Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

# Enhanced Cyber Security Obligations – Cyber Security Exercise

Part 2C Division 3 *Security of Critical Infrastructure Act 2018*
Guidance

Contact us

Enquiries regarding the licence and any use of this document are welcome to sons@homeaffairs.gov.au, or:

Systems of National Significance Branch,
Department of Home Affairs
PO Box 25, BELCONNEN, ACT 2616

# Contents

# Preface

This guidance has been prepared to assist responsible entities for Systems of National Significance to comply with the Cyber Security Exercise Enhanced Cyber Security Obligation as part of the *Security of Critical Infrastructure Act 2018 (SOCI Act)*.

# Systems of National Significance

Systems of National Significance (SoNS) are Australia's most important critical infrastructure assets by virtue of their interdependencies across sectors and the potential for cascading consequences to other critical infrastructure assets and sectors if disrupted. The power to declare an asset a SoNS is held by the Minister for Home Affairs.

Under the SOCI Act, SoNS may be subject to one or more Enhanced Cyber Security Obligations (ECSOs). The ECSOs have been designed to give Australians confidence that critical infrastructure entities have well-tested plans in place to respond to and mitigate against a cyber attack. Over time, the ECSOs will support the sharing of near-real time threat information to provide industry and Government with a more mature understanding of emerging cyber security threats and the capability to reduce the risks of a significant cyber attack.

In addition to the ECSOs, SoNS remain subject to all obligations that applied to that critical infrastructure asset under the SOCI Act before it was declared a SoNS.

This document provides guidance to SoNS entities required to implement and comply with the Cyber Security Exercise obligation, to ensure that our most important critical infrastructure assets are protected from those that wish to do us harm.

## Enhanced Cyber Security Obligations

The ECSOs are outlined in Part 2C of the SOCI Act. Each obligation is separate and is individually applied to an asset.

The ECSOs include:

- developing cyber security incident response plans to prepare for a cyber security incident;
- undertaking cyber security exercises to build cyber preparedness;
- undertaking vulnerability assessments to identify vulnerabilities for remediation; and
- providing system information to develop and maintain a near-real time threat picture.

# What is a cyber security exercise?

A cyber security exercise tests an entity's ability and preparedness to respond to cyber security incidents, as well as mitigate those impacts. Ultimately, an exercise is designed to reveal whether the existing resources, processes and capabilities of an entity sufficiently safeguard the system from being impacted by a cyber security incident. Working through the reality of what needs to happen when responding to a cyber attack is a vital element of an entity's cyber preparedness and maturity.

Exercises can be conducted in different formats designed to achieve different outcomes and test different capabilities. They may include:

- discussion-based or table-top exercises, where teams or individuals talk through how they would respond to an incident and explore issues that might arise during an incident; or
- operational or functional exercises, where teams or individuals perform their roles and responsibilities in implementing plans, processes, and procedures to respond to a simulated incident.

Regardless of the format, exercises should be followed by a de-brief with those who participated and an evaluation report which outlines what occurred during the exercise, what worked well, what did not work well, lessons learned, areas for improvement, and actions required. This report is essential for an exercise to be worthwhile.

# What are the Cyber Security Exercise obligations under the SOCI Act?

The Secretary of the Department of Home Affairs (or a delegate) may, by written notice, require a responsible entity for a SoNS to undertake a cyber security exercise within a certain timeframe to test the responsible entity's:

- ability to respond appropriately to one or more incidents that could have a relevant impact on the system;
- preparedness to respond appropriately to one or more incidents that could have a relevant impact on the system; and
- ability to mitigate the relevant impacts that one or more incidents could have on the system.

Before giving a written notice, the Secretary must consult the responsible entity and consider the cost, reasonableness and proportionality of applying the obligation, as well as any other matter the Secretary considers relevant. This may include whether a similar or equal regulation already applies to the SoNS.

If the obligation is applied, the notice will specify whether the exercise should be in relation to all types of cyber security incidents or in relation to one or more specified types of cyber security incidents (sections 30CM(1) and 30CM(2) respectively).

In practice, a cyber security exercise in relation to all types of cyber security incidents will be used to test an entity's general cyber response preparedness, mitigation and response capabilities. In contrast, a cyber security exercise in relation to a specific incident will be used to test responsiveness, preparedness and mitigation capability in relation to a particular threat scenario, for example a ransomware attack. This requirement may be applied to certain SoNS where critical risks or threats have been identified within a specific sector or asset class.

The written notice will also specify the period within which the exercise must be undertaken. The period will not be earlier than 30 days from when the notice was given.

After completion of the exercise, the entity must provide a copy of an internal evaluation report of the exercise to the Secretary. The timeframe to provide the written report will be specified in the written notice. If the Secretary is of the view that an internal evaluation report has not been prepared, or has not been prepared appropriately, the Secretary may require the entity to appoint an external auditor to prepare an external evaluation report – the entity will be consulted prior to this requirement being enlivened.

To ensure the Government has visibility of the way the exercise is being conducted and the outcomes of the exercise, the notice may also require the responsible entity to allow one or more designated officers to attend and observe the exercise. A designated officer is an employee of either the Department of Home Affairs or the Australian Signals Directorate who has been appointed by the Secretary as a designated officer under the SOCI Act.

## Designated Officers

Designated Officers are employees of the Department of Home Affairs or the Australian Signals Directorate appointed by the Secretary to be a designated officer under the SOCI Act.

An entity may be required to involve designated officers during an exercise in the following ways:

- allow designated officers to observe the exercise;
- provide designated officers access to the premises for the purposing of observing the exercise;
- provide designated officers with reasonable assistance and facilities necessary for them to observe the exercise;
- allow designated officers to make such records as are reasonably necessary for the purposes of monitoring and compliance; and
- give those designated officers reasonable notice of when the exercise will begin.

Initially, the Department will not seek to require designated officers to observe an exercise, but would consider invitations by responsible entities on a voluntary basis.

## Evaluation Report

An evaluation report must be provided to the Secretary after the completion of an exercise. The timeframe in which the report must be provided will be specified in the written notice.

The purpose of the evaluation report is to provide an evaluation of the entity's preparedness and ability to respond appropriately to cyber security incidents, as well as their ability to mitigate the relevant impacts of cyber security incidents on their SoNS.

The evaluation document must be a written document. The Department has not prescribed any other requirements for what format an internal evaluation report should take or what information it should contain. However, to assist in completing this report we recommend including the following:

- provide a summary of the exercise and the scenario tested;
- explain how the exercise tested your incident response plan and who took part in the exercise;
- consider any strengths and weaknesses found when undertaking the cyber-security exercise, including for the incident response plan and future exercises; and
- corrective actions/treatment in relation to issues and areas for improvement.

An internal evaluation report can be completed by a third party on behalf of the entity. However the SoNS responsible entity remains responsible for meeting the requirements of the obligation.

The report should be provided via the Department's secure upload portal.

See page 7 for links to available templates and pages 10 – 15 for further guidance.

**Cyber Security Exercise**

**Reflect on the exercise**

**Evaluation Report**

# The Department's approach

## The initial approach to the Cyber Security Exercise obligation

The Department's initial approach to implementing the Cyber Security Exercise obligation is to ensure an entity's incident response plan is well-tested and evaluated on a regular basis. To achieve this, the Department will prioritise applying the obligation to SoNS responsible entities under section 30CM(1) of the SOCI Act, requiring entities to test their incident response arrangements through a cyber security exercise on an annual basis over a three year period.

For SoNS entities that became subject to this obligation in December 2023, the requirement is that the first exercise is completed by 31 December 2024, the second exercise by 31 December 2025 and the third exercise by 31 December 2026. Rules have not been made in relation to the Cyber Security Exercise obligation. This means entities are able to determine the format of the exercise and the cyber incidents they test.

The Department acknowledges that entities are best placed to run their own exercises relevant to their SoNS, their incident response plans and their organisational structures. For example, entities may choose to do one exercise per SoNS asset or one exercise that tests their incident response arrangements against multiple SoNS assets.

Following the completion of each annual exercise, an evaluation report must be completed and provided to the Secretary within 60 days of the exercise being completed (unless otherwise specified in the notice).

If an entity has more than one SoNS asset and plans to undertake multiple cyber security exercises throughout the year, there may be scope to provide a single overarching evaluation report that takes into account each of the exercises rather than one report per exercise. Entities in this position should contact sons@homeaffairs.gov.au to discuss their circumstances.

## Future application of the Cyber Security Exercise obligation

In the future, the Cyber Security Exercise obligation could be applied in a manner that requires responsible entities to participate in an exercise that:

- tests the entity's ability to mitigate the relevant impact of a cyber security incident;
- is applied in a targeted manner to certain SoNS in key sectors where cyber security incidents might require coordinated engagement with multiple government entities;
- involves the Department and other relevant agencies/regulators with oversight of the SoNS responsible entity, its assets, or its sector;
- involves other SoNS responsible entities within the same sector or from a range of sectors;
- focuses on developing an understanding of how government and industry would work collaboratively to respond to a cyber security incident;
- explores how various regulatory frameworks interact in order to obtain information about an incident and direct action to respond to the incident; or
- outlines specific requirements for the responsible entity's internal evaluation report.

Should this type of exercise be required, the Department will lead the planning, development and facilitation of the exercise. The Department will work with responsible entities to ensure appropriate confidentiality arrangements are in place for any confidential, sensitive and protected information.

Responsible entities would be required to participate in the exercise and develop an internal evaluation report.

Consultation would be undertaken with entities prior to applying the obligation in this manner. The timeframes and requirements of the exercise would be clearly set out in the notification.

## Templates

There is no requirement to use a specific template for the cyber securitiy exercise or the evaluation report. However, the following resources may be useful:

- The Australian Signals Directorate's Exercise in a Box
- The Cybersecurity and Infrastructure Security Agency's (United States Government) After Action Report template

## The Department's approach to regulatory compliance

The Cyber and Infrastructure Security Centre's Compliance and Enforcement Strategy (April 2022) outlines the Department's regulatory principles and approach.

In applying the Enhanced Cyber Security Obligations, our focus is on education and engagement with SoNS responsible entities, and ensuring all SoNS have in place well-tested plans for responding to cyber security incidents that could have a relevant impact on their systems.

# Applying the obligation
# What to expect: a step-by-step guide

The process to apply the Cyber Security Exercise obligation is similar to the SoNS declaration process, as the responsible entity must be consulted prior to the obligation being applied. A key difference is that the power to declare an asset a SoNS is held by the Minister, whereas the power to apply any one of the ECSOs is held by the Secretary (or a delegate).

**1 Consultation**

Responsible entities will receive written notification from the Department advising that the Secretary (or a delegate) is considering applying the Cyber Security Exercise obligation. This letter commences the consultation process and invites entities to provide a written submission. The Department will also consult any relevant Commonwealth regulators with functions relating to the security of the SoNS. During consultation, the Secretary will consider costs, reasonableness and proportionality of applying the obligation.

*Consultation timeframe* – there is no minimum timeframe for consultation under this provision within the SOCI Act. The Department will specify the timeframe in the consultation letter.

*Consultation form* – this will consist of town hall-style information sessions and one-on-one meetings. Entities can choose to provide a written submission.

**2 The obligation is applied**

Following the consultation process, the responsible entity will receive a written notice from the Secretary (or a delegate) advising whether or not the obligation has been applied. If it has been applied, the responsible entity will be required to undertake a cyber security exercise within the timeframe specified and taking into account any requirements specified in the notice.

*Requirements* – there are no requirements currently specified in rules for the format or type of exercise that must be undertaken. This means exercises can take any form as long as they test the entity's responsiveness, preparedness and mitigation capabilities in relation to cyber security incidents that may have a relevant impact on their SoNS.

*Timeframe* – the period specified in the notice must not be earlier than 30 days from when the notice is given. Entities that had this obligation applied in December 2023 are required to undertake a cyber security exercise on an annual basis over a three year period, with the first exercise to be undertaken by 31 December 2024, the second by 31 December 2025 and the third by 31 December 2026.

**3 Prepare and provide an internal evaluation report**

Once an entity undertakes a cyber security exercise, it will be required to provide a written evaluation report to the Secretary within the timeframe specified in the written notice. The report should evaluate the entity's preparedness, mitigation and response capabilities.

*Timeframe* – the SOCI Act provides that the entity prepare and give a copy of the evaluation report to the Secretary (or a delegate) within 30 days after the completion of the exercise (or longer if the Secretary allows). For entities that had this obligation applied in December 2023, the Secretary's delegate has extended this timeframe to 60 days.

*An 'adequate' report* – the evaluation report should outline the exercise that was undertaken and provide an evaluation of the entity's preparedness, mitigation and response capabilities in relation to cyber security incidents that may impact the SoNS.

# Protecting sensitive information

## What documentation do responsible entities need to provide?

The responsible entity is required to provide a copy of the written evaluation report to the Secretary (via the secure document portal). Entities may also wish to provide additional documents related to the exercise, including exercise planning documents and response plans or playbooks used in the exercise (although this isn't required).

## What will the Department do with an entity's evaluation report?

The Department will review evaluation reports to:

- determine if an exercise meets the requirements of the Cyber Security Exercise obligation as applied to the SoNS and as set out in the notice;
- understand the exercise maturity of SoNS responsible entities within certain sectors and across the SoNS cohort as a whole;
- understand the cyber response and preparedness capabilities of SoNS responsible entities, including whether their incident response plans are fit for purpose and can be operationalised;
- identify opportunities to support the uplift of cyber response and preparedness capabilities, as well as exercise capabilities of individual SoNS responsible entities;
- identify opportunities to undertake sector specific or cross sector exercises; or
- determine if the internal evaluation report has been appropriately prepared.

## How safe is the entity's information submitted via the secure portal?

Entities should provide their written evaluation report and any supporting documents via the Department's secure document portal.

The secure portal has been developed to ensure that sensitive information provided for the purpose of meeting obligations under the SOCI Act, such as incident response plans and related documents, is immediately safe-dropped from the website link to a classified systems location.

Thereafter, multiple layers of security protect the data. It is stored on the Department's SECRET system and within a restricted portal created solely for the purpose of storing information relating to the Enhanced Cyber Security Obligations.

Government employees with a minimum Negative Vetting 1 security clearance require a business need-to-know in order to access this information. This information must be handled carefully in accordance with the SECRET classification of the system, the protected information provisions under the SOCI Act, as well as with integrity and professional standards frameworks.

The Department's SECRET network and the Enhanced Cyber Security Obligations portal is managed by appropriately cleared Departmental staff. No third parties have access to the portal.

More broadly, we operate under the Protective Security Policy Framework (PSPF) which ensures that all information created, stored, processed, or transmitted in or over government information and communication technology systems is properly managed and protected throughout all phases of a systems life cycle.

# Cyber Security Exercises – What Good Looks Like

The below framework provides guidance to entities when planning, undertaking and evaluating a cyber security exercise.

## Overview

- Responsible entities are best placed to run their own exercises relevant to their SoNS, their incident response plans and their organisational structures.
- To support entities in the planning, running and evaluation of an exercise, the Department has developed the following framework which considers five key criteria.
- The Australian Signals Directorate and the U.S. Government's Cybersecurity and Infrastructure Security Agency also have a number of useful resources for planning, undertaking and evaluating cyber security exercises.

### Purpose of this section

It is important to note that this framework is not mandatory. It has been developed to support entities with their approach to continual incident response improvement.

## The Criteria

| Criterion code | Criterion name |
|---|---|
| **EX.1** | Alignment to responsible entity's cyber security strategy/policy/management framework |
| **EX.2** | Summary of scenario tested |
| **EX.3** | Assessment of ability to perform a cyber security exercise |
| **EX.4** | Contents of the cyber security exercise report |
| **EX.5** | Exercise report recommendations |
| **Criticality** | Each criteria includes sub criteria which has been designated a level of criticality: critical, high and medium. This criteria can be used to assist entities to prioritise certain components when developing and reviewing an incident response plan. |

## Criterion EX.1: Alignment to responsible entity's cyber security strategy/policy/management framework

### Outcome

The exercise should be aligned to the responsible entity's risk management program (RMP) (if Part 2A of the SOCI Act has been applied to the SoNS assets). If you are a responsible entity not subject to the risk management program, you might be subject to another similar regulatory regime that would achieve the same purpose. Aligning your exercise to other applicable risk mitigation frameworks ensures a holistic and proactive approach toward identifying, preventing and mitigating risks within a cyber-security exercise context.

Identifying the most likely tactics, techniques and procedures that will be used against a SoNS will allow defenders to undertake an exercise that is realistic, responding to the most likely and/or most impactful attack scenarios. The scenario should be broad and serious enough to demonstrate the ability of the responsible entity to implement all aspects of their incident response plan.

As part of developing an RMP, the responsible entity will identify the most critical components of their critical infrastructure assets. Identifying the most business-critical components will guide the defensive and remediation efforts within an incident response playbook. Given the importance of these systems to the SoNS and Australian society, it is expected that these would be included in any exercise. The exercise should be aligned to the organisation's wider cyber security RMP or a program similar to an RMP to ensure an accurate assessment of a responsible entity's cyber capability as well as provide the best training experience. An effective exercise should consider the most likely and/or most impactful attack scenarios.

### Considerations

| Consideration | Well Implemented | Partially Implemented | Not Apparent |
|---|---|---|---|
| Does the cyber security exercise scenario align to the most likely and/or most impactful threat scenario?<br>***(Critical)*** | The cyber security exercise scenario is closely aligned to the threats that the responsible entity faces, particularly the most likely and most impactful cyber attack scenarios.<br>*OR*<br>The scenario was issued by the Cyber and Infrastructure Security Group (CISG).<br><br>The exercise report outlines the alignment between the exercise and the most likely and/or most impactful threats faced by the responsible entity. | The cyber security exercise scenario is influenced by the threats that the responsible entity faces.<br>*OR*<br>The scenario was issued by the CISG.<br><br>The exercise report outlines the influence of the most likely and/or most impactful threats, faced by the responsible entity, on the exercise scenario. | There is no clear relationship between the threats faced by the responsible entity and the cyber security exercise. The responsible entity has disregarded more likely and more impactful scenarios in the development of the exercise.<br>*OR*<br>The scenario issued by the CISG was not used.<br>*OR*<br>The report does not attempt to demonstrate any alignment between the cyber security exercise scenario and the most likely and/or most impactful threats faced by the responsible entity. |
| Does the cyber security exercise adequately test key cyber security capabilities and the incident response plan?<br>***(High)*** | The cyber security exercise scenario adequately tests most key cyber security capabilities, and the implementation of all [material] aspects of the incident response plan (and playbooks). The scenario and report clearly demonstrate the ability of the responsible entity to fully implement their incident response plan in response to a significant cyber incident. | The cyber security exercise scenario tests some key cyber security capabilities, and most aspects of the incident response plan (and playbooks). The scenario and report demonstrate the ability of the responsible entity to implement some parts of their incident response plan in response to a significant cyber incident. | The cyber security exercise tests a limited number of key cyber security capabilities and some aspects of the incident response plan (and playbooks). The scenario and report do not demonstrate the ability of the responsible entity to effectively implement their incident response plan in response to a significant cyber incident. |

| Consideration | Well Implemented | Partially Implemented | Not Apparent |
|---|---|---|---|
| Does the exercise align to wider cyber security strategy and outcomes? ***(High)*** | The cyber security exercise outcomes align to the responsible entity's cyber security strategy or uplift outcomes. The assessment report describes this alignment. | The cyber security exercise outcomes partially align to the responsible entity's cyber security strategy or uplift outcomes. The assessment report describes this partial alignment. | The cyber security exercise outcomes do not align to the responsible entity's cyber security strategy or uplift outcomes.<br>*OR*<br>The assessment report does not describe the alignment of the Cyber Security Exercise policies and outcomes. |
| Does the exercise align to the security testing and assurance program? ***(Medium)*** | The cyber security exercise outcomes align to the overall security testing and assurance program.<br>The cyber security exercise report describes this alignment.<br>*OR*<br>The responsible entity does not have a security testing and assurance program. | The cyber security exercise outcomes partially align to the overall security testing and assurance program.<br>The cyber security exercise report describes this partial alignment. | There is no explicit alignment between the cyber security exercise outcomes and the overall security testing and assurance program.<br>*OR*<br>The cyber security exercise report does not describe the alignment between the cyber security exercise outcomes and the overall security testing and assurance program. |

## Criterion EX.2: Summary of scenario tested

### Outcome

The exercise evaluation report should include a detailed summary of the scenario that was tested, including what SoNS the scenario was tested against. The report should also include a summary of the outcomes and learnings from the exercise, including any lessons and provide options for future improvement of the exercise and incident response plan.

### Considerations

| Consideration | Well Implemented | Partially Implemented | Not Apparent |
|---|---|---|---|
| Does the exercise report include a summary of the scenario tested? ***(Critical)*** | The exercise report includes a detailed summary of the scenario tested and relevant assumptions of the scenario. | The exercise report includes a summary of the scenario tested. | The exercise report does not include information regarding the scenario tested. |
| Does the exercise report include a record of the exercise? ***(High)*** | The exercise report includes a detailed and fulsome record of the exercise. This could be in a variety of formats, including:<br>• Audio-visual<br>• Minutes<br>• Transcription.<br>The report should detail the actions of the responsible entity in response to the scenario. | The exercise records include some of the categories noted in the instructions.<br>*OR*<br>A recording covers most of the exercise. | The exercise report does not include a record of the exercise. |
| Does the exercise report include a list of the systems involved in the scenario? ***(Medium)*** | The exercise report contains a list of high-level systems being tested and their descriptions.<br>Descriptions include a summary of the system and what the intended use of the system is. All systems mentioned during the exercise correlate to systems listed in the exercise report. Both lists include the SoNS being tested. | A list of high-level systems being tested is provided. Some systems are listed with partial or no descriptions. Many systems mentioned in the exercise records are not listed in the exercise report. At least one of the lists include the SoNS being tested. | The exercise report does not contain a list of high-level systems tested.<br>None of the systems mentioned in the exercise records are mentioned in the report.<br>*OR*<br>Neither the exercise report nor the exercise records include any of the organisation's SoNS. |

| Consideration | Well Implemented | Partially Implemented | Not Apparent |
|---|---|---|---|
| | | | *OR*<br>The exercise report does not contain a list of high-level systems tested.<br>*OR*<br>The exercise records are not detailed enough to determine which systems were exercised. |

## Criterion EX.3: Assessment to demonstrate entities ability to operationalise their incident response plan

### Outcome

The purpose of the cyber security exercise is to test a responsible entity's ability to respond to and mitigate the effects of a cyber-security incident.

This assessment should test a responsible entity's ability to adhere to an effective incident response plan. To develop a mature cyber security profile, a responsible entity should have an effective incident response plan and not rely solely on the individual capabilities of their defenders.

### Considerations

| Consideration | Well Implemented | Partially Implemented | Not Apparent |
|---|---|---|---|
| Does the responsible entity demonstrate an ability to effectively implement their incident response plan?<br>**(Critical)** | The responsible entity implemented their IRP effectively. The exercise scenario has content which relates to all phases of the incident response plan. The phases detailed in the IRP were followed in almost all circumstances. | The responsible entity implemented their IRP with moderate effectiveness. There are some phases of the incident response plan which do not match with any content in the scenario. These phases or steps may not be possible to test during the exercise. The phases detailed in the IRP were successfully carried out in some circumstances. | The responsible entity did not effectively implement their IRP. The exercise scenario does not relate to any phases of the incident response plan, most likely if insufficient or incorrect information about the scenario is provided or due to the incident response plan being vague.<br>OR<br>None of the phases detailed in the IRP were followed.<br>OR<br>All of the phases of the response from the IRP or playbooks that were followed encountered significant issues. |
| Did the responsible entity adhere to their incident response plan and justify any deviations?<br>**(High)** | The responsible entity adhered closely to their IRP. Deviations occurred from the incident response plan, at least some of which were identified, and workarounds were implemented. Justification for these workarounds is provided in the exercise notes. | The responsible entity mostly adhered to their IRP. Deviations occurred from the incident response plan and workarounds were applied. Some of these workarounds were justified, while others had no justification provided. | The responsible entity did not closely adhere to their IRP. Deviations occurred from the incident response plan but were not identified or rectified.<br>OR<br>Notes from the exercise were not sufficient to determine if any deviations occurred or if workarounds were applied. |

## Criterion EX.4: Contents of the cyber security exercise internal evaluation report

### Outcome

As a legislative requirement under s30CQ of the SOCI Act, an internal evaluation report must be developed to document the outcome of the cyber security exercise. The content of the evaluation report must include an evaluation of the entity's ability to respond, prepare and mitigate appropriately the cyber security incidents specified in the notice given by the department. The report should contain sufficient detail about the exercise to inform stakeholders who did not observe the exercise. The report should also include an assessment of whether the responsible entity can appropriately respond to a cyber-incident and whether your incident response is appropriate.

In addition, your internal report may include a reflection on the exercise, including who participated, what the exercise scenario was, what systems were tested and other relevant information. Supplementary documentation may include a facilitator handbook, a participant's handbook, or materials provided as part of the exercise, etc. The report should also include a section that explains how the responsible entity responded to the scenario, what went well, and what went poorly.

### Considerations

| Consideration | Well Implemented | Partially Implemented | Not Apparent |
|---|---|---|---|
| Does the report list the participants and observers of the exercise? **(High)** | The report lists all the participants and observers of the exercise. This list includes their position and role. | The report lists some the participants and observers of the exercise. This list does not include their position and role. | The report omits the participants of the exercise. |
| Does the report include information on the key decision points and decision makers? **(High)** | The report includes detailed information on all the key decision points, decision makers and relevant reasoning in the exercise. | The report includes detailed information on some of the key decision points, decision makers and relevant reasoning in the exercise. | The report does not include information on key decision points and decision makers in the exercise. |

## Criterion EX.5: Exercise report recommendations

### Outcome

A key outcome of the cyber security exercise is to identify areas of potential cyber security uplift. The report should include a series of recommendations based on the findings of the exercise.

These recommendations should aim to uplift the cyber security maturity of the responsible entity across relevant people, processes, and technology. Findings from the exercise may also inform updates to the incident response plan, or they may require further investigation through vulnerability assessments or follow-up exercises.

Exercises should, where possible, aim to test the resolution of recommendations from previous exercise reports. The responsible entity should aim to test these recommendation resolutions where possible, in the context of the scenario/guidance provided by the CISG. The exercise report should identify the new recommendations and comment as to whether any previous recommendations have been repeated. If a responsible entity is receiving the same recommendations on multiple occasions and failing to implement resolutions, this would be cause for concern.

Recommendations in the exercise report should be allocated to reasonable implementation timeframes based on the difficulty of resolving the recommendation, and the security risk associated with not resolving the recommendation.

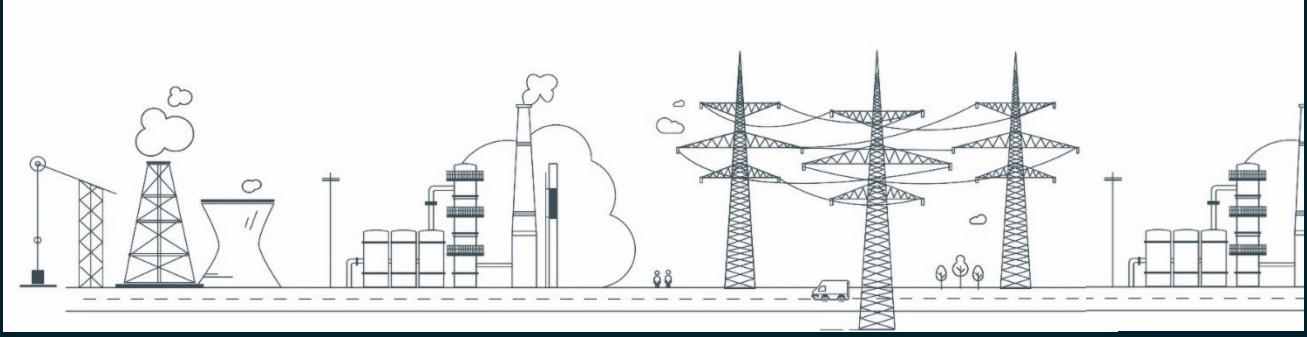
## Considerations

| Consideration | Well Implemented | Partially Implemented | Not Apparent |
|---|---|---|---|
| Does the report include recommendations to improve the incident response plan? ***(Critical)*** | The report includes detailed recommendations to improve the IRP. All recommendations made are included in the report. If there are no recommendations to improve the IRP, the consideration is marked as well implemented. | The report includes recommendations to improve the IRP, however these do not contain sufficient detail. All recommendations made are included in the report. | The report does not include recommendations to improve the IRP. |
| Does the report include recommendations to improve cyber security capability (people, processes, and technology)? ***(Critical)*** | The report includes detailed recommendations to improve the responsible entity's cyber security capability. All major occurrences of these issues that have been identified in the exercise notes are reflected in the recommendations for the incident response plan. If there are no recommendations to improve the responsible entity's cyber security capability which is justified in the exercise report, the consideration is marked as well implemented. | The report includes recommendations to improve the responsible entity's cyber security capability. At least one major issue identified in the exercise notes has not been included in any of the recommendations. | The report does not include recommendations to improve the responsible entity's cyber security capability. *AND/OR* No issues that have been identified relating to cyber security capability have been reflected within the recommendations within the incident response plan. |
| Does the exercise test the resolution of recommendations from previous exercises? ***(High)*** | Some recommendations from the previous scenario are tested and the exercise scenario methodology/reasoning includes recommendations. *OR* No previous exercise recommendations are available, and no previous exercises have been performed as ECSO. | Most recommendations from the previous exercise will not be tested by the scenario and the scenario methodology/reasoning did not consider recommendations. | None of the recommendations from the previous exercise will be tested by the scenario. *OR* An exercise was previously performed but the recommendations from that exercise have not been provided. |
| Do recommendations from the incident match with appropriate resolution timeframes? ***(High)*** | All recommendations include a timeframe until resolution is expected to be complete. | All recommendations are accompanied by a timeframe for resolution, but the timeframe is too long. *OR* Some recommendations in the newly provided list of recommendations are not accompanied by a timeframe for resolution. | No timeframes for resolution are included. |
| Are the newly issued recommendations different from previous recommendations? ***(Medium)*** | The provided list of recommendations from the previous exercise have been resolved or are on track to be completed within their resolution timeframe. All entries in the newly provided list of recommendations relate to new issues, or are recurring issues accompanied by an explanation of why the issue has recurred. *OR* The report notes that no previous exercises have been run under the ECSO framework. | Several recommendations from the list of recommendations from the previous exercise are repeated in the new list with no explanation, despite their timeframe. *OR* Several recommendations are not due to be complete yet, but no resolution is evident from the results of the exercise, and the recommendations are not accompanied by an explanation. | Many recommendations from the previous exercise are repeated following the new exercise, despite the timeframe for their resolution having lapsed, and no explanation is included. |

## Questions

The Department has a dedicated team to work with the owners and operators of Systems of National Significance to ensure the Enhanced Cyber Security Obligations are well understood and appropriately applied, and that entities are meeting their obligations under the SOCI Act.

For further information please contact us at : **sons@homeaffairs.gov.au**



Australian Government

Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE