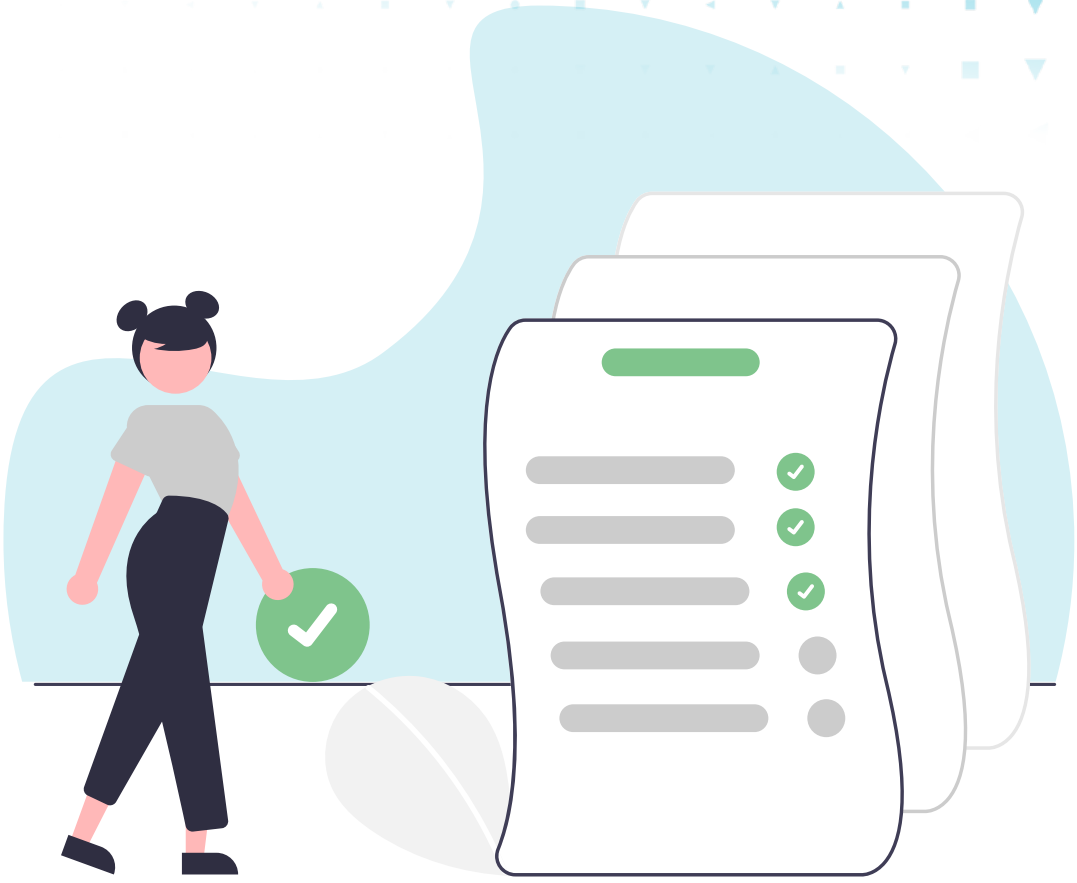
Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre



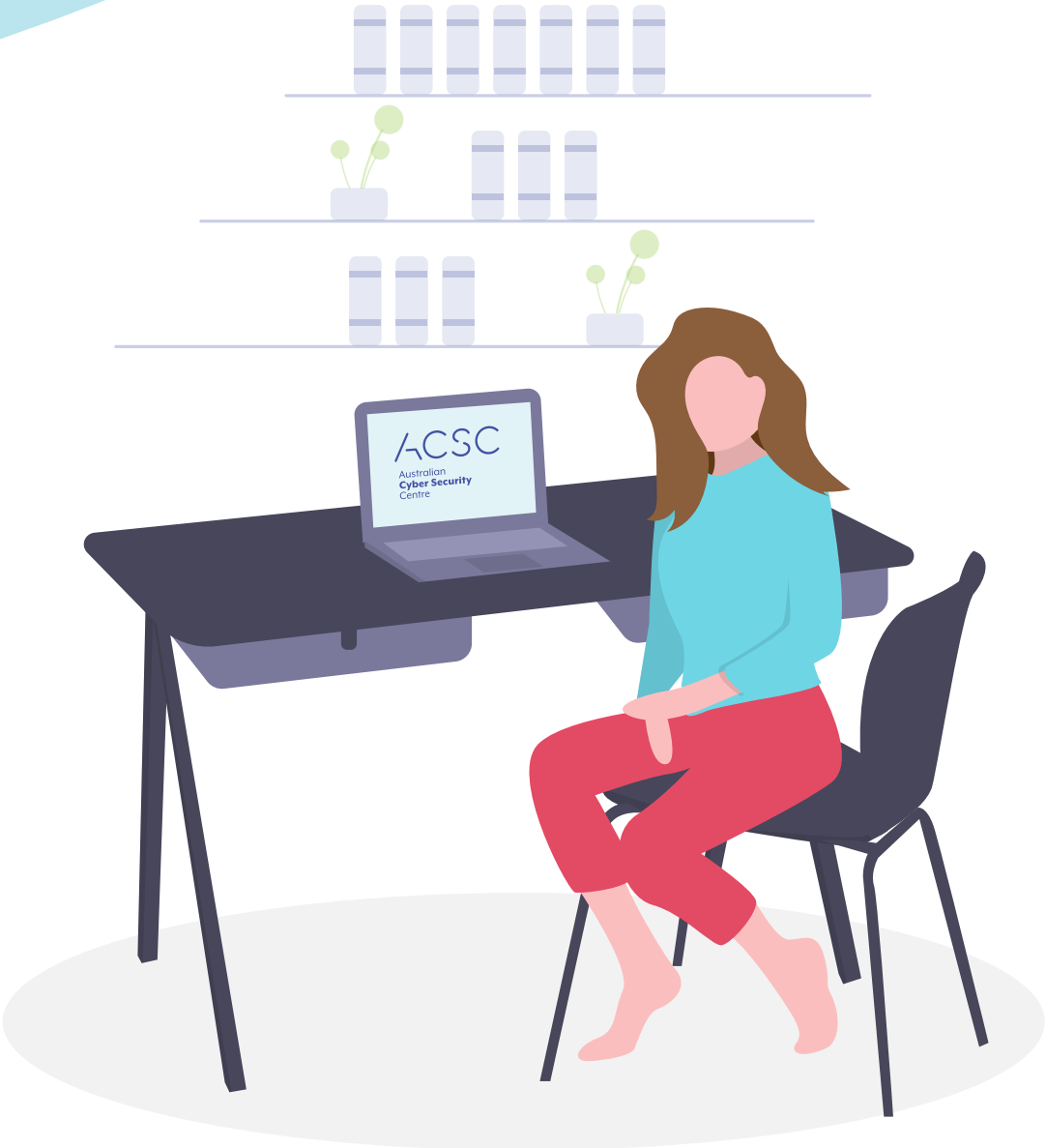
CYBER INCIDENT RESPONSE PLAN

READINESS CHECKLIST

cyber.gov.au

Introduction

This checklist is to aid your organisation's initial assessment of its readiness to respond to a cyber security incident. This checklist is not an exhaustive list of all readiness activities.



Cyber Incident Response – Readiness Checklist

PREPARATION	
☐	Your organisation has a cyber security policy or strategy that outlines your organisation's approach to prevention, preparedness, detection, response, recovery, review and improvement. • For example, does your organisation have a position on, for example, paying ransom, reporting incidents to government, publicly acknowledging cyber incidents, sharing information about incidents with trusted industry and government partners?
☐	A Cyber Incident Response Plan has been developed, which: • Aligns with your organisation's operating environment and other processes, including emergency management and business continuity processes. • Has been reviewed or tested in an exercise to ensure it remains current and responsible personnel are aware of their roles, responsibilities and processes. • Templates have been prepared, for example Situation Reports.
☐	Staff involved in managing an incident have received incident response training.
☐	Up-to-date hard copy versions of the Cyber Incident Response Plan and playbooks are stored in a secure location (in case of electronic or hardware failure) and are accessible to authorised staff members.
☐	Specific playbooks to supplement the Cyber Incident Response Plan have been developed, that define step-by-step guidance for response actions to common incidents, and roles and responsibilities.
☐	A Cyber Incident Response Team (CIRT) and a Senior Executive Management Team (SEMT) – or equivalents - have been formed to manage the response, with approved authorities.
☐	All relevant IT and OT Standard Operating Procedures (SOPs) are documented and have been reviewed or tested in an exercise to ensure they remain current and responsible personnel are aware of their roles, responsibilities and processes.
☐	Arrangements for service providers, including cloud and software as a service, to provide and retain logs have been established and tested to ensure these include useful data and can be provided in a timely manner.
☐	Log retention for critical systems have been configured adequately and tested to confirm that they capture useful data. Refer to the ACSC publications including Windows Event Logging and Forwarding for specific guidance.
☐	Your organisation has internal or third party arrangements and capabilities to detect and analyse incidents. If these capabilities are outsourced, your organisation has an active service agreement/contract.

Cyber Incident Response – Readiness Checklist

PREPARATION (cont...)	
☐	Critical assets (data, applications and systems) have been identified and documented.
☐	Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for use of facilities and communications technologies in response to cyber incidents, and these resources are confirmed as available. This includes for alternative/back-up ICT-based channels.
☐	Incident logging/records and tracking technologies used to manage a response are confirmed as available and have been tested.
☐	Role cards have been developed for each person involved in the CIRT and the SEMT. Individual actions will depend on the type and severity of the incident. Example role card is available in the CIRP Template.
☐	Your organisation has internal or third party arrangements and capabilities to monitor threats. Situational awareness information is collected from internal and external data sources, including: • Local system and network traffic and activity logs • News feeds concerning ongoing political, social, or economic activities that might impact incident activity • External feeds on incident trends, new attack vectors, current attack indicators and new mitigation strategies and technologies.

DETECTION, INVESTIGATION, ANALYSIS AND ACTIVATION	
Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for:	
☐	Detection mechanisms which can be used to identify potential information security incidents, such as scanning, senses and logging mechanisms. These mechanisms require monitoring processes to identify unusual or suspicious activity, for example behaviour and logging, commensurate with the impact of an incident. Common monitoring techniques include: **a)** network and user profiling that establishes a baseline of normal activity which, when combined with logging and alerting mechanisms, can enable detection of anomalous activity; **b)** scanning for unauthorised hardware, software and changes to configurations; **c)** sensors that provide an alert when a measure breaches a defined threshold(s) (e.g. device, server and network activity); **d)** logging and alerting of access to sensitive data or unsuccessful logon attempts to identify potential unauthorised access; and **e)** users with privileged access accounts subject to a greater level of monitoring in light of the heightened risks involved.[1]

1 APRA Prudential Practice Guide CPG 234 Information Security.

DETECTION, INVESTIGATION, ANALYSIS AND ACTIVATION (cont...)	
☐	Incident detection, including self-detected incidents, notifications received from service providers or vendors, and notifications received from trusted third parties (e.g. ACSC).
☐	Incident analysis, including how incidents are to be categorised, classified and prioritised, and controls related to how data is stored and transmitted (i.e. if out-of-band transmission is required).
☐	Activating a Cyber Incident Response Team (CIRT) to manage critical incidents, with roles and responsibilities assigned.
☐	Activating a Senior Executive Management Team (SEMT) to manage critical incidents, with roles and responsibilities assigned.

CONTAINMENT, EVIDENCE COLLECTION AND REMEDIATION	
☐	Standard Operating Procedures (SOPs), playbooks and templates, have been developed, and roles and responsibilities assigned for containment, evidence collection and remediation. These can be included as appendices to the Cyber Incident Response Plan.
☐	A secure location is available for storing data captured during an incident, which could be used as evidence of the incident and the adversary's tradecraft, and ready to be provided to third-party stakeholders if needed.

COMMUNICATIONS	
☐	Policy, plans, Standard Operating Procedures (SOPs) and templates have been developed to support communicating with: • Internal stakeholders (e.g. Board, staff) • External stakeholders (e.g. stakeholders to assist with the response and stakeholders with an interest in the response)
☐	Policy, plans, Standard Operating Procedures (SOPs) and templates for media and communications professionals have been developed, and roles and responsibilities assigned, to support public and media messaging.
☐	You organisation has assigned a public and media spokesperson, who is supported by subject matter experts.
☐	Staff have been trained to implement the communications processes and execute their roles and responsibilities.

Cyber Incident Response – Readiness Checklist

COMMUNICATIONS (cont...)	
☐	Staff who are not involved in managing incidents are cognisant of your organisation's policy and processes and their responsibilities when an incident occurs (e.g. exercising discretion, using approved talking points, referring enquiries to the designated officer).

INCIDENT NOTIFICATION AND REPORTING	
☐	Processes and contact details are documented to support the organisation to meet its legal and regulatory requirements on cyber incident notification, reporting and response, with roles and responsibilities within your organisation are assigned. This includes the processes for obtaining authority to release and share information.
☐	Processes are documented for insurance requirements.

POST INCIDENT REVIEW	
☐	A process is documented to conduct Post Incident Reviews (PIR) following conclusion of an incident and PIR reports with recommendations are submitted to management for endorsement.
☐	A process is documented to ensure actions following incidents and/or exercises are tracked and completed (e.g. Action Register).

Notes

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre