ENTERPRISE INCIDENT RESPONSE PROGRAM

DESIGN PORTFOLIO

Incident Response Planning • Exercise Design • IRP Development

PORTFOLIO EDITION

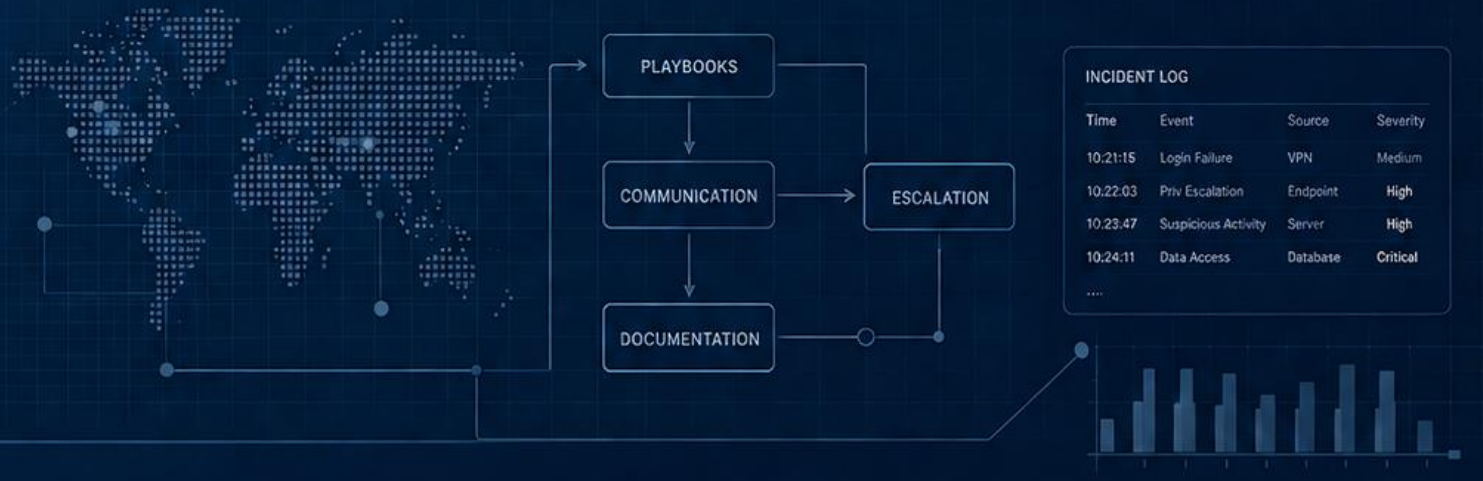
PREPARE
Build capability and readiness

DETECT
Identify and analyze threats

RESPOND
Contain, investigate and eradicate

RECOVER
Restore operations and services

IMPROVE
Learn and strengthen for the future



PREPARED BY

Markus Walker

CYBER SECURITY PROFESSIONAL

Portfolio Context Statement

This document is a mock-up Incident Response Program and Incident Response Plan portfolio piece. It is based on a previous cyber security planning document I created and has been sanitised for public presentation. Names, organisations, contacts and entities used in this document are fictional or replaced with placeholders. The document is intended only to provide a cursory view of my capability in cyber security planning, incident response documentation, stakeholder communication, project coordination and IRP development.

Scenario Context

<my employer> has assigned me to plan and oversee the development of an Incident Response Team for <the client>. The task involves establishing a project team, evaluating the existing Incident Response Plan, and developing an updated Incident Response Plan. The key focus is a cyber security-based project using current applications and preparing the organisation for Incident Response Team activities. The project also requires the selection of a suitable online project management and collaboration application so that planning, coordination, communication and documentation can be managed online.

Contents

Project Charter

Revision History

Date	Version	Modification	Modifier
08/03/2026	1.0	Initial Project Charter Draft	Markus Walker

Introduction

<the client> has identified the need for a structured incident response capability. This project aims to design, run and evaluate an Incident Response Team exercise to test how well the organisation can detect, respond to and recover from cyber threats. The exercise will give the team practical experience and also help reveal gaps in current procedures.

The project will simulate realistic cyber incidents using the TryHackMe lab environment. Activities will involve red, blue and observation teams working through controlled scenarios. Results from the exercise will be used to improve the organisation's Incident Response Plan and overall security readiness.

Purpose

The purpose of this project is to evaluate and strengthen <the client>'s incident response capability. The project reviews the current draft Incident Response Plan and tests how effectively the organisation can detect and respond to cyber security incidents.

The exercise also provides hands on experience for security staff while identifying weaknesses in processes, communication and technical controls. Findings from the project will support the development of an improved Incident Response Plan aligned with recognised industry practices such as the NIST Computer Security Incident Handling Guide.

Scope and Boundaries

Scope

The project includes planning, executing and evaluating a cyber security incident response exercise for <the client>. Major activities include reviewing the draft Incident Response Plan, creating team playbooks, running the simulated attack and defence scenarios and documenting lessons learned.

Boundaries

Testing will only occur in the approved TryHackMe lab environment. No production systems or customer data will be used. Only authorised tools and techniques approved by the project team will be allowed during the exercise. All activities must follow the defined Rules of Engagement.

Objectives and Expected Outcomes

Objectives

- Assess the effectiveness of the current Incident Response Plan.
- Develop an improved IRP aligned with NIST SP 800-61.
- Conduct a realistic incident response exercise involving red and blue teams.
- Measure the ability of the team to detect and respond to cyber threats.
- Identify weaknesses in security processes and recommend improvements.

Expected Outcomes

- A revised Incident Response Plan with clearer procedures and roles.

- Improved preparedness of the incident response team.
- A final project report summarising findings, recommendations and lessons learned.

Methodology (or approach)

The project will follow a structured incident response project approach.

Preparation and planning will involve reviewing the existing IRP, assigning roles and defining communication channels. The exercise scenarios will then be designed and tested in the TryHackMe environment.

During the exercise the red team will simulate attacks while the blue team monitors systems and performs defensive actions. Observers will record the sequence of events and response actions. After the exercise the results will be analysed and the Incident Response Plan updated where needed. This process helps identify where procedures may need improvement or where response times were slower than expected

Key Project Milestones

Milestone	Estimated Completion
Project initiation and charter approval	Week 1
IRP review and planning phase	Week 2
Development of playbooks and rules of engagement	Week 3
Incident response exercise execution	Weeks 4 and 5
Analysis and evaluation of results	Week 6
Final documentation and reporting	Week 7 and 8

Deliverables

1. Team Briefing Report
2. Communications Plan
3. Updated Incident Response Plan
4. Red Team Playbook
5. Blue Team Playbook
6. Rules of Engagement
7. Observation Team Checklist
8. Stakeholder Status Reports
9. Lessons Learned Report

Timeline

The project will run for approximately eight weeks. The early stage focuses on planning and reviewing the current IRP. Mid stage work includes creating playbooks and conducting the incident response exercise. The final stage focuses on analysing results and producing the final documentation for <the client> stakeholders.

Work Breakdown Structure

1. Project initiation and planning
2. Review of existing Incident Response Plan
3. Establish project team and communication plan
4. Develop red team and blue team playbooks
5. Prepare incident response exercise scenarios
6. Execute simulated cyber attack exercise
7. Analyse team performance and collected evidence
8. Produce final report and updated IRP

These tasks will be tracked using an online project management platform such as ClickUp or Trello to keep the team coordinated.

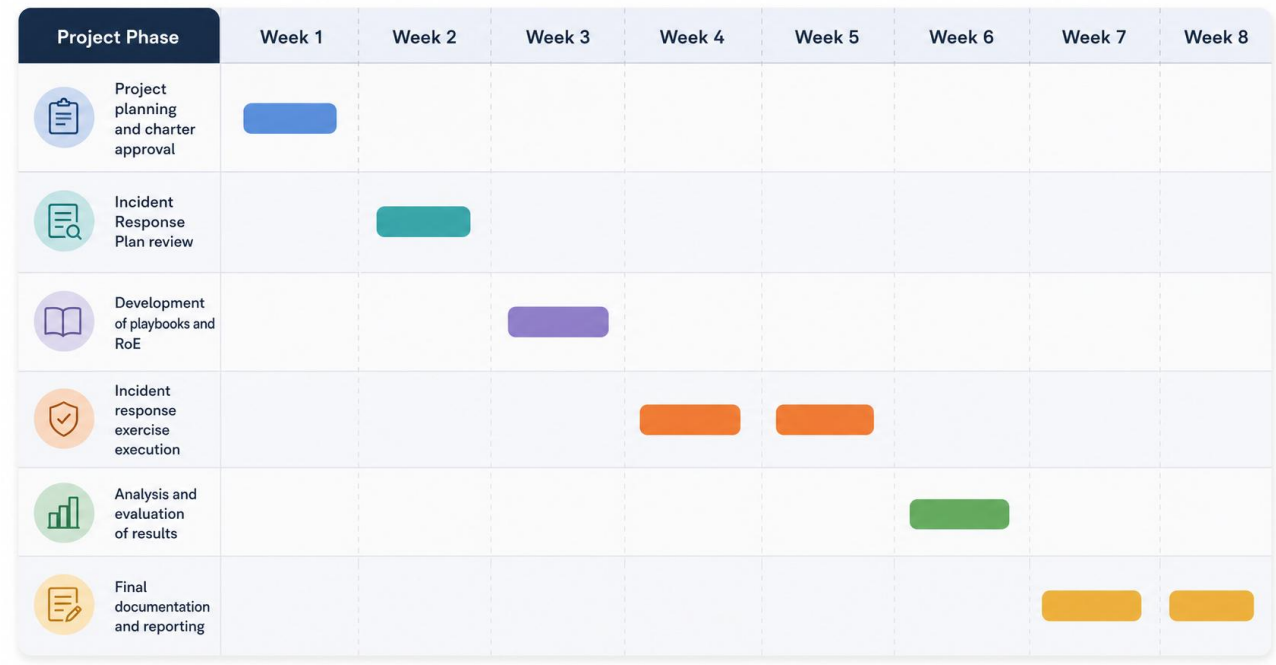
Budget

This project primarily uses internal resources and existing lab platforms.

Estimated costs include:

- TryHackMe training environment access: educational licence
- Project management tools: free tier platforms
- Staff time and training participation: internal resource allocation
- Documentation tools: existing organisational software
- Overall the project cost is minimal because it relies on existing infrastructure and internal staff.

Gantt Chart



Project Team Briefing Report

Introduction

This briefing report sets out the team structure for the <the client> incident response exercise and explains how the project team will operate during planning, execution and review. It supports the wider Incident Response Project Report by clarifying who is involved, what each member is responsible for and how performance will be measured across the exercise.

The exercise will be completed in a controlled lab environment rather than production systems, which allows realistic testing without creating operational risk. The team structure also supports the project communication model already established for <the client>, including weekly coordination meetings and fortnightly updates to the sponsor.

Team Composition

The project team uses a layered structure so governance, exercise control and technical delivery remain clearly separated. Sponsor oversight sits above day to day coordination, while red, blue and white or purple team functions operate alongside support roles such as communications, quality assurance and forensic advice.

This approach helps the exercise stay fair, measurable and safe. It also makes it easier to assign ownership during planning, run the exercise in a controlled way and capture lessons learned for the updated Incident Response Plan.

Role	Assigned Member	Team Function
Project Sponsor	Amelia Hart	Governance
Project Manager / White Team Lead	Priya Nair	Coordination and oversight
Incident Manager and IRT Lead	Lachlan Reed	Operational coordination
Red Team Lead	Noah Bennett	Offensive simulation
Blue Team Lead	Sophie Tran	Defensive operations
Communications Lead	Emily Chen	Project communication
Quality Assurance Lead	Daniel Foster	Quality control
Forensic Analyst / SME	Olivia Grant	Evidence and investigation support
Systems Administrator / Green Team Support	Ethan Brooks	Engineering support

Roles and Responsibilities

The sponsor provides authority, approves scope and major deliverables and resolves significant issues that cannot be handled at the working level. The project manager and white team lead coordinates meetings, confirms readiness, monitors scope and makes sure the exercise remains controlled from start to finish.

Operational delivery sits with the incident manager and the red and blue team leads. The incident manager coordinates the exercise timetable and response workflow. The red team lead plans approved offensive activity and keeps records of actions and findings. The blue team lead manages monitoring, triage, containment and recovery activity during the simulated incident.

Supporting roles strengthen the quality of the exercise. The communications lead record decisions, prepares updates, and maintains meeting documentation. The quality assurance lead checks that outputs are complete and aligned with project requirements. The forensic analyst supports evidence preservation and investigation quality. Green team support can be used where system changes, logging improvements or infrastructure fixes are required, while Gold Team input may be needed for higher impact business decisions.

Fundamental Red, Blue and Purple Team Activities

Red team activity is focused on realistic attacker simulation within approved boundaries. This includes threat modelling, reconnaissance, scanning, credential attacks, exploitation, post exploitation activity and limited lateral movement to test how well the organisation can detect and respond.

Blue team activity is focused on defense and incident handling. This includes log review, SIEM and EDR monitoring, triage, incident classification, evidence collection, containment, eradication, recovery support and incident reporting.

White and purple team activity is focused on exercise control and learning. This includes scenario coordination, safety oversight, timing approval, metric capture, issue escalation, scope control and debrief facilitation. In practice, purple team review is used to compare red team actions against blue team detections so logging gaps, detection rules and response processes can be improved rather than simply judged as pass or fail.

Team	Purpose	Fundamental Activities
Red Team	Simulate attacker behaviour within scope.	Threat modelling, scanning, credential attacks, exploitation, post exploitation and objective simulation.
Blue Team	Detect, analyse and contain malicious activity.	Log review, SIEM and EDR monitoring, triage, incident analysis, containment, eradication, reporting and evidence collection.
White / Purple Team	Control the exercise and turn results into improvement.	Scenario coordination, observation, timing control, metric capture, issue escalation, safety oversight and debrief facilitation.

Performance Metrics

Performance will be measured using a small set of practical metrics that reflect both speed and effectiveness. The selected measures are Mean Time to Detect, Mean Time to Respond and Detection Coverage Rate.

These metrics give a straightforward view of how quickly the team notices malicious activity, how quickly it takes action and how much of the attack path was actually observed. They are also useful because they can be reviewed during the final debrief and compared against expected process, evidence quality and communication performance.

Metric	What It Measures	Why It Matters
Mean Time to Detect	How quickly the blue team identifies suspicious or malicious activity.	Shows whether monitoring, alerting and analyst triage are effective.
Mean Time to Respond	How quickly the team contains or manages an identified incident.	Shows whether the response process is timely and controlled once a threat is found.
Detection Coverage Rate	How many important red team actions were identified and documented by the blue team.	Shows whether key attacker behaviour was actually seen and recorded during the exercise.

Conclusion

The proposed team structure gives <the client> a clear operating model for the incident response exercise. It separates governance, attack simulation, defensive action and oversight while still keeping communication and quality control visible.

Communications Plan

Revision History

Date	Version	Modification	Modifier
08/03/2026	V1.0	Documentation Creation	Markus Walker

Introduction

This communication plan supports the <the client> incident response exercise and sets out how information will be shared across the project. It explains who needs updates, what type of information they require, which channels will be used and how often communication will occur. A clear plan helps keep the exercise organised and makes it easier for the team to respond to issues without confusion.

Purpose

The purpose of this communication plan is to make sure all stakeholders are informed, engaged and coordinated throughout the <the client> IRT exercise. Clear communication supports timely decision making, reduces misunderstandings and helps the project stay aligned with its incident response objectives.

Stakeholders

The main stakeholders for this project include the project sponsor, project manager, incident manager, red team, blue team, communications lead, quality assurance lead and relevant technical specialists. Each group needs a different level of detail, so communication has to be practical, timely and suited to their role.

Internal Contacts

Role	Name	Title	Phone	Email
Project Sponsor	Amelia Hart	Chief Security Officer	07 5550 0101	amelia.hart@client.example
Project Manager	Priya Nair	White Team Lead	07 5550 0102	priya.nair@client.example
Incident Manager	Lachlan Reed	Incident Response Coordinator	07 5550 0103	lachlan.reed@client.example
Red Team Lead	Noah Bennett	Red Team Lead	07 5550 0104	noah.bennett@client.example
Blue Team Lead	Sophie Tran	Blue Team Lead	07 5550 0105	sophie.tran@client.example

External Contacts

Role	Name	Title	Phone	Email
Security Advisor	Mia Collins	External Cybersecurity Consultant	07 5550 0202	mia.collins@consult.example

Other Stakeholders

Role	Name	Title	Phone	Email
Communications Lead	Emily Chen	Project Communications Coordinator	07 5550 0301	emily.chen@client.example
QA Lead	Daniel Foster	Quality Assurance Lead	07 5550 0302	daniel.foster@client.example
Forensic Analyst	Olivia Grant	Digital Forensic Analyst	07 5550 0303	olivia.grant@client.example
Systems Administrator	Ethan Brooks	Infrastructure Support Officer	07 5550 0304	ethan.brooks@client.example

Scope

This plan covers communication for the full incident response exercise lifecycle, including planning, preparation, execution, reporting and final review. It applies to formal project updates, meeting records, escalation of urgent issues and the distribution of lessons learned. It does not replace technical response procedures, but it supports them by making sure the right people get the right information at the right time.

Goals and Objectives

The communication goals are to provide timely updates, keep messages clear and accurate, ensure important matters are escalated quickly and maintain good records of meetings, decisions and incident activity. Another objective is to support transparency across the exercise so that progress, risks and outcomes are visible to all key participants.

Communication Roles

Communication responsibilities are shared across the project team. The project manager coordinates routine updates, the incident manager handles urgent incident notifications, the communications lead prepares formal reports and meeting records, and team leads provide role specific progress updates from the exercise environment.

Project Team Directory

First Name	Last Name	Position	Email	Phone Number
Priya	Nair	Project Manager	priya.nair@client.example	07 5550 0102
Lachlan	Reed	Incident Manager	lachlan.reed@client.example	07 5550 0103
Emily	Chen	Communications Lead	emily.chen@client.example	07 5550 0301
Daniel	Foster	QA Lead	daniel.foster@client.example	07 5550 0302

Schedule of Meetings

Chair: Priya Nair, Project Manager

Minute Taker: Emily Chen, Communications Lead

Frequency of Meetings

Formal meetings will occur weekly for the project team, with sponsor updates every second Friday. During the exercise week, short daily stand ups will be held each morning. Extra meetings can be scheduled when risks, blockers or urgent decisions need attention.

Meetings Reports

Meeting agendas and minutes will be created for each formal meeting and stored with the project records. Status reports will be issued every two weeks and will summarise completed work, current risks, key decisions and the next actions. Incident notifications will be documented separately when major exercise events occur.

Structure of Meetings

Concept development meeting: held once at the start of the project to confirm the exercise concept, expected outcomes and initial stakeholder expectations.

Initial planning meeting: used to confirm scope, roles, milestones, communication channels and any early risks or constraints.

Mid-point meeting: reviews progress against the schedule, identifies blockers and confirms that deliverables are still on track.

Final planning meeting: completed before exercise execution to confirm readiness, reporting expectations and escalation pathways.

Weekly or fortnightly updates: short progress updates are shared through meetings, collaboration tools and email depending on audience needs.

Final report: summarises exercise outcomes, key findings, communication effectiveness and recommended improvements.

Plan Updates and Approvals

This communication plan will be reviewed by the project sponsor and updated if project needs change or if lessons learned show that communication arrangements need improvment. Any major revision should be approved by the sponsor and communicated to the project team so everyone is working from the current version.

IRP and CSOC Recommendations

To	Amelia Hart, Chief Security Officer	Date	08/03/2026
From	Markus Walker	Subject	IRP and CSOC Recommendations

Purpose

This document summarises the priority actions recommended for <the client>'s current Incident Response Plan (IRP) after review against NIST SP 800-61 and the broader exercise planning work. The current plan gives a basic intent, but it still needs stronger classification, triage, escalation, evidence handling, recovery validation and post incident review processes.

Without these controls, incident handling may become inconsistent and slower than it should be. The recommendations below are designed to make the plan more operational and establish a practical Cyber Security Operations Centre foundation.

Summary of Need

The review identified three consistent problems. First, governance is too high level, which makes incident severity, approval paths and communications harder to manage under pressure. Second, the procedures don't give responders enough step by step guidance for triage, evidence preservation, containment and recovery. Third, monitoring and case handling aren't integrated well enough to support timely detection or meaningful reporting.

CSOC Foundation

<the client> should implement a staged CSOC model. The initial capability should include centralised log collection and SIEM monitoring, endpoint alerting, incident case management, threat intelligence input, playbooks, analyst ownership, defined escalation paths and routine reporting against MTTD and MTTR. This approach would improve detection, coordination and accountability without requiring a large stand alone function on day one.

Recommendations

#	Last Name	Position
1	Create an incident classification and severity matrix	This would link business impact to escalation thresholds, authority and communications requirements so high risk events can be managed consistently.
2	Standardise triage and incident case management	A defined triage workflow and single incident record would improve accountability, evidence tracking and handover between responders.
3	Develop playbooks for key incident types	<the client> should document practical playbooks for ransomware, insider data theft and web application compromise so staff don't need to guess under pressure.
4	Strengthen forensic readiness and evidence handling	The IRP should require chain of custody, evidence preservation steps and access to basic forensic tooling to support investigation quality and legal defensibility.
5	Implement a staged CSOC capability	The first phase should combine SIEM monitoring, endpoint visibility, case management, threat intelligence and defined analyst escalation to support earlier detection and coordinated response.
6	Align response, continuity and improvement activities	Recovery priorities, post incident review and metrics such as MTTD, MTTR and detection coverage should be built into the IRP so the capability keeps improving.

Conclusion

These recommendations would give <the client> a more usable and defensible incident response capability. They also provide a realistic path to implement core CSOC functions without making the uplift bigger than it needs to be at this stage.

Incident Response Plan

<the client> Incident Response Plan

Document	Value	Document	Value
Organisation	<the client>	Version	1.1
Document Owner	Chief Security Officer	Date Approved	08/03/2026
Operational Custodian	Incident Manager and IRT Lead	Review Cycle	Every 6 months, after any major incident, or after each formal exercise
Scope	Approved TryHackMe exercise environment, supporting procedures and nominated exercise assets	Status	Approved for controlled exercise use and future operational uplift

This Incident Response Plan gives <the client> a practical structure for detecting, managing, documenting and learning from cyber incidents. It is designed for the approved incident response exercise, but it is also written as a usable operational baseline for future uplift work across the company.

The plan follows ACSC Cyber Incident Response Plan guidance and fixes the main gaps identified in the earlier draft IRP, especially around classification, escalation, evidence handling, recovery validation, communication control and post incident review. It also folds in the Rules of Engagement, the Red Team and Blue Team playbooks, the observer checklist and the resources needed to test the plan properly.

Document Control and Review

Field	Details
Author	Markus Walker
Owner	Amelia Hart, Chief Security Officer
Operational Custodian	Lachlan Reed, Incident Response Coordinator
Endorsed By	Priya Nair, Project Manager and White Team Lead
Review Triggers	Scheduled review, post incident review, major system changes, lessons learned from exercises, or changes to legal, regulatory or insurance requirements
Distribution	Project team, sponsor, incident management personnel and approved exercise participants

Version Control

Version	Date	Approved By	Description of Change
1.0	08/03/2026	Amelia Hart	Initial issue of the new Incident Response Plan
1.1	08/03/2026	Amelia Hart	Reframed as a standalone company IRP and expanded with Rules of Engagement, playbook detail, observer criteria and exercise reporting support

1. Authority and Review

This plan is authorised by the Chief Security Officer and applies to <the client> cyber incidents and controlled cyber security exercises that fall within the approved scope. For this exercise cycle, the active scope is the <the client> lab environment hosted on TryHackMe. No production systems or customer data are in scope.

The plan must be reviewed every six months, after any High or Critical incident, after each formal exercise cycle and whenever material changes affect systems, logging capability, third party dependencies, legal obligations or communication arrangements. The Incident Manager maintains the working copy and submits revisions for approval.

2. Purpose and Objectives

The purpose of this plan is to support a swift, controlled and well documented response to cyber incidents. It gives responders a practical structure they can follow under pressure without needing to guess what happens next.

Provide a clear incident response framework that is easy to follow during live incidents and exercises.

Define roles, responsibilities, accountabilities, authorities and escalation paths.

Support timely communication, internal coordination and external reporting where required.

Preserve evidence and support defensible investigation outcomes.

Link response activity to business continuity and recovery priorities.

Drive continuous improvement through metrics, lessons learned, training and controlled updates.

3. Standards and Frameworks

This plan is informed by ACSC Cyber Incident Response Plan guidance, NIST SP 800-61 and general Australian good practice for reporting, evidence handling and post incident review. It also aligns with the project charter, communications plan, team briefing and recommendations work already completed for the <the client> exercise.

Reference	How It Informs This Plan
ACSC Cyber Incident Response Plan Guidance	Provides the overall section structure, governance approach, communications model, appendices and response process.
NIST SP 800-61	Supports the response lifecycle, triage discipline, containment planning and post incident review approach.
<the client> Project Charter	Defines the lab based scope, expected outcomes, milestones and exercise boundaries.
<the client> Communications Plan	Defines reporting cadence, sponsor oversight and the need for clear internal and external communication paths.
IRP and CSOC Recommendations	Drives improvements to classification, playbooks, evidence handling, case management, metrics and monitoring capability.

4. High Level Incident Response Process

<the client> uses a five stage response model so technical action, communication, evidence handling and decision making keep moving together. This is a practical flow, not just a policy diagram.

Stage	Purpose	Core Outputs	Lead Role
1. Prepare	Maintain the plan, tools, contacts, training, monitoring and playbooks before an incident occurs.	Current plan set, trained team, ready tooling, approved communication paths	CSO and Incident Manager

2. Detect, Investigate, Analyse and Activate	Confirm whether an event is a cyber incident, classify severity and activate the right response level.	Incident record, severity rating, activation decision, initial situation summary	Blue Team Lead and Incident Manager
3. Contain, Collect Evidence and Remediate	Limit damage, preserve evidence and plan controlled remediation actions.	Containment actions, evidence register, remediation plan	Incident Manager with technical responders
4. Recover and Report	Restore services safely, validate system integrity and report status to decision makers.	Recovery approval, stand down decision, incident report	Incident Manager and system owners
5. Learn and Improve	Capture lessons, assign actions and update the plan, playbooks and training.	Post incident review, action register, updated controls	Project Manager and QA Lead

5. Common Security Incidents and Responses

5.1 Common Threat Vectors

Threat Vector	<the client> Relevance
Email and identity	Phishing, malicious links, password spraying and credential theft are realistic entry points for the exercise and for future operational risk.
Public web services	Web applications may be targeted for exploitation, defacement, credential theft or data exposure.
Remote access	VPN, RDP or other remote access services may be abused if credentials are weak or monitoring is poor.
Insider misuse	Authorised users or contractors may intentionally or accidentally expose data, bypass controls or misuse trusted access.
Malware delivery	Scripts, malicious binaries and living off the land techniques may be used to establish footholds or persistence.

5.2 Common Cyber Incidents and Minimum Initial Response

Incident Type	Description	Minimum Initial Response
Ransomware	Malware that encrypts data or disrupts service availability.	Isolate affected hosts, protect backups, preserve volatile evidence and escalate immediately if important services are involved.
Web application compromise	Exploitation of a public facing or internal web service leading to code execution, unauthorised access or data exposure.	Contain exposure, preserve web and application logs, assess user impact and involve the system owner before restoration.
Insider data theft	Unauthorised access, copying or exfiltration by a trusted user or contractor.	Restrict account activity where authorised, preserve audit logs and involve management and compliance support early.
Phishing or credential compromise	Deceptive messages or login abuse used to obtain credentials or deliver malicious content.	Preserve the message, reset compromised accounts if needed, search for related indicators and begin case logging.
Malware infection	Trojan, downloader or other malicious code on a host or service.	Quarantine affected systems where possible, capture logs or memory and assess whether spread has occurred.

6. Roles and Responsibilities

6.1 Points of Contact for Reporting Cyber Incidents

All staff and exercise participants must report suspected cyber incidents as soon as they are identified. During the exercise, the primary reporting path is the Blue Team Lead or the Incident Manager. If normal channels are unavailable, staff must use the backup phone or SMS path.

Role	Name	Title	Phone	Email
Project Sponsor	Amelia Hart	Chief Security Officer	07 5550 0101	amelia.hart@client.example
Project Manager	Priya Nair	White Team Lead	07 5550 0102	priya.nair@client.example
Incident Manager	Lachlan Reed	Incident Response Coordinator	07 5550 0103	lachlan.reed@client.example
Blue Team Lead	Sophie Tran	Security Operations Lead	07 5550 0105	sophie.tran@client.example
Communications Lead	Daniel Cho	Communications Coordinator	07 5550 0106	daniel.cho@client.example

6.2 Cyber Incident Response Team (CIRT)

Organisation Role	CIRT Role	Core Responsibilities
Chief Security Officer	Sponsor and executive decision maker	Provides authority, approves major decisions, receives escalations and approves external messaging where required.
Incident Manager and IRT Lead	Operational response lead	Coordinates the response, assigns work, maintains control of the incident log and chairs key decision points.
Blue Team Lead	Detection and defensive lead	Oversees monitoring, triage, containment, remediation advice and detection improvement.
Red Team Lead	Exercise adversary lead	Plans approved attack activity, controls red team actions and maintains accurate offensive logs during exercises.
White or Purple Team Observer	Exercise control and fairness lead	Monitors scope, records outcomes, measures performance and facilitates lessons learned.
Forensic Analyst or SME	Evidence and analysis lead	Advises on evidence preservation, artefact collection and investigation quality.
Communications Lead	Incident communications coordinator	Prepares updates, meeting records, stakeholder messages and final response reporting.
Quality Assurance Lead	Governance and quality reviewer	Checks that documentation, process use and improvement actions remain complete and consistent.

6.3 Senior Executive Management Team

For Critical incidents, <the client> may convene a small executive decision group led by the Chief Security Officer. This group confirms business priorities, approves high impact external communication, considers legal or insurance issues and supports recovery decisions where business risk is high.

6.4 Roles and Relationships

The Incident Manager controls the active response and tasking during live incidents.

The Blue Team Lead owns technical triage and works closely with the Forensic Analyst on evidence decisions.

The Communications Lead drafts updates but does not release public messaging without approval.

The White Team Lead can pause or stop an exercise if scope, safety or fairness is at risk.

The CSO retains final authority for major external reporting, legal escalation and Critical incident stand down.

7. Communications

7.1 Internal Communications

Internal communication must stay simple, controlled and role based. Initial reports go to the Blue Team Lead or Incident Manager. During High and Critical incidents, the Incident Manager issues regular situation updates that cover current impact, actions completed, actions in progress, blockers and decisions needed.

Primary channels are approved email, project collaboration tools and the incident log repository.

Backup channels are phone, SMS and a pre agreed meeting bridge.

Status updates should be more frequent during Critical incidents and can settle to milestone based updates once the incident is stable.

Team members not involved in the response must direct enquiries to the Communications Lead or Incident Manager.

7.2 External Communications

External communication must only occur through approved channels. The Chief Security Officer approves statements to customers, regulators, insurers, service providers or the media. Communications should be accurate, factual and timed carefully so the response team is not working against conflicting messages.

8. Supporting Procedures and Playbooks

8.1 Supporting Standard Operating Procedures

Procedure or Artefact	Purpose	Owner
Incident Log	Provides a single running record of actions, times, decisions and ownership.	Incident Manager
Evidence Register	Tracks evidence items, hashes, handlers, storage location and integrity notes.	Forensic Analyst
Situation Report	Supports concise status updates during active incidents.	Communications Lead
Remediation Action Plan	Tracks fixes, owners, due dates and recovery dependencies.	Incident Manager
Post Incident Review Template	Captures lessons, strengths, gaps and required follow up actions.	QA Lead

8.2 Rules of Engagement

The Rules of Engagement define the boundaries for the exercise so it stays controlled rather than chaotic. All participants must acknowledge these rules before the live exercise begins.

Threat Vector	<the client> Relevance
Authority and approvals	The CSO authorises the exercise. The Incident Manager can start, pause or stop it. Team leads are responsible for ensuring their members comply.
Scope and targets	Only systems listed in the approved scope are in scope. No production systems, third party assets or other participant environments may be targeted.
Prohibited actions	Uncontrolled denial of service, destructive actions, malware that propagates without control, out of scope social engineering and exploitation of the training platform itself are prohibited.
Allowed tactics	Reconnaissance, vulnerability scanning, exploitation of approved weaknesses, credential attacks, privilege escalation, lateral movement and defensive monitoring are allowed within scope.
Engagement protocols	Red Team activity starts only after the formal start signal, stays within scheduled windows unless approved and must notify White Team at major milestones.
Evidence and ethics	Blue Team must preserve evidence before disruptive actions where possible. All collected data is for educational use only and must be handled professionally.
Penalties	Breaches may lead to immediate removal from the exercise and formal reporting to the program sponsor.

8.3 Red Team Playbook

The Red Team playbook provides a repeatable structure for simulating a realistic adversary. It keeps offensive activity ethical, documented and aligned with the approved scope.

Phase	Expected Activity
Reconnaissance	Perform OSINT, passive DNS and service enumeration, then conduct low rate password spraying or portal testing where approved.
Initial access	Use approved weaknesses, compromised credentials, VPN access or in scope phishing simulation to establish a foothold.
Privilege escalation	Enumerate and exploit local weaknesses, harvest credentials where approved and identify paths to higher privilege.
Lateral movement	Map relationships, move between hosts using approved methods and record each movement path for later review.
Persistence	Use controlled persistence methods that do not destabilise systems and can be removed cleanly after the exercise.
Objective execution	Simulate access to sensitive data, execute the agreed mission objective or capture planted flags without causing destructive harm.
Documentation and debrief	Maintain a detailed time stamped activity log and provide offensive findings to the White Team during the debrief.

Approved tooling may include Kali Linux, Metasploit and related security testing tools used within the Rules of Engagement.

Where useful, pre prepared PCAP files may be loaded into the SIEM so the Blue Team can practise detection against known patterns.

The Red Team must stop immediately if instructed by the Incident Manager or White Team.

8.4 Blue Team Playbook

The Blue Team playbook defines the defensive services, workflows and evidence handling steps used during detection, response and recovery.

Service	How It Supports the Response
Log collection and SIEM monitoring	Collects and correlates system, network and application logs to identify suspicious behaviour and support triage.
Threat detection	Uses detection rules, ATT&CK mapping and analyst review to identify malicious activity such as suspicious logons, PowerShell use or scanning.
Incident analysis	Scopes affected hosts, validates alerts and determines severity and likely impact.
Containment and response	Isolates hosts, resets credentials, blocks indicators and removes malicious artefacts in a controlled way.
Forensics and evidence gathering	Collects memory, disk and other artefacts using approved forensic tools while preserving integrity.
Remediation and recovery	Restores systems from clean states, validates functionality and confirms monitoring is back in place.
Reporting and documentation	Maintains the incident record, status updates and final incident reporting.

The Blue Team follows the NIST style cycle of detection and analysis, containment, eradication, recovery and post incident activity.

Short term containment must be separated from longer remediation so evidence is not lost by accident.

Evidence must be hashed where possible, stored securely and tracked through a clear chain of custody.

8.5 Observer Checklist and Exercise Control

The Project Manager acts as the White or Purple Team observer and uses a checklist to confirm whether the Blue Team followed process, whether the Red Team stayed within scope and whether escalation, reporting and evidence handling occurred at the right time. This gives the exercise a fair and structured review path.

9. Sector, Jurisdictional and National Incident Response Arrangements

<the client> is responsible for managing incidents affecting its own environment. Where support or reporting is needed, the organisation coordinates through the Incident Manager, the Chief Security Officer and any required legal or compliance support. For significant cyber incidents, <the client> may seek advice or assistance from the Australian Cyber Security Centre. If criminal activity is suspected, referral to law enforcement may also be considered.

National support may include reporting significant cyber incidents to the ACSC and following triage or support advice.

Jurisdictional reporting or police liaison must be coordinated through authorised management channels, not handled ad hoc by technical staff.

Where privacy or contractual notification issues may apply, legal or compliance review should occur before external notices are issued.

10. Incident Notification and Reporting

Internal notification starts as soon as an incident is suspected. External notification depends on the nature of the incident, likely harm, affected systems and any contractual, regulatory or insurance requirement. <the client> uses approved role titles and decision points rather than leaving reporting to individual responders.

Trigger	Notify	Responsible Role	Timing
Critical or High severity cyber incident	Chief Security Officer and sponsor	Incident Manager	Immediately after initial classification
Significant cyber incident requiring national advice or support	Australian Cyber Security Centre	Chief Security Officer or delegate	As soon as significant impact or serious compromise is confirmed
Possible eligible personal information breach	Privacy and legal review, then OAIC process if required	Legal or compliance support with CSO approval	As soon as facts suggest serious harm may be likely
Incident affecting a managed service or supplier	Relevant service provider or partner contact	Incident Manager	When external coordination is required for containment or recovery
Cyber insurance relevant event	Insurer or broker	Chief Security Officer	Early in the incident where policy conditions may be triggered
Customer or stakeholder service impact	Affected stakeholders through approved channels	Communications Lead with CSO approval	When facts are stable enough to support a clear message

11. Detection, Investigation, Analysis and Activation

Incidents may be detected through user reports, SIEM alerts, endpoint protection events, firewall or IDS logs, authentication anomalies, packet captures, service provider notifications or observer identified issues during exercises. The Blue Team Lead performs the initial triage and the Incident Manager confirms activation when the incident exceeds business as usual handling.

11.1 Incident Classification

Severity	Typical Indicators	Minimum Response

Critical	Severe business impact, important systems unavailable, high confidence data loss risk, active lateral movement or major loss of control.	Immediate CIRT activation, CSO notification, frequent situation reporting and recovery planning from the outset.
High	Important systems affected, credible risk to sensitive data, material service degradation or broad attacker activity.	CIRT activation, sponsor update, controlled containment and formal evidence handling.
Medium	Limited system impact, contained malware or suspicious behaviour requiring structured investigation.	Managed through the incident process with Incident Manager oversight and clear review points.
Low	Minimal impact or a small event that still requires recording and validation.	Handled through standard triage with documentation and de escalation if resolved.

11.2 CIRT Activation

The CIRT is activated for any Critical or High incident and for any Medium incident that shows potential for spread, sensitive data impact, business disruption or management attention. Activation includes naming the Incident Manager, opening the incident log, confirming communication channels, assigning task owners and confirming evidence preservation requirements.

11.3 Investigation Questions

What is known so far and how was the event detected?

What systems, accounts, services or users appear affected?

What was the likely initial access method?

Is privilege escalation or lateral movement suspected?

Has data been accessed, altered, encrypted or exfiltrated?

What evidence is available now and what could be lost if action is delayed?

What containment actions are safe right now and what approvals are needed?

What is the current business impact and could it get worse quickly?

11.4 Escalation and De-escalation

Severity	Escalation Trigger	De-escalation Trigger	Minimum Authority
Critical	Confirmed major business impact, widespread compromise or serious data risk	Impact reduced and stable evidence supports High classification	Chief Security Officer
High	Spread beyond initial scope, important service disruption or strong data risk	Containment is stable and impact reduced to a managed operational level	Incident Manager
Medium	Clear business impact, confirmed compromise or failed initial containment	Evidence shows limited impact and no ongoing compromise	Blue Team Lead with Incident Manager oversight
Low	New evidence increases impact or confirms compromise	False positive or trivial issue confirmed and documented	Blue Team Lead

12. Containment, Evidence Collection and Remediation

12.1 Containment

Containment must reduce harm without destroying useful evidence or creating unnecessary outage. Short term containment may include isolating hosts, blocking indicators, disabling accounts or restricting access. Longer

term containment may include patching, rebuilds, credential resets, network segmentation or configuration changes once evidence has been secured.

12.2 Documentation

Every material action must be recorded in the incident log with time, owner, rationale and outcome. High and Critical incidents should also use a formal situation report. It sounds simple, but this is often where teams fall apart if they rush.

12.3 Evidence Collection and Preservation

Record who collected each item, when it was collected and where it came from.

Capture volatile evidence early when safe to do so, including memory, live connections and active processes where relevant.

Preserve host logs, SIEM events, firewall logs, packet captures, screenshots, configuration files and investigator notes.

Hash acquired artefacts where possible and record storage location and access history.

Maintain chain of custody for any evidence that may support formal review, insurance handling or legal follow up.

12.4 Remediation Action Plan

After containment and evidence capture, the Incident Manager develops a remediation action plan that lists required fixes, owners, deadlines, dependencies and validation steps. Recovery priorities should follow business impact, not simply technical convenience.

13. Recovery

Recovery focuses on safe restoration of services, validation of system integrity and controlled stand down. Systems should only return to normal operation after the responsible owner and Incident Manager confirm the service is functioning, monitored and trusted enough to go live again.

Recovery Check	Expectation
Service restoration	Systems are restored in approved order based on business impact and dependency mapping.
Validation	Logs, configurations, access controls and monitoring confirm the system is stable and not obviously compromised.
User communication	Affected users receive clear guidance about service status, workarounds and any required account actions.
Stand down	The CIRT stands down only after containment is stable, important recovery tasks are complete and the sponsor has visibility of residual risk.

14. Learn and Improve

Every incident or exercise event that activates this plan must result in some level of review. High and Critical incidents require a formal post incident review chaired by the Project Manager or delegate. The review should capture what happened, what worked well, what slowed the team down and what needs to change in the IRP, playbooks, monitoring or training program.

Track improvement actions in an action register with owners and due dates.

Review whether MTTD, MTTR and detection coverage improved or declined.

Update playbooks when repeated confusion or missed steps are found.

Retest important changes through tabletop review, purple team validation or a future controlled exercise.

Provide targeted training where weak documentation, handover or evidence handling is identified.

Annex A. Incident Severity Matrix

Factor	Low	Medium	High	Critical
Availability	Minor or temporary effect on one non critical service	Noticeable disruption to limited business activity	Major disruption to important services	Critical services unavailable or the organisation cannot operate normally
Confidentiality	No sensitive data involved	Possible exposure of low sensitivity data	Likely exposure of important or sensitive data	Confirmed exposure or high confidence risk to sensitive or regulated data
Integrity	Minor unauthorised change with easy rollback	Limited compromise of data or configuration	Material compromise of trusted records or admin settings	Widespread compromise of trusted data, identity or control
Response level	Standard triage and logging	Managed incident process	Formal CIRT activation	Immediate full activation and executive oversight

Annex B. Key Investigation Questions

What is the incident type and what evidence supports that view?

Which users, systems, services, logs and artefacts are in scope right now?

How did the incident start and when did it likely begin?

Is the actor still active, and what access do they appear to hold?

What indicators can be searched across the rest of the environment?

What evidence is most time sensitive to collect first?

What is the likely business impact if no further action is taken in the next hour?

What does the team need to tell the sponsor or affected stakeholders now?

Annex C. Incident Log Fields

Field	Purpose
Incident ID	Unique case reference
Date and time opened	Starting point for tracking and metrics
Reporter	Who raised the event or alert
Incident type	Working classification of the event
Severity	Low, Medium, High or Critical
Summary	Short plain language description
Systems affected	Assets, services, accounts or data in scope
Actions taken	Chronological record of decisions and response activity
Current owner	Role or person responsible for next action
Status	Open, contained, recovering, closed
Next update time	Control point for communications and coordination
Closure notes	Outcome, lessons and required follow up

Annex D. Evidence Register Fields

Field	Purpose
Evidence item ID	Unique item reference
Description	What the item is
Source	System, host, account or location collected from
Collected by	Person or role who collected the item
Date and time collected	Supports chronology and integrity
Hash value	Integrity verification where applicable
Storage location	Where the item is held
Handled by	Chain of custody tracking
Notes	Context, sensitivity or handling constraints

Annex E. Observer Checklist Criteria

Scenario Phase	Red Team Check	Blue Team Check	Observer Focus
Preparation	Uses only agreed software and methods	Initial logging, Sysmon, backups and monitoring are ready	Baseline readiness and scope control
Reconnaissance	Recon and password spray stay within approved targets	Blue Team detects and responds to suspicious login or scanning activity	Time to detect and quality of triage
Initial access	Foothold gained through an approved vector	Blue Team detects the new access or exploited service	Containment timing and decision quality
Privilege escalation	Escalation uses an approved technique	Blue Team identifies or blocks escalation behaviour	Rule tuning and investigative depth
Credential harvesting	Credential access is documented accurately	Blue Team identifies dumping, ticket abuse or related indicators	Detection coverage and evidence quality
Lateral movement	Movement methods remain in scope and are logged	Blue Team detects and contains remote execution or movement between hosts	Spread control and response coordination
Persistence and objective	Persistence and flag capture are controlled and documented	Blue Team finds persistence or delays the final objective	Whether the plan works under pressure
Debrief	Red Team provides a full activity log	Blue Team provides evidence and timeline records	Lessons learned and action quality

Annex F. Exercise Resources

Resource Category	Required Resources

People	Project sponsor, project manager, incident manager, Red Team Lead, Blue Team Lead, Communications Lead, Forensic Analyst, QA Lead, systems support and optional external advisor.
Lab infrastructure	Approved TryHackMe environment, target systems, test accounts, segmented network paths and recovery snapshots where available.
Monitoring and defensive tools	Firewalls, IDS or IPS, endpoint protection, SIEM or central log collection, packet inspection and incident case logging.
Offensive tooling	Kali Linux, Metasploit and related approved security testing tools used under the Rules of Engagement.
Forensic and evidence tooling	Volatility, KAPE, Velociraptor, Autopsy, hashing tools, secure storage and evidence templates.
Communications	Email, collaboration channel, phone, SMS path, meeting bridge and status report template.
Time	Time for planning, execution, review, remediation tracking and final documentation.

Annex G. Situation Report Fields

Field	What to Include
Overall status	On track, at risk or off track, plus a short explanation of current incident or exercise health.
Work completed this period	Key response actions, completed investigations, evidence captured and controls applied.
Work planned next	Next response steps, validation tasks, recovery work or review actions.
Issues and risks	Current blockers, operational risks, tool gaps or dependencies that may affect the response.
Decisions required	Approvals or management calls needed and the date they are required by.
Additional notes	Important observations, scope changes, stakeholder reminders or coordination notes.
Attachments	Incident log, evidence summaries, screenshots, minutes or technical artefacts attached to the update.

Annex H. Playbook Summary and Process Map

Playbook or Artefact	Where It Fits	Primary Owner
Rules of Engagement	Preparation and exercise control before activity begins	Project Manager
Red Team Playbook	Controlled adversary planning and execution	Red Team Lead
Blue Team Playbook	Detection, analysis, response and reporting	Blue Team Lead
Observer Checklist	Live oversight and final review	White Team Lead
Situation Report	High and Critical incident communications	Communications Lead
Incident Log	Whole of incident timeline and record keeping	Incident Manager

Evidence Register	Evidence collection and preservation	Forensic Analyst
Remediation Action Plan	Containment through recovery	Incident Manager
Post Incident Review	Learn and improve phase	QA Lead