

Conducting Table Top Exercises:

Guide, Scenario, and Inject Keys For Facilitators

Exercise Scenarios: Terror Attack at Workplaces



**SINGAPORE
POLICE FORCE**



**MINISTRY OF
MANPOWER**

INTRODUCTION

The table-top exercise (TTX) guide was jointly produced by Singapore Police Force (SPF) and Ministry of Manpower (MOM) to allow all workplaces, regardless of size, to conduct a TTX.

Facilitators may adopt this guide to conduct a TTX with your workplace. Your workplace should have drafted a contingency plan or have a plan in place as the TTX aims to identify gaps in the plan. Going through the TTX with your staff would allow them to practice procedures they may have been trained in and evaluate if they require additional training or if the plan needs amendments. It is also a good lead up to a ground-deployment exercise, which would help validate your plans.

The pointers given in the guide may be utilized to guide discussion, but facilitators should bear in mind that the list of responses is not exhaustive and may differ due to the different considerations such as the nature of terrain, profile of building occupants, or existing processes in place. You may wish to consult your Neighbouring Police Centre (NPC) liaison while conducting the TTX. If there are any questions related to business continuity or recovery, you may wish to send your query to sgsecure_workplaces@mom.gov.sg.

OBJECTIVES

The objectives of the TTX should be to identify gaps in the current contingency plan in dealing with terror attacks. The following are some examples that can be adopted:

- a. Roles and responsibilities of all relevant personnel during an attack before Police arrival, and upon Police arrival
- b. Evacuation and lockdown procedures
- c. Communication protocol amongst various stakeholders and with emergency forces
- d. Link up procedures with Police
- e. Key information that would be useful for Police
- f. Staff accounting measures
- g. Business continuity and recovery processes

EXERCISE PARTICIPANTS

You may wish to consider conducting the TTX with the following participants. The list is not exhaustive and you are encouraged to include anyone you think may benefit from this TTX.

- a. Key appointment holders
 - Leadership
 - Facilities Management
 - Human Resources
 - Fire Safety Warden
 - Emergency Response Team
- b. Building Owner
 - Property Manager
 - Security Team
- c. Emergency Responders
 - Police
 - SCDF

Step by Step to Facilitating the Session

STEP	FACILITATOR'S ACTIVITY
PREP	<input type="checkbox"/> You are paired up in a team. Discuss among yourself: <ul style="list-style-type: none"> ○ Who should be the main facilitator ○ Who should take detailed notes for AAR to be submitted to Exercise Controller after the TTX ○ Who should be the Timekeeper
ONE	<input type="checkbox"/> Introduce yourself to the exercise participants <input type="checkbox"/> Have the exercise participants introduce themselves
TWO	<p>1. Conduct ice breaker, if required.</p> <p><i>Example of an icebreaker: Tell Us About Yourself - Pass around a bag of candy. Tell the participants to take as many as they want. Once all the participants have their candies, tell them that for each candy they took they have to say one thing about themselves. For instance, if a participant took 10 candies, he/she would have to say 10 things about himself/herself.</i></p>
THREE	<p>2. Explain to participants the following:</p> <ul style="list-style-type: none"> ○ They are participating in a simple TTX. There is no time pressure. They are here as a team to discuss their roles and responses during a terror attack. ○ Responses may differ due to different considerations, such as nature of terrain, profile of building occupants, or existing processes already in place. ○ Let them know that the TTX is meant raise issues, get them to review the way they conduct their emergency operations and help them develop or enhance their emergency plans, as well as think through their business continuity and recovery plans. The more issues they manage to surface, the more they can strengthen their business processes. ○ Although the exercise scenario is set in a fictional time and location, inform the participants that it is alright to talk about the incident from their own experiences or in the context of their workplace. ○ Exercise injects are crafted in a manner to encourage feedback and discussion among the participants. Exercise scenarios are also purposely crafted in a manner that reflect a real emergency.
FOUR	<p>3. Define objectives of the exercise, which aim to identify gaps in their current contingency plans in dealing with a terror attacks.</p>

STEP	FACILITATOR'S ACTIVITY
	<ul style="list-style-type: none"> ○ Define the roles and responsibilities of all relevant personnel during an attack before Police arrival, and upon Police arrival ○ Discuss evacuation and lockdown procedures ○ Communication protocols amongst the various stakeholders and with emergency forces ○ Business continuity and recovery processes
FIVE	<p>Begin the exercise by reading out the main points of the scenario presented earlier in the video/slides. Encourage recorders to take down the key points. Observe how the participants set themselves up to facilitate discussion.</p>
SIX	<p>Deliver the first inject and let the discussion evolve naturally amongst the participants. If necessary, get the discussion going by nudging the participants with non-leading questions, such as “what would you do in this situation?” Avoid yes or no questions. If there is silence for a long time, you can try to direct the question at an individual, preferably the leader. You can also refer to the Facilitator’s Notes to help jump start the discussion.</p> <p>Inform the participants of the time allocated to each inject (which is written as part of the inject).</p>
SEVEN	<p>Be sure to take detailed notes during the discussions.</p> <p>These notes should be submitted to the exercise organisers for evaluation and review as soon as possible.</p> <p>Leave at least 15 minutes for wrapping up and getting the teams prepared to present on the injects.</p>



Contingency Response:
What can you do before Police arrival?

GUNMEN SCENARIO

Opening Narrative, Scenario Development and Injects

Inject ONE (Approximately 30 minutes)

Opening Narrative

You are gathered at the [insert location] on [insert date and time] to discuss the appropriate course of action to take in response to an incident which occurred at [insert location] [insert date and time].

The salient facts of the incident are as follows:

- On [insert date and time] at [insert venue], a male and female subject enters Building Y and inform the staff that they are scheduled to see the CEO of Company X.
- The male subject rushes into the building lobby, brandishes a gun, and starts shooting at people

Issues to Address

1. What measures do you have in place to deter or detect the threat?
2. What would be the immediate response of the security officers and staff on duty?
3. What information should be given to the Police?
4. How do you communicate the information to your tenants? Is there a dedicated alarm or mode of communication to alert tenants to evacuate or lockdown?
5. Are staff aware of the evacuation routes or hiding places in the office? Are you able to tell staff promptly to avoid a certain area?
6. Are there staff who can render first aid if needed? Do they know when it is safe to do so?

Facilitator's Notes (Points to Consider)

1. The contingency plan should have a segment on dealing with such an incident. This inject serves to assess the response protocol in place to deal with the incident. Protective security measures can be implemented by the 4Ds, Deter, Detect, Delay and Deny, and may be in the form of Operations, Technology or Physical Measures. These measures are listed in Table 1 below.

Table 1. Protective Security Measures

Operations	Technology	Physical
<ul style="list-style-type: none"> • Limit access to floor plans and documents containing sensitive security information • Implement security checks at entry points • Develop and exercise building lockdown protocol • Have strict access control measures • Prepare the security team through relevant courses and ensure they are licensed to conduct checks • Ensure security officers and staff are trained to recognize suspicious behavior/items and report them • Have clear incident reporting procedures in place 	<ul style="list-style-type: none"> • Have adequate CCTV coverage of the building in line with the Video Surveillance System (VSS) standards • 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 would delay the advancement of perpetrators 	<ul style="list-style-type: none"> • 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 ass congregation. This may include installation of bollards and planters to slow down a hostile vehicle • Have pre-identified rooms, preferably hardened, where employees can hide during an attack should evacuation be impossible

You may refer to advisories on protective security and contingency planning for further information.

2. What would be the immediate response of security officers and staff in the vicinity?
 - a. The inject serves to assess if the staff know what to do in the event of an attack. In the event of a weapons attack, “Run, Hide, Tell”. Evacuate people and keep them as far away from the surrounding area and provide first-aid to casualties if possible.
3. What type of information should be given to Police?
 - a. **“T.E.L.L.”** framework
 - T** – Total number of attackers
 - E** – Equipment or weapons being carried
 - L** – Look of attackers
 - L** – Location of attackers (where they are now and moving towards)
 - b. Appoint someone to monitor the CCTV and track movement of the attackers if possible and provide updated information to the Police
4. The inject serves to assess if the premises have a communication plan in place to alert tenants if an attack has happened. To facilitate evacuation or dynamic lockdown and provide first-aid if necessary.
 - a. **Evacuation**
 - i. Who will decide if evacuation is needed?
 - ii. Are there appointed reps to facilitate evacuation?

- b. **Dynamic lockdown.** Dynamic lockdown is the ability to quickly restrict access and egress to a site or building (or part of) through physical measures in response to a threat, either external or internal.
 - i. How can you track where the attacker has moved to?
 - ii. Is this location safe for you to monitor the attacker?
 - iii. Are you able to manage access control of your premise from this location remotely, i.e. locking certain doors via the electro-magnetic door lock system?

 - c. **Communication**
 - i. Trigger alarm, preferably different from a fire alarm
 - ii. Inform tenants/staff of what happened through appointed reps/floor reps if any via pre-established channels such as WhatsApp groups
 - iii. Inform tenants of situation updates where applicable, such as which area is inaccessible
5. Workplaces can consider appropriate trainings (e.g. SGSecure) and drills so that staff would be familiarized with evacuation routes or hiding places in the buildings.

Inject TWO (Approximately 30 minutes)

Scenario Development

The following are developments prior to the incident:

- Police arrive at the location, but need to find a liaison from the building

Issues to Address

1. Who will be appointed the Liaison?
2. What are the link up procedures with the Police?
3. What key information should the building management/FCC have prepared in advance that would be useful for the Police? What key information should the Liaison know?
4. How do you track the movement of attackers?

Facilitator's Notes (Points to Consider)

1. The aim of this inject is to allow the participants to think through their actions which would aid the Police in times of an emergency. During an attack, it would be important for Police to link up with someone at the premises to have details on what is taking place on the ground during time of incident.
2. Is there a RV point for the liaison to link up with the Police?
3. Key information such as contingency plans, ground layout, floor plans, location of fire exits, EHA, CCTV, AED, fire hose locations, means of communication (e.g. walkie-talkie) should be readily available to be handed over to emergency forces if needed.
4. The location of the CCTVs in the premises should be mapped out so that the movement of attackers can be tracked via CCTV if possible and updated to the Police. Areas which are not covered by CCTV should also be mapped out.

Additional Injects (Approximately 20 minutes)

Scenario Development

An Improvised Explosive Device (IED) is planted and detonates minutes later. The perpetrators' whereabouts are unknown.

Issues to Address

1. What will be the response to this explosion?
2. Is there an assembly area? If there is an attack at the assembly area, what should be done?
3. How do you account for your staff?

Facilitator's Notes (Points to Consider)

1. Similar to the first inject, this serves to assess if there is any response protocol in place to deal with the incident. Refer to advisories on protective security and contingency planning for further information.
2. **Assembly Area**
 - a. The Assembly Area (AA) is vulnerable to secondary attacks. Building occupants running away from a terrorist attack should not assemble or be ushered to the AA as they could be exposed to further dangers. Do not use the AA in such cases.
 - b. If the building owner must use the AA, the building evacuation team should check that the AA is safe for use (e.g conducting a visual check for any threats) before ushering evacuees to the AA. The evacuees should also be alert and look out for any threat while they are at the AA. Should the evacuation team be unsure if the AA is safe for their use, they should not use it.
3. There are many ways of accounting for staff, and it need not be done via the AA. It may be via a virtual AA, where staff account for their safety via WhatsApp, Google Forms or mobile applications such as Microsoft Kaizala.

RESOURCES

1. Advisories on Protective Security and Contingency Planning
2. Guidelines on Enhancing Building Security (GEBSS)
3. You can consider explaining the 'SAFE' response to guide workplaces on what is required as part of Police incident response. The accompanying table summarizes key actions workplaces can take during an attack.

Make **Sense** of what is happening – Use the **T.E.L.L** framework

Alert the police and everyone within your premises of the attack

Facilitate evacuation or implement dynamic lockdown to save lives

Establish links with SPF and SCDF to facilitate rescue operations and to check that all are safe

Facilitators' Guide for TTXs

Approach	Tenant	Premises owner
<p>Make Sense of what is happening – use the T.E.L.L framework</p>	<ul style="list-style-type: none"> • Run, Hide, Tell' in the event of an attack • Communicate with building security team to understand the situation and communicate situational updates • Constantly monitor communications channels such as Whatsapp group for latest update from the security team or building management 	<ul style="list-style-type: none"> • Proceed to FCC or safehouse where CCTV monitors are installed, only when safe • Appoint someone to monitor the CCTV and track movement of the attackers to provide updated information to the Police
<p>Alert the Police and everyone within your premises of the attack - use the T.E.L.L framework</p>	<ul style="list-style-type: none"> • Know what type of information to provide to emergency responders if they come across anything suspicious ('TELL') • Provide details about the attackers <ul style="list-style-type: none"> T – Total number of attackers E – Equipment or weapons being carried L – Look of attackers L – Location of attackers (where they are now and moving towards) 	<ul style="list-style-type: none"> • Trigger alarm (preferably different from fire alarm) • Inform tenants/staff of what has happened through appointed reps/floor reps • Communicate with appointed reps/floor reps through pre-established channels, such as Whatsapp Groups
<p>Facilitate evacuation or implement dynamic lockdown to save lives</p>	<ul style="list-style-type: none"> • Facilitate evacuation or dynamic lockdown or provide first-aid if necessary • Be familiar with evacuation route and places to hide in the office if they cannot run • Inform company employees (where applicable) of any situational updates, such as which exit is inaccessible 	<ul style="list-style-type: none"> • Check fire exits and ensure they are unlocked before police arrival if necessary, only when safe • Conduct security sweep of assembly areas for suspicious articles, e.g IEDs • Dynamic lockdown to restrict access and egress to a site or another part of the building if evacuation is not possible • Deny or restrict access to attackers by remote locking methods if available
<p>Establish links with SPF and SCDF to facilitate rescue operations and to check that all are safe</p>	<ul style="list-style-type: none"> • To update building security of latest headcount and report missing individuals 	<ul style="list-style-type: none"> • Ensure access to FCC or safehouse is secured and let Police access the area - <i>If someone requires access to FCC or safehouse, allow entry only if identity is confirmed and poses no safety risks to personnel within FCC or safe house</i> <ul style="list-style-type: none"> • Check that key information such as contingency plans, ground layout, floor plans, fire exits, EHA, CCTV, AED, fire hose locations and means of communication (e.g walkie talkie) is available and ready to hand over to police • Identify rendezvous point and liaison to link up with emergency forces • Facilitate emergency forces access to any areas of the building



**Business Continuity and
Recovery:**
MOM SGSecure for Workplaces injects

Inject ONE (Approximately 15 minutes)

Scenario Development

The following are developments to the incident:

Videos of the attack started to go viral on social media. Since then, several netizens started speculating the citizenship, race and religion of the attackers and made sweeping statements against them, causing tension and distrust in the community. Workers from the targeted community fear that they will be ostracised. A growing number of them did not turn up for work over the next few days.

What will be your course of action to address the tension, calm, unite your workforce and pre-empt public speculation?

Issues to Address

1. What are your crisis communications plans for internal and external audience?
2. How do you trigger plans to calm the ground and restore confidence?
3. Think about communications to the workforce who are
 - i. directly affected as they are onsite
 - ii. off shift or on leave (not at work) when the attack happened
4. Think about communications to
 - i. general public
 - ii. business partners (sub-contractors, suppliers, clients etc)

Facilitator's Notes (Points to Consider)

1. Work closely with the Police and other relevant agencies to provide feedback to aid in investigation and to gather accurate information.
2. Do not circulate any information/photos/videos onto social media, and that anyone with relevant information should submit it to the Police to facilitate investigations. Corporate Communications should also advise the public not to circulate the videos and assure them that they are working closely with authorities to assist those who are affected from the incident.
3. Direct any attack-related media queries to the Police.
4. Establish procedures to disseminate accurate information regularly and in a timely manner, to allay fears and quell rumours.
5. Verify authenticity of videos and work with the Police to inform the public what is being done to secure and keep occupants safe.
6. The company should remind all tenants/employees to refer questions by external parties to the building management Corporate Communications team. Ensure that

all tenants/employees are aware of the Corporate Communication team's contact details.

7. Leverage on existing easy-to-use technology such as mobile messenger applications to create group-based communication channels to share and gather information – make sure everyone is accounted for, and that they are aware and understand the instructions given to them.
8. Create a tenants/employees and next-of-kin call directory so that you can facilitate communication during crisis. Buildings are also encouraged to register an SGSecure rep with MOM at www.mom.gov.sg/sgsecure and have their tenants to each assign and register an SGSecure rep. Ensure that the information is regularly updated.
9. Make use of mobile messaging applications to create group-based communication channels, e.g Whatsapp group chats. However, companies should be cautious not to have too many group chats to avoid confusion. Ensure there is one official channel specifically dedicated for communications and assurance to all your employees.
10. Update tenants of the situation and provide a platform for them to voice their concerns.
11. Prepare a list of important stakeholders, such as key customers, suppliers and sub-contractors, and establish strong channels of communications with them.
12. Inform business stakeholders on situation, and measures taken by the building management to reduce impact, and if grace period is needed as the building management overcomes and recover from the crisis.

Inject TWO (Approximately 20 minutes)

Scenario Development

The following are developments to the incident:

The attack has adversely impacted the workforce sentiments. Employees are traumatised as they see the severe injuries sustained by their colleagues, and customers - some of whom are as young as 3 years old. Their workplace is ridden with bullet holes and blood was spilled over the equipment. Meanwhile, employees resting on their off days are worried and tried to call the company to find out more but could not get through.

Despite the initial rallying for employees to stay united and preserve harmony, there is still underlying uneasiness among employees. How are you going to manage your employees' sentiments and restore confidence in the workplace?

Issues to Address

1. How do you keep track of injured workers?
2. What are your plans to strengthen the workplace cohesion during peacetime and crisis and also address the issue of workplace discrimination and mistrust?
3. What could be done to focus on building the psychological resilience of your workforce?
4. What could you do to support the employees who are experiencing Post Traumatic Stress Disorder (PTSD)?

Facilitator's Notes (Points to Consider)

1. Ensure that there is a system in place to keep track of all the status of all tenants and employees.
2. Senior management to condemn the attack and update tenants/employees on measures taken to safeguard their wellbeing and safety; as well as to rally tenants/employees together and reiterate the importance of being united, staying alert and staying strong.
3. Establish HR guidelines in handling terror attack incidents, e.g to visit colleagues, or attend the funeral of a deceased colleague. The company is to assist the victim's families during this difficult time.
4. Provide feedback channels and develop grievance handling procedures.
5. Organize regular gatherings to strengthen bonding and to build an inclusive and harmonious working environment.

6. Organize activities to help tenants identify each other's similarities during orientation or team building sessions, to build neighbourliness.
7. Allow flexible work arrangements to minimize disruptions to business. *(NA for building management/tenants)*
8. Identify a team of responders comprising of employees who are equipped with lifesaving and other relevant skills that can minimise damage and loss during and in the immediate aftermath of crises
 - Identify a group among your tenants to be equipped with fire-fighting, CPF-AED, and First Aid training. Building management can also train a group of employees/tenants with Psychological First Aid skills so they can help others cope with difficult situations.

Inject THREE (Approximately 20 minutes)

Scenario Development

The following are developments to the incident:

The attack has disrupted your business operations. One of your worksites is affected, and you are unable to access your work location. That is also where all your critical systems and data are stored. This will affect not only your internal operations, but also affect the services which you are supposed to deliver to your customers. How will you restore business functions and ensure business continuity?

Issues to Address

1. Have you done a risk assessment on the security risks and put in place measures to mitigate the risks? Does your tenants also understand the risks and are able to mitigate them?
2. Activate your business continuity plans (BCP). Do you have a BCP in place?
3. Does the BCP affects your tenants? How can you align the BCP with your tenants' plans?
4. How do you ensure your BCPs remain relevant?
5. What could be done to reduce the impact of the business disruption?
 - How do you ensure your data are not lost?
 - How do you regain the confidence of your tenants and customers to return to your premise again?

Facilitator's Notes (Points to Consider)

1. Perform risk assessment and business impact analysis for different crisis scenarios, and consider the control measures that would reduce the impact, to enable your organization to continue, recover and resume critical prioritised business activities with acceptable time frames.
2. Sign up for Workplace Safety and Health Council's bizSAFE programme to improve your workplace's safety, health and security capabilities. SGSecure content has been incorporated into bizSAFE levels 1-3 to help companies better assess and manage security risks at your workplace.
 - Encourage your tenants to sign up for the bizSAFE programme.
3. Annually review, evaluate and update your BCPs, including implementation of continual improvements.

4. Regularly conduct BCP exercises, and surprise security exercises to test vigilance levels, and feedback performance to tenants/employees.
5. Hold annual training and awareness activities to reinforce tenants' understanding of their roles, responsibilities and accountabilities as part of your BCP.
6. Identify your critical functions, and ensure that you have supporting resources to ensure swift resumption of functions.
 - Building management should keep a list of contractors to ensure adequate facilities support in the aftermath
 - Further strengthen building security in the aftermath
7. Safeguard your data by performing periodic backups on a secure platform.
8. Ensure that alternative work arrangements, if applicable. e.g work from home, are in place so that business operations can continue.
9. Consider having alternate worksites arrangements, if applicable.
10. Building management and building tenants can consider joining the Singapore Police Force (SPF)'s Corporate First Responder (CFR) Scheme to gain access into restricted cordoned area post-incident when safety permits, even while rescue, recovery and post-incident investigation activities are ongoing, to enable businesses to sustain essential business functions and take mitigation measures that will help maintain the businesses' viability after the incident.

Inject FOUR (Approximately 20 minutes)

Scenario Development

The following are developments to the incident:

The attack has disrupted your business partner, who supplies you with one of the components required for operations. You have no more stock of the required component in your warehouses, and this will affect your daily operations and the services which you are supposed to deliver to your customers. How will you restore business functions and ensure business continuity?

Issues to Address

1. Have you done a risk assessment on the security risks and put in place measures to mitigate the risks? Look at your current supply chain. Do you have an alternative supplier to minimize disruption to your supply chain?
2. Activate your business continuity plans (BCP). Do you have a BCP in place for this situation?
3. How do you ensure your BCPs remain relevant?
4. What could be done to reduce the impact of the business disruption?
 - How do you regain the confidence of your tenants and customers to ensure minimal disruption to your business?

Facilitator's Notes (Points to Consider)

1. Perform risk assessment and business impact analysis for different crisis scenarios, and consider the control measures that would reduce the impact, to enable your organization to continue, recover and resume critical prioritised business activities with acceptable time frames.
2. Make a list of your important stakeholders, such as key customers and suppliers, and establish strong channels of communication with them.
3. Prepare a list of potential business partners who can support our business operations in the event that current ones are affected by crisis, to reduce your disruptions to the minimum.

RESOURCES

1. SGSecure Guide for Workplaces
www.mom.gov.sg/sgsecure
2. Contingency Planning and Protective Security Advisories for Premises
www.police.gov.sg/cppsa