

CONTINGENCY PLANNING AND PROTECTIVE SECURITY ADVISORIES

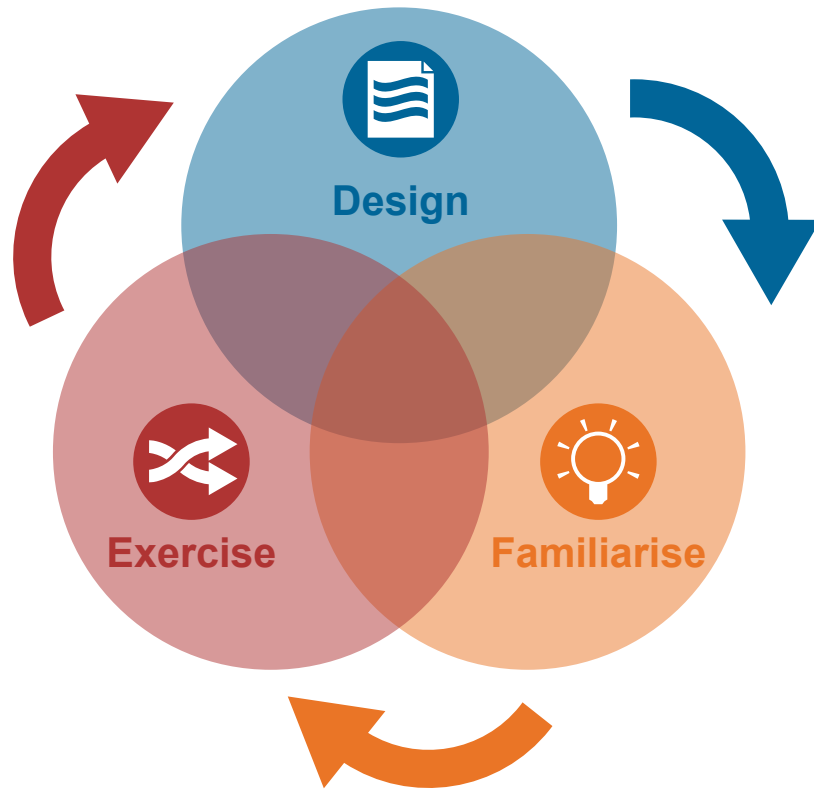
FOR WORKPLACES

LEE WEE NAM LIBRARY
李偉南圖書館



SINGAPORE
POLICE FORCE

With the threat of terrorism at its peak in recent years, it is extremely important that premises owners prepare contingency response plans in the possibility of a terror attack.



**PREPARE A CONTINGENCY
RESPONSE PLAN**





1. DESIGN

- Premise owners should designate a person to be in charge of preparing and coordinating response plans to deal with contingencies. These plans should clearly indicate who can make decisions on behalf of the organisation when a terror attack occurs.
- The contingency response plan should take into account the risk of different types of terror attacks. When designing your plan, consider the following elements:



A. Detecting the threat

Your employees and other premise users should know how to spot a threat, identify the steps to report the threat to the Police at the earliest opportunity, and when to trigger your contingency response.



B. Locking down your premises

Have a process to lockdown your premises to prevent attackers from entering your premises. (If this is feasible).



C. Getting the word out

Establish a process to inform people in your premises of an attack. For example, have pre-prepared broadcasts over a Public Announcement system for different types of contingency situations or other means for instant communications such as a mobile phone chat group among employees.



D. Evacuate

If an attack is imminent or has commenced and it is not possible to lock-down your premises, evacuate if possible.

Plan for multiple routes of evacuation. Inform people to leave the premises once they are outside. Do not congregate outside the building as this presents an easy target.



E. Hide

Consider designating safe rooms for people to hide in should evacuation become impossible.



F. Link up with the Police

Have a designated and alternate point of contact whom the Police can liaise with during the incident. The designated point of contact should be in touch with the local Neighbourhood Police Centre. In normal time exchange contacts and maintain a regular channel of communication.



2. FAMILIARISE



- Ensure all staff in your organisation are familiar with the contingency plan.
- Have a security induction for new staff to be familiarised with contingency plans.
- Identify gaps in planning and discuss the responses to specific scenarios with colleagues in your organization.
- More information on specific scenarios is available in the accompanying 'Planning Guidelines for Specific Terror Attack Scenarios'.
- Encourage staff to pick up relevant advisories and life-saving skills. Refer to the SGSecure advisories and website for more information.
 - How to recognise and respond to suspicious items and behaviour.
 - 'Run, Hide, Tell'.
 - Improvised First Aid Skills 'Press, Tie, Tell'.
 - Download and learn to use the SGSecure App to alert the Police in the event of an attack.



3. EXERCISE



- Conduct regular drills and exercises to ensure all staff are familiar with evacuation routes and hiding places, as well as their roles during an attack.
- Use these drills and exercises to identify gaps or flaws in your contingency plans.
- Regularly review your plans to ensure that they are feasible, up-to-date and easy for staff to follow.

In addition to having robust contingency response plans, premise owners should consider implementing protective security measures to mitigate risk.

For more information, see our "Advisory on Protective Security Measures".

**PLANNING GUIDELINES
FOR SPECIFIC TERROR
ATTACK SCENARIOS**

In addition to the general principles on contingency planning, it may be useful to consider the following pointers when planning for specific scenarios:

i. Armed Attacker Incident

Ensure access to the Fire Command Centre is secured. Allow the Police to access the area.

Track movement of attackers via CCTV if possible and update the Police.

Designate security points-of-contact who can link up quickly with Police responding forces to provide information on your premises. Useful information include the building layout, profile of occupants, CCTV images and key cards.



ii. Suspicious Item Found

When an unattended item is found, confirm whether the item exhibits suspicious characteristics. For example:

- Has the item been deliberately hidden away?
- Does the item have wires, circuit boards or a ticking sound?
- Is the item typical of what you would expect to find in the location?

If the item is deemed suspicious, do not touch it. Keep people away from the item.

Call the Police, and alert the building security immediately. Do not use communication devices such as handphones, walkie-talkie sets within 15 metres of the item, as these may inadvertently set off the item.

Cordon off the item if possible. Wait for Police's arrival to assess the item.



**PLANNING GUIDELINES
FOR SPECIFIC TERROR
ATTACK SCENARIOS**

iii. Explosion

- Provide first aid to casualties if it is safe to do so.
- Be on the alert for possible unexploded devices in the vicinity of the first explosion.

Vehicle(s) used as a weapon

- Evacuate people from the surrounding area.
- Keep people as far away from the vehicle(s) as possible.
- Provide first aid to casualties if it is safe to do so.



iv. Suspected Chemical Agent Release

- There is a possibility that a chemical agent may be present if three or more persons in close proximity collapse and appear incapacitated without a reason.
- Evacuate as quickly as possible. Call the Police immediately.





Premise owners should implement protective security measures to mitigate the risks of possible terrorist attacks.



**Decide what
to protect**

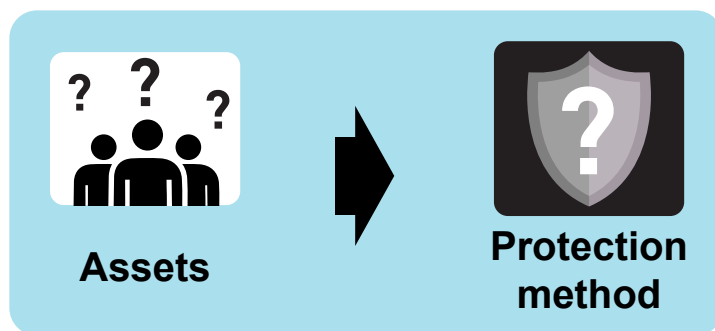


**Identify
threats**



**Design
mitigation
measures**

HOW TO IMPLEMENT PROTECTIVE SECURITY MEASURES



1. DECIDE WHAT TO PROTECT

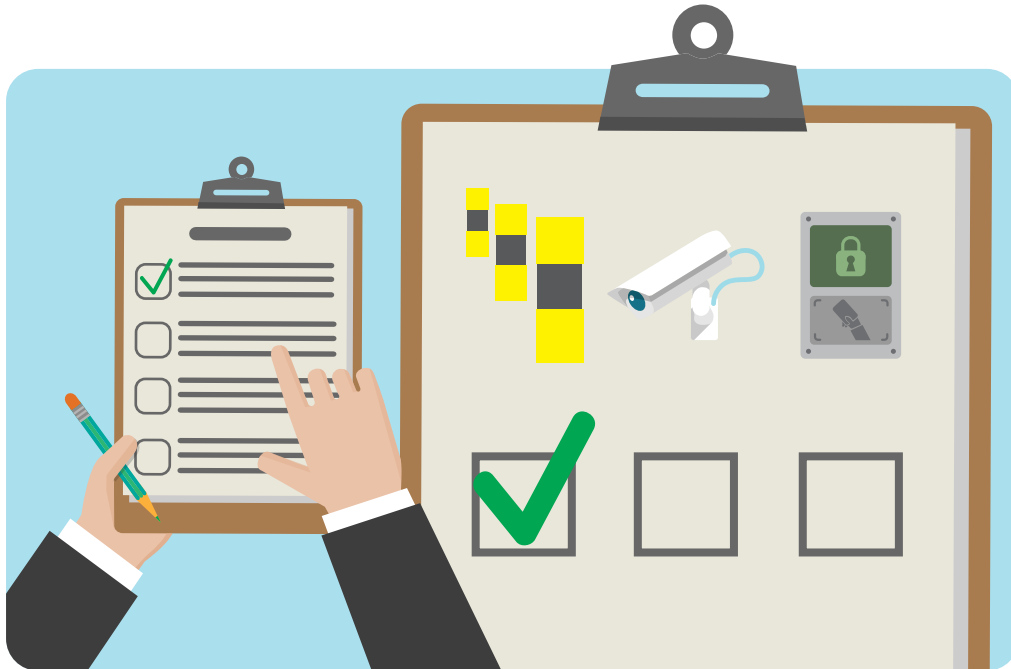
- Human lives are the topmost priority. Know where your employees and other premise users congregate.
- Identify other assets that are essential to your functions such as Uninterrupted Power Supply (UPS) Room, Main or Intermediate Distribution Frame (MDF or IDF) Room and Sensitive Materials.
- Prioritise these assets based on how critical they are to help you determine what measures have to be taken to protect them.

2. IDENTIFY THREATS

- Know that terror attacks can take the various forms:
 - Armed attackers – with firearms, knives or other weapons.
 - Vehicles used as weapons.
 - Explosives in a vehicle, on a person or in a bag or other containers.
 - Chemical or biological agents.
- Identify features of your premises that may increase the risk of an attack or make you vulnerable to specific forms of attack. Examples include:
 - Areas of mass congregation in your premises which make it an attractive target; close proximity of your premises to the road which allows vehicles to be used as an effective weapon.



3. DESIGN MITIGATION MEASURES



- Identify gaps and review existing security measures to determine their effectiveness. Things to consider include: CCTV systems, current model of deploying security staff, currency of standard operating procedures and emergency response plans.
- Based on your assets, threats and existing security measures, prioritise mitigation measures where there is high risk. Consider the following:
 - **Threat:** What is the easiest for someone to attack?
 - **Vulnerability:** Which area in your premises is an attack most likely to succeed?
 - **Consequence:** What areas will cause the greatest impact on your business if disrupted by an attack?
- Apply the 4Ds to mitigate risks according to your priorities – **Deter, Detect, Delay and Deny**.
- Measures to achieve the 4Ds come in the form of operations, technology and physical measures.

**HOW TO IMPLEMENT
PROTECTIVE SECURITY
MEASURES**



DETER

Prevent an attack by making it clear to an attacker that he is likely to fail. This includes having visible physical measures, presence of security officers and prominent signages that the premises are protected.



DETECT

Have ways to identify threats early and raise an alert. This include looking out for potential attackers conducting reconnaissance or suspicious persons loitering. Threats can be detected by measures such as CCTV systems, intrusion detection systems, and bag and person checks.



DELAY

Create obstacles that can slow down attackers to allow more time to carry out contingency plans. Examples include forced-entry resistant doors, doors with electro-magnetic locks, physical barriers, or bollards to delay vehicles.



DENY

Ensure that only authorised persons can access important areas such as the Fire Command Centre, Air Handling Units, safe rooms for hiding from an attacker, and other areas containing critical assets. Access control measures include biometric or card access, lock and key, and security clearance policies that allow you to differentiate staff and visitors.

For more information on developing contingency response plans, see our 'Contingency Planning Advisory for Premises'.



**EXAMPLES OF MEASURES
TO REDUCE SECURITY RISKS**



OPERATIONS MEASURES

- Limit access to floor plans and documents containing sensitive security information.
- Implement security checks at entry points to deter and detect potential attackers and their weapons.
- Develop and exercise a building lock-down protocol.
- Have strict access control measures into protected areas such as staff passes with biometric features, visitor escort, and card access.
- Prepare the security team through relevant courses (e.g. Workforce Skills Qualifications Courses). Ensure that they are licensed to conduct checks on persons, vehicles and belongings.
- Ensure security officers and staff are trained to recognise suspicious behaviour/items and to report them.
- Have in place clear incident reporting procedures.



TECHNOLOGY MEASURES

- Have adequate CCTV coverage of the building in line with the Video Surveillance Systems (VSS) standards. Supplement CCTV with data analytic features where possible. The VSS standards can be found on the Police website at the following:
URL: http://police.gov.sg/img/advisories/misc/vss_standard_for_buildings.pdf
- Ensure security systems are maintained and operating effectively.
- Install alarm systems.
- Consider where feasible, having the capability to centrally lock down the different areas of the premises from the Fire Command Centre (FCC). This is to delay the advancement of the perpetrator(s).



PHYSICAL MEASURES

- Adopt visible security measures, such as regular patrols by security officers around the perimeter of the building, and put in place warning signs.
- Have a clear line of demarcation between vehicular and pedestrian access so as to prevent vehicle ramming attacks into areas of mass congregation. This may include the installation of bollards and planters to slow down a hostile vehicle should it attempt to attack pedestrians.
- Have pre-identified rooms, preferably hardened, where employees can hide during an attack should evacuation becomes impossible.



**SINGAPORE
POLICE FORCE**