GET LICENSED

DOOR SUPERVISOR TOP UP TRAINING

STUDY NOTES

Level 2 Award

For Door Supervisors in the Private Security Industry (Top Up)

Dear Student,

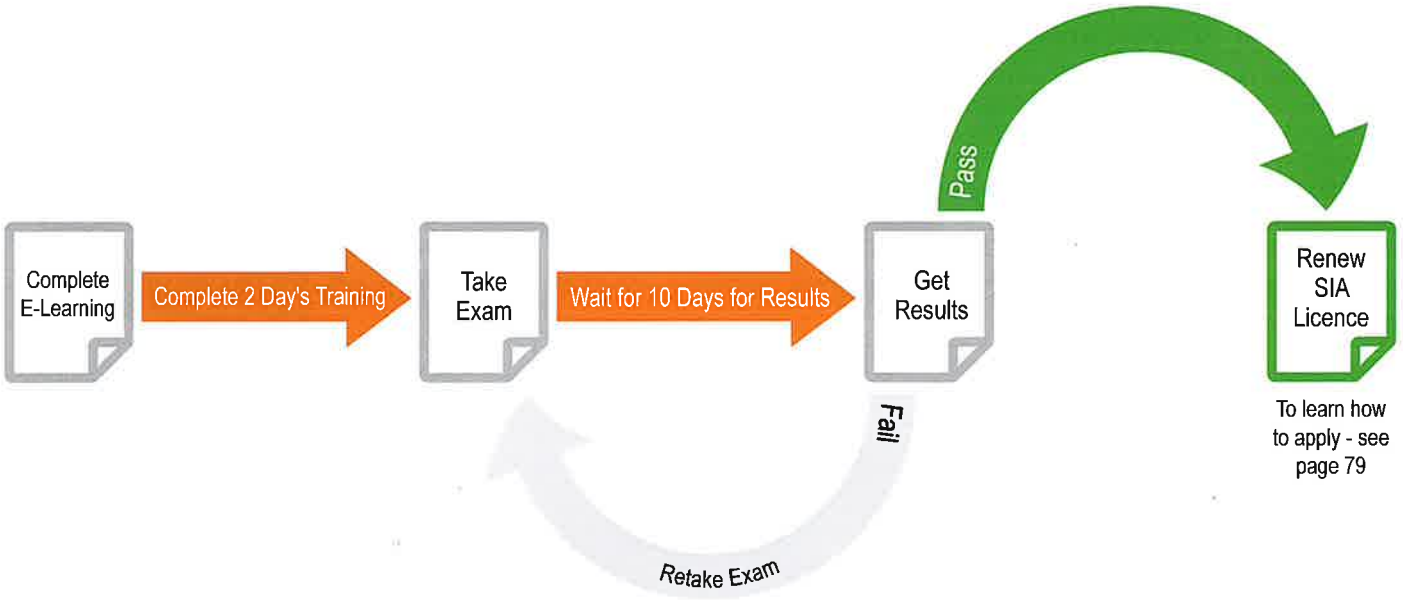
Greetings and welcome to the Door Supervisor Top Up training. Please read the following information carefully.

The Door Supervisor Top Up course has three units and runs over **two days.**

Remember:

1. You must attend both full days of training.
2. Bring the relevant ID Documents.
3. Complete your pre-course e-learning module, including proof of ACT training
4. Participate actively in the training process.

Training Provider Name	
Instructor Name	
Exam Date	
Expected Results Date	



FAQ

Q. When is the exam?

A. The exams are on the last day of the course.

Q. How long will it take to get the results?

A. Results are sent via email and SMS message as soon as the exam body marks them. Please allow ten working days from the date of your exam to get your results.

Q. When can I apply for the SIA Licence?

A. You can apply for the SIA Licence once you have received your result and you have passed all four units.

Q. What if I fail my exam?

A. In the unlikely event of failing one or more units, you will have to come to retake the exam(s). The current exam retake fee is £90, if you have the Flexi+ package, you can take unlimited exam retakes at no extra cost. If you are worried about your exams and would like to upgrade to Flexi+ -- please speak with your instructor.

Q. What if I am not happy with the course?

A. If you are unhappy with any aspect of your course, first speak with your Instructor, if you are not happy with the outcome, please inform Get Licensed, and we will **do the right thing!**

Your success is our success!

Door Supervisor Exams and Assessments

Door Supervisor Exams and Assessments

Course Duration: Classroom of 14 Hours 35 min* taught over 2 Days:

Exam Name	Number of Questions	Pass Mark	Time Allowed
Principles of Terror Threat Awareness in the Private Security industry	10	7 (70%)	20 Min
Principles of Using Equipment as a Door Supervisor	5	4 (80%)	10 Minutes
Application of Physical Intervention in the private Security Industry Theory	30	24 (80%)	45 Minutes
Practical Assessments including: Use of Radios Physical Intervention	NA	NA	NA

*Course will be reduced to 13 hrs 35 min once the SIA releases their online ACT for Security E-Learning (Expected Summer 2021)

Mock Exams - scan to take a mock exam.

Identity documents required for SIA courses

- ☑ One identity document from the list Group A **and**
- ☑ Two documents from the list Group B **and**
- ☑ A passport size photo of yourself

Out of the three documents, at least one document must show your current address and at least one document must show your date of birth. Each document should be the original, physical document. The SIA will not accept a scan or photocopy.

Group A documents list

A1 Current, valid UK passport.

A2 Current, valid passport of any other nationality.

A3 Current, valid photocard driving licence if it was issued by the DVLA in Great Britain.

A4 Current, valid photocard driving licence and its paper counterpart issued by the DVA in Northern Ireland.

A5 UK original birth certificate issued within 12 months of birth.

A6 Current, valid UK biometric residence permit card.

Group B documents list

B1 Bank or building society statement issued to your current address, less than three months old. You can use more than one statement as long as each is issued by a different bank or building society.

B2 Utility bill (gas, electric, telephone, water, satellite, cable) issued to your current address within the last three months. You can only submit one utility bill in support of your application.

B3 A credit card statement sent to your current address within the last three months. You can submit more than one statement as long as each is issued by a different issuer.

B4 Council Tax statement issued in the last 12 months.

B5 Mortgage statement issued in the last 12 months.

B6 Letter from H.M. Revenue & Customs, Department of Work and Pensions, employment service, or local authority issued within the last three months. You can submit more than one letter as long as each is issued by a different Government department or a different local authority.

B7 P45 statement of income for tax purposes on leaving a job issued in the last 12 months.

B8 P60 annual statement of income for tax purposes issued in the last 12 months.

B9 Current UK driving licence - paper version (not the paper counterpart to a photocard).

B10 Driving licence photocard (without a paper counterpart) issued by the DVA in Northern Ireland.

B11 Pension, endowment or ISA statement issued in last 12 months.

B12 Valid UK firearms licence with photo.

First Aid Requirement for Door Supervisor and Security Officer training

You must complete the First Aid qualification as part of your training package unless you already have a current and valid First Aid or Emergency First Aid certificate which you must bring on your course (your certificate must be valid for at least 12 months from the start date of your security course).

Table of Contents

PRINCIPLES OF TERROR THREAT AWARENESS IN THE **PRIVATE SECURITY INDUSTRY**

CHAPTER 1 Terror threats and the role of the Security Operator

Terrorism:

Terrorism is the use or threat of action, both in and outside of the UK, designed to influence any international government organisation or to intimidate the public. It must also be for the purpose of advancing a political, religious, racial or ideological cause

Terrorism Threat Levels:

The official source of UK Threat Level is (MI5) and their website is https://www.mi5.gov.uk/threat-levels.

As well as knowing what each level means an operative would ideally need to know how it may impact the response level their location may have

LOW - means an attack is highly unlikely

MODERATE - means an attack is possible, but not likely

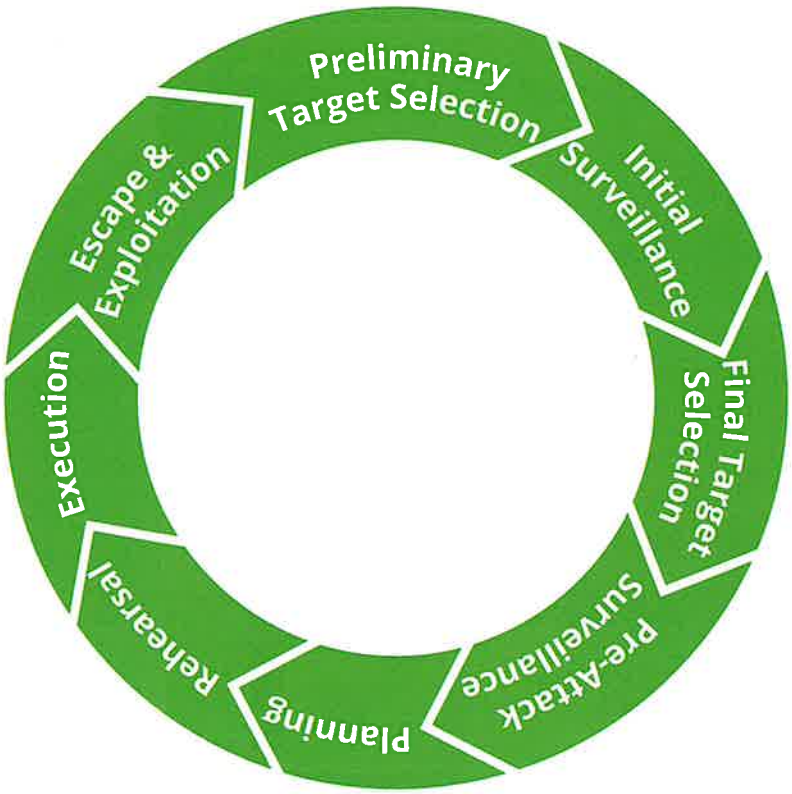
SUBSTANTIAL - means an attack is likely

SEVERE - means an attack is highly likely

CRITICAL - means an attack is highly likely in the near future

Security operatives need to understand how the current terrorist threat level will affect them at their own place of work, this should be outlined in their assignment instructions.

Common Terrorist attack methods:



Current Terrorist Attack Methodologies:

Marauding Terror Attack (MTA)

This type of attack could use firearms, knives, sharp objects or blunt objects while on foot to attack people in the area

Types of Explosive Devices commonly used in attacks:

- Improvised Explosive Device (**IED**)
- Person-Borne Improvised Explosive Device (**PBIED**)
- Vehicle-Borne Improvised Explosive Device (**VBIED**)
- Leave Behind Improvised Explosive Device (**LBIED**)

Vehicle Attacks:

More often vehicles can be used as a weapon.This can be known as VAAW. Vehicles are used to target crowds and ram into people to cause severe damage such as the Westminster Bridge Terror attack which took place in London on 22 March 2017. This attack resulted in 6 deaths and 49 people injured.

Chemical Attacks:

Chemical warfare was widely used in World War 1 which resulted in many deaths including those of civilians as there was little way to control where the chemicals travelled once they were deployed. After the war most countries agreed not to use chemical or biological weapons in future conflicts. However terrorists can manufacture weapons using many products available over the shelf and use these against the wider population

Biological Attacks:

Bioterrorism is the use of biological agents to cause illness or death in humans, plants or animals. They can be made using viruses, funghi, toxins or bacteria. These could be naturally occurring or man made or man manipulated. They can be spread through water supplies, through the air, through food or through contaminated surfaces

Radiological Attacks:

Commonly known as a "Dirty Bomb", these types of devices are designed to spread radioactive material across a wide area with the intent to do harm. Radioactive materials are used in a lot of different industries including in medicine and research laboratories but can also be acquired by those who intend to do harm

Nuclear Attacks:

Since the Atom bombs were dropped on Nagasaki and Hiroshima in 1945, no other country has used a Nuclear weapon in an act of warfare. In order to produce a nuclear weapon, a significant amount of weapons-grade plutonium needs to be acquired. It is plausible that a terrorist cell or individual could purchase a ready made nuclear weapon from a third party

Acid Attacks:
Although not commonly used by terrorists, acid attacks can be used against individuals or groups of people. Sulphuric acid is very strong and can cause major injuries and permanent damage to victims

Cyberterrorism:
This refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. For example hacking into computer systems, introducing viruses to vulnerable networks, website defacing, Denial-of-service **attacks**, or terroristic threats made via electronic communication

Insider threats:
A person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.

This includes insider knowledge of:

- Access and egress procedures
- Access to sensitive information
- Access to computer systems and networks etc
- Evacuation and assembly points

Actions To Take in the Event of a Terrorist Attack:
Vigilant Security personnel who are confident in recognising and reporting suspicious behaviour may not only provide early warning of an attack but may even deter an attack that is still in the early planning stages.

If an attack is underway then Security Operatives must act quickly to limit the risks to all concerned, this would include early reporting and also following the government's guidelines of **RUN, HIDE, TELL**:

Run:

Move yourself and guide others as swiftly and as safely as possible away from the danger

Hide:

Once secured make sure that all members of the public as well as the team remain out of site of the attackers

Tell:

Call 999 or your control room as soon as possible and give as much information as is possible to the police operator, this should include things like:

- The number of attackers involved
- The last known location of the attackers
- What weapons they appear to be carrying/nature of the attack
- Known number of casualties
- Your location and situation

Company and Venue Policies Regarding Terrorist Attacks:

As members of front line security, it is vital that Security Operatives are well versed and understand the policies and plans in place in the event of an attack. People will look to the security team to help and lead them during these events. Knowing these procedures will be vital in both the security operative's as well as other staff members and customers overall safety.

Evacuation procedures may be different from fire evacuation procedures.

Use your local knowledge of the area to help make dynamic decisions based the information available to keep yourself, your colleagues and customers safe

Reporting Terrorist incidents to the police:
On contacting the police the following information should be passed across:

- What you have seen
- What has happened
- Who you saw
- What they looked like (Ethnicity, gender, height, build, clothing, etc)
- Where the situation happened
- Where you are
- When did it happen

Be aware of the expected emergency services response times

For non emergency activity:
The telephone number to report suspicious activity to is the **Anti terrorism hotline:**

0800 789 321

This phone line is available 24/7 and is manned by specialist officers who take all reports seriously. There are also online tools that most police services offer that can be used to report activity as well.

Public Sector Counter Terrorist Experts:

Centre for the protection of National Infrastructure (CPNI): Are leaders in security, providing resources, guidance and expert advice to help protect and keep businesses secure from external threats.

The National Counter Terrorism Security Office (NaCTSO): is a police unit that supports the 'protect and prepare' strands of the government's counter terrorism strategy. They work directly with the Home Office.

ACT: Action Counters Terrorism is a government and police initiative that encourages the public to report anything that they believe to be suspicious to the

police. There is a business App available as well as a free online course that all Security Personnel should all complete.

See Check and Notify (SCaN) is designed to help businesses and organisations maximise their safety using their existing resources, this includes training staff to look for things such as criminal activity, unlawful protest and terrorism

The Pros and Cons of Invacuation vs Evacuation:
Definitions:

Invacuation - Moving customers inside a building for safety reasons

Evacuation - Removing customers from a building

When **evacuating** personnel **out** of a building for a fire this can lead them to safety, however it can also lead to people rushing, falling and suffering from injuries as a result.

When **invacuating** personnel **into** a building that can lead them out of immediate danger, however the risk here is that people are then crowded together and could be an easy target for an attacker

Procedures when dealing with Suspicious Items:
Remember HOT Principles:

Hidden - does the item appear to be hidden

Obviously Suspicious - does the item have visible wires or other signs that look like it could be an explosive device

Typical - Is the object typical of the workplace or does it look out of place

Remember the 4 C's:

Confirm - Confirm that the package or bag doesn't belong to anyone nearby

Clear - Get people away from the area

Communicate - calmly communicate with customers and staff or police

Control Safety Distance - Make sure to set a cordon a safe distance away

Distancing vs Object size:

Suspected device in a Rucksack or bag - No closer than 100 m

Suspected device in a small Vehicle - No closer than 200 m

Suspected device in a large Vehicle - No closer than 400 m

In order to better visualise the distances, remember that 100 meters is roughly equivalent to the length of a football pitch

Important:
Do not use radios or mobile phones within 15 meters of the suspected device

Signs of Suspicious behaviour:
Any observed behaviour that could indicate signs of terrorism or terror related crime

This could include any of the following:

- Individuals taking an interest in the security of the site
- Making unusual requests for information
- Testing the security teams response by breaching restricted areas
- Loitering
- Tampering with utilities
- Individuals trying to avoid security staff
- Individuals carrying out activities inconsistent with the nature of the building or environment

- Forged documents or ID's
- Inappropriately dressed for the season
- Taking photographs or drawing diagrams of the site
- Parked vehicles or unattended vehicles left for long periods of time
- Multiple sightings of the same person, vehicle or activity over a period of time

Actions that can deter or disrupt hostile reconnaissance:

- Ensuring visible presence of vigilent security personnel
- Frequent patrols that are done at irregular intervals
- Maintaining good search procedures
- Good access and egress procedures
- Secure emergency exits when not in use to prevent unauthorised entry

How to respond to Suspicious behaviour:

- Use customer service skills to disrupt potential hostile reconnaissance (example: approaching a person taking photographs of the site and asking them if they are ok or need any assistance with anything)
- Using positive and professional behaviour to act as a deterrent
- Having visible security including CCTV cameras as well as security operatives on site

Report all suspicious activity:

- Follow your internal procedures
- Contact the counter terrorism hotline (0800 789 321)
- British Transport Police (BTP) 0800 40 50 40 or text 61016
- Non Emergency 101
- Active Counters Terrorism (ACT) report form

In an emergency always dial 999

PRINCIPLES OF USING EQUIPMENT AS A **DOOR SUPERVISOR**

CHAPTER 1 Equipment Relevant to a Door Supervisor

Equipment used to manage venue capacity:

- **Clickers and other counters** - Used to count customers in and out of a venue
- **CCTV** - Can help staff keep an accurate record of numbers entering and leaving as well as any potential suspicious activity
- **Radios** - Controlling the venue numbers when you have multiple entrances and exits

Different Types of Personal Protective Equipment:

Wearables:

- Waterproof clothing
- High Visibility clothing
- Headwear
- Stab Vests
- Gloves (Needle, Slash Resistant, or medical for first aid)
- Face Shields
- Ear Defenders
- Eye Protection
- Safety Boots (Be aware that these are not ordinarily allowed to be worn in night clubs, pubs etc)

Equipment:

- Metal Detectors
- Body Worn Cameras
- Radios, Mobile phones
- Personal Alarms
- Torches
- Equipment as it applies to the any incidents

The Purpose of Body Worn Cameras (BWC):

- Securing evidence against offenders
- Deterring Crimes
- Self-Protection
- Curbing behaviour (Both DS and Customer may think twice about their actions)
- Identification of offenders

Effective Communication Using Equipment:

Equipment:

Radios and Earpieces

- Internal communications over one or more channels
- Externally linked Radios for communication with Council control rooms (Pub-link)
- Airwave Radio systems for direct communication with the police

Other types of communication Equipment:

- Mobile Phones
- Internal phones
- Intranet (internal internet used for shift handovers, documentation etc)
- Tannoy systems/Use of DJ to communicate with customers in an emergency

Using Radios:

- Test radios when you come on shift (fully charged and correctly functioning)
- Think about what you need to say
- Accurate Brief and Clear
- Always listen out for active communications on frequency before transmitting
- Press the PTT button to transmit
- Keep the microphone about a fist away from your mouth (5 - 8 cm)
- Speak at a normal volume
- Speak at a normal speed
- Use pro-words

Examples of Radio Pro-Words:

Callsign - a name that is assigned to you
Over - transmission complete, expecting a response
Out - transmission complete not expecting a response
Received - message received and understood
I say again - I'm repeating the information again
Say again - I need you to repeat the last message
Negative - No or I cannot
Affirm - Yes
Go ahead - Pass your message
Stand By - Wait
ETE - Estimated time of Event
ETA - Estimated time of Arrival
ETD - Estimated time of Departure

Always use the NATO phonetic alphabet when using radios to communicate:

NATO PHONETIC ALPHABET

A alpha	B bravo	C charlie	D delta	E echo		
F foxtrot	G golf	H hotel	I india	J juliett	K kilo	L lima
M mike	N november	O oscar	P papa	Q quebec	R romeo	S sierra
T tango	U uniform	V victor	W whiskey	X xray	Y yankee	Z zulu

Phonetic pronunciation of Numbers over the radio:

0 - Zero
1 - Wun
2 - Two
3 - Tree
4 - Fower
5 - Fife
6 - Six
7 - Seven
8 - Ate
9 - Niner

100

Pronounce numbers such as 1024 as wun, zero, two, fower **not as** one thousand and twenty four.

End of Principles of Working as a Door Supervisor in the Private Security Industry

PHYSICAL INTERVENTION IN THE **PRIVATE SECURITY INDUSTRY**

CHAPTER 1 Physical Intervention in the Private Security Industry

Definitions:

Defensive physical skills:
Physical skills used to protect yourself or others from an assault.

Physical Intervention:
The use of direct or indirect force through mechanical means (handcuffs, etc.) or bodily contact, it is made up of:

- **Non-restrictive interventions** - subject could move away, i.e. a breakaway or nonrestrictive escort.
- **Restrictive Interventions** - involves more force in order to control a customer and remove their ability to easily move away; this can be achieved through either mechanical restraints or bodily contact.

Primary controls:
Following employer policies and procedures, as well as the correct use of equipment (radios, access controls and CCTV etc.)

Secondary controls:
The correct use of conflict management techniques and teamwork used to try to de-escalate situations and reduce the use of the physical intervention.

Always use physical intervention as a last resort for the following reasons:
- Increased risk of injury to all parties involved
- Can result in legal proceedings if the use of force is seen as excessive and unreasonable
- Can lead to loss of SIA license and employment

Avoiding Conflict:
- Give customers space
- Always give all parties a clear exit path

100

- Remain calm
- Use conflict management techniques.

The law regarding the use of physical force:

- Physical force can be used to defend yourself provided the force is only used to create a window of opportunity to escape and nothing more.
- All force must be Reasonable.
- Reasonable = Necessary and proportionate in the circumstances

Risks of dealing with physical restraints on the ground:

- Most serious injuries and deaths from physical interventions result from customers being restrained face down on the ground
- Death can also result from someone being bent forward or hyperflexed as well as, in some cases prolonged seated restraints
- Impact injuries can result from forceful take downs
- Glass or debris injuries from the ground
- Vulnerability to assault from others

Dealing with Physical Interventions on the Ground Appropriately:

- Avoid going to ground if possible
- Get off the ground as quickly as possible
- While on the ground, monitor the restrained individual to ensure their breathing is not compromised
- Where there is more than one member of the team present, someone should take charge of the situation and take responsibility for overall safety of all concerned
- The team leader should try to verbally communicate and defuse the situation and bring the restraint to an end as quickly as possible
- If the team leader is not in a position to communicate with the restrained individual, they should position a colleague to do so
- De-escalate force at the earliest opportunity and immediately if there are signs of a medical emergency

Medical risk factors (Serious harm or death can result from):

- Customers being forced to the ground
- Customers held in prone restraint (face down on the ground)
- Any lengthy physical intervention
- Any use of restraint that impairs breathing
- Any neck holds or chokes.

Positional Asphyxia:

Death which is a result of putting a restraint on a person which leaves them in a body position that leads to an inability to breath, this could be from laying them face down on the ground (prone) and putting pressure on their back.

Stress and Emotional Trauma:

- Physical restraints and methods can be particularly difficult for people who have suffered abuse and trauma
- Staff need to respect the dignity of individuals that they are managing, however challenging they find them

Acute behavioural disturbance (ABD), also known as Excited Delirium:

- Excessive strength
- Hot to touch
- Constant physical activity without apparent fatigue
- Insensitive to pain
- Confused emotional, mental state
- Vomiting
- Increased heart rate and breathing
- It is a medical emergency until proven otherwise.

Psychosis can result from an underlying mental disorder or it could be drug induced it can result in any or all of the following:

- Hallucinations
- Paranoia
- Extreme fear as part of delusional beliefs

Both Acute Behavioural Disturbance and Psychosis can lead to sudden death so should be treated as a medical emergency. The preference should be on using conflict management defusing techniques in these situations as far as is reasonably practical

Other Impact factors to consider when using Physical Intervention:

- Age, Size, Weight
- Physical health
- Mental health
- Physical exhaustion
- Recent ingestion of food
- Pre-existing medical conditions
- Alcohol or Drug use

Vulnerable Groups:

- Children and young people
- Older adults
- Individuals suffering from mental health issues

If staff are working in an environment which involves routinely working with vulnerable groups they should receive additional training in the use of physical interventions

People fighting (Risk assessment):

- Use a dynamic risk assessment.
- How many involved?
- Are they carrying or using weapons?

- Innocent bystanders nearby in danger?
- Have you called for help?
- Are there any other non-physical options available to us?

Use teamwork:

- Most fights are over within under a minute.
- Most people don't want to fight.
- There may be drugs or alcohol involved.
- Some people will fight in front of you so you will stop it quickly without them losing face.
- If people are not fit and trained they will run out of explosive energy rapidly and go to ground
- Always use clear commands to tell people to stop before physically intervening; this is to build up a legal case and also show witnesses we did not want to use physical force.
- Always request assistance before engaging or you may not get a chance to access your radio.

Reducing the risk of Harm:

- Choose the least forceful restraint possible in the circumstances
- Avoid high risk solutions and take downs if at all possible
- Avoid the use of neckholds as these can result in lack of circulation to the brain as well as breathing difficulties
- Maintain ongoing communication with all parties involved including the subject
- Monitor the wellbeing of the subject for adverse effects
- Work as a team with a designated team leader
- Follow all established policies and procedures
- De-escalate as quickly as possible to reduce exposure to risk
- Immediately release and provide assistance to the subject if they show signs of breathing difficulties

Dynamic Risk Assessment can be used to:

- Assess the risks involved in using a physical restraint to all parties when deciding if physical restraint is appropriate
- Evaluate the options available when looking at a situation to determine if to intervene and how
- Identify when assistance is needed
- Continuously monitor the levels of risk faced by all parties involved and adapt accordingly
- Determine if its appropriate to withdraw/De-escalate

Managing and Monitoring a Persons Safety during Physical Intervention:

Monitor:

- Observe the risk factors (situational as well as individual)
- Ensure that nothing impedes the subjects ability to breath or their circulation
- Check Airway; Breathing and Circulation constantly

Actions to Take:

- If person is unconscious but breathing place them in the recovery position
- Immediately commence CPR/Defibrillation if the subject is unconscious and not breathing or showing any signs of life
- If the subject is breathing and conscious, talk to the subject and take them seriously as people can still talk if they are experiencing positional asphyxia or any other form of medical distress
- Act on red flags:
    - Effort/Difficulty in breathing
    - Blocked airway
    - Vomiting
    - Becoming very passive or reduced consciousness
    - Non-Responsiveness

- Signs of head or spinal injury
- Facial Swelling
- Evidence of alcohol or drug overdose
- Signs of cyanosis (blue lips or fingertips)
- High Temperature
- Bizarre behaviour

Post Incident:

- Duty of care for the customer (even the aggressor)
- Provision of medical care
- Brief police/emergency services in attendance
- Preserve all evidence
- Remember to follow local policies on report writing.
- Learn from what's happened
- Share good practice

De-Briefing:

- All staff should be involved
- Time should be taken to analyse feedback from all parties involved as well as reviewing any CCTV footage
- Feedback to all staff
- Good teams should always be open to improve
- Learn from the incident in the view of handling it better if a similar incident were to occur
- Identify what we did well
- Identify what we could do better
- Is anyone in need of further training

Post Incident Support:

Following a violent incident, staff may require professional help and support. Under health and safety legislation, this should be provided by the workplace.

It is designed to help:

- Promote wellbeing
- Reduce sickness absence
- Identify post-incident effects.

Report writing:

- If you have to use force, it is a requirement that the incident is fully recorded.
- This will assist in any legal matters that may arise later.
- Protects the organisation
- Protects the individual

The importance of Maintaining Physical Intervention Knowledge and Skills:

- Legislation can change
- Skills fade (proficiency deteriorates over time which could decrease effectiveness and increase risk
- Security providers may not be compliant with Health and Safety legislation (they are responsible for employees acts and omissions) if they fail to make sure that their staff are adequately trained and refreshed on their skills regularly

End of Physical intervention theory module

ADDITIONAL RESOURCES:

https://www.gov.uk/government/news/act-awareness-elearning

Mock Exams

Scan the QR Code to access mock exams.

BECOME CERTIFIED SECURITY PROFESSIONAL

GET LICENSED
Certified Security Professional

Acclaim by Credly

The Get Licensed Certified Security Professional status is a mark of recognition for front-line security professionals who have completed a varied of front-line training to a superior standard.

Earning Criteria:

- Door Supervisor Training / Security Officer Training
- CCTV Training
- Emergency First Aid at Work
- Basic Handcuff Training

To learn more about Certified Security Professional scheme, scan the QR code:

alid SIA licence? Create your Get Licenced worker passport today and Get Working.

gn Up

our details and n some quick o activate your ccount

Get Notified

Get notified of new matching opportunities in your area.

ect Shift

r shifts to suit edule and work our availability.

Get Paid

No more waiting for payday, get paid the same day after completing your shift.


GET
LICENSED