

After Action Report

[Exercise Name]

**Prepared by**

**Sun Chaser Cyber**

Purpose and use: This document summarises the observations, learnings, risks and opportunities for improvement identified during the exercise. This artefact can be used in a multitude of ways depending on your organisational requirements, e.g. be provided to senior executives following the exercise, be provided to participants following the exercise, used to identify and drive uplift activities, used to support business cases and funding requests, used as evidence for compliance requirements, etc.

Document information

**Handling instructions**

[Preamble on document sensitivity – e.g. *This document contains information that is for EXERCISE USE ONLY and NOT FOR PUBLIC DISTRIBUTION. Members are requested to protect this document from public distribution. The information in this After Action Report is intended for the exclusive use of this exercise*.]

**Document approval**

The [tabletop exercise] after action report has been approved by

|  |  |  |
| --- | --- | --- |
| Name | Role | Date |
|  |  |  |

**Contact information**

Enquiries in relation to any aspect of [tabletop exercise] including this document should be directed in the first instance to

|  |  |  |
| --- | --- | --- |
| Name | Role | Email |
|  |  |  |

Table of Contents

[1. Executive Summary 1](#_Toc166146411)

[2. Exercise Summary 2](#_Toc166146412)

[2.1. Exercise details 2](#_Toc166146413)

[2.2. Exercise need 2](#_Toc166146414)

[Exercise aim and objectives 2](#_Toc166146415)

[Exercise scope 2](#_Toc166146416)

[3. Key insights and treatment options 3](#_Toc166146417)

[3.1. Insights from injects 3](#_Toc166146418)

[3.1.1. Inject 1 insights 3](#_Toc166146419)

[3.1.2. Inject 2 insights 3](#_Toc166146420)

[3.1.3. Inject X insights 3](#_Toc166146421)

[3.2. Key themes of insights 3](#_Toc166146422)

[3.3. Treatments 3](#_Toc166146423)

[3.4. Follow-up actions 4](#_Toc166146424)

[Appendix A 5](#_Toc166146425)

# Executive summary

* Provide context on the exercise:
	+ What is a tabletop?
	+ When and where was it held?
	+ Who participated?
	+ What was the aim and objectives?
	+ What was in scope?
* Summarise key insights gleaned from the exercise.

# Exercise summary

## Exercise details

* Note the date, time, and location of the exercise.
* Note the exercise participants and their composition.

|  |  |  |
| --- | --- | --- |
| Role | Name | Position |
| Facilitator |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Observer |  |  |
| Observer |  |  |

## Exercise need

* Note the exercise’s need and purpose – this section can be an opportunity to highlight the importance of cyber security as a business function.
* You may like to highlight that your organisation has many policies, procedures and plans to detect, respond, and recover from a cyber security incident – and tabletop exercises provide an opportunity to validate these and promote continuous improvement.

## Exercise aim and objectives

* List aim and objectives.

## Exercise scope

Define broad scope, then detail at high level each inject. E.g.

*[Team] and boarder organisational incident management plans and procedures were within scope of the tabletop exercise.*

*The exercise included [x number] special ideas, which were injected and discussed throughout the time period. These included:*

* *[List injects]*

# Key insights and treatment options

## Insights from injects

### Inject 1 insights

* Note the key insights observed through discussion around inject 2.

### Inject 2 insights

* Note the key insights observed through discussion around inject 2.

### Inject X insights

* Note the key insights observed through discussion around inject X. Repeat this section for all injects.

## Key themes of insights

* Group together and summarise the key themes of insights.

## Treatments

* Summarise suggested treatment options to address any gaps / opportunities for improvement.

## Follow-up actions

*In addition to the treatments outlined in the section above, the exercise may have produced actions for immediate follow up or confirmation. They can be outlined in the table below.*

|  |  |  |  |
| --- | --- | --- | --- |
| Follow-up action | Description | Expected Timeframe | Responsible |
| [Summarise action] | [Describe action] | [Timeframe for completion] | [Person responsible] |
|  |  |  |  |
|  |  |  |  |

# Appendix A

[Include any relevant appendices, such as planning documents or observer evaluations]