A guide to cyber exercises

plan + conduct + evaluate

VICTORIA State Government
Premier and Cabinet

Contents

Cyber exercise guide

Purpose

This guide provides Victorian Government organisations with advice on how to create and run an effective cyber exercise.

The Victorian Government Cyber Incident Response Service and the Victorian Government Cyber Incident Management Plan recommends that Victoria's public sector bodies undertake an annual cyber exercise to improve their incident response capabilities.

Audience

This guide should be used by information technology (IT) security managers and cyber security leads across the Victorian Government.

Members of the public and business organisations may also benefit from the advice contained in this guide.

Before using the guide

There are several steps you should take before using this guide:

- Develop a cyber incident response plan and establish a cyber incident response team to lead your organisation's response to cyber incidents.
- Think about the types of cyber security risks that your organisation manages – for example, risks associated with phishing, ransomware, malware, denial of service and data breaches.
- Get support from your executive leadership group to conduct a cyber exercise via your incident response team, with a focus on your organisation's cyber security risks.

Need help using the guide?

If you need any help using this guide, contact the Victorian Government Cyber Incident Response Service at cybersecurity@dpc.vic.gov.au.

You can also find more information online at Cyber Security in the Victorian Government.

Plan, conduct and evaluate

The following section outlines how to plan, conduct and evaluate a cyber exercise.

Get support from your executive leadership group

All organisations that draw on digital information, systems and services should be prepared to respond to a cyber incident. It is no longer a case of ‘if’ but ‘when’ an incident will occur.

Have a conversation with your executive leadership group about your organisation’s cyber security risks and capabilities.

Seek support from your executive leadership group to conduct a cyber exercise to help your organisation practice and improve its response to cyber incidents.

Form an exercise planning team

A cyber exercise requires a planning team to coordinate its format, content, conduct, logistics and evaluation. The Planning Team should ensure that exercises are relevant, realistic, achievable, align with your operating environment and meet the exercise need, aim and objectives. The Planning Team should oversee and finalise most of the following activities.

Identify the exercise need

The cyber exercise Planning Team should begin by identifying and confirming why your organisation needs to conduct an exercise. This need may be influenced by:

- emerging cyber security threats and trends
- changes in staff or team members (particularly those working in IT or cyber security)
- changes to policy, operating procedures or equipment
- workforce learning and development, particularly for cyber security best practice
- legislative or regulatory requirements.

Define the exercise scope

The exercise scope defines the boundaries of a cyber exercise and its content. The scope comprises the processes (i.e. your cyber incident response plan and other relevant processes) to be included, as well as the processes not to be included.

The exercise scope should list:

- the processes that participants can use and refer to during the exercise (e.g. incident response plans, procedures, policies, regulations, legislation etc.)
- if appropriate, the processes not in scope for the exercise (to prevent irrelevant or distracting exercise activity from taking place).

Define your aim and objectives

Although the exercise aim and objectives might seem very similar, they influence different parts of a cyber exercise (see below for examples).

There is only one aim for an exercise, which is a high-level statement that describes an exercise's intended outcome. Your aim will be informed by your exercise need.

There can be multiple objectives for an exercise. Objectives flow from the aim and cover the specific tasks and achievements intended for exercise participants.

The aim and objectives should be realistic and facilitate the evaluation of an exercise by including only outcomes that can be quantified and measured.

Features of a good aim and objectives

There are three features that make a good aim and objectives. These are:

1. an **action** the exercise must undertake, such as 'practice' or an equivalent action
2. the **process** to be actioned, such as an 'incident response plan'
3. if appropriate, the hypothetical **context** in which the exercise occurs.

In addition to 'practice', the following actions are recommended for an aim and the objectives:

- validate
- explore
- develop
- assess
- test
- review.

In addition to a cyber incident response plan, the following processes are often practiced etc. during a cyber exercise:

- policy, procedures and arrangements
- contracts and agreements
- roles and responsibilities
- specialist response actions and tasks.

Examples of an aim (① action, ② process, ③ context):

- To ①practice the Agency X ②cyber incident response plan due to a ③significant cyber incident affecting the state government.
- To ①validate the ②Memorandum of Understanding for cooperation between Agency X and Agency Y when ③responding to a cyber emergency.
- To ①explore ②response procedures for a ③cyber incident that impacts critical communications infrastructure in this state.

Examples of objectives (① action, ② process, ③ context):

- ①Assess ②policies for managing outages when ③emergency services communications are disrupted by a cyber incident.
- ①Test the ②intelligence sharing procedures between Agency X and Agency Y when ③responding to cyber incidents.
- ①Practice carrying out ②communications roles in response to a ③significant cyber incident that receives widespread public and media attention.

Choose the exercise format

Cyber exercises most often use formats that have participants:

- discuss responding to a hypothetical cyber incident, or
- operationally respond to a simulated cyber incident.

The two most common exercise formats are:

Discussion Exercise – asks participants to discuss a hypothetical cyber incident and nominate approaches for its remediation and recovery, with reference to incident response plans and other processes. Also known as a ‘tabletop exercise’, this format enables in-depth and considered discussion to produce decisions that may not be arrived at, or have not yet been experienced, under the pressure of real-world events. A Discussion Exercise is led by an Exercise Facilitator and may require up to 2-3 months of planning. It is recommended that organisations undertaking their first cyber exercise begin with a Discussion Exercise format.

Functional Exercise – will take place in a simulated operational environment in which participants perform the specific roles and functions in a cyber incident response plan and other processes. This format enables an organisation to test its equipment, hardware, software and communications skill-sets when responding to a cyber incident. The practical components of a functional exercise can include:

- conducting analysis of incident events and impacts
- producing intelligence advice and delivering verbal briefings
- preparing media statements and responses to media enquiries.

A Functional Exercise is led by a Control Team and may require several months of planning due to its logistical scale and complexity.

Design exercise scenarios

The cyber exercise scenario is the story or case-study through which a hypothetical cyber incident is introduced to exercise participants. Select a cyber threat or hazard that is relevant to your organisation and make sure that it aligns with the exercise aim and objectives.

The scenario should only be revealed to participants on the day of the exercise in order to provoke deliberations and/or actions in real-time. The scenario should be:

- connected to the aim and objectives and help keep these achievable
- realistic and relevant to the current operating environment
- within the agreed scope of the exercise.

Introduce exercise scenarios

A cyber exercise scenario should be designed to be introduced in stages. The amount of information provided to participants is at the discretion of the exercise Planning Team, but a typical exercise scenario will be divided into the following:

General Idea – is a broad introduction to the topics or themes of the exercise and how they are applicable to the participants and their current operating environment. The General Idea may be given to participants in advance of the exercise, but should not contain any description of the exercise's cyber incident.

Special Ideas – are also known as 'injects' and describe your exercise's hypothetical cyber incident, including the events and impacts before, during and after the incident occurs. The complete scenario should be divided into multiple (up to 3-4) chronological Special Ideas so it is introduced in stages and events can escalate as they might in the real world.

Appoint an exercise facilitator

A facilitator usually leads a discussion exercise. The facilitator reveals the cyber exercise scenario to participants by introducing, at intervals, the Special Ideas to inform discussion of how the incident might be approached and resolved in the real world.

A facilitator usually introduces the Special Ideas through a written narrative, including with multimedia aides where desired.

A facilitator should:

- follow a script but be flexible and responsive to the discussion
- maintain the flow of discussion, pose questions and keep to agreed time limits
- manage group dynamics and summarise participant contributions.

Appoint an exercise control team

A Control Team usually leads a functional exercise. The Control Team deploys, at intervals, exercise effects and impacts to simulate the real world and introduces context to the cyber exercise scenario through Special Ideas and other information as appropriate.

A Control Team may use a variety of technical or multimedia aides to introduce the Special Ideas through mock broadcast media, social media posts, scripted phone calls and any other technical effects or controlled consequences that are feasible with available resources.

A Control Team should:

- follow a script to initiate predetermined effects and impacts in a timely manner
- cause participants to engage in the roles and responsibilities to be practiced or reviewed etc.
- be capable of overseeing a large body of participants exercising in multiple locations.

Conduct the exercise

The next step is to conduct your cyber exercise. Please consider:

- **Exercise duration** – allow enough time for the exercise to cover the aim, objectives, Special Ideas and a hot debrief. The typical discussion exercise can occur over approximately three hours and a functional exercise will take at least the same amount of time or can progress over a full day or multiple days.
- **Exercise location** – find a location with enough space for participant activities and for your exercise facilitators, controllers or evaluators to oversee proceedings. The location should also accommodate supplementary materials, equipment and multimedia during the exercise conduct.
- **Number of participants** – the number of participants involved in your exercise should reflect your aim and objectives and the variety of staff and skillsets suitable to fulfil these. You may also invite observers or evaluators to watch the exercise who have no (or limited) active participation.

Evaluate the exercise

The cyber exercise Planning Team should decide how to evaluate the exercise against the aim and objectives. This involves the collection of data on the exercise conduct, analysis of this data and a record of key findings. The evaluation may be undertaken internally by your own organisation or professional evaluators can be engaged.

It is recommended that an evaluation is informed by:

- scribes capturing outcomes during the exercise
- participant evaluation forms
- a hot debrief post exercise to capture participant insights and impressions.

The evaluation should be recorded in a report and shared with all participants. Participants should incorporate the key findings and any recommendations into incident response plans or other processes.

Exercise documentation and supplementary materials

At the discretion of the cyber exercise Planning Team, and depending on the scale of your exercise, the following documents and supplementary materials may be useful:

Concept Document – is for the Planning Team and managers or those with the authority for approving an exercise. A Concept Document outlines the need, aim, objectives and all content, logistical and participant aspects of an exercise. Further, this document will also outline expected budget available and any risk management issues.

Participant Handbook – serves as joining instructions for exercise participants and includes the exercise location/s, timings, aim, objectives and General Idea and/or general background information. No detail on the exercise scenario or Special Ideas should be in the Participant Handbook, which can be distributed to participants in advance of the exercise.

Facilitator Handbook – is for a discussion exercise facilitator. This is identical to the Participant Handbook and, in addition, will contain the exercise scenario, timings for the introduction of the Special Ideas and questions, discussion prompts and notes etc. for the facilitator to employ with the exercise participants. The Facilitator Handbook may help to brief your facilitator prior to the exercise.

Control Handbook – is for the Control Team of a functional exercise. This will show the exercise controllers the flow of exercise events and timings for deploying exercise effects and simulations. Depending on the complexity of a functional exercise, a Control Handbook may contain a detailed running sheet for all exercise locations and instructions to ensure events and activities are coordinated centrally by Control Team members.

After Action Report – is a report on the conduct of your exercise, depending on how formally you want to record your evaluation and findings. This style of report usually contains an executive summary, an assessment on whether the aim and objectives were met and a description of the key findings.

Multimedia presentations, digital displays or hardcopy handouts – can communicate your Special Ideas as well as any other exercise content, messages, scheduling or ground rules to your participants.