



# Instructions

## Exercise in a Box (EiaB)

First published: May 2025

Duration: 90 to 120 minutes

## Discussion-based exercise

### Managing a vulnerability disclosure

**Context:** A discussion-based cyber security exercise, often called a tabletop exercise, is a simulated, non-physical event where participants discuss a hypothetical cyber incident and their organisation's response. It focuses on communication, decision-making, and role clarity without any actual systems being impacted.

**Goal:** Understand best practice for managing and responding to a vulnerability disclosure on one of your online systems.

- This scenario assumes that your organisation has a public-facing system or application, such as a website where customers or users log in.
- This scenario covers the events following the disclosure of a vulnerability in a public facing web application run by your organisation. It includes:
  - managing communication between your organisation and a person reporting a vulnerability
  - the process of responding to a vulnerability disclosure
  - mitigating further problems by implementing an effective vulnerability disclosure process.
- Discussion of the above topics will help you explore your organisation's current approach to vulnerability disclosure.
- It is recommended that you have a technical representative in the group taking part, with appreciation of vulnerability disclosure guidance such as that in the UK's National Cyber Security Centre (NCSC) [Vulnerability Disclosure Toolkit](#).

### Essential attendees

- Senior decision maker – someone who can make important decisions for your business.
- Senior IT stakeholder/decision maker – someone who has overall responsibility for your IT landscape.
- Technical IT security adviser – someone who can provide advice on how you operate technically with awareness of vulnerability disclosure practice.

## Desirable attendees

- Media/press/comms representative – someone who would manage your internal/external communications during an incident if needed.
- Company policy adviser – someone who has oversight of your company policies, such as HR and business continuity.
- Scribe – someone to take notes during the exercise delivery.

## Exercise pack contents

Exercise in a Box	
<b>Exercise presentation</b>	Your primary aid for delivering this exercise. You could use printed copies, but it is recommended you display this on a projector or share on your screen if running the exercise virtually.
<b>Scribe sheet</b>	For a notetaker/scribe to capture observations during each injection and key discussions from participants. These notes will assist in the preparation of the exercise report after completing the exercise.
<b>Exercise report</b>	To capture lessons learned and opportunities for improvement. Ideally share this report with your leadership team for their awareness and/or utilise it as part of a business case if requesting support for remediation activities.

## Next steps

We recommend that you familiarise yourself with the exercise by performing a dry run (practice session) prior to arranging to run the exercise with participants.

### Checklist

- ☐ I have identified participants and a scribe to take part in the exercise.
- ☐ I have organised a room in which to hold the exercise with internet access.
- ☐ I have confirmed we will be able to put exercise material on a screen or projector.

## ACSC cyber security resources

- [Small business cyber security guide](#) – a cyber security guide for small businesses
- [Essential Eight](#) – essential Windows cyber mitigation strategies
- [Information security manual \(ISM\)](#) – technical cyber security framework
- [Strategies to mitigate cyber security incidents](#) – advice on mitigating cyber security incidents
- [Personal security guides](#) – a series of guides to use to protect yourself and be cyber secure.

Additional information is available from [cyber.gov.au](https://www.cyber.gov.au) and you can [contact us](#) for assistance.

## Frequently asked questions (FAQ)

### How many people should attend an exercise?

The ideal size will vary between organisations, but we recommend between 5 and 10 participants. Consider who is required, and whether individuals attending or not attending will make the exercise more difficult to run. Too few participants may mean you're not representing the entire organisation; too many and it becomes difficult to moderate, with the risk of overly long discussions.

### Do participants have to attend the whole of an exercise?

Not necessarily. If you think it's worth somebody attending for part of an exercise, consider asking them to contribute by phone, or ask them to work nearby so they can be called upon when needed.

### Where should I run the exercise?

Best run in a dedicated space, so we recommend you use a normal meeting room, or somewhere further afield with fewer distractions. You'll also have to consider which participants need to attend, and when.

### What materials do I need to run the exercise?

At various points during the exercises, you'll need to share your screen so that the participants can take part. So in addition to a laptop/computer with access to the internet, you'll need: A projector, whiteboards or flipcharts with marker pens, printouts from the exercise packs and refreshments for your participants so they stay comfortable and productive.

### How is the exercise structured?

Exercises start by introducing an event, which could be (for example) 'your organisation's IT is being attacked'. In exercising jargon, these events are known as 'injects'. The exercise continues by asking a set of questions relating to the inject. EiaB does not require you to enter a simple answer to these questions; they are intentionally worded to solicit discussion. Often there is no simple answer.

### How should I record the discussions?

The exercise pack includes scribe sheets for you to make notes as you go along. In addition, you might want to use a recording device to make sure that you don't miss any contributions (there are numerous voice recording apps available on modern smartphones). The group discussion questions at the end of each exercise are a further opportunity for participants to reflect and review the discussions.

## **What happens when the exercise is complete?**

When you've finished an exercise, we strongly recommend that you complete the associated report to ensure that the exercise is a learning experience with useful outcomes.

## **Do participants have to be present to produce the report?**

No. The reporting section can be completed by the facilitator alone, or with the help of the participants. The most important thing is that it's completed within a couple of days of the exercise, while the exercise is still fresh in the mind.

## **How can I use the report to improve cyber security in my organisation?**

The exercise report should allow you to prioritise the actions your organisation should take. For minor issues relating to a specific IT system, actions could be assigned to that system's manager. More serious issues (that is, issues that present an unacceptable risk to your organisation) should be escalated to an appropriate risk owner or responsible person in your organisation. This may vary in your organisation, and could be a director, company owner or senior IT manager/officer.