Swedish Civil Contingencies Agency

Polisen
Swedish Police

GUIDANCE

Guideline on Protection of Public Spaces

Protection against terrorism in crowded places

Guideline on Protection of Public Spaces
– Protection against terrorism in crowded places

Layout: Advant

Order No.: MSB1474 – February 2020
Swedish edition: MSB1448 – October 2019
ISBN: 978-91-7383-997-6

Preface

In recent years, Sweden and several other countries nearby have been struck by acts of terror. Even if Sweden is a country that has been relatively spared from terrorism compared with many other countries, future attacks cannot be ruled out. In recent years, the trend has been that the terrorist attacks have been more directed at the public than at the institutions of society to a greater extent than before. The attacks directed at the public often involve major consequences and often entail extensive damage.

A modern, democratic and open society is vulnerable to terrorism. Even if the risk of being a victim of an attack is very small for each individual, various businesses, sectors and actors that are active in places with a public presence need to prepare for the threat in their security work. Sweden's counter-terrorism efforts are dependent on actors other than authorities also working to increase the protection against terrorism.

In the Swedish counter-terrorism strategy, the fight against terrorism is divided into three areas: preventing, preempting and protecting. In addition to this, society must also have an ability to handle the consequences of a terrorist attack.

The prevention efforts aim to counter and reduce the intent to commit or support terrorist attacks. The preemptive efforts aim to counter and reduce the capabilities and opportunities to commit terrorist attacks. The protective efforts aim to create and maintain protection for individuals and to reduce society's vulnerability to terrorist attacks.

This guideline was prepared for the protective efforts. The aim is to create conditions for greater safety and security in public spaces in which many people are present. The guide was prepared by the Swedish Civil Contingencies Agency and the Police Authority.

Camilla Asp
Head of department
MSB

Stefan Hector
National Operations Department
Police Commissioner
Head of Operations Division
The Swedish Police Authority

Table of contents

About the guideline

About the guideline

This guideline was prepared to strengthen the protection against terrorist attacks directed at the public according to the Swedish counter-terrorism strategy. The guideline is for private and public actors that work in settings where many people are present, such as security and operational managers and others who have a need for knowledge about protection against terrorist attacks.

The operations that the guide primarily addresses are actors that work within:

- Nightlife, hotels and restaurants
- Cinemas, theatres and tourist attractions
- Stores and shopping centres
- Healthcare
- Places of worship
- Sports arenas and events
- Public transport
- Banks and financial institutions
- Schools and other education providers.

Society's ability to handle and reduce the consequences of terror attacks and other hostile acts depends on the efforts of many actors. The actors at which this guide is directed are of central importance in the work to protect the public against terrorist attacks since they work in or are responsible for places where many people gather, or places that are of major importance to certain groups or society in general.

The time aspect in terrorist attacks is very critical as the damage is greatest at the beginning of a terrorist attack. Consequently, it is very important what security measures have been implemented before a terrorist attack, but it is also important what decisions and actions are taken during an on-going attack.

Sweden's counter-terrorism efforts rely on actors other than authorities also implementing protective measures against terrorism, both before and during a terrorist attack.

The advice in the guide is based on extensive research and analysis from the United Kingdom, where earlier incidents were examined and current threats were evaluated. Guidance is also provided on how various operations can increase security in their respective business operations or organisations. This guide also builds on sections from the English guide Crowded Places Guidance prepared by the National Counter Terrorism Security Office (NaCTSO).

The guideline is intended to provide an overall description of risk management, attack methods and the protective measures that can be implemented. The advice is general and needs to be adapted to the unique settings of each operation. Some of the protective measures described in the guide are not relevant to some of the actors addressed by the guide. Similarly, some attack methods are more relevant to certain operations and less relevant to others. The guide is intended to undergo continuous development.

Sweden's national strategy

The point of departure for Sweden's long-term national and international counter-terrorism efforts is described in Prevent, preempt, protect – The Swedish counter-terrorism strategy that was prepared in 2015. The strategy presents how the Government believes that the counter-terrorism work should be done and how it can be made more effective. The goal of all counter-terrorism activities is to keep terrorist attacks from being carried out. One important premise is also that fundamental rights and freedoms and the principles of the rule of law are ensured in all actions to combat terrorism.

The objective of a strategy is to structure the work, clarify roles and point out the needs that exist for new legislation and new tools. The work is divided into three areas called prevent, preempt and protect. In addition to these areas, society must also have an ability to handle a terrorist attack.

Prevent

Particular focus is on the prevent area, where measures aim to prevent people from developing an intent and capability to commit terrorist attacks Measures in this area are intended to counteract radicalisation and recruitment to extremist and terrorist groups, and to influence the intent of individuals to commit or support terrorist crime.

Preempt

The preempt area is about countering and reducing both the capabilities and opportunities to commit terrorist attacks. This is done mainly by law enforcement authorities having access to and being able to exchange information and having the possibility of acting with appropriate tools under the rule of law.

Protect

This area is about creating and maintaining protection for individuals and reducing society's vulnerability to terrorist attacks. If a terrorist attack is nevertheless carried out, society must also be able to manage the resulting consequences.

Sweden's counter-terrorism work

Extensive work is conducted in Sweden to prevent and preempt terrorist attacks. In the event of an attack, several authorities will work together and in parallel to manage the consequences of the act. A party that is responsible for an operating area in society is normally also responsible for this area in a crisis. For example, the Police are responsible for security, cordons and criminal investigations. The Rescue Service is responsible for rescue efforts and ensures that injured people get help, and the Swedish Transport Administration and the various transport providers ensure that transportation works and that trains continue to run. The county councils are responsible for emergency medical care and transports of ill and injured patients and the National Board of Health and Welfare is responsible for healthcare in general. In upcoming sections, there are examples of authorities that work with various parts of the prevention, preemption and protection work.

Centre against Violent Extremism

The Swedish Center for Preventing Violent Extremism develops the work to prevent violent extremism on a national, regional and local level. This is done in part by providing support to municipalities, authorities and other actors, gathering and disseminating information, and striving to coordinate the prevention work against extremism. The Center is placed with the National Council for Crime Prevention (Brå).

The Swedish Security Service

The primary task of the Swedish Security Service within counter terrorism is to prevent terrorist attacks in Sweden or against Swedish interests. The objective is to prevent terrorist crime at an early stage, which is done by preventing and preempting terrorist activities, such as financing, logistical support, training, recruitment and radicalisation. The prevention work takes place, for example, through intelligence work, meaning gathering, processing and analysing information.

Swedish Police Authority

The police have the overall responsibility for order and security in Sweden. The police are society's first resource for directly intervening against a commenced terrorist attack or other attack with severe and extensive violence. The police also conduct the preliminary investigation in the event of an attack that was committed and also support the Security Service in, for example, investigations and surveillance against suspected preparation of terrorism. The Police Authority is also responsible for the Counter Terrorist Unit, which has the main task of operationally combating terrorism. They handle situations that are so serious, risky or unusual that they cannot be handled within regular police operations. Besides terrorist attacks, this also includes hostage situations and operations in the event of aggravated robbery.

Swedish Civil Contingencies Agency (MSB)

The Swedish Civil Contingencies Agency (MSB) has the task of developing society's capability of preventing and handling accidents and emergencies. When a serious accident or emergency occurs, MSB provides support to those who are responsible for handling the emergency. MSB's mission in the area of protection against terrorism primarily aims to protect the public from possible terrorist attacks. MSB is to support the work of private and public actors on protection against terrorism in public spaces with the help of guidance and education.

National collaboration

Agencies in Sweden collaborate regarding terrorism. The Counter-Terrorism Cooperative Council comprises 14 Swedish agencies that cooperate to strengthen Sweden's counter-terrorism capabilities. A large part of the collaboration concerns exchanging information and assessments. There are also national collaborations in certain sectors or areas, such as the National Council for Railway and Public Transportation Protection (NRJK), which is a council for protection issues in railways and public transport.

Protection of public spaces and regulations

The term public spaces is used in the guide. The term can be explained as settings that are accessible to a large number of people on a predictable basis. Public spaces are therefore a broader concept than a "public place" and encompasses, for example streets, roads, squares, arenas, stores, hotels, cinemas, tourist attractions, parks, event areas and various means of transport, such as the railway and metro. "Public spaces" is not a legal term, in contrast to "public places".

The area of security in a public space is not regulated in a statute and should not be confused with the work that aims to protect security-sensitive activities from espionage, sabotage, terrorist crime, etc. that can cause damage on a national level, which is called protective security. The work on protective security is regulated in the Protective Security Act (2018:585). Even if the protective measures to some extent may be similar, the purpose is different and there are regulations and obligations pursuant to the Protective Security Act, which is not the case with the area of security in public spaces. However, there is a very small portion of the operations that the guide is addressed to that are covered by the Protective Security Act.

There are also other regulations that in various ways are adjacent to and influence the work on security in public spaces. Mentionable here are:

- The Civil Protection Act (2003:778)
- The Camera Surveillance Act (2018:1200)
- The Public Order Act (1993:1617)
- The Swedish National Board of Housing, Building and Planning's building rules and the Swedish Work Environment Authority's various regulations.

It is important to note that it is applicable regulations that govern the work and where the guide's descriptions are regulated by legislation, it is noted in the text.

Analyse and plan

Analyse and plan

This chapter focuses on how various operators can assess and manage risks and threats. Many operators have their own procedures and systems for assessing and managing risks and threats, at the same time that there may be statutes that regulate, for example, requirements on risk analyses – such as the Act on Municipal and County Council Measures prior to and in the event of Extraordinary Incidents and during High Alert (2006:544).

Even if the various statutes require risk analyses, they have different purposes, however. This chapter is therefore primarily addressed to actors that do not have their own procedures or requirements on risk analyses and risk management and is intended to provide an overall view of what a risk management process may look like.

There is also a standard (SS-ISO 31000:2009) that describes principles and guidelines for the risk management process. In addition to the standard for risk management, there is also guidance from various authorities, such as MSB. Even if the purpose and methods are largely different, they may nonetheless serve as a good guide for analysing risks and vulnerabilities.

Risk management

Risk management is about identifying, evaluating and managing risks. The purpose is to be able to remove, reduce or accept a risk. Identifying and evaluating possible risks is a good way of increasing risk awareness and understanding in the entire organisation.

Working so that a large part of an organisation will be a part of the risk management process. If the operation already has a risk management process, the various processes should be integrated. This way, the different kinds of risks are put into a context (see Figure 1).

Risk management cycle

A good starting point in the risk management process is to describe the operation and the context the operation is in. For example, what statutes are there to take into consideration, the organisation's objective, previously conducted risk analyses and a description of what is to be protected. What is worthy of protection may either be people (such as employees, visitors, customers, contractors and the public) or physical objects and operations (such as buildings, equipment, information, processes and deliveries). Brands and reputation may also be worthy of protection.

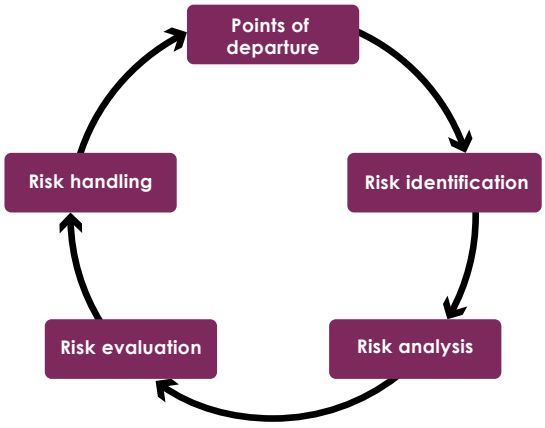


Figure 1. Illustration of a risk management cycle.

The choice of method(s), potential delimitations and the intended work method should also be clarified in the points of departure for the risk management process.

Risk identification

Risk identification is more about scenario identification, which is trying to conclude what can happen. This is because it is difficult to identify sources of risk without thinking in terms of potential risk scenarios. In practice, this means identifying sources of risk, such as a cistern with toxic gas, and risk scenarios, such as a release of toxic gas.

In order to identify risks, it is necessary to have knowledge of what methods perpetrators use and understanding of what intentions and capacity terrorists have of conducting an attack.

In the section on Attack methods, we go through the threat and risk scenario and some of the potential attack methods. The most common methods are the use of firearms, stabbing weapons, vehicles as weapons or different kinds of improvised explosive charges. In the most basic risk management, these attack methods should be the focus, but depending on the operations' nature, other methods such as arson, use of drones or Chemical, Biological, Radiological and Nuclear (CBRN)-related methods could be considered to be a part of the prevailing threat and risk scenario.

Below are some suggested questions that can be asked to assess risks linked to terrorism and hostile threats:

- What do we know through the Security Service's threat scenarios or other open sources about threats and risks from, for example, the National Centre for Terrorist Threat Assessment, the Police Authority, MSB, the Swedish Armed Forces, the National Defence Radio Establishment (FRA) or the Swedish Defence Research Agency (FOI)?
- Could the operation's location, visitors, sponsors, contractors, tenants, staff, our activities or something in the surrounding area influence the threat scenario and encourage a terrorist attack?
- Are we in some way associated with known individuals or organisations that could be targets?
- Could we be affected is a nearby building or installation is subjected to an attack?
- Would an attack entail major consequences to the functionality of the rest of society?
- Do a large number of people spend time in or pass by the building or installation?
- Does the operation have a symbolic value?
- What information on crime and other problems in our area can the Police Authority provide?
- Are there vulnerabilities in our operations that perpetrators could use for an attack, such as deficient security?
- Is it easy for a perpetrator to obtain knowledge about our security procedures and physical protection, for example?
- What attack methods may be relevant to our operations? Are there examples from other parts of the world for operations that are similar to ours?
- Is there anything in the nature of the operations that means that the threat situation could change quickly?

Risk analysis

A risk analysis is usually focused on answering the three questions "What can happen?", "How likely is it?" and "What are the consequences?". The answer to the first question has been partly answered in connection with the risk identification. In the risk analysis, it is a matter of refining the descriptions of the risk scenarios and assessing how likely it is that each of the identified scenarios occur.

A terrorist attack is a very rare event, which is why the assessment of how likely an attack is should be toned down or even excluded. In terms of terrorism and hostile threats, focus should instead be on assessing what consequences a certain event will have and what vulnerabilities there are for the operations.

The consequences that the operation – despite some capability – does not succeed in predicting, resisting, managing and recovering from indicate how vulnerable the operation is to a specific event.

Risk evaluation

Risk evaluation means that an analysis is used to assess if a risk level is acceptable or not, and what possibilities there are of reducing or removing the risk. Since there is no established level for what constitutes an acceptable or tolerable risk, the risk evaluation in a risk management process is often about evaluating a number of alternatives for how the risk can be reduced. The actual evaluation is based on weighing advantages and disadvantages of the proposed measures and arriving at whether or not the measures should be implemented.

The evaluation should be based on the effect that the proposed measures are estimated to have on the risk level, i.e. how much they reduce the risk and the costs that the measure entails. One problem in this context is that it may be difficult to show the measures' risk-reducing effect, which is crucial for the analysis to be able to be used as a basis for a decision.

Risk handling

Risk handling aims to reduce or remove risks and is based on the risk evaluation. The starting point may be an assessment of the security measures that already exist regarding how effective they are and where the weaknesses are. There may also be security measures that aim more for protection against, for example, accidents or crime that are also effective against terrorism.

The measures identified in the risk handling should be described in a security plan. Describe for example your objectives as to what is to be achieved, who should be responsible for the various measures and what time circumstances apply to the various measures.

Examples of security measures are described in more detail in the chapters Attack methods, Physical protection and Personnel security.

Training

Practice is an important part of the operations' security measures. Practice is a good method to improve the capability of handling an attack, but also to test and check if implemented security measures are adequate. Through practice, the operations' vulnerability can also be identified and practice should be done regularly or if circumstances change. For example, if an attack takes place somewhere else or if the threat situation against you, your suppliers, contractors or stakeholders changes.

Practice need not always demand major resources, but can often be done using simple means and methods. Table 1 presents examples of various kinds of exercises and the resources required and what the objectives of the exercise may be.

Table 1. Various kinds of exercises and the resources required

Discussion-based exercise	Table-top exercise	Practical exercise
Requires little resources and can be handled internally No disruptions or interruptions in the operations	Requires major resources and more planning. Can also involve external actors	Significantly more resource-intensive to plan and implement
Can identify problems in security measures implemented	Scenarios can be used to identify vulnerabilities	All employees have the opportunity to practice their roles
Does not identify the effectiveness of implemented security measures	The effectiveness of implemented security measures can be assessed to some extent. Practical problems do not arise as in a practical exercise	Practical exercises can create confidence that real events or incidents can be handled.

Threat and preparedness levels

Assessment of terror threat levels

The Swedish Security Service makes decisions on the level of terrorist threats for Sweden. The National Centre for Terrorist Threat Assessment (NCT) provides input to the decision based on continuous assessments of the terrorist threat level in Sweden and against Swedish interests abroad. The NCT is a permanent working group that consists of personnel from the National Defence Radio Establishment (FRA), the Military Intelligence and Security Service (MUST) and the Security Service. The assessment is based on information from the three agencies.

The NCT assesses the likelihood of there being actors with intent and capability to commit terrorist attacks against Sweden. In Sweden, a five-point scale is used to express the threat level and the level steps are as follows: no threat (1), low threat (2), elevated threat (3), high threat (4) and very high threat (5). The assessments are limited in time and are most often valid for one year. The terrorist threat level is evaluated continuously and can be adjusted at any time during the year.

The threat level has been deemed to be at level 3 of 5 since 2010. Level 3 means an elevated terrorist threat and that an attack can occur. For the current assessment, see the Swedish Security Service website.

Preparedness levels

In Sweden, there are no set or established preparedness levels linked to the national threat levels. For actors that work in public spaces, there may, however, be reason to consider suitable security measures in the operation in relation to the threat level. The proposed security measures that should be implemented at different times are influenced by the current national threat level, but are also adapted to the operation's specific risks and vulnerabilities.

The national terrorist threat assessment is strategic and pertains to an assessment of actor's capabilities and intent to carry out an attack on a national level. This means that the terror threat assessment is not directly transferable to every operation and that every operation must itself define what the terrorist threat assessment means for them, meaning operationalising their own threat situation. Each operation must assess and decide on changes to the preparedness levels the operation uses. It is just as important to be able to raise the preparedness level as it is to lower it and such a decision on increasing or reducing the preparedness level must be made by the operation itself. The security measures used at different preparedness levels should not be made public since it is not good if potential perpetrators find out what we know and how we act.

Basic preparedness that all operations should have, regardless of their threat situation, can include access control and security checks, for example. An increase in the preparedness

Table 2. Sweden's five-point scale to indicate the threat level

Threat level	1. No threat	2. Low threat	3. Elevated threat	4. High threat	5. Very high threat
Definition	The probability that actors have the intent and capability to commit terrorist attacks does not constitute a threat	The probability that actors have the intent and capability to commit terrorist attacks is low	The probability that actors have the intent and capability to commit terrorist attacks is elevated	The probability that actors have the intent and capability to commit terrorist attacks is high	The probability that actors have the intent and capability to commit terrorist attacks is very high

level requires, however, security measures in addition to the basic protection. These are intended to be applied during a limited period of time and in an extraordinary situation.

The security measures that are to be implemented at each preparedness level are an issue for every operation and organisation to decide, and the decision depends on a number of circumstances. All measures should be identified before the preparedness level is changed and personnel should be given clear information. It is important to test and practice measures for each preparedness level. Using a system for preparedness levels that is a way for an operation to be able to operationally reflect its security work and its security planning against a changed terrorist threat assessment.

Table 3 presents an example of how a preparedness system can be structured.

Table 3. Examples of how the preparedness system may be structured

Preparedness level	Description
Special preparedness	Maximal security. Several security measures are implemented to address specific threats and minimise vulnerability and risks. Ordinary operations end, are reduced or are substantially affected.
Elevated preparedness	Extra extensive security measures are implemented that are maintained for some time. A significant reinforcement of security measures in the operation that affect ordinary operations. Ordinary operations are periodically implemented.
Partly elevated preparedness	Reinforcement of security measures adapted to one's own operations that can partly affect ordinary operations.
Basic preparedness	Routine security. Reasonable security measures applicable to one's own operations are implemented. Ordinary operations are not affected.

Examples of security measures depending on preparedness level

- Searching of incoming vehicles, individuals and belongings.
- Access cards and authorisation must be worn visibly.
- Special procedures for postal and package handling.
- Access limits to some places even for own personnel.
- Practice of evacuation, invacuation and use of protected spaces.
- Training in procedures and attack methods.
- Use of security personnel, such as security guards.
- Extended information on threats, risks and vulnerabilities within one's own operations.

Attack methods

Attack methods

In recent years, the trend has been towards terrorist attacks to a greater extent than before being committed by lone perpetrators or a small group that has used basic methods and where the target of the attack is the public. Historically, the methods for attack have changed nature on several occasions, however, which is why it should not be ruled out that more complex and large-scale attacks may be carried out in the future as well.

In recent years, the most common attack methods have been the use of small arms, improvised explosive charges and the use of vehicles as weapons, or stabbing weapons. It is also these methods that have caused the greatest consequences in the form of the number of deaths. However, there are also other methods that to-date have not been used to the same extent, but that nonetheless must be seen as a part of the prevailing threat situation, such as CBRN attacks, the use of drones and arson.

Various phases of the attack

A terrorist attack can be carried out within planning and without actual preparations. A passing impulse or the occasion being deemed advantageous may be enough for a perpetrator to attack. The decision to carry out an attack may be an impulsive act or triggered by events in the surroundings.

However, many attacks are carefully planned, mainly to avoid detection before the attack and to achieve as much damage as possible. Attacks that are carried out with simple means and methods can also be very carefully planned. A planned attack can be described in various phases (see Figure 2).

Target selection

The perpetrator often has some form of knowledge or relationship to the chosen target and can thereby assess the possibilities of succeeding with an attack. The target can, for example, be associated with some form of symbolism or that the perpetrator is often at or passing the location of the chosen target.

Planning

During the planning phase, the perpetrator assesses the security level at the site of the

Figure 2. Illustration of a risk management cycle.

attack and what vulnerabilities can be used. During the planning phase, there is information gathering or reconnaissance, which can take place on site, online or through contact with employees. During the planning phase, there is also a selection of method, tactics and what materials will be used.

Training

There is often a preliminary practice prior to the attack. The objective may be to assess the time used, what problems may arise, what response can be expected from the surroundings or if there is a need for alternative approaches.

Attack

The attack is carried out quickly and is often over in a few minutes. The implementation of the attack may be the result of preparation that has been under way for a very long time.

Exploitation

It is common that the perpetrator tries in various ways to amplify the effects of the attack carried out. This may, for example, take place through communications sent, the use of social media or image and film materials that mean that the attack lives on.

Detect suspicious behaviour and reconnaissance prior to an attack

Prior to a criminal act or a terrorist attack, it is very common that individuals or groups are on site and gather information. Perpetrators can obtain information about an installation or an event by visiting the site, for example online or with the help of an insider.

The more advanced an attack, the more planning and reconnaissance is required. The need for information and planning increases the chance of detecting suspicious behaviour before an attack is carried out.

Purpose of reconnaissance:

- Identifying targets.
- Detecting weak points and vulnerabilities.
- Assessing the security level and the response in an attack.
- Determining the best attack method against the site.
- Assessing the probability of success.
- Determining the best time for an attack.

In order to detect suspicious behaviour, one first needs to be clear about what is not suspicious behaviour. Taking time to observe and get to know one's working environment, people and activities, daily routines and changes that take place regularly is an initial step. The more you have observed an environment, the more clearly you can see deviations. You cannot recognise a perpetrator on external signs, such as age, gender, ethnic origin or clothing, but rather the assessment shall be made based on what people do – not what they are.

Examples of suspicious behaviour may be that the person:

- Takes several pictures of the surroundings and the environment, perhaps through selfies or of objects.
- Is in areas that are not open to the public or where access it restricted.
- Shows an interest in entrances, exits, surveillance cameras, security equipment or personnel.
- Asks unusual questions.
- Tries to make contact with and create a relationship to personnel.
- Tries to conceal his or her face or change appearance.

Reconnaissance can also be done with vehicles. Be attentive of vehicles that are incorrectly parked or that drive the same route repeatedly.

Improvised explosive devices

Improvised explosive devices (IED) can be an effective weapon for terrorists. In addition to IEDs, commercial and military explosives can also be used in terrorist attacks.

Even if explosive devices are made of home-made explosives, they can be just as powerful as commercial or military explosives. IEDs can be divided into three main groups: vehicle-borne, placed or personnel-borne.

There are some versions of IEDs that are used often. In the Western World, it is most common for IEDs to be placed at the scene of the attack in a bag or in some form of container, such as a waste bin. Explosives are also placed in a vehicle or in parcels, such as letters and packages.

In the list below, there are also the English abbreviations used extensively that may be good to know. The various abbreviations can be used in different combinations depending on how the IED is placed or triggered for example.

Common versions of IEDs:

- RCIED – Radio Controlled IED
- TCIED – Timer Controlled IED
- VBIED – Vehicle Borne IED
- UVIED – Under Vehicle IED
- SIED – Suicide IED
- Postal IED.

Radio and timer controlled IEDs

Radio controlled IEDs are triggered electronically and wirelessly using a transmitter and a receiver, such as a mobile phone, radio, cordless phone or pager. A timer controlled IED is triggered using a timer. The IEDs are placed where they will create as little suspicion as possible and can therefore be difficult to detect.

Figure 3. Radio controlled IED

Figure 4. Timer controlled IED

However, there are signs of timer controlled IEDs:

- Proximity to conceivable targets, such as locations where many people gather.
- Deviates from the normal picture – placed where it permits extensive shrapnel damage.
- Is hidden, for example, in luggage, bags, boxes and waste bins.
- May give off a smell of fuel, acetone, vinegar and ammonium.
- Nobody wants to claim the object.

Car bombs

A vehicle-borne IED is delivered to the target with a vehicle. There are no kinds of vehicles that are used more often in such attacks than others. The vehicle may be old or new, anonymous or equipped with company labels, for example. The vehicle may be adapted to not attract attention and it may be a motorcycle, car, van or lorry.

VBIEDs often entail major damage with many deaths and extensive material damage, especially when they have been parked close to crowds and buildings or driven into them by a suicide bomber.

The consequences are especially large if the bomb contains materials that can cause shrapnel, such as nails and scrap metal, or that the surrounding environment causes further shrapnel, such as glass shards from buildings. This kind of attack may be carried out in combination with firearms, stabbing weapons and the use of vehicles as weapons.

Below are some examples of what can characterise suspicious behaviour or a suspicious characteristic in drivers or vehicles.

Suspicious behaviour in drivers or vehicles

- A suspicious driver may pass the intended target several times to gain access to a good placement of the vehicle if the location is heavily trafficked otherwise.
- If any of them parks and leaves a vehicle quickly.
- If any of them shows signs of stress or tries to hide his or her face when parking the vehicle.
- If any of them does reconnaissance for a previous attack, practices placement and evaluates the surroundings' response.
- If the driver has a deviating driving style, such as driving extra carefully over speed bumps.

Suspicious characteristics in vehicles

Suspicious characteristics are if the vehicle

- is parked close to conceivable targets
- deviates from the normal, may be wrongly parked, abandoned or have warning blinkers or headlights on
- has a strange load, such as gas cylinders, wires or modified electric devices
- has different registration numbers on the registration plate and a possible parking permit in the windscreen
- has registration plates that were recently installed, are unclear or hidden
- has a modified appearance, such as a different body or uneven painting
- gives off an odour that may indicate explosives.
- is heavily loaded and shielded from insight
- has visible smoke inside the vehicle.

Under Vehicle IED

Improvised explosive devices under vehicles are small bombs that are usually attached or placed under a vehicle and are intended to kill or seriously injure the people in the vehicle. Depending on design, sign and placement, they can also kill or injure others who are nearby and cause material damage to the surrounding environment. The method is well known and has previously been used in attacks.

Since the explosives are often homemade, they can vary widely in appearance and size. For example, plastic lunch boxes, metal pipes and wood boxes can be used. Paint and oil dirt can be used to hide the bomb or designed to look like a normal car part.

The bombs are most often placed in relatively easily accessible locations since they usually must be placed there quickly. Common placement of car bombs.

- on the vehicle's underframe
- above or behind a wheel
- attached to the exhaust pipe
- on the ground under the vehicle.

Read more under Watchfulness if you are under a threat

Postal IEDs

Are bombs enclosed in envelopes, packages or the like and are intended to be triggered by the victim or using a timer or remote control.

Read more about Postal and package handling

Suicide IEDs

Suicide IEDs mean that the bomb is carried to the target and triggered by a perpetrator who is him- or herself killed or injured. This can be done using a vehicle (SVIED), an aircraft or a person. The bomb can also be placed on an involuntary victim and is then called a person-borne IED (PBIED).

There are no special characteristics or psychological profiles for suicide bombers. Anything that deviates from the norm can create suspicion, however. Perpetrators may have:

- Large and bulky clothes to conceal explosives, weapons or a protective vest.
- An abnormal walk due to the weight from the IED.
- Nervous behaviour with an evasive and shifting gaze, although they may also be calm and focused.
- A carried bag or backpack with an unusual shape or weight.
- Communication equipment or a remote trigger. Note where the person has his or her hands.

Identifying and handling suspicious items

It is very common for people to forget backpacks, bags, boxes and packages or for them to be left to be picked up later by, for example, visitors, travellers, suppliers and craftsmen. In most cases, there is a natural explanation even if it may seem suspicious at the moment.

Lost bags are handled daily in a large number of different public spaces without it being threatening or suspicious. It is often the public that notices items that nobody wants to claim. There is extensive uncertainty in deeming whether an item is suspicious or not. Therefore, it is important that there are simple methods to assess and handle suspicious items.

Anyone who is responsible for a building, installation or operation has a responsibility for the immediate assessments and actions taken due to a suspicious item. These assessments and actions often need to be done before the police arrives on scene and does an assessment. It is important to not postpone the decision making process while waiting for the police to arrive.

Identifying a suspicious item

Assessing if an item is suspicious or not is largely about confirming if something is out of the ordinary in the existing setting. The following questions may be good to work from:

- Is the item forgotten or has there been an attempt to conceal the item? If it is a forgotten item, it is less likely that it seems concealed.

Figure 5. Suicide belt

Figure 6. Suicide vest

- Is there anyone near the item who wants to claim it? Ask questions if they have any idea of who may own the item.
- Is it obvious that the item is suspicious? Does it have wires, circuit boards or batteries? Does it contain liquids or explosive-like substances? Is the item emitting smoke or odours?
- Is it typical for the setting? Is it an item the fits into the norm? A piece of luggage can be said to fit into the norm for a train station, but is out of the ordinary at an outdoor event.

Handling a suspicious item (CCCC)

The following is advice on what steps should be taken in the event of a suspicious item. Get help from several colleagues so that several steps can be taken at the same time.

- **Confirm** – Identify and confirm that the item is suspicious. Do not touch the item and do not use a radio or mobile phone within 15 metres of the item.
- **Clear** – Clear the area within a radius of at least 100 metres if it involves a small item, such as a backpack. Tell people to take cover behind something robust and to avoid places surrounded by windows or skylights.
- **Control** access to the area – Ensure that nobody else enters the risk area. Cordon off the area if possible.
- **Communicate** – Report the item to those in charge and alert the police.

The effects of improvised explosive devices

IEDs can cause extensive damage. It is not only the actual blast wave that can be deadly – shrapnel from both the IED and the surroundings, such as glass shards and metal fragments, can be a danger far away from the actual explosion. Depending on size, shape and exit velocity, individual pieces of shrapnel from the IED can fly more than 1,000 metres and fragments from broken windows can cause damage at very large distances from the actual explosion.

Table 4. Consequences of improvised explosive devices

	Light structural damage to buildings, damage to windows, door trims and roof tiles (5 kPa)	Severe structural damage to buildings. Buildings partially destroyed (40 kPa)	Limit for window damage (1 kPa)	Risk area for initial evacuation. Urban environment or open terrain
Hand grenade, package, pipe bomb <1 kg			175 m	100 m–200 m
Carried charge, bag, backpack <10 kg	35 m	10 m	500 m	200 m–400 m
Car <100 kg	150 m	40 m	1 000 m	400 m–800 m
Van, small lorry <1,000 kg	400 m	85 m		

Table 4 presents approximate values for the consequences that explosives can cause at different distances and charge size.[1] The table also shows the guide values for the initial police and rescue service risk areas for evacuation.[2]

If you believe that your installation is at risk of bombing, there are both physical measures and procedures that can reduce the risk.

Protective measures to consider

The most effective protective measure against explosives is to increase the distance between what is to be protected and the presumed attack site. Just a few metres can considerably reduce the effect of the explosive. Another measure may be to reduce the effect of fragments from glass in buildings, for example, or that buildings have sufficient resistance to explosions.

However, there are many measures not associated with large costs:

- Attacks may be preceded by reconnaissance and practice – document and take note of suspicious behaviour.
- Camera surveillance and monitoring by security personnel can deter a perpetrator or expose preparations.
- Establish access restrictions; ensure that unauthorised personnel are not in areas not accessible to the public.
- Carry out access control and security checks.
- Use physical barriers to keep vehicles from driving into the area or installation through entrances or the like, or through spaces below ground.
- Establish procedures for receipts of deliveries.
- The presence of alert and trained personnel may be enough for a perpetrator to refrain from an attack.

Bomb threats

The vast majority of bomb threats are false and are intended to cause fear and disruptions. It does happen that terrorists make real bomb threats, but false threats are also made to scare the public, businesses, authorities or special groups. The aim may also be to draw attention to their cause or to mislead the police.

Many bomb threats are made over the phone, but it is becoming increasingly common for them to be made by email or social media. Regardless of how unrealistic a threat seems to be, it is a crime and should be reported to the police at 112. It is important that every-

1. Handbook Ammunition and Mine Disposal, Protective Measures, Swedish Armed Forces.

2. ACTION CALENDAR First on scene for events with hazardous substances CBRNE, MSB

one who can conceivably receive a threat is prepared and knows how they should note information and forward it to the police and that relevant steps are taken.

The bomb threat's message

It is unusual for somebody to make a threat with correct and exact information well in advance of a real attack. It is hard to determine the exact motives for false threats, but it may involve revenge, extortion, a desire to impress one's surroundings or other more hard-to-understand motives.

Making the threat

A bomb threat can be made in many different ways. It is most likely made over the phone by somebody who calls in, but it can also be pre-recorded or written down or made directly through person-to-person contact. Threats are increasingly made by email or social media, such as Twitter, Instagram and the like. A threat can also be conveyed by a third party, meaning a person or organisation that has no ties to the potential target, but has just been selected to convey the message.

Immediate actions in the event of a bomb threat

Anyone on the staff who has a direct phone line, mobile phone, computer or tablet can receive a bomb threat. All such personnel should therefore know what they are expected to do if they receive a threat.

If you get a threat over the phone, you should:

- Stay calm and listen carefully.
- Have access to a checklist of important information that is to be written down.
- If possible, try to get the caller to continue talking while you have a colleague call 112.
- Write down the number of the caller if it is shown on the phone.
- Write down as much as possible if the threat consists of a recorded message.
- Do not respond, forward or delete it if it is made as an SMS; instead, write down the number and follow the police's instructions.
- Know who you have to contact in your organisation, such as the security manager or another manager, so that he or she can assess the threat.

Read more under Checklist – Bomb threats

If the threat is made in a letter, a note or as graffiti, you should treat it as evidence and keep others from touching it while awaiting the police.

If the threat comes by email or social media, you should not respond, forward or delete the message. Write down the sender's email address or user name and save any possible logs so that the police can investigate them later.

Assessing the credibility of a bomb threat

It is difficult to determine the credibility of a threat, especially if the attack is said to be impending. This is a common method to place further pressure on the recipient of the threat. The police will evaluate the threat as soon as possible, but there may also be a need for business operators to make an initial assessment themselves to determine what immediate steps need to be taken.

If the police have more information, they will provide suitable instructions, but if there is no detailed information, it will be necessary to take a number of factors into consideration:

- Is the threat a part of a series of threats? If so, what happened before and elsewhere?
- Is it possible to determine exactly where the alleged bomb is supposed to be? If so, is there a visible bomb at that location?
- Keeping in mind that people who make false threats want to influence other people's behaviour, is there any reason to believe what is said?

- If the threat is vague: could an evacuation lead to people unintentionally being guided closer to the danger?
- Can a suspicious item be seen?

Chemical, biological, radiological and nuclear attacks (CBRN attacks)

Chemical, biological, radiological and nuclear attacks can cause extensive damage and major disruptions, but at the same time, they are difficult to carry out and often require specialist knowledge.

To-date, no such attacks have been carried out in Sweden. Other attack methods, such as explosives, are more reliable, safer and easier for terrorists to acquire and use. But it is nonetheless fully possible that terrorists try to use CBRN materials in attacks against Sweden in the future.

What is a CBRN attack?

Recognising a CBRN attack

Just like other kinds of threats, a CBRN incident can occur completely without warning. It may not even be apparent what has happened at first.

The first signs of a CBRN attack may be:

- People showing inexplicable signs of skin, eye or respiratory irritation, nausea, vomiting, spasms, sweating, confusion, breathing difficulties
- Steam, haze, powders, fluids or oily droplets that have no obvious explanation
- Plants and vegetation that has withered
- Signs of unease in animals
- Strange odours or tastes.

Handling a CBRN attack

The steps taken by an organisation in direct connection to a CBRN attack may be of major importance to how extensive the damage becomes. If there is a plan drafted to limit the effects of an attack, people in buildings and installations can be protected to the furthest extent that is reasonably and practically possible.

Examples of planned measures that may be relevant in a CBRN attack:

- Alert the rescue services by 112 and follow their instructions.
- If a dangerous item can be isolated by evacuating the area, you should do so as quickly as possible. Close doors and windows after evacuation.
- Move those who are directly affected by an incident to a safe location, i.e. away from the source of contamination. If it is safe and practically possible, one should choose a location that minimises the spread of contamination.
- Consider removing contaminated clothing, considering the possibilities on site. Avoid pulling clothing over the head; cut it off if necessary. Place the clothes in a tightly sealed plastic bag.
- Remove all chemical substances from the skin with dry rags or pieces of cloth. Then rinse the skin continuously with water.
- Be prepared to give first aid.
- Ensure that there are instructions to close outer windows in the event of

Table 5. Three kinds of CBRN attacks

Chemical	Biological	Radiological and nuclear
Poisoning or damage caused by chemical substances, such as military chemical weapons or dangerous industrial and household chemicals	Diseases caused by intentionally released bacteria or viruses or by biological toxins	Illness resulting from exposure to radioactive materials

a warning or incident if they are not permanently sealed.
- Investigate if it is possible to turn off the ventilation system in an emergency.

Protective measures to consider in a CBRN attack

Good physical protective measures and procedures increase the ability to handle CBRN incidents. It is usually extremely costly to provide complete protection against CBRN, but steps can be taken at a relatively low cost that can limit the effects of a CBRN attack to some extent.

Here are some initial steps that are recommended to strengthen the ability of handling a CBRN attack:

- Review the physical security equipment in the parts of your installation that may be extra vulnerable to attack due to their function, such as doors and entrances.
- Do an assessment of the ventilation system from a security perspective, such as placement of intake and exhaust vents. Avoid air intakes at ground level or close to ground level.
- Make sure that actions in the event of CBRN incidents are included in the operation's overall emergency plans.
- Plan evacuation routes.
- Consider using pre-prepared announcements.
- Install air filters that are better adapted to the assessed risk.
- Check that the staff has knowledge about how to turn off the ventilation system if necessary.
- Limit access to water tanks and other vital functions.
- Review the security in the handling of food and drinks for the entire supply chain.
- Think about whether you need to install special equipment for packages, such as a separate room for postal processing (perhaps with its own ventilation system) or enable handling of post outside the area.

Armed attacks

Armed attacks can take place with firearms or stabbing weapons. Armed attacks can also take place in combination with the use of IEDs or with vehicles used as weapons. Attacks carried out using fully or semi-automatic weapons, for example, generally entail very extensive damage during a very short period of time.

The steps taken by individuals and organisations – often before the police arrive on scene – are therefore of major importance to reducing the damage. Steps that only slow-down a perpetrator for a short while can also reduce the damage considerably.

It is very difficult to fully protect against armed attacks since operations often require accessibility and being perceived as an attractive environment. However, there are some measures that can make them harder to commit and can reduce the damage.

This section contains advice on basic security measures that can be implemented and what protection is required to protect against weapons fire. Under the section Personal security, there is advice on how individuals can act in an armed attack.

Read more about Run, hide and tell

Protective measures to consider in the event of an armed attack

- Access controls to installations and buildings from entrances, evacuation routes, garage driveways and unloading bays.
- Searches of personal belongings and vehicles for access to buildings and installations.
- Greater presence of alert and attentive personnel in places trafficked by many people.
- Sectioning of installations and buildings to make it impossible for a perpetrator to move between different parts of the in-

stallation freely and without obstruction.

- Increasing the possibilities of buildings or installations to be able to quickly warn and provide instructions to staff and visitors in the event of an armed attack, such as over a loudspeaker system.
- Reinforce especially vulnerable parts of installations or buildings, such as entrances, reception areas, windows and doors for better protection against weapons fire and make it harder for a perpetrator to force their way in.
- Ensure that evacuation routes have enough capacity to enable a rapid evacuation of a large number of people, and review the installation's or operation's possibilities of invacuation, lockdown or using secure spaces.

Read more about Physical protection

Protection against firearms

In the event of an armed attack where firearms are used, knowledge of protection against firearms may be crucial to escape an attack. Presenting as small a target as possible and using the surroundings' possibilities of protection can lessen the effect of firearms. Even laying down on the ground without cover otherwise can reduce damage.

The following thicknesses of different kinds of materials are needed to protect against firearms of the most common kinds of ammunition for firearms (see Table 5). However, there are differences in terms of ammunition types and differences in protective levels for the same kind of materials, which is why the table should be viewed as approximate.

Unmanned aerial vehicles (UAV) or unmanned aerial systems (UAS)

Unmanned aerial vehicles (UAV) or unmanned aerial systems (UAS) refer to drones or aircraft without a pilot on-board.

The development of small drones (under 25 kg) has gone quickly and now constitutes a growing threat. Inexpensive electronics, advanced GPS systems, technology for autonomous control, greater load capacity, lighter batteries, more efficient motors and a signifi-

Table 6. Approximate thicknesses of different kinds of materials

Steel	Concrete	Gravel, crushed aggregate and stone chips	Wood	Compact soil
1 cm	20 cm	25 cm	70 cm	70 cm

Figure 7. Approximate thicknesses of different kinds of materials

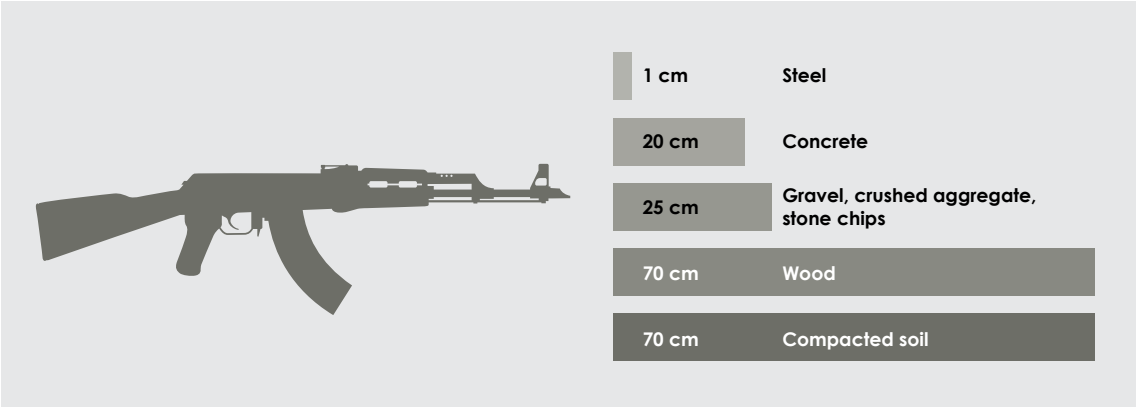


Table 7. Possible areas of use for drones

Danger to air traffic	Smuggling	Protest groups	Espionage	Physical attack	Reconnaissance
caused by drones flying over an airport or flying adjacent to an airport	of prohibited goods to closed installations	use drones to disrupt the private lives of others or to disrupt events	to gather sensitive information that can reveal capabilities, capacity and vulnerabilities	a terrorist tries to carry out an attack on a location or person, such as by having a drone carry an IED or a chemical or biological weapon	to plan terrorist attacks, such as by gathering information about a location that can then be used in the planning of an attack or a protest action

cant increase in the number of incidents mean that this threat should be taken seriously.

Drones are popular for many reasons, and the majority of those who use them do so without malicious intent. In recent years, drones have also been used on a large scale in international conflicts, such as carriers of weapons payloads or to obtain intelligence.

The knowledge and ability to use drones to commit a terrorist attack should therefore be considered to be widespread. Drones can also be used to obtain intelligence prior to an attack or to mislead and disrupt an on-going operation against an attack.

Handling a drone incident

The following advice may be useful in the event of a drone incident:

- Identify the drone.
- Assess the situation.
- Locate and contact the pilot.

Identify the drone

- Try to locate the drone visually and alert your surroundings.
- Is it carrying anything?
- Is it filming?
- Is it focused on a particular location?
- Can you work out where it came from?
- Keep in mind how you act as it is likely that your actions are being filmed.

Assess the situation

- Is the situation disruptive or is it a threat?
- Have people been injured or property been damaged?
- Are people in immediate danger to their lives?
- Is the location a sensitive or important site?
- Is the drone there to provoke a reaction, check responses, carry out an attack or to gather information?

Locate and contact the pilot

- The pilot is probably close to the drone.
- The pilot is probably standing at a good outlook with an unobstructed view.
- The pilot may be using a mobile phone, tablet, laptop or a transmitter.
- The pilot may be standing still or walking around and may be surrounded by spectators.
- The pilot is probably acting differently than his surroundings.
- The pilot may being wearing First Person View (FPV) goggles.
- Do not try to take control over the drone unless it constitutes a serious threat. Instead, wait for the battery to run out, which usually takes 20-30 minutes.
- In contact: ask the pilot to land the drone as quickly as possible and to turn off the drone and remote control.

- Keep your composure – most people flying drones do not have any hostile intentions.

Handling of drones

- Try to preserve the drone, considering its value as evidence.
- Handle the drone as little as possible for a potential technical examination by the police.
- Do not remove the drone's batteries or memory card.
- Turn off the drone and pack it down into a box.
- Choose a suitable means of storage since it might still be recording.

Protective measures to consider

- Concealment can be installed around buildings, installations and site boundaries or at the most vulnerable locations to make it harder to see in. Concealment can be comprised of vegetation, window film, fencing, awnings or shutters.
- Protect the object by placing a physical barrier around it, which may consist of vegetation, wires or netting – which impedes flight.
- The furnishing indoors can also be adapted to reduce vulnerability; for example, computer screens should be placed so that they are not visible from outside.

Vehicles as weapons

Vehicles can be used to deliver an explosive, for example. A vehicle can also be used as a weapon and break through perimeter protection, ram and damage infrastructure or injure and kill people. This is called "vehicle as a weapon" (VAW) attack.

The VAW method is not particularly complex and has been used by terrorists to attack targets where many people are gathered, which often results in extensive damage. VAW attacks require little or no training or practice and are therefore relatively easy to carry out.

The attack method can be used in combination with handguns, stabbing weapons and IEDs. Combinations of attack methods can be used to carry out a planned attack or as backups if, for example, the vehicle gets stuck or breaks down.

There are many kinds of vehicles that can cause a large number of deaths and serious injuries and it can also be difficult to stop a heavy vehicle.

Read more about Hostile vehicle mitigation

Arson

For several reasons, arson is a relatively basic method for causing extensive damage. Setting fires requires little or no training or special knowledge. Nor does it require any major preparations and it is easy to obtain flammable liquids and the like that can be used to accelerate the spread of the fire.

Fire and smoke from fire can entail extensive risks to and injury to people and damage to property. Fires with injuries and fatalities often receive extensive media coverage. Arson as an attack method is not common, but can take place for example through the placement of incendiaries with timer triggers to start the spread of fire or through the use of fire bombs that are thrown at buildings or people.

Statistics show that set fires normally begin in flammable materials, such as paper, boxes and rubbish. A flammable liquid is often used to hasten the spread of fire.

The fires are usually set in spaces without any natural overlook or insight, such as stairwells, hidden corridors, toilets and, not least, the outside of buildings.

To increase the protection against arson, there are a number of security measures to consider, which are described below.

Regulation of fire safety

The Civil Protection Act (2003:778) stipulates that the owner of buildings or installations or the business operator must implement necessary measures to a reasonable extent in order to prevent fire and prevent or mitigate damage resulting from fire. Meeting these requirements often requires both technical and organisational fire safety measures.

In addition, the Swedish National Board of Housing, Building and Planning regulates and provides guidelines regarding the dimensioning of building fire safety in the construction and modification of buildings, which for example encompasses division into fire cells and the design of evacuation routes.

In addition to this, the Swedish Work Environment Authority also has regulations and guidelines on fire extinguishers, signs and markings, evacuation plans and evacuation alarms at workplaces.

The various regulations can, for example, entail the following:

- External evacuation routes, such as emergency exits and external stairs, must be kept unobstructed, clear of snow and with skid-protection. Doors must be easy to open from the inside.
- Passability for rescue vehicles must be good and not impeded by obstructions, such as parked cars, gates, containers, etc.
- Evacuation plans must be clearly placed at entrances.
- Evacuation signs and guiding markings must be whole and visible. Electric signs must be illuminated.
- Fire equipment must be adapted to the operations and clearly placed and marked.
- Evacuation doors and corridors that constitute evacuation routes must be free from flammable materials and unobstructed.
- The building is divided into a number of so-called fire cells to prevent the spread of fire and smoke. Doors between fire cells must normally be closed or held open with magnet holders that are released upon an automatic fire alarm. The doors may not be held up in other ways, such as with a wedge doorstop.
- If the property has an automatic fire alarm and/or sprinkler system, this should be checked regularly so that it is not out of operation.

Protective measures to consider in the event of arson

The basic idea to increase the protection against fire is to reduce the amount of flammable materials, reduce the possibilities of bringing in flammable liquids into buildings and installations, ensuring that evacuation alarms work and that evacuation routes are unobstructed and ensuring that fire extinguishing equipment, such as sprinkler systems and hand-held fire extinguishers work and are accessible.

In addition to that regulated by the various authorities' statutes, there are a number of other measures to increase the protection against arson. A few examples of such measures:

- The unloading bay may be a vulnerable point if flammable materials are left over night. Keep loading bays clear of pallets, wagons and other loose flammable materials.
- Waste bins can be a fire hazard if they are left overfull and if they are placed under protecting roofs or attached to walls. Preferably choose non-combustible materials.
- Benches, waste bins, sand boxes or large flammable objects that can be used to start a fire should not be placed against the façade. They should preferably be placed 6 metres from the façade and chained or anchored in place if they are easy to move. Containers that are close to a building can also constitute a fire hazard.

- Other loose flammable materials in courtyards or alcoves, which can become fuel for a set fire, must be regularly cleaned away. For example, boxes, rubbish, broken furniture and leaf piles.
- Ground-floor windows can be made of unbreakable glass and be closed to prevent break-ins or keep things from being thrown in.
- Storerooms or temporary storage spaces may not be placed too close to the main building.
- Letter drops can constitute a risk of arson or burglary. A freestanding letter box may be preferable.
- Good external lighting can deter a perpetrator from setting a fire.
- Bushes and vegetation near the building should be kept low to improve visibility, which can reduce the risk of burglary or arson.
- A lot of packaging and rubbish in storerooms and possible waste rooms constitute an unnecessary fire burden. Keep these as clear as possible from unnecessary flammable materials.

Physical security

Physical security

Physical security measures are an important protection to remove or reduce risks and vulnerabilities to terrorism and hostile threats. The scope of physical security measures shall always be weighed against the operation's needs for accessibility and the possibility of being perceived as an inviting environment.

Security is usually more effective and least expensive if consideration is already taken to physical security requirements when an installation is planned and built.

Four basic principles for designing security measures:

- Deter
- Detect
- Mitigate
- Respond.

Deter means that a perpetrator refrains from carrying out the attack on the intended site. The design of the security measures means that the perpetrator deems that the risk of failure is too great, which may also mean that the perpetrator does not have the whole picture of which security measures have been implemented.

Detect means security measures that aim to verify that an attack is under way and to provide decision input for counter measures. Examples of detection measures are manned security and technical surveillance systems.

Mitigate means delaying a perpetrator's possibilities of carrying out an attack and mitigating the consequences of an attack. Examples of such measures are fencing, access control systems, vehicle barriers and structural building reinforcement.

Respond means measures intended to stop and discontinue an attack, mainly by security personnel or the police.

An effective physical security at a location where many people gather is best achieved through multiple layers of measures. This is usually called "defence-in-depth" or the "onion approach" since the basic idea is that security does not necessarily need to decrease radically because one layer is lost.

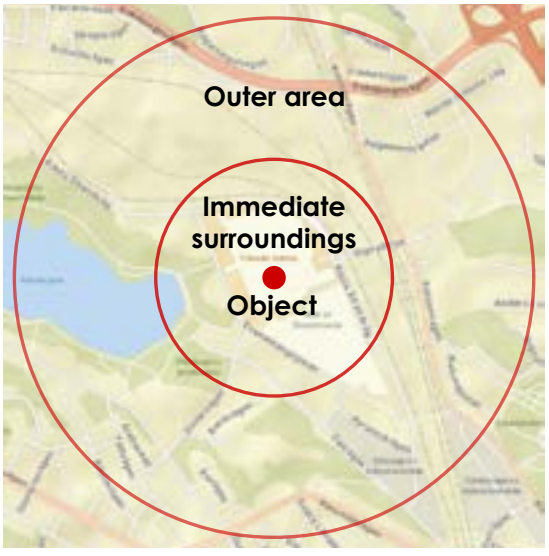


Figure 8. Sensitive object, immediate surroundings and outer area

Interactive security measures

Alarms, camera surveillance, lighting and other technical equipment are often used to deter and detect perpetrators and disrupt an attack or a crime.

Intrusion alarms can be both a deterrent and provide the possibility of detection. Camera surveillance may be of help to determine if an alarm is real and is often very important in investigations after an incident. However, camera surveillance is only effective if it is managed and monitored well. A well-conceived external lighting helps security staff and increases the benefit of camera surveillance.

Other security measures may be to establish access restrictions, conduct searches and access checks, reinforce the physical protection and plan for evacuation, invacuation, lockdown and protected spaces.

The protective measures that are implemented should be integrated so that they work in an effective and cohesive manner. Otherwise, there is a risk that implemented security measures in an area increase the vulnerabilities in another area or space. For example, if searches of bags and personal belongings to enter an arena mean that a long queue forms outside the arena, a new vulnerability is thereby created.

Keep in mind that security measures that are simple by nature can also have a considerable effect to deter and detect an impending attack. It may sometimes be enough to have visible and present personnel who welcome visitors and passengers at the entrance of an installation or an area.

Evacuation, invacuation, lockdown and protected spaces

Being able to handle an attack where the perpetrator attacks with firearms or stabbing weapons requires planning for the use of evacuation, invacuation, lockdown and protected spaces.

Attacks where perpetrators use weapons often take place very quickly and generally entail a large number of injuries and fatalities. The immediate decisions and actions taken therefore have a major impact on the damage outcome. It is therefore important that decisions are made and carried out quickly even if the situation is chaotic and perhaps even life-threatening to the person making decisions. Decisions and actions should not be postponed to await instructions or intervention from the police.

After a threat or during an attack, it is difficult to understand the full scope or predict how the situation will develop. The probability that staff and managers can act quickly and correctly increases if they are familiar with various kinds of threats and attacks and their typical features and what efforts may be relevant.

Regular training and practice is therefore necessary. Training and practice contributes to managers and staff being able to make quick decisions on deficient input, making good risk assessments and increasing the organisation's ability to handle an attack through experience.

If an attack could not be prevented, it may nonetheless be possible to disrupt and delay the attackers and significantly reduce the number of deaths through evacuation, invacuation, lockdown or the use of protected spaces.

Regulation of evacuation and fire safety

This chapter contains advice and experience that may be good to consider when planning and implementing evacuation, invacuation, lockdown and use of protected spaces.
The area of evacuation as a result of fire is regulated by the Swedish National Board of Housing, Building and Planning and the Swedish Work Environment Authority.

The Swedish National Board of Housing prescribes and provides guidelines on the dimensioning of buildings' fire safety and the design of evacuation routes in the construction and modification of buildings. The

Swedish Work Environment Authority prescribes and provides guidelines on evacuation route lighting, signs and markings, evacuation plans and evacuation alarms at workplaces.

It is important that it is primarily applicable regulations that govern this work, even if the advice presented in this chapter are not in conflict with the regulations issued by the various authorities.

Various kinds of efforts in the event of evacuation and fire safety

There are a number of different alternatives to protect people in an attack, fire or other danger:

- Complete evacuation
- Partial evacuation
- Targeted evacuation
- Invacuation and secure spaces
- Lockdown.

Complete evacuation

Evacuation in a suitable measure when the police or rescue services issue instructions for it or when the threat appears credible and an evacuation means that people move towards a relatively safe place. Evacuation can take place through the closest exit or by reference being made to special exits.

Information on evacuation times from exercises, analyses and the time it takes for individuals to follow the evacuation routes should influence decisions and instructions. The security along the evacuation routes can at the same time change during an attack.

Evacuation routes that go quickly can at the same time mean that new dangers arise. For example, the use of lifts entails a rapid movement to ground level at the same time that an attacker may be there. However, lifts shall never be used in a fire evacuation unless the lifts are especially intended for this purpose.

Partial evacuation

A partial evacuation is good if one needs to prioritise the people who are closest to the threat and are subjected to a major risk. This kind of evacuation can be chosen to limit the number of people who are moved in order to not overload internal and external passages and thereby create further risks due to crowding. This is especially relevant at events and arenas with large audiences and a high personnel density.

In buildings, the approach is similar to that for fire when one may choose to initially evacuate the floor or fire cell in which fire has been detected. Partial evacuation can also take place in several stages to minimise the number of people who are moving and thereby the return to the normal situation can take place more quickly.

Targeted evacuation

Targeted evacuation should be used if an area is or may become dangerous or if a certain evacuation route would mean passing through or near a threatened area. This alternative may entail a longer evacuation time, but at the same time entail higher security.

In a target evacuation, staff and visitors must be aware of the different routes, which means that they must be clearly marked with different designations. At the same time, there must be a possibility to communicate to visitors and staff what evacuation routes are to be used through lighting, loudspeakers or staff on site who provide information, for example.

In some of the scenarios, it is advantageous to communicate without warning the attackers, perhaps by using a code word. If so, this code word needs to be included in planning, training and practice.

In CBRN incidents, one should try to evacuate towards a higher place and against the wind. If the incident has occurred inside a building, one should stay away from the building's heating and ventilation systems during the evacuation.

Invacuation and secure spaces

If threats or danger arises outside an installation or building, it may be safer to let people stay there since an evacuation can subject people to danger from a passing attacker, for example. Since installations and buildings may look different, in some cases it is not possible to plan for invacuation or use of secure spaces.

In an assessment of the possibilities for an invacuation, it is important to identify:

- all points where one can enter and exit, both spaces that are open and those that are closed to the public (doors, windows, etc.)
- the possibilities of securing the entry and exit possibilities by physical means
- the possibilities of preventing people from leaving or entering the facility and guiding them away from the danger
- the possibilities that the installation can be divided into zones so that particular areas can be closed off.

Since glass shards and other shrapnel from explosives can kill and injure from a significant distance, it is often safer to move personnel within the actual installation than to take them out onto the street.

Invacuation works best if it has been planned for in advance and experts have been consulted to identify protected spaces in the building. These spaces should be included in the planning. Ensure to take into account air supply, toilets, seating, drinking water, lighting and communication possibilities. All of this must be in place in order to stay there for a prolonged period.

Protected spaces should be located:

- in parts of the building that are surrounded by brick walls, such as corridors, toilet spaces or conference rooms with doors that open inwards
- at a distance from windows, outer walls, stairwells and lifts
- on the ground floor
- in a space that fits an adequate number of people.

Lockdown

If an attack could not be prevented, it may nonetheless be possible to disrupt and delay the attackers and significantly reduce the number of deaths by conducting a lockdown. The difference between invacuation and lockdown is that, in a lockdown, the entire building or installation is used. In an invacuation, only parts of the building are used as protection.

Just like in an invacuation, it is not always possible to plan for a lockdown considering the nature of the building, the area or the installation. In an assessment of the possibilities of conducting a lockdown, the same criteria are used as in an invacuation.

A lockdown, especially during admission to an event, can lead to many people being locked out and more vulnerable to the perceived threat. If the admission is allowed to continue, it may, however, happen that the threat is let into the installation and make the people inside more vulnerable. Each case must be assessed based on the information at hand at that time and it is therefore crucial to have good internal and external information and communication systems.

Evacuation that takes place in the event of an attack can differ from fire evacuation

In Sweden, there is extensive experience and knowledge about how to reduce the risks and consequences of fires. It is therefore likely that staff and visitors are familiar with procedures in the event of a fire, including evacuation.

But evacuation need not be the best action in all situations – and even when evacuation is the best option, it is not certain that it should be carried out in the same way as in a fire. In a fire, it is appropriate to use every available exit. In an attack, it may be appropriate to instead direct people to particular exits, which affects the planning.

Evacuation alarms for fire can also be used for evacuation in an attack even if it is better to have different procedures for fire and an attack. It is primarily the possibilities and access to means other than an evacuation alarm for fire that are the deciding factors for what method is used, such as a loudspeaker system or the possibility to use staff to assist in the evacuation. If there is a loudspeaker system, it can provide greater flexibility so that information and instructions can be given that are adapted to the incident and confirmation can be provided to staff and visitors that it involves a real emergency.

Risks during movements in crowded spaces

When a large number of people suddenly begin to move, it entails special risks. The movement may just as well be due to the perceived threat as to a real threat. People can get scare and the crowd can move in opposite directions in a quick and disorganised manner.

However, research shows that most people behave rationally based on the information they have in emergencies. A rapid and disorganised movement away from a real or perceived threat is a natural and logical reaction.

When many people move quickly or in a disorganised manner in a crowd, there is a greater risk that somebody trips or falls, which can lead to the person being trampled down or entering areas they cannot get away from due to crowding. These risks can be worsened by pavement, stairs and escalators. Stairs that are to be used by large crowds, such as at arenas, should therefore be designed with handrails as dividers and other measures to reduce the pressure on individual bottlenecks.

Disorganised movements can also increase the risks to those who are more vulnerable, such as children and people with disabilities.

Personal evacuation plans

Anyone who owns or uses buildings or installations must take steps to prevent or limit damage as a result of fire. Depending on the activities conducted, there must therefore be a plan for the evacuation of those who are in the installation or building, which also includes people with disabilities. The planning should also include situations when there is not a fire, but that nonetheless require evacuation, invacuation or moving to protected spaces.

At some workplaces and public premises, there may be a special evacuation point, where people with diminished movement or orientation capacity can await continued evacuation.

Assembly points in evacuation

Whether people are evacuated to an assembly point or dispersed from the site depends on the operation conducted and the circumstances at that location, which applies to both fires and attacks.

The primary objective of an assembly point is to be able to count personnel and visitors in order for the rescue command or police to get information if anyone is still in the installation or building. Another objective may be to keep a large number of people in movement from being in the way or disrupting on-going rescue or police operations.

If there is no possibility or need to count people or there is little risk that people in movement are in the way for the rescue effort, there is also no need for assembly points.

If the operation is responsible for children or people with disabilities, who cannot be expected to take responsibility for themselves, there is however nonetheless a reason to consider an assembly point.

However, assembly points are not always a good alternative during an attack since the people who are at the assembly point can be attacked as a part of the terrorist attack. People naturally seek each other out after an incident and the staff should therefore receive training in encouraging them to disperse when it is appropriate.

If an assembly point is not used, evacuation routes should be guided to the extent possible and people encouraged to get far enough away from the incident. Here, a guideline may be 500 metres.

If an assembly point is used, there should be functionaries appointed to meet at there during an evacuation and the location should be located outside assessed police or rescue command cordons. There should be an assembly point that is a main option and a backup option in a different direction.

Checklist – What should an evacuation plan include?

- Plan drawings of evacuation routes and emergency exits.
- The functions that serve as evacuation leaders and functionaries.
- Information for evacuation leaders and functionaries.
- Procedures for the staff who remain to shut down critical processes that cannot be immediately shut down upon an evacuation alarm.
- Access to first aid and fire extinguishing equipment.
- Location for command and communication.
- Location and responsibility for emergency bag.
- Possible assembly points and possibilities of checking which staff members are missing.

Checklist – Planning of evacuation

- Assess risks and vulnerabilities and possible approaches in the event of an attack.
- Under what circumstances are efforts necessary?
- Assess if the possibilities to detect a terror attack are good enough.
- Prepare a clear chain of command for which staff members have authority to order an evacuation and lead the work. The authority must be real and perceived by the rest of the staff.
- Appoint which staff members or functions are responsible for serving as functionaries during incidents.
- Appoint the staff members or the functions that are responsible for shutting down operations, such as critical processes.
- Make it known to staff and visitors where evacuation routes, emergency exits and protected spaces are located. Evacuation plans are posted according to applicable regulations.
- Plan for how communication will be made to staff and visitors.
- Train and conduct exercises with the staff.
- Arrange emergency bags.
- Assess the need for transports in the event of a full evacuation.

Checklist – During an evacuation

- Stay calm.
- Gather information; differentiate between facts, judgements and rumours.
- Dial 112.
- Analyse the situation. Determine the kind of event, attackers, dangers and weapons.
- Decide on a complete evacuation, invacuation, lockdown or use of protected spaces. A decision may also be to not take any action. Do not await decisions from the police or rescue services.
- Keep others from entering the area before it is safe.
- Decide on a possible search.
- Cooperate with police, rescue and emergency services.
- Communicate with staff and visitors.
- Follow the news.
- Try to check what potential attackers are doing, where they were last seen through surveillance cameras, for example.

Checklist – After an evacuation

- Find out where staff and others are.
- Assess if there is a need for psycho-social care.
- Document steps taken.
- Assess if the site needs to be searched.
- Use possible lessons learned to train staff and improve the organisation.
- Gathered information to your own staff and organisation about the chain of events and steps taken.

Command and communication in connection with evacuation

If there is a control room or command centre, actions should be taken to reinforce the security around them. In many cases, there is no control room or if the security there is deemed to not be good enough, an alternative command location can be considered. The command location may be outside the installation.

There should also be a plan for how the organisation will communicate internally and how the communication with the public or visitors should take place. The plan must enable instructions to staff, the public and visitors to evacuate or take other necessary steps. Some alternatives to such measures:

- Evacuation alarm, as for evacuation in the event of fire.
- Loudspeaker systems. Use special sound signals or pre-recorded messages. If communication is only to occur with staff, codewords should be used. Remember that codewords that are used often in public spaces are soon recognised by regular visitors.
- Flexible signs or bulletin boards.
- Verbal communication.
- If possible, different signals should be used for different incidents. Keep in mind that it may be difficult to remember and differentiate different kinds of signals.
- Internal systems, such as two-way radio, SMS, email, pagers, group messages, the organisation's own systems or pop-up messages on computer screens.

Camera surveillance

This section provides an overall description of the use of camera surveillance as a protective measure. Camera surveillance can serve as a complement to other protective measures and may be significant to detecting an impending terrorist attack or other incidents and accidents.

Cameras are also of significance to obtaining a good situation overview and thereby an improved possibility of making well thought through decisions during an on-going attack. The technology is also of significance to subsequent criminal investigations. The use and need for cameras should at the same time be weighed against the infringement of people's personal integrity that it entails.

Camera surveillance is a part of a security system with several possible solutions. It is crucial that the use of cameras is integrated with other security measures so that it is effective as possible – especially the design and placement of lighting and alarms, access restrictions in the form of fences and entrances, and the possibilities of responses by security personnel, such as security guards.

All kinds of camera surveillance are, however, dependent on the knowledge and capabilities of security personnel. Through training, particularly knowledge of possible methods in a terrorist attack, and practice, the ability of personnel to detect threats and make relevant decisions improves.

Regulation of camera surveillance

All camera surveillance that, without being controlled on site, takes place in a way that entails lasting and regularly repeating personnel monitoring is covered by the area of application of the Camera Surveillance Act (2018:1200). The objective of the legislation

is to meet the need for camera surveillance for justified purposes and to protect people from infringement of personal integrity in such surveillance. Among other things, the law regulates requirements and prerequisites for permits and exemptions from permits.

Permits are not always required to be permitted to conduct camera surveillance. But even if permits are not required, the operation must instead be sure to meet the requirements in the EU's General Data Protection Act (GDPR). GDPR applies over Swedish law and the Camera Surveillance Act is a supplemental national legislation that applies to those using camera surveillance in Sweden.

By law, authorities and others who perform tasks of public interest need a permit for camera surveillance if they conduct camera surveillance in a place accessible to the public. In locations not accessible to the public, the use of cameras can take place without a permit, but then the rules in GDPR must be followed.

The requirements on informing data subjects are more extensive than before. Anyone conducting camera surveillance must set up signs or provide information about the surveillance in some other way. The information must include who is conducting the camera surveillance and contact information to the organisation. There must also be some other information, such as on a website, for example contact information to a potential data protection officer, the purpose of the camera surveillance and the legal grounds on which the camera surveillance rests. If sound is recorded, this must be indicated separately. On the Swedish Data Protection Authority's website, there is more detailed information on the application of the Camera Surveillance Act.

Areas of use for camera surveillance

It is important that there is a well-defined purpose for the camera surveillance. Camera surveillance can be effective in order to

- Detect intrusion, reconnaissance for an attack or preparation for a crime
- Deter perpetrators from committing crime
- Verify alarms or observations
- Provide decision input during an ongoing incident
- Support criminal investigations and evaluations after incidents.

Camera surveillance methods

There are three main methods used in camera surveillance:

- Operator-monitored camera surveillance
- Alarm-activated camera surveillance
- Camera surveillance with video analysis.

Operator-monitored camera surveillance

Means that an operator detects, verifies and alerts upon an event. An effective surveillance with the help of operators requires a good work environment in addition to high-quality cameras. Size and placement of screens, use of high-quality tables and chairs, regulated temperature, good lighting and limitation of the operators' screen time are crucial to a good work environment. There should also be a balance between how long a certain camera image is shown and how many times the image is shown during a certain time frame.

Alarm-activated camera surveillance

Alarm-activated camera surveillance means that cameras are only activated by an alarm, which means that the screen that shows the camera images is normally off. The method can also be used in combination with operator monitoring.

Camera surveillance with video analysis

Used to determine if any changes occur in the places monitored. An alarm is issued if there are changes in colour, size, speed and direction, for example. In the use of video analysis, the camera issues an alarm in the event of the correct conditions and at the same time sorts

out normal movements and thereby reduces the number of alarms. Camera surveillance with video analysis can also be used in combination with operator monitoring.

Advanced camera technology

In addition to traditional camera surveillance, there is also more advanced technology. For example, thermal cameras and technology that uses biometric information or analysis of movement patterns. Thermal cameras use thermal radiation from an object in contrast to regular cameras that use available light.

Thermal cameras allow a good chance for early detection, both in daylight and in darkness, but at the same time, mean that it is difficult to identify various characteristics, such as colours of vehicles and clothes.

Biometric cameras use human characteristics where the most common method is facial recognition. Technical development is progressing quickly and in recent years, technology has been developed that also allows an analysis of movement patterns, such as for people and vehicles that deviate from the norm.

Remember that when technology for facial recognition is used, the data processed in the identification counts as biometric data. Biometric data belongs to a category of personal data that is considered particularly sensitive in the data protection rules. There are therefore special provisions concerning biometric data in GDPR that must be taken into account when using facial recognition technology.

Access restriction

Access restriction is an important part of security and can consist of access control and security checks of people, items and vehicles. Access controls aim to ensure that unauthorised personnel are not in places not accessible to the public. Security checks are intended to ensure that nothing that threatens security is brought into buildings, areas or installations.

How access control and security checks are done varies widely depending on the operation's requirements on accessibility and being perceived as an inviting and inclusive atmosphere. The scope of the access control and security checks should be proportional to the risks that exist for the operation or the installation.

Regulation of access restriction

Even if the site is open to the public, there may be conditions to gain access, such as what may be brought into the installation or the building. Some access restriction is regulated in statutes, such as the Public Order Act (1993:1617) and the Installations Protection Act (2010:305). The Public Order Act regulates some access provisions for certain public transport and sports events. The Installations Protection Act regulates provisions on access to protected objects, which is something that cannot be addressed in this guide, however.

Access control

Access control aims to ensure that unauthorised personnel are not in places not accessible to the public and can take place through:

- access controls for entry and exit
- access controls of vehicles
- structural building measures, such as locks, fencing and sectioning.

Access controls for entry and exit

Determine if staff and visitors are to have access to all areas or if there should be special access areas. Staff should wear employee and access cards visibly, which can be equipped with colour codes based on what areas access covers. There should be clear procedures for the issue of employee and access cards with confirmation of identity at pick-up. There should also be procedures for the handling of temporary employee and access cards.

Visitors who have been granted access to installations and buildings should be given visitor

badges that are worn visibly and returned when leaving. Visitors can be signed into a ledger with information on arrival time, visit host and what organisation they represent. The visit ledger should be saved for a certain period of time. Decide if your own staff should escort visitors.

Access control can be done by automatic systems at places where access is required. Automatic control systems can also be used for different sections within a building or installation. A personal code should be used with automatic systems at the same time that all entries and exits are logged. For entry and exit controls of visitors, the control should be manned.

Access controls of vehicles

If the operation requires access controls for vehicles, there are a number of things to keep in mind. The best solution is to limit the number of vehicles that have access to the installation or the area. Vehicles that need access frequently should be equipped with access cards and be linked to a certain vehicle. The handling of access cards should be managed in the same way as in all other access control.

It is best if access is only given to vehicles that are pre-registered and where the identities of the driver and passenger(s) are confirmed. Automatic number plate identification using surveillance cameras may sometimes be of use.

Structural building measures

There are some structural building measures that contribute to maintaining access restrictions for the installations and buildings, such as locks, fencing and sectioning. These kinds of security measures contribute to being able to exercise some control over what takes place within the area.

Sectioning

Determine what areas or parts of the building or installation the public has access to. It is important that the boundaries between the different areas are easy to perceive, which can be done using fencing, various lock systems or signs, for example.

Locks

Locks can be electronic, mechanical or a combination of both. Mechanical locks require keys while electronic locks can be opened using access cards or codes. Mechanical locks require a careful key management.

A list should be kept over which keys are handed out and regular checks should be done to keep unauthorised personnel from gaining access to the area or installation. There should also be a procedure worked out for which steps are taken if keys are lost.

If electronic locks are used that are opened with access cards or codes, it is important that the card handling is careful and that codes are personal and changed regularly.

Fencing

Fencing is an important protective measure and can be used together with other protective measures, such as camera surveillance and lighting, to increase security. Fences should be checked regularly so that they are in good condition and fill their purpose. Fences can be good in order to:

- mark the boundary between areas that the public has access to and those that are not accessible
- deter perpetrators from committing crime
- disrupt and delay an on-going attack
- serve as protection against vehicles as weapons
- increase the protected zone in attacks where explosive are used
- impede insight
- in some cases limit the effects of explosions and small-calibre weapons fire.

Security checks

Security checks are intended to ensure that nothing that threatens security is brought into buildings, areas or installations. It is

important that the scope of the security checks are proportional to the risks that exist for the operation or the installation. Security controls usually focus on:

- searches of buildings and adjacent areas
- searches of people and belongings
- searches of vehicles.
- Searches of buildings.

Searches can be done as a part of the daily routine for property inspections, for example. The police and rescue services can conduct searches in buildings in connection with a response call, but there are also times when business operators have a need for searches.

The building or installation should be divided into different areas in searches. If there is a natural sectioning in the form of different floors, for example, it should be used. Each area should be of a manageable size. Keep in mind that stairs, emergency exits, corridors, toilets, lifts, parking lots, service spaces, boiler rooms, etc. should be a part of the search plan. The plan should be worked out in advance and the staff should be well aware of it.

It is good if searches are done by personnel who work in pairs so that they are as thorough and systematic as possible. The staff generally know their workplace the best and if they know what they are looking for, the possibility of an effective search increases. As the various subsections are searched, this should be reported to the person responsible for the search.

If staff or visitors are still in the installation or area, it is important that search is done without unnecessary concern arising. Use radio, mobile phone or coded messages on the loudspeaker system.

Screening people and belongings

Searches of people and belongings reduce the risk of explosives, stabbing weapons, handguns and other dangerous items being brought into the installations, areas and buildings. Normally, only a police officer may conduct such searches pursuant to the Police Act (1984:387).

For special occasions, however, a security guard can be empowered to carry out personal searches and checks of belongings. Security guards may be empowered, for example, to serve at security checks at public meetings in municipalities and county councils or at courts according to the Security Guards Act (1980:578).

In addition to such occasions, there is also a possibility to carry out a so-called conditional check at arenas and events, for example. This means that private individuals can deny a search, which at the same time means that he or she is not given access to the event or the arena. The organiser can at such times decide itself what is permitted to bring in, as a part of the agreement of gaining access to the arena.

For a search to be effective, it is important that the implementing staff is aware of what is being sought and is prepared for what happens if a suspicious or dangerous item is found.

To keep in mind for personal searches

- There should be clear information to visitors that checks may be carried out.
- The method for searches is adapted to the risks to the installation, area or building.
- Consider the possibility of providing advance information, such as when sending tickets, that time-consuming security checks may be conducted.
- The spaces for checks are adequately dimensioned and protected against weather and wind.
- The capacity for checks is adequately dimensioned based on the estimated through-put of people. The formation of queues entails new risks.

Methods for screening people

Table 8. Methods for screening people

Method	Objects	Area of use	Note
Manual	• Explosive charges • Firearms • Stabbing weapons • Other dangerous items	• Often used for secondary checks in detection in metal detectors	• Requires no technology • Labour-intensive and time-consuming • Effective with thorough searches • Can be perceived as integrity violating • Items concealed in other objects can be hard to detect • Risks to personnel in the presence of sharp items
Metal detectors, stationary	• Firearms • Metal stabbing weapons • Metal components in IEDs	• Requires manual searches upon detection • Requires special examination of found objects	• Fast and allows large through-put of people • No detection of non-metal objects • Extensive risk of false alarms and sense of discomfort • Requires large area and can negatively affect the impression of the installation • Expensive equipment
Metal detectors, hand-held	• Firearms • Metal stabbing weapons • Metal components in IEDs	• Can be used as a complement to stationary metal detectors or individually	• Slower than stationary metal detectors • Can be used to find very small objects • No detection of non-metal objects • Requires correct handling by the personnel
Body scanners	• Explosive charges • Handguns • Stabbing weapons • Other dangerous items	• Requires manual searches upon detection • Requires special examination of found objects	• Detects metal and non-metal objects • High cost for purchases and operation • Relatively low through-put of people • Requires extensive training for handling • Requires large area and can negatively affect the impression of the installation

Table 9. Methods for screening bags and belongings

Method	Objects	Area of use	Note
Manual	• Explosive charges • Firearms • Stabbing weapons • Other dangerous items	• Often used for secondary checks upon detection from x-ray equipment or individually	• Requires no technology • Effective with thorough searches • Labour-intensive and time-consuming • Can be perceived as integrity violating • Items concealed in other objects can be hard to detect • Risks to personnel in the presence of sharp items • Speed and through-put can be adapted
X-ray	• Explosives • Firearms • Stabbing weapons • Other dangerous items • Items hidden in other objects	• Requires manual secondary check	• High cost for purchases and operation • Relatively low through-put of people • Requires extensive training for handling • Requires large area and can negatively affect the impression of the installation
ETD – explosive trace detector	• Explosives or traces from explosives	• Can be used as a complement to x-ray	• Requires collection of particulates from surfaces that are frequently touched • A detection need not mean a large occurrence of explosives • Only detects explosives • Requires specially trained personnel

Methods for searches of vehicles

Searches of vehicles can contribute to explosives and weapons not being brought into buildings, installations or areas. Searches of vehicles should only be seen as a risk-reduction measure that is done together with other measures when the risk and threat are deemed to be especially serious. Just conducting access controls and interrupting unexpected deliveries can reduce the risk significantly.

Vehicles can be used to transport vehicle-borne improvised explosive devices (VBIED), IEDs, handguns, ammunition or other items used by a perpetrator in an attack or other crime.

At the same time, it is probably not practically implementable or cost-effective to search all vehicles for smaller objects. It is therefore important to distinguish between what is necessary to detect and what is desirable to detect.

It is normally only police officers that have the possibility to conduct searches in places other than protected objects. However, in some cases, security guards can be empowered. Conditional access as described in the previous access may also be applicable.

A risk assessment should be done of the people driving the vehicles or an assessment of what vehicle types entail greater risks. Known and pre-registered contractors, deliveries or own personnel entail a smaller risk than with temporary visitors or the public.

At the same time, larger vehicles entail a greater risk than smaller vehicles. The most basic format for searches, and perhaps the most common, is a quick visual check in the loading and passenger spaces supplemented with the use of inspection tools, such as mirrors, to check the places that otherwise cannot be checked. If deliveries are involved, checks can take place to ensure that the delivery corresponds to what is expected.

In addition to the above methods, there are also advanced technical systems with, for example, explosive detectors and x-ray equipment and that allow the vehicle to be driven though the inspection site. There are, however, very few installations or buildings where such systems are cost-effective as the technology is very expensive.

To keep in mind for vehicle searches

- Determine what is expected and acceptable queue formation. Queue formation means that new risks arise.
- Searches of vehicles require specially trained personnel.
- Consider if it is possible to search vehicles outside the installation, the area or the building.
- The location for the search should be screened off from the surroundings and protected from wind and weather.
- Provide clear information at a search will be conducted and information on what is to be prepared by the driver.
- Consider arranging a freight centre for reloading from which further transport into the operation takes place by your own staff with dedicated vehicles.

Postal and package handling

An attack method that has been historically used is sending letters and packages with explosives or other hazardous substances. Most companies and organisations usually receive a lot of post and deliveries, making dangerous shipments an attractive attack method for a perpetrator. However, the method must be seen as relatively uncommon in terror contexts.

Upon suspecting a dangerous shipment, there is a small likelihood that the recipient knows what kind of hazardous substance is involved, which is why procedures and measures must include all kinds of hazardous substances. Examples of hazardous substances used historically in the post are explosives, anthrax, ricin, insecticides and nerve gases.

Indicators for a suspected hazardous postal item

- Discolouration or oil stains.
- Leakage of substances from the item, solid, liquid or gas.
- Odours coming from the item.
- Strange labelling, such as "may only be opened by" or "private".
- The item is addressed to the organisation or a title instead of a person.
- Strange shape and weight or uneven weight distribution.
- No sender, incorrect address or a sender address that cannot be verified.
- Unexpected origin from the postal stamp or sender address.
- More stamps than are required, considering the item's size and weight.
- Labels and excessive amount of tape and packaging materials, which means that the recipient is guided to open the package at a certain end or in a special way.
- Uncommon or poor handwriting.
- The item contains additional letters or packages or other content that may be hard to remove.
- Visible aluminium foil or wiring.
- Envelope that is completely glued shut. Envelopes are often glued shut just on a part.
- Unexpected objects or materials, loose or in containers, such as sticky, powdery, crystalline or granular substances.
- Sudden illness symptoms.

Poisoning symptoms

- Constricted pupils
- Runny nose
- Increased salivation
- Skin irritation
- Blurred vision
- Increasing problems breathing
- Muscle cramps
- Reduced awareness.

Immediate actions in the event of an incident

- Alert the police, rescue services and ambulance care by 112.
- Avoid unnecessary handling, set the item aside on a level and clear surface.
- Keep the suspicious item separate from other post.
- Evacuate the closest area and adjacent rooms.
- Close doors and windows.
- Decide on the need for further evacuation.
- Keep others from entering the evacuated area.
- Take the people who came into contact with the item to a separate and safe place if there are signs that it is a CBRN incident.
- Register the people who came into contact with the item or were in its immediate vicinity.
- Do not use mobile phones or radio devices in the immediate vicinity of the item, within around 15 metres, if there are signs that it may involve an IED.
- Close the ventilation if possible.

Planning and procedures for postal and package handling

- Plan evacuation routes so that affected staff do not need to go through common spaces and that other staff and visitors do not need to evacuate through a dangerous area.
- Check if it is possible to shut off the ventilation.
- Do all post and package handling at the same place. Preferably in a separate building or a space that can be isolated.
- Train the staff that handles post and packages in procedures in the event of an incident and how they can recognise a dangerous item.
- Think through what physical protection is necessary, such as protection from explosions, especially ventilation systems and laundry and showering possibilities.

Keep in mind that it may be difficult to quickly change the physical protective measures if the threat situation changes quickly.

- Consider if there is a need for equipment for improvised decontamination of contaminated individuals.

Hostile vehicle mitigation

Besides transporting explosives, vehicles can also be used to break through boundaries, ram and damage infrastructure or injure and kill people. This method is called a "vehicle as a weapon" (VAW) attack. The method was used several times in Europe in recent years to attack crowded places. The risk of such attacks can be reduced with physical obstacles and traffic-control measures.

In most cases, traffic-control measures are measures that individual business and service operators have a possibility to influence only in exceptional cases. This is largely an issue for municipal urban planning. The traffic-control measures can, for example, involve restrictions for heavy vehicles, traffic-calming measures, such as roundabouts and chicanes, or controlling what times of day deliveries are made.

In addition to traffic-control measures, urban planners can also work with natural obstacles, such as rivers, ditches, embankments and tree planting. Other common objects in the urban environment, such as flower boxes, artwork and bicycle stands, can also be placed and designed considering protection against vehicles as weapons. This section largely focuses on the protective measures that can be implemented on site for those who are to be protected. Mainly with various kinds of vehicle barriers.

Vehicle barriers

Vehicle barriers can be divided into three different types: passive, active and temporary.

Passive

Are permanent barriers that cannot be controlled or lowered. The barriers can be extensively designed so that they blend into the existing environment. However, passive barriers may entail limitations to passability for emergency vehicles, for example, which must be taken into account in the planning. Passive barriers must generally be anchored in order to be effective.

Active

Active barriers can be deactivated or controlled to let vehicles through during restricted hours. Often used in places with guarding and are generally a costly solution. Active barriers require continuous maintenance.

Figure 9. Passive vehicle barriers.
Photo: Sebastian Ihre

Figure 10. Passive vehicle barriers.
Photo: Sebastian Ihre

Figure 11. Active vehicle barriers.
Photo: Sebastian Ihre

Figure 12. Active vehicle barriers.
Photo: Sebastian Ihre

Figure 13. Temporary vehicle barriers. Photo: Sebastian Ihre

Figure 14. Temporary vehicle barriers. Photo: Sebastian Ihre

Temporary

Temporary barriers mean that the obstacles are placed out temporarily as protection if the risk and vulnerability for a certain location increase during a period of time, such as at an event. Prefabricated temporary barriers are not generally as resilient as active and passive barriers. Temporary solutions may also be heavy vehicles and containers.

Standards for vehicle barriers

Several international standardisation institutes have drafted standards for vehicle barriers, Including the British BSI, the American ASTM and ISO. Among other things, the different standards regulate test methods and instructions on installations. Many companies have products that have been designed according to the different standards that exist.

The advantage of products designed based on standards is that they are tested and thereby allow users to dimension vehicle barriers correctly. However, it is important to note that standards can have different criteria for what is considered to be secure, which is of special significance in the design of vehicle barriers where every metre counts to reduce damage beyond the barrier.

Dimensioning, placement and design of vehicle barriers

Barriers that have not been tested generally do not allow the same level of protection as tested barriers, but may nonetheless be of major importance to reduce speeds or to deter perpetrators from carrying out an attack. The advantage is also that they can be tailored so that they better blend into the existing environment.

A disadvantage is that it may be difficult to predict how the barrier acts in a vehicle collision. The barriers may, for example, be crushed, pushed aside or forced under the vehicle. In general, vehicle barriers must be anchored in the ground in order to be effective.

Table 10 shows examples of how vehicles and barriers can interact with each other.

Untested barriers must be designed and constructed based on estimated speeds and vehicle weights and thereby what impact energy arises at the instant of the collision. There are also other factors that influence the effectiveness of the barriers, such as placement, mutual distance and estimated impact angle.

Figure 15 presents the inertia that the barriers must withstand to fully stop a vehicle. However, it is most often not possible to design vehicle barriers with the objective that they should take up all inertia at the instant of the collision.

The vehicle's inertia is, as previously noted, dependent on the vehicle's weight and speed. The speed is of the greatest significance to the achieved inertia. Steps should therefore be taken to reduce the possibilities of vehicles to accelerate over longer distances. It is also desirable to change the collision angle between vehicle and barrier to thereby redirect some of the force from the vehicle to the side.

The design and placement of the barrier is of significance to how much force can be absorbed by the barrier and how the vehicle interacts with the barrier. The following recommendations can be seen as guidelines with regard to the barriers' mutual placement and height.

Figure 15. Vehicle-barrier interaction

Barrier causes vehicle to rotate

A large part of the inertia is absorbed by barrier

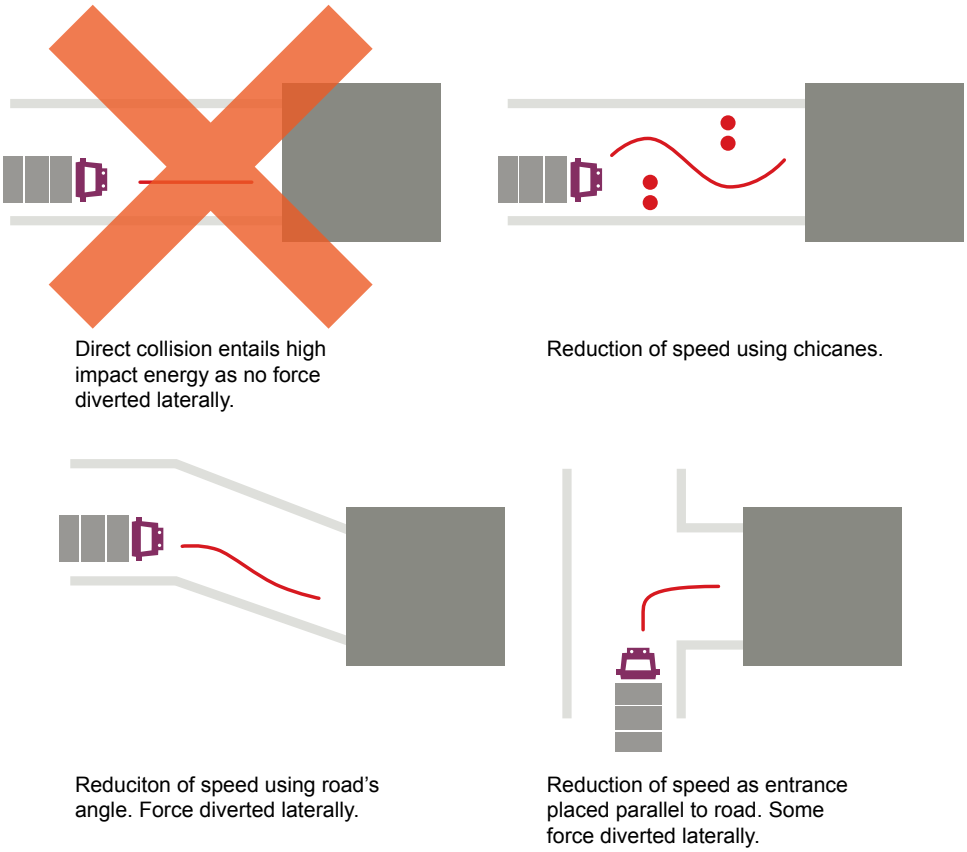
Barrier pushed ahead of the vehicle

Vehicle gets stuck in the barrier

Table 10. Vehicle impact energy

Vehicle weight	80 km/h	64 km/h	48 km/h
7,5 ton	1852 kJ	1185 kJ	667 kJ
3,5 ton	864 kJ	553 kJ	311 kJ
2,5 ton	617 kJ	395 kJ	222 kJ
1,5 ton	370 kJ	237 kJ	133 kJ

Figure 16. Methods for speed reduction



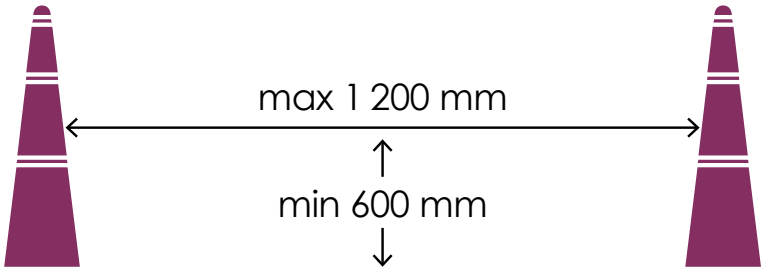
Direct collision entails high impact energy as no force diverted laterally.

Reduction of speed using chicanes.

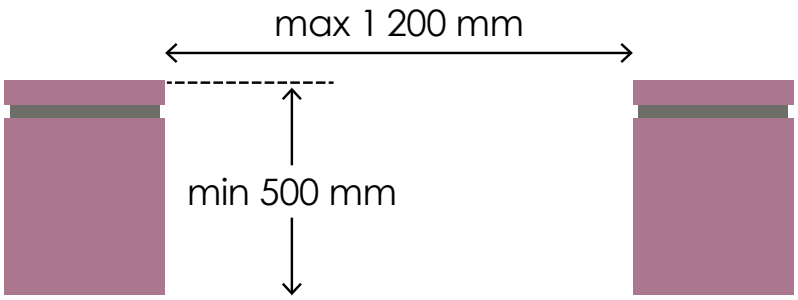
Reduciton of speed using road's angle. Force diverted laterally.

Reduction of speed as entrance placed parallel to road. Some force diverted laterally.

Figure 17. Technical requirements



The maximum clear distance between adjacent VSB must be no greater than 1200 mm, this distance must be measured between structural elements at a height of 600 mm above ground level.



The minimum height for vertical fixed structure is 500 mm. An increased height of 900 mm will make the measures more conspicuous.

Property maintenance

Good property maintenance contributes to buildings and installations being nicer and more attractive, but it also contributes to improving the possibilities of discovering and managing a terrorist attack.

If premises are continuously cleaned and maintained, it makes it easier to detect what is out of the ordinary. For example, it is harder to place out IEDs or conceal dangerous items that can be used during an attack. It becomes easier to detect, for example, flammable items and rubbish that blocks evacuation routes and that can catch fire in an attack.

To keep in mind during property maintenance:

- Avoid having waste bins in vulnerable or sensitive locations, such as close to glass sections and load-bearing structures.
- Review waste bins and examine their placement and the size of the opening.
- Use clear bags in the waste bins so that it is easier to conduct an initial search for suspicious items.
- Keep public, common and outer areas, such as entrances, toilets, corridors and open spaces, clean, neat and well lighted.
- Limit furnishings, such as furniture and equipment on the walls in vulnerable locations.
- Lock offices, rooms and storage cabinets that are not being used.
- Ensure that everything has a place and that things are put back in their place after use.
- Put security seals on inspection doors.
- Cut trees and other vegetation, especially at entrances, so that it is easier to get an overview and keep items from being hidden.
- Ensure that first aid equipment and fire extinguishers are checked and serviced.
- Security systems that are dependent on electricity should have an uninterrupted power supply and should be tested regularly.
- Check that evacuation routes are not blocked and that emergency exits work.

Personnel security

Personnel security

The employees are an important resource in the security work of organisations. A good security culture among the employees contributes to reducing risks and vulnerabilities in the organisation and that attacks and incidents can be effectively handled.

Creating a good security culture

A good security culture involves employed staff having knowledge about the threats that exist, how the organisation's security is structured and the knowledge and desire to contribute to improving and maintaining security. Here, leadership and management are important factors for creating a good work environment and a good security culture, which in turn entails loyal employees that are motivated and committed in their work.

The security measures the organisation has implemented should be clear and simple to achieve without infringing on the daily work too much. It should be endeavoured to create an environment where the desire to do the right thing is greater than the fear of making mistakes.

If the security measures are too extensive or if the employees do not feel enough loyalty to the organisation, personnel may give the appearance of following security procedures, but actually not care about following them. This may in turn lead to greater risks, financial damage and damage to trust, as well as an atmosphere that feeds insider threats.

Insider threats

A common explanation for insider threats is that they consist of current or former employees, contractors, suppliers or business partners who have access to the organisation's premises, systems and information, and who deliberately or unconsciously use this to damage an organisation. The objective may be sabotage, theft, espionage, fraud or to create business advantages.

An insider threat can arise if employees unconsciously violate security procedures without intent to cause harm. A threat may also arise from pure negligence where employees deliberately break rules in order to save time or to make their own work easier, for example.

Insider threats that arise unintentionally or due to negligence can largely be addressed with security procedures that are continuously followed up and developed. Here, it is especially important that there are possibilities to discover if procedures are not followed.

The third kind of insider threat is employees that have the intention of damaging an organisation. The employee may be driven by personal conviction or be recruited by a third party. This kind of insider threat can be very difficult to detect and handle as steps are often taken to conceal a criminal intent.

The motives for the person that has an intention of damaging an organisation may vary. The employee may be persuaded or threatened by a third party to carry out harmful acts. The employee may also be driven by ideological and financial reasons or driven by vindictiveness towards the organisation. Nor is it uncommon that the motive can be that the employee is simply seeking some form of excitement in his or her life.

In summary, insider threats can be said to be an abuse of trust.

Indicators of insider threats

Below are some examples of characteristics and prerequisites that mean that employees could be more receptive to carrying out an insider threat.

- Double loyalties between the organisation and personal friendship, for example, or a host country and one's own nationality.
- Life experiences, such as marriage, conflicts, upbringing, drug abuse, financial circumstances, ideological or religious conviction that in different ways can affect the loyalty to the organisation.
- Personal characteristics such as ethical and moral approaches that affect the loyalty to the organisation.
- The relationship to the surroundings and the rest of society. An inability to establish personal relationships or perceive prevailing norms, rules and etiquette. The absence of personal integrity and values.
- The questioning of their own personality and identity that is expressed in the form of low self-confidence or immaturity, for example.
- An unstable personality that can be expressed in the form of exaggerated emotionality, anger, imaginativeness, impulsiveness or self-absorption.

Security measures to consider

- Examples of measures that may be effective to counter insider threats are below.
- Conducting risk and vulnerability analyses, where risks are also evaluated based on possible insider threats.
- A good physical security in the form of, for example, access restrictions and access controls.
- A good information security in the form of information security procedures, use of social media, information classification, authorisation division and logging, for example.
- Raising awareness through training existing personnel, also encompassing insider threats.
- A recruitment process that takes into account security and insider threats, as well as follow-up by existing personnel.

Prior to employment

Good and well-conceived employment procedures are important to every organisation's security. Reducing the risk that an employee will be able to misuse his or her authorisation is significant in order to avoid or detect everything from criminality to terrorism.

Before a person is employed, it is important to check the information that the person has provided. The control measures should be weighed against the organisation's needs and how vulnerable and sensitive the prospective employment is.

When necessary, the identity of the applicant should be verified and possible residence and work permits should be presented to the employer. Identity can be verified with a passport or a national identity card, for example. Stated qualifications and employment history should be checked so that they agree with reality.

Stated and independent references should also be checked. The applicant should also be informed that incorrect information being submitted, such as fake qualifications or certificates, may be grounds for refusal of employment and that it may be a criminal act. Using fake qualifications and certificates may form the basis for legal action even after employment has begun.

For some professional categories, there is often a requirement to present a transcript from the police's criminal records, including employments in healthcare, schools and welfare services. For employment outside the aforementioned professional categories, an employer does not have a right to request record transcripts. The employee can independently choose to present a transcript, but there is no support in the legislation for an employer to request such a transcript.

An employer must generally respect the employee's private life, which also includes activities that take place on social media, for example. It is not permitted to gather information on the applicant's activities on social media, for example, even if it is a good source for information about the employee. It is to be viewed as processing of personal data according to the General Data Protection Regulation (GDPR).

During employment

Even if employees were checked at recruitment, procedures are needed to also do follow-ups at regular intervals. People's circumstances and attitudes can change over time or after special events. It is not uncommon that insider crime is committed by personnel that was employed for a number of years and for some reason changed their loyalty during their employment.

An important aspect to avoid and counter insider crime, besides good procedures for checks, is good leadership and ensuring that the employees remain motivated, committed and productive. A good way to follow up employees is to continuously carry out structured discussions on development, assignments, results and general life situation to be able to detect changes in attitudes and other circumstances that may affect the work.

An employer may choose to carry out drug tests of employees, among other things when there is a suspicion of abuse or prior to employment. Drug tests are to be viewed as a major change of the working conditions, which is why such a procedure should be regulated in collective bargaining agreements or in the individual employment contract.

However, control measures, such as drug tests and transcripts from criminal records, should be handled carefully as they can largely be considered to be infringements of personal integrity for the employees.

Security training for personnel

Security training for personnel should be based on the operation's procedures and can beneficially be carried out in the setting in which the personnel works. Consider if tailor-made training is needed for some of the personnel.

Prepare a training plan that extends over a certain period of time with recurring refresher courses. Keep in mind that personnel turnover influences how often training needs to be done. The security training can also be a part of the introductory training for new employees.

Changes of the interiors and design of installations, elevated threats or the introduction of new security procedures can also affect when training needs to be done. Also work to involve the police and rescue services, for example, in planning, training and practice.

The training can contain the following:

- Knowledge of attack methods and insider threats.
- Procedures for invacuation, evacuation, lockdown and protected spaces.
- Procedures for command, communications and alarms.
- Procedures for information security.
- Steps in the event of threats.
- Knowledge about and actions upon detection of suspicious behaviour and suspicious items.
- First aid and knowledge about how to stop bleeding.

Personal security

Personal security

Our own security, and the safety of those close to us, is of utmost importance. Our private security can be affected by our work and our professional role. What the threat situation looks like to each person determines what kinds of steps may need to be taken for one's own security, both at work and privately. This section provides general advice on how to protect oneself privately, such as in the home, at work, travelling and online. The steps should be adapted to the threat situation and what is practically possible.

Home security

There are a number of simple measures you should consider to protect yourself and ensure that your home is secure.

Protection begins with the outer boundary of your home:

- Make sure that you have good outdoor lighting that covers outer doors, parking areas and walkways to the building. The lighting should be placed where it makes it hard for a perpetrator to hide.
- If there is a lot of vegetation that restricts insight from the surrounding environment and neighbours, there may be reason to remove it.
- Check that tools and ladders, which could be used to enter your home, are put away and stored under lock and that everything that could be used to cause damage is removed, such as loose tiles, large stones and garden decorations.

Other advice is to have so-called perimeter protection, meaning securing the most common intrusion routes:

- All outer doors and windows must have good quality locks and preferably a protective level that corresponds to burglary protected doors according to the current standard.
- Installing a peephole on the front door is advisable.
- If you live in an apartment, a safety door with an externally reinforced letterbox is the best protection.
- If you have a letter drop in the front door, a preventive measure may be to install a safety letterbox with fire protection on the inside of the door.
- Instead of a letter drop, you can have an external lockable letterbox or a post-office box.
- If you live in a house, you should have a letterbox with a lock.
- If you live under a threat, you should plan for alternative evacuation routes in your home.
- If you live in a villa, avoid having glazed sections in or next to the front door.
- If there are glazed sections, they can be equipped with protective glass or grating.

- To protect windows, you can install a special plastic film on the inside of the glass that provides some insight and projectile protection.
- Never let house keys be out and visible. Keep them in a secure place if a fire were to occur.
- Do not write out where keys are to. Instead, use colour coding.
- Replace the lock if a key is lost or missing.
- Never give your keys to anyone you do not trust. Keep in mind the risk that the keys are copied.
- Replace the locks if you change homes.

If you install an alarm, you should choose a company that you know about. The alarm may be a sound alarm, a siren or a silent alarm that is transmitted to an alarm centre. Today, most monitored alarms can be supplemented with smoke detectors, which creates a higher level of protection in the event of fires. It is also common for the alarm equipment to include an attack alarm. When necessary, the fixed alarm installation may be supplemented with a mobile attack alarm, such as through your mobile phone.

Vigilance under a threat

Do not let unknown people into your home. Check the identity of craftsmen or messengers, for example. Never leave unknown visitors alone in the house and teach your children to never open the door or let strangers into the home. Have the habit of always locking the door to your home even when you are home.

When travelling or commuting

If you are to travel or commute between different places, you should plan your journey before you leave. Choose secure routes and avoid isolated or poorly lighted small streets or isolated parking lots. If you are worried when you are out, you should try to stay close to crowds and other people. Walk against the traffic if possible to keep vehicles from being able to approach from behind.

Never accept an offer of a ride from anyone you do not know well or anyone unknown. Be attentive to your surroundings; if you are talking on the phone or have earphones, for example, you cannot perceive your surroundings as effectively. Be extra cautious when you handle cash or use cash points and do not show that you are carrying cash.

If you suspect that you are subjected to some form of mapping, it is good to vary routes and travel times. If you have the same route daily, it is easy to predict what times you will be at what places. Vary routes when driving and departure times as much as possible.

If you end up in a situation where you feel threatened, you should avoid getting out of the car and making direct contact. You can avoid this by communicating through the window, calling for help or going to a place where there are other people.

Have the habit of always having locked doors when travelling by car. If you use a taxi, you should preferably preorder the car and only spontaneously take taxi-registered cars and with drivers that have a taxi identification well visible.

Anonymous phone calls and threats

Anonymous phone calls and threats can be very unpleasant. They are most often intended to cause fear and anxiety. Listen attentively and do not interrupt if you get a threatening phone call. Note the time, any background noise, gender, age, dialect and similar factors. It is a crime to make threatening phone calls and offensive phone calls so you should file a police report if you receive one. In a potential criminal investigation, there is a possibility to trace calls, both those made and to create preparedness to trace possible future calls. But you can yourself also request call lists from your telephone operator.

Park safely and check your vehicle

If you cannot park the car in a locked garage or a secure parking lot, you should park it so

that it is visible to other people. Try to park in well-lighted places and preferably within your sight and the sight of others. Try to not have set daily routines that make it possible to predict where your vehicle will be. Consider installing lighting with motion detectors, surveillance cameras or fencing for deterrence.

Do not just rely on these security measures – you may also need to do checks of your vehicle. There is some risk that you attract attention to yourself when you check your vehicle, but there is a risk that must be weighed against the consequences of a bomb attack. Inspect your vehicle every morning if there is a threat because it is most vulnerable at night.

Do not let friends or family members get close to the vehicle before you have inspected it carefully and are certain that nothing is abnormal or suspicious. Get to know what your car looks like underneath. It will then be easier to discover if something looks different. This is especially important for larger vehicles where the underframe area may be more complicated and offer more possibilities to conceal an object. Also be attentive to fresh tracks on the ground that may indicate that somebody placed something under your car.

If you find anything suspicious, you should not touch the object or any part of the vehicle. Move away from the vehicle and ensure that others do likewise. If possible, prevent others from approaching the vehicle. Call the police over 112 once you are at least 15 metres away and explain what has happened. Seek cover behind something solid, such as a wall or building, and avoid glass sections.

Read more about Car bombs

Post and packages

Post and packages that you receive at home may contain unpleasant surprises. You should therefore be careful of unordered and strange packages and ask your family to act the same way. If you receive a suspicious package, you should not touch or open it. Report it to the police.

Read more about Postal and package handling

Consider what information you have that is valuable and if there are any risks in how you handle it. Personal ID numbers, passwords, card information, passport numbers, photographs, receipts, contracts and business information are examples of important information, whether it is your employer's or your own. In order to reduce the risk of being subjected to mapping, threats and violence or theft and fraud, you should keep from disclosing information on your personal circumstances.

The technical equipment that we use often makes our daily life and our work easier, but it also makes us more vulnerable. Others can access your personal information in member lists, address lists, email lists, phone books and social media platforms and other websites if they break into your computer or mobile phone. Therefore, make a deliberate choice about what information you share over the Internet.

Secure handling of mobile phones and computers

- Use code locks or your fingerprint on mobile phones.
- Avoid connecting mobile phones or computers to an open wifi network.
- Make it a habit to turn off wireless transmission of data that you do not use, such as Bluetooth and wifi.
- Use antivirus software and do not accept unexpected and unknown program installs.
- Update computers, mobile phones, software and use applications with the producer's latest security updates.
- Do not use unknown memory cards or USB memory in mobile phones or computers.
- Keep mobile phones and computers under watch when you are outside your workplace.

- Be careful with your login information so that unauthorised personnel do not gain access to them.
- Note codes and numbers to be able to freeze subscriptions if anything were to happen. Keep in mind to not save them in connection with your equipment.
- Never use the same password in private contexts that you use at work.
- Use strong passwords when logging in. For example, by putting together three random words together with figures, special characters and caps and lowercase letters. Use long passwords, at least 12 characters.
- Use a password manager if you have a lot of passwords to keep track of.

Secure handling of social media

Think about what you publish online and in social media. Information on employment, private address or working address, family members, hobbies and vehicles may be very valuable to perpetrators.

You should regularly revise your integrity settings in social media so that your information is not visible to people who you do not know. Your family or your friends could also disclose important information about you unintentionally if they do not make sure to protect their profiles.

If you are under a threat, you should avoid saying where you will be in advance. Do not let apps or websites get information on your geographic location so that others can find out where you are or have been. Do not use check-in functions, for example.

Tell about things you have done, not about things you will do. This is to avoid mapping or that perpetrators seek you out. Avoid exposing or providing insight into your habits about places that you regularly visit.

Run, hide and tell

The most common methods in an attack are the use of firearms, stabbing weapons, vehicles as weapons or improvised explosive charges. Below is advice on how individuals should act when the perpetrator uses firearms. Even if the advice is structured for armed attacks, it may also be applicable in other situations. It can often be difficult to form a clear perception of what is happening and the different attack methods can be used in combination with each other.

Run

- Run if you can.
- Determine if it is safest to run or to hide.
- Is there a safe escape route? Can you get there without exposing yourself to more danger?
- Insist that others follow you, but do not wait on those who hesitate.
- Leave your belongings.

Hide

- If you cannot run – hide!
- Seek cover from shooting; if you suspect that the cover will not protect against gunfire, lie down and present as small a target surface as possible!
- If you can see the attackers, it is possible that they can also see you. You not being visible need not mean that you are safe because bullets can go through glass, brick, wood and metal.
- Determine if there are other escape routes.
- Avoid being shut in.
- Be silent; turn the sound off on your phone.
- Be attentive of what you see and hear.
- Lock and barricade yourself in, but avoid barricading yourself in rooms without an escape possibility.
- Move away from the door.

Tell

- Call 112 – What do the police need to know? If you cannot talk or make noise, you should just listen to the instructions you get.
- Where and when did you last see the attackers?
- Describe the attackers, how many they are, their weapons and clothing.
- Give information on where you are, possible hostages, injured people, types of injuries, information on the building like entrances and exits.
- Try to distinguish between what you believe and what you know.
- Warn others nearby.

Think about the following if you run, hide and tell

- Do not call on your mobile phone if you do not have to. If the network gets overloaded, it can be hard for vital calls to get through.
- Follow the instructions of the police, rescue services, ambulance care and other authorities.
- Do not share unconfirmed information online or otherwise.
- Be prepared that further attacks may take place.

Armed police response

- Follow the police officers' instructions.
- Stay calm.
- Avoid sudden movements that can be perceived as threatening.
- Keep your hands visible.

The police may:

- Point guns at you.
- Treat you firmly.
- Question you.
- Have difficulty distinguishing you from the attackers.

Advice when travelling abroad

Advice when travelling abroad

Every organisation has a responsibility for its employees who travel abroad on the job. Good security procedures for travel abroad are important and they should indicate what help employees can get if an emergency were to happen on the trip, such as a terrorist attack.

Organisation's responsibility

The organisation should inform its employees of the procedures that apply to foreign travel and how the employee should act him- or herself. This section provides advice on how to reduce the risks to employees on travel abroad and at the same time, provides practical advice to you as a traveller. The advice should be adapted based on the current threats at the destination and the advice provided in this section is mainly intended for destinations that are associated with major risks, such as countries in conflict.

In a first step, one should think about whether the trip is necessary. Are there other, less risky ways of achieving the same objective as with the trip, such as a video conference?

In a second step, a risk analysis can be done based on the destination and the travel plan. Assess the risk of various kinds of threats, such as terrorism, other crime, espionage, etc. Use credible information sources, such as the Ministry for Foreign Affairs' travel information, when the organisation does its assessment.

When necessary, the employee who is to travel should receive a security review with information adapted and relevant to the destination. Provide information about the threat situation and how the employee should best relate to it.

Ensure that employees know what support there is during travel, such as security advice and healthcare, and how they should act in an emergency situation.

The person who is to travel should be able to contact the organisation around the clock in an emergency situation. Make sure that the traveller has current contact information on hand during the trip. It is also important that the employer knows the destination, housing, contact channels and what meetings are to be held. Prepare a plan for risk and crisis management where it states how everyone involved should act if an employee were to get into a critical situation abroad.

Have clearly defined roles and division of responsibility upon an event. Make sure that there is always a person available if anything were to happen and the traveller were to need help. Consider if you will engage a company that offers assistance with security and medical care on travel and that can provide assistance 24 hours a day in emergencies.

Air travel

When you are to travel abroad by air, there are some things to keep in mind. The risk of being subjected to an attack or other crime is considerably less within the security checked area than in the departure lounge or on the

trip to and from the airport. Spend as little time as possible in the departure lounge and be attentive of your surroundings. Keep your luggage under watch and avoid using earphones when you otherwise can miss important information, which applies in all kinds of travel. Reduce the risk of exposure by packing correctly so that you do not have problems in the security check and preferably choose bags without pockets on the outside so that somebody cannot place items in one. Avoid having some form of external marking on luggage or clothes that can indicate ties to your work if it may be sensitive. If possible, booking travel with layovers in high-risk countries or arriving at the destination late at night should be avoided as the risk of being subjected to crime is then greater. Take along a copy of your passport and extra photos and keep them separately from your passport. If you lose your passport, the copy and the photo can be used to get a new passport.

Taxi and transfer trips

The trips taken at the destination and the travel to and from the airport may be risky. Make an assessment, depending on what the destination is and what time of day it is, if it is safer to travel by taxi or to use public transport. In general, one can say that the risk of an attack is greater in travel by public transport, but depending on other circumstance, such as traffic and the time of day, public transport may nonetheless be preferable. The traffic on roads and streets is generally a very large risk. Regardless of whether it is a counterparty that meets you at the airport with their own car or if you take a taxi, you should make it a habit to keep the doors locked when riding. Do not be afraid to ask the driver to slow down if they are driving too fast and always use a seat belt. If you are picked up by the counterparty, you should find out the driver's name and number.

Find out what taxi companies are reliable and do not ride with vehicles that are not clearly marked as taxis. Take a print-out with at the hotel to avoid misunderstandings and never ride with a taxi that has unknown co-passengers. When travelling, you should try to keep track of where you are and if the trip feels unpleasant, feel free to call a colleague or the party you are to meet and say that you are on the way.

Hotel and accommodation

When you book a hotel, you should choose safe accommodation where you can feel secure. Ask colleagues who have been at the destination before. In general, the security is better at large well-known hotel chains at destinations in, for example, countries in conflict. Avoid staying on the ground floor since it can increase the risk of break-in. Also keep in mind that the risks may be greater living on a high floor in the event of a fire. Study the evacuation plan for the hotel and find out where emergency exits are. Find out if there is an assembly point. Consider if you need a smaller bag or backpack where the most essential items are packed if you have to leave the hotel quickly. Make it a habit to lock in valuables, such as money, passports, medicines and computers if you do not carry them with you. Make an assessment of the safe before you use it.

To keep in mind for travel abroad

- Read up on the destination and study maps of the local environment so that it feels familiar.
- Be restrictive about sharing information about your travel and route online, such as on websites or in social media.
- Plan the transportation to and from your destination. What taxi companies are safe to ride with? What possible means of transport are there upon arrival?
- Give a detailed itinerary to a relative and to your organisation.
- Take copies of passports and travel documents and keep them separate.
- Ensure that you have suitable health insurance.

- Enter contact information into your phone. Find out important numbers in the country you are visiting, such as alarm numbers.
- Avoid taking valuables to the furthest extent possible as it may make you more exposed to pick-pockets and robbery.
- Have a charged mobile phone with you and have a battery charger on hand.
- Follow the local news reporting so that you are aware of the security situation.
- Notify the contact persons if your travel plans change.
- Be aware of your surroundings. Avoid using earphones and other items that are distracting since they decrease your ability to react if you were to end up in a threatening situation. If you look alert, you also look like a tougher victim, which can be a deterrent.
- Be alert to people acting suspiciously and items, such as bags and packages that have been left unattended. Rely on your gut feeling and if something does not feel right, report it to the security personnel or police.
- If possible, vary travel times, means of transport and travel routes.
- Be careful if somebody shows an unusual amount of attention.
- Avoid clothing or behaviour that may draw attention to yourself. Also avoid situations that make you stand out from the crowd or mean you can be attacked because you are a foreigner, for example.
- If possible, avoid walking alone in the evening.
- Do not get intoxicated.
- If you drive a car, make sure that the vehicle is in good condition and that nothing has been placed at or on the vehicle. Have all windows closed during the journey.
- Do not open the hotel room door to visitors if you are not certain who they are.
- Never agree to transport an item where you are not familiar with its contents.
- Find out where the emergency exits and possible evacuation routes are.
- Bring necessary medicine as the supply in the country you travel to may be limited.

Checklists

Checklists

Bomb threats

How you should react to a bomb threat

1. Stay calm and talk calmly with the caller.
2. If possible, ask a colleague to alert the police.
3. Write down the caller's number if it is shown on your phone.
4. See the section further down on threats made by email and social media.
5. Record the call if possible.
6. Write down the threat word for word, exactly as it is expressed:

Ask these questions and write down the answers as carefully as possible:

1. Where exactly is the bomb right now?
2. When will it explode?
3. What does it look like?
4. What does the bomb contain?
5. How will it be triggered?
6. Is it you that put the bomb in place? If not, who did?
7. What is your name?
8. What is your address?
9. What is your phone number?
10. Do you represent a group or are you acting alone?
11. Why did you put the bomb in place?

Time that the call ended:

Name and phone number of the person informed:

Time of the call:

This part is to be completed once the caller has hung up and the police has been informed

Date and time of the call:

Length of the call:

Phone number to the receiving phone:

About the caller:

☐ Man ☐ Woman

Approx. age _____

Language/accent _____

Caller's language:

☐ Eloquent ☐ Irrational

☐ Pre-recorded ☐ Coarse language

☐ Incoherent

Caller's voice

☐ Calm ☐ Slurs ☐ Lisps ☐ Familiar

☐ Crying ☐ Upset ☐ Fast

☐ Clearing throat ☐ Stutters ☐ Deep

☐ Accent/dialect

☐ Angry ☐ Distorted ☐ Laughs

☐ Nasal ☐ Slow ☐ Hoarse

Other (specify)

Other noises, background noises:

☐ Street noise ☐ Engine noise ☐ Loudspeaker system ☐ Office noise

☐ Property noise ☐ Open surface ☐ Enclosed, booth

Other noises, specify

☐ Animal noise ☐ Other voices ☐ Music

☐ Porcelain (dishes, cutlery) ☐ Static noise ☐ Machinery

Notes

Other comments:

Signature **Texted name** **Date**

_____ _____ _____

What you should do if you get a bomb threat by email or social media

1. Let the message remain! You should not reply, forward or delete it.
2. If it is made by email, note who the sender is.
3. If it is made by social media, what media was used and who is the sender?
4. Call 112 and follow the police's instructions.
5. Save all web log files so that the police can examine them

Signature	Texted name	Date

Emergency bag

It may be good to have an emergency bag that contains the most essential items to be able to handle incidents even if a building or installation is evacuated. It can be placed in a reception area or other readily accessible location. Appoint a function that is responsible for the bag and check and update the contents regularly. The list below is not exhaustive and should be adapted to the nature of the operation.

A bag can contain the following:

Documents	Yes
Instruction card with roles and responsibilities	☐
List of employees with contact information and closest relatives	☐
Contact information to the property services, security company and other important actors	☐
Drawing over the premises, which also shows where to shut off gas, electricity and water	☐

Equipment	
First aid materials	☐
Radio with extra batteries and charger	☐
Safety jackets and megaphone	☐
Extra keys, key cards and codes	☐
Torch, spare batteries and charger	☐
Cordon tape, warning tape	☐
Note-taking materials	☐
Mobile phone with charger or power bank	☐
Respiratory protection	☐
Protective goggles	☐
Helmet	☐
Water	☐

Suspicious behaviour

Date: _____ **Time:** _____ **Location:** _____

	Yes	No	Number of people involved:
Surveillance pictures/other pictures:	☐	☐	

Activity – Why is the behaviour suspicious?

(photos, films, watches a long time, enters prohibited area, etc.)

Person

Description	Gender	Ethnicity

Facial features	Clothes/shoes	Build

Hairstyle, hair colour	Approx. height

Special features

(Such as tattoos/scars/facial hair, birthmarks, piercings, etc.)

Speech/dialect/accent/wording/expressions

Have you seen the person(s) before? _____

Is there equipment taken with (bag, camera, etc.)? _____

Have you seen the equipment before? _____

How did the person arrive (by foot, train, car, etc.)? _____

Have you seen the vehicle before? _____

Information on the vehicle:

Registration number _____

Make _____ Model _____ Colour _____

Other characteristics (buckles, brands, injuries, etc.) _____

Was the person(s) addressed? _____

How did the person(s) react? _____

Additional information _____

A cooperation between:

Swedish Civil Contingencies Agency

Polisen Swedish Police

SE-651 81 Karlstad Phone +46 (0)771-240 240 **www.msb.se**
www.msb.se/en MSB1474 – February 2020 ISBN 978-91-7383-997-6