. They pride themselves on their skills and abilities, and they work to maintain their professional status. Their job in the team is to be an expert in an area, and they commit themselves fully to that field of expertise. This may limit their contribution and can lead to a preoccupation with technicalities at the expense of the bigger picture.

Decision-making in teams

Teams are most effective at decision-making when they contain complementary skills and personalities. Complementary skills allow team members to examine issues from various angles and to see the implications of their decisions from various perspectives. Teams use problem-solving techniques to make decisions after looking at all the options. To solve problems effectively, a step-by-step decision-making process is used, such as this:

- Recognise the problem – The first step in decision-making is to recognise that a problem exists that must be addressed.
- Define the problem – The next stage is to define exactly what the problem is.
What is its root cause? How long has it been going on, and how big is the problem?
- Gather information – Once the problem has been defined, the team can begin to gather information to confirm the findings in step 2 and come up with solutions.
- Develop alternative solutions – This is where the team value becomes obvious. The different roles in the team use techniques such as brainstorming to come up with a variety of potential solutions to the problem.
- Select the best alternative – All the options are explored, and each team member's views are negotiated, until a consensus is reached on the best option. The decision is then made.
- Implementing the solution – The decision is applied in the workplace once the team is ready.
- Evaluation – The effectiveness of the solution is evaluated. If it works, then the decision-making was a success. If it does not, then the team returns to step 3 and begins again.