

TECHNICAL PRODUCT BRIEF

Incident response readiness review

Make your incident response plan usable under pressure.

Why customers use this service

Review plans, roles, access, evidence sources and decision paths through representative scenarios to identify gaps that could delay containment, investigation or recovery.

What we assess

Roles and authority	Decision ownership, escalation and emergency authority.
Plans and playbooks	Practical guidance for representative incident types.
Detection and escalation	Triggers that move an event into coordinated response.
Technical access	Availability of systems, tools and emergency credentials.
Evidence readiness	Logs, timelines and preservation arrangements.
Communications	Internal, customer, supplier and adviser coordination.
Containment and recovery	Executable actions, dependencies and restoration priorities.
Exercises and improvement	Scenario walkthroughs, recorded gaps and owned actions.

Engagement outcome

A readiness report with scenario results, material gaps, accountable actions and a prioritised improvement roadmap.

[How the engagement works](#)

How we test or review

Damocles reviews plans and evidence, interviews decision owners and responders, and observes a tabletop or simulation when included. Document presence, exercise performance and technical validation are reported distinctly; no exercise creates uncontrolled production impact or legal conclusions.

Testing and review perspectives

Plan and evidence reviewer

Compares plans, playbooks, contact paths and technical prerequisites with representative incident scenarios.

Included when: Used to assess documented readiness and evidence availability.

Access: Current plans, playbooks, inventories, retention settings and prior improvement records.

Limitations: Document presence does not prove responders can execute the procedure.

Incident commander or decision owner

Walks through authority, severity decisions, escalation and business trade-offs during interviews or exercises.

Included when: Used where decision governance and command responsibilities are in scope.

Access: Named role holders, delegation rules, decision matrix and escalation thresholds.

Limitations: Interview or exercise decisions do not prove performance during a real crisis.

Technical responder

Demonstrates access to evidence and explains containment and recovery actions for the scenario.

Included when: Used to validate technical dependencies beyond document review.

Access: Representative tooling access, logs, response procedures and system-owner participation.

Limitations: No uncontrolled containment or recovery action is performed in production.

Exercise participant and observer

Responds to approved injects while Damocles records decisions, timing, communication and unresolved dependencies.

Included when: Used when tabletop or simulation activity is included.

Access: Participants, scenario, inject schedule, exercise rules and observation access.

Limitations: Exercise performance is scenario-specific and is not a prediction of every incident.

Customer access or evidence typically required

Current plans, playbooks, inventories, retention settings and prior improvement records.; Named role holders, delegation rules, decision matrix and escalation thresholds.; Representative tooling access, logs, response procedures and system-owner participation.; Participants, scenario, inject schedule, exercise rules and observation access.

What you receive

A readiness report with scenario results, material gaps, accountable actions and a prioritised improvement roadmap.

Detailed technical coverage

Plans and playbooks

What is assessed	Damocles compares incident plans and playbooks with representative scenarios, technical dependencies, owners and current operating practice.
Perspective / access	Plan and evidence reviewer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for plans and playbooks.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to plans and playbooks.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Plans and playbooks when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled plans and playbooks; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Roles and authority

What is assessed	Damocles interviews command and decision owners and walks through severity, authority, delegation and business-impact decisions.
Perspective / access	Plan and evidence reviewer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for roles and authority.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to roles and authority.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Roles and authority when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled roles and authority; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Escalation criteria

What is assessed	Damocles traces escalation criteria from event recognition through technical, executive and external handoffs.
Perspective / access	Plan and evidence reviewer. Incident plans and playbooks, the severity or classification model, escalation thresholds, role and contact matrix, representative scenarios or exercise injects, and applicable external-provider or adviser escalation paths.
Evidence	Evidence records the documented escalation trigger, responsible role, expected notification or handoff, participant decision during a walkthrough or tabletop where performed, and identified gaps or ambiguities.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies when escalation decision-making is included in a readiness review, walkthrough or exercise.

Limitations	This assesses defined and exercised escalation behaviour but cannot prove every real incident will be recognised or escalated correctly; it provides no legal advice or guarantee of regulatory notification compliance.
--------------------	--

Internal and external communications

What is assessed	Damocles walks through internal and external communication paths, contact maintenance, approvals, alternates and out-of-band channels.
Perspective / access	Plan and evidence reviewer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for internal and external communications.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to internal and external communications.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Internal and external communications when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled internal and external communications; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Technical access

What is assessed	Damocles asks responders to demonstrate access to representative security tooling, evidence stores, emergency accounts and required systems.
Perspective / access	Technical responder; Plan and evidence reviewer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for technical access.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to technical access.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Technical access when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled technical access; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Evidence preservation

What is assessed	Damocles reviews collection, chain-of-custody, time, integrity, storage and transfer procedures for representative evidence types.
Perspective / access	Plan and evidence reviewer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for evidence preservation.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to evidence preservation.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3

Applicability	Applies to Evidence preservation when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled evidence preservation; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Logging availability

What is assessed	Damocles reconciles scenario evidence needs with log sources, retention, access and known collection gaps.
Perspective / access	Exercise participant and observer. Log-source inventory, representative event identifiers, workflow records and responsible contacts.
Evidence	Source-health state, event timestamps, investigation timeline and linked action or escalation record.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Performed when the relevant telemetry and analyst or customer workflow can be observed during the review window.
Limitations	Absent or delayed telemetry prevents a detection conclusion, and observation of one event cannot prove continuous detection of all attacks.

Containment dependencies

What is assessed	Damocles walks through containment decisions, authority and dependencies for accounts, endpoints, networks, cloud services and third parties.
Perspective / access	Exercise participant and observer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for containment dependencies.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to containment dependencies.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Containment dependencies when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled containment dependencies; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Recovery dependencies

What is assessed	Damocles walks through restoration prerequisites, backups, validation, business acceptance and return-to-service decisions.
Perspective / access	Exercise participant and observer. Architecture, dependency list, monitoring view, authorised failover window and rollback owner.
Evidence	A timestamped failover observation showing state, convergence, service checks, monitoring and recovery or rollback.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Performed only when a customer-approved recovery or failover scenario, observer and rollback window are available.

Limitations	The result covers the exercised failure mode; activity stops at the rollback threshold and does not predict every compound failure.
--------------------	---

Legal and regulatory notification dependencies

What is assessed	Damocles identifies notification decision points, evidence, owners, advisers and time dependencies without providing legal advice.
Perspective / access	Exercise participant and observer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for legal and regulatory notification dependencies.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to legal and regulatory notification dependencies.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Legal and regulatory notification dependencies when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled legal and regulatory notification dependencies; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Tabletop and simulation approach

What is assessed	Damocles delivers approved exercise injects and records participant decisions, timing, communications, assumptions and unresolved dependencies.
Perspective / access	Plan and evidence reviewer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for tabletop and simulation approach.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to tabletop and simulation approach.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Tabletop and simulation approach when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled tabletop and simulation approach; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Lessons and improvement tracking

What is assessed	Damocles traces observations into owned improvement actions, due dates, acceptance evidence and subsequent review.
Perspective / access	Plan and evidence reviewer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for lessons and improvement tracking.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to lessons and improvement tracking.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3

Applicability	Applies to Lessons and improvement tracking when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled lessons and improvement tracking; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Document review versus exercise and technical validation

What is assessed	Damocles labels each conclusion as document review, interview, exercise observation or separately authorised technical validation.
Perspective / access	Exercise participant and observer. Assessment requires current plans, role holders, escalation paths, technical dependencies and exercise participation where agreed, selected specifically for document review versus exercise and technical validation.
Evidence	Evidence records the plan section, role matrix, contact path, inject, participant decision, timeline, dependency or improvement action relevant to document review versus exercise and technical validation.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Document review versus exercise and technical validation when the readiness capability is selected for document review, interview, walkthrough or exercise.
Limitations	The conclusion is limited to the sampled document review versus exercise and technical validation; evidence does not predict every incident and no legal conclusion or uncontrolled production action is provided.

Methodologies and standards

Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3 — Guides incident-response preparation, exercise analysis and improvement reporting.

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — Provides Release 5.2.0 control context only where a verified mapping is declared.

Information Security Manual June 2026 — Provides ASD ISM control context only for the declared mapping and observed behaviour.

Prudential Standard CPS 234 Information Security effective 1 July 2019 — Provides supporting regulatory context for the entity's broader control-testing program.

Prudential Practice Guide CPG 234 Information Security published June 2019 — Provides prudential guidance context without establishing compliance.

Standards and control mappings

Prudential Standard CPS 234 Information Security effective 1 July 2019 — supporting-evidence

References: CPS 234 paragraphs 35-36

Assessed: The authorised technical scope as one input to the regulated entity's systematic testing program.

Evidence: Dated scope, coverage, findings, remediation and limitations.

Applicability: Only for an APRA-regulated entity that places the engagement within its control-testing program.

Limitations: Does not assess annual program coverage, independence governance, Board reporting or obligations outside scope.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Incident response readiness review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Coverage matrix

Records coverage matrix produced from the authorised Incident response readiness review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Retest and residual-risk record

Records retest and residual-risk record produced from the authorised Incident response readiness review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Incident operating model

Records incident operating model produced from the authorised Incident response readiness review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Playbook assessment

Records playbook assessment produced from the authorised Incident response readiness review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Exercise decision timeline

Records exercise decision timeline produced from the authorised Incident response readiness review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Scope and safety limitations

- Only expressly authorised assets, identities, locations and activities are assessed.

- Higher-risk, disruptive, destructive and third-party activity requires separate written authority.
- Point-in-time evidence cannot establish continuous operation or conditions outside the engagement.

Assurance boundary

Damocles maps assessed coverage and observations to agreed objectives as traceable technical evidence. The review is not a certification, does not establish complete compliance, and does not confirm controls outside the authorised scope.

Review metadata

Owner: Technical Assurance

Last reviewed: 2026-08-10

Next review due: 2026-12-10

Scope this engagement with Damocles Security
damocles.com.au/contact

Assurance boundary

Damocles maps assessed coverage and observations to agreed objectives as traceable technical evidence. The review is not a certification, does not establish complete compliance, and does not confirm controls outside the authorised scope.

This brief supports engagement scoping. The authorised scope, rules of engagement and applicable agreement govern delivery.