Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

CYBER INCIDENT RESPONSE PLAN

GUIDANCE

cyber.gov.au

Context

The Australian Government defines cyber security as measures used to protect the confidentiality, integrity and availability of systems and information. A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.[1]

Australian organisations are targeted by malicious cyber adversaries. The Australian Cyber Security Centre's (ACSC) assessment is malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, and sophistication. As adversaries become more adept, the likelihood and severity of cyber attacks is also increasing due to the interconnectivity and availability of information technology platforms, devices and systems exposed to the internet.

To illustrate the volume of cyber incidents occurring in Australia, the ACSC responded to over 1500 cyber security incidents between 1 July 2020 and 30 June 2021.[2] While many of the incidents reported to the ACSC could have been avoided or mitigated by good cyber security practices, such as implementation of ASD's Essential Eight security controls, risks will still remain when organisations operate online.

Managing responses to cyber incidents is the responsibility of each affected organisation. All organisations should have a cyber incident response plan to ensure an effective response and prompt recovery in the event security controls don't prevent an incident occurring. This plan should be tested and regularly reviewed.

To be effective, a cyber incident response plan should align with the organisation's incident, emergency, crisis and business continuity arrangements, as well as jurisdictional and national cyber and emergency arrangements. It should support personnel to fulfil their roles by outlining their responsibilities and all legal and regulatory obligations.

While organisations are responsible for managing incidents affecting their business, Australia's Cyber Incident Management Arrangements (CIMA) outline the inter-jurisdictional coordination arrangements and principles for Australian governments' cooperation in response to national cyber incidents.[3]

Purpose

The Cyber Incident Response Plan (CIRP) Template and the Cyber Incident Response Readiness Checklist (Appendix B) are intended to be used as a starting point for organisations to develop their own plan and readiness checklist.

Each organisation's CIRP and checklist need to be tailored according to their unique operating environment, priorities, resources and obligations.

In addition to a CIRP, organisations can develop more detailed, day-to-day procedures to supplement the cyber incident response plan. This could include more detailed playbooks to aid the response to common incident types, such as ransomware or data breaches, and standard operating procedures (SOPs) to respond to incidents affecting specific assets.

1 *Australian Cyber Security Centre, cyber.gov.au, 'Glossary', accessed 16 December 2020.*
2 *Australian Cyber Security Centre, cyber.gov.au, ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021.*
3 *https://www.cyber.gov.au/acsc/view-all-content/news/cyber-incident-management-arrangements-australian-governments, December 2018.*

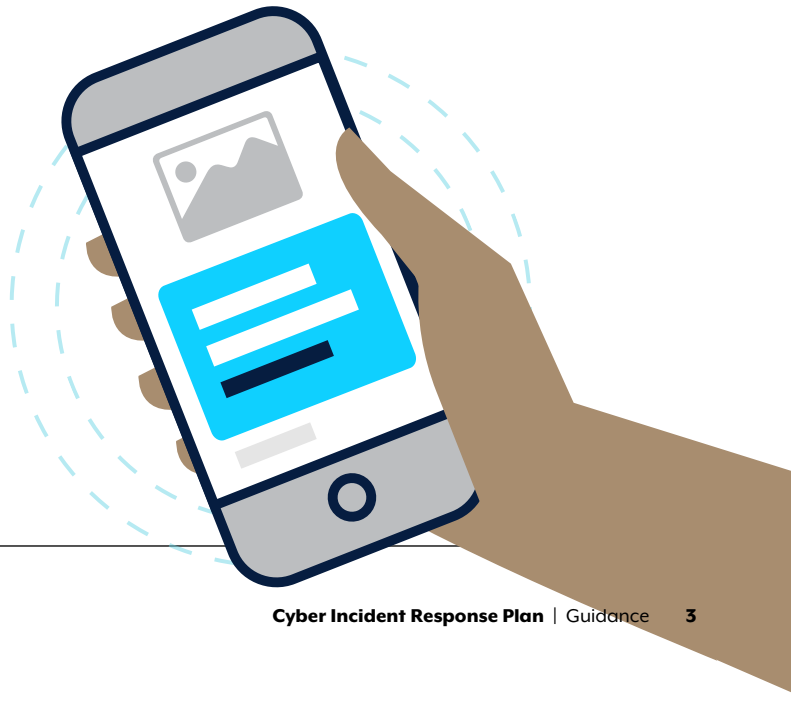
Acknowledgements

This document was created by the ACSC using multiple resources. The ACSC acknowledges the following resources used to develop this template:

- The Australian Government Information Security Manual (ISM).
- Australian Prudential Regulation Authority (APRA) Prudential Practice Guide CPG 234 Information Security June 2019 (https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_1.pdf).
- A Cyber Incident Response Plan template developed by efforts of the Australian Energy Sector Readiness and Resilience Working Group in 2019, specifically with support from the Australian Energy Market Operator (AEMO), Tasmanian Department of State Growth, the Victorian Government Department of Premier and Cabinet and the ACSC.
- Victorian Government Incident Response Plan template 2019 (https://www.vic.gov.au/prepare-cyber-incident).
- Queensland Government Enterprise Architecture Incident management guideline 2018 (https://www.qgcio.qld.gov.au/documents/incident-management-guideline).
- United States National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide 2012 (https://www.nist.gov/privacy-framework/nist-sp-800-61).
- International Organisation for Standardisation standards:
  - ISO/IEC 27035-1, Information technology – Security techniques – Information security incident management, Part 1 Principles of incident management,
  - ISO/IEC 27035-2, Information technology – Security techniques – Information security incident management, Part 2 Guidelines to plan and prepare for incident response,
  - ISO/IEC 27035-3, Information technology – Information security incident management, Part 3 Guidelines for ICT incident response operations.
- Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Incident & Vulnerability Response Playbooks 2021 (https://us-cert.cisa.gov/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability).

Questions and Feedback

Questions and feedback about this document should be directed to the ACSC via email at asd.assist@defence.gov.au or phone at 1300 CYBER1 (1300 292 371).



How to use this document

This document includes guidance that organisations can follow to support the development of their own CIRP. A separate CIRP template is available for organisations to fill in.

The template is not exhaustive. Each organisation's CIRP should be tailored according to its unique operating environment, priorities, resources and obligations.

Some fields will contain example text in red. This text is demonstrative only, and should not be used as the basis of your CIRP.

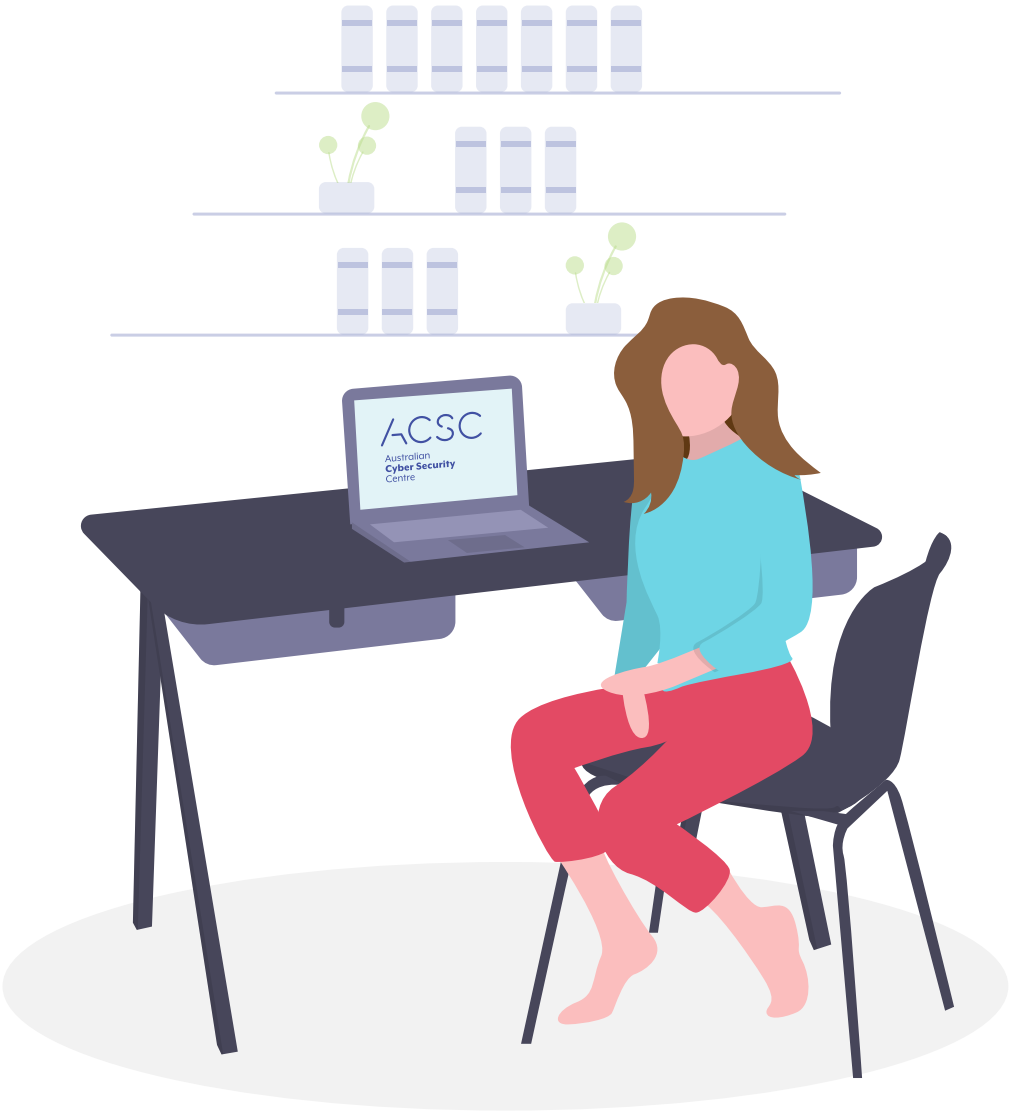


Table of Contents