

TECHNICAL PRODUCT BRIEF

Cloud security review

Validate the controls protecting your cloud environment.

Why customers use this service

Review cloud identities, configuration, networking, data services and operational controls to expose excessive access, unintended exposure and weak recovery or monitoring paths.

What we assess

Identity and privilege	Roles, policies, federation and administrative access.
Network exposure	Public services, trust boundaries and private connectivity.
Data protection	Storage access, encryption and sensitive-data exposure.
Workload security	Compute, container and serverless configuration.
Secrets and keys	Credential storage, key lifecycle and service access.
Logging and monitoring	Coverage, retention and visibility of material events.
Resilience and recovery	Backups, recovery controls and critical dependencies.
Governance guardrails	Configuration baselines, exceptions and change controls.

Engagement outcome

A prioritised cloud review with configuration evidence, affected resources, remediation guidance and validation outcomes.

How the engagement works

How we test or review

Damocles uses a read-only cloud role and platform exports to trace identity, exposure, data and administrative paths, with bounded external checks where authorised. Configuration evidence is point-in-time and is not a complete cloud compliance assessment; write actions and resilience tests require separate approval.

Testing and review perspectives

Read-only cloud configuration reviewer

Enumerates in-scope accounts, resources and policies through a read-only platform role and configuration exports.

Included when: Used for identity, network, storage, key, logging and workload configuration review.

Access: Read-only role, account or subscription inventory, regions and excluded resources.

Limitations: Point-in-time configuration does not prove continuous operation or complete compliance.

Identity and privilege-path reviewer

Traces role assignments, policies, trust relationships and administrative paths to sensitive cloud resources.

Included when: Used where cloud identity escalation or excessive privilege is in scope.

Access: Identity inventory, policy documents, role trust and representative principal context.

Limitations: Does not validate every principal, session or conditional policy unless represented.

External exposure validator

Confirms approved public endpoints, storage exposure and network reachability from outside the cloud boundary.

Included when: Used to corroborate public-exposure configuration with live observations.

Access: Approved hostnames, addresses, resources and test windows.

Limitations: Does not authorise exploitation or testing of provider-managed infrastructure.

Workload or service owner where evidence is required

Explains ownership, operational intent and remediation dependencies for sampled workloads and services.

Included when: Used when configuration cannot be interpreted without service context.

Access: Named owners, intended data classification, availability needs and operational procedures.

Limitations: Owner statements are supporting context, not proof that technical controls operate.

Customer access or evidence typically required

Read-only role, account or subscription inventory, regions and excluded resources.; Identity inventory, policy documents, role trust and representative principal context.; Approved hostnames, addresses, resources and test windows.; Named owners, intended data classification, availability needs and operational procedures.

What you receive

A prioritised cloud review with configuration evidence, affected resources, remediation guidance and validation outcomes.

Detailed technical coverage

Identity and privileged access

What is assessed	Damocles enumerates principals, roles, policies, trust relationships and privileged assignments and traces representative administrative paths.
Perspective / access	Identity and privilege-path reviewer. Assessment requires read-only cloud access, account inventory, representative resources, owners and configuration exports, selected specifically for identity and privileged access.
Evidence	Evidence records the account, principal, policy, endpoint, network, storage, key, log or workload configuration evidence relevant to identity and privileged access.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Identity and privileged access when the platform resource and responsibility are included in the read-only review.
Limitations	The conclusion is limited to the sampled identity and privileged access; findings are vendor-neutral and point-in-time; write actions, live resilience and complete compliance remain outside scope.

Public exposure

What is assessed	Damocles identifies public endpoints, addresses and resource policies and corroborates approved exposure from an external position.
Perspective / access	Read-only cloud configuration reviewer. Assessment requires read-only cloud access, account inventory, representative resources, owners and configuration exports, selected specifically for public exposure.
Evidence	Evidence records the account, principal, policy, endpoint, network, storage, key, log or workload configuration evidence relevant to public exposure.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Public exposure when the platform resource and responsibility are included in the read-only review.
Limitations	The conclusion is limited to the sampled public exposure; findings are vendor-neutral and point-in-time; write actions, live resilience and complete compliance remain outside scope.

Network controls

What is assessed	Damocles reviews virtual networks, security groups, network policy, routing and private-service boundaries against intended flows.
Perspective / access	Read-only cloud configuration reviewer. Assessment requires read-only cloud access, account inventory, representative resources, owners and configuration exports, selected specifically for network controls.
Evidence	Evidence records the account, principal, policy, endpoint, network, storage, key, log or workload configuration evidence relevant to network controls.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Network controls when the platform resource and responsibility are included in the read-only review.
Limitations	The conclusion is limited to the sampled network controls; findings are vendor-neutral and point-in-time; write actions, live resilience and complete compliance remain outside scope.

Storage configuration

What is assessed	Damocles examines storage resource access, public settings, encryption, retention and representative identity permissions.
Perspective / access	Workload or service owner where evidence is required. Assessment requires read-only cloud access, account inventory, representative resources, owners and configuration exports, selected specifically for storage configuration.
Evidence	Evidence records the account, principal, policy, endpoint, network, storage, key, log or workload configuration evidence relevant to storage configuration.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Storage configuration when the platform resource and responsibility are included in the read-only review.
Limitations	The conclusion is limited to the sampled storage configuration; findings are vendor-neutral and point-in-time; write actions, live resilience and complete compliance remain outside scope.

Key and secret management

What is assessed	Damocles reviews key and secret stores, access policy, rotation metadata, workload retrieval paths and administrative custody.
Perspective / access	Workload or service owner where evidence is required. Assessment requires read-only cloud access, account inventory, representative resources, owners and configuration exports, selected specifically for key and secret management.
Evidence	Evidence records the account, principal, policy, endpoint, network, storage, key, log or workload configuration evidence relevant to key and secret management.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Key and secret management when the platform resource and responsibility are included in the read-only review.
Limitations	The conclusion is limited to the sampled key and secret management; findings are vendor-neutral and point-in-time; write actions, live resilience and complete compliance remain outside scope.

Logging

What is assessed	Damocles reconciles required cloud log sources with enabled destinations, retention and representative event availability.
Perspective / access	Workload or service owner where evidence is required. 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	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
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.

Monitoring and alerting

What is assessed	Damocles reviews alert rules, coverage, destinations and operational ownership for selected cloud security events.
Perspective / access	Read-only cloud configuration reviewer. 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	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
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.

Workload configuration

What is assessed	Damocles examines representative workload identity, image or runtime settings, exposed interfaces, update controls and service configuration.
Perspective / access	Workload or service owner where evidence is required. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results; the record names the tested workload configuration object, path or control and its observed result.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when current configuration evidence and a representative endpoint or device are included in the review.
Limitations	A configuration snapshot cannot prove continuous enforcement across excluded nodes; validation avoids changes unless implementation work is authorised.

Data protection

What is assessed	Damocles traces classified data through selected storage, processing, transfer and deletion controls using configuration and owner evidence.
Perspective / access	Read-only cloud configuration reviewer. Assessment requires read-only cloud access, account inventory, representative resources, owners and configuration exports, selected specifically for data protection.
Evidence	Evidence records the account, principal, policy, endpoint, network, storage, key, log or workload configuration evidence relevant to data protection.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Data protection when the platform resource and responsibility are included in the read-only review.
Limitations	The conclusion is limited to the sampled data protection; findings are vendor-neutral and point-in-time; write actions, live resilience and complete compliance remain outside scope.

Resilience and recovery

What is assessed	Damocles reviews backup, replication, recovery settings and documented exercises without claiming live recovery unless observed.
Perspective / access	Read-only cloud configuration reviewer. 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	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
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.

Administrative paths

What is assessed	Damocles traces console, API, automation and emergency administrative paths to sensitive accounts and resources.
Perspective / access	Read-only cloud configuration reviewer. Named source and destination test points, expected flow matrix and a safe test window.
Evidence	Source-to-destination results linked to rule, route or boundary evidence.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when both ends of the network path and the enforcing device are owned or expressly authorised for testing.
Limitations	Results cover the tested source, destination, protocol and route; testing stops on instability and does not authorise third-party or denial-of-service activity.

Ownership and operational responsibilities

What is assessed	Damocles maps sampled resources and controls to named service owners, platform responsibilities and remediation dependencies.
Perspective / access	Workload or service owner where evidence is required. Assessment requires read-only cloud access, account inventory, representative resources, owners and configuration exports, selected specifically for ownership and operational responsibilities.
Evidence	Evidence records the account, principal, policy, endpoint, network, storage, key, log or workload configuration evidence relevant to ownership and operational responsibilities.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Ownership and operational responsibilities when the platform resource and responsibility are included in the read-only review.
Limitations	The conclusion is limited to the sampled ownership and operational responsibilities; findings are vendor-neutral and point-in-time; write actions, live resilience and complete compliance remain outside scope.

Platform-specific applicability

What is assessed	Damocles records account, subscription or project, region, service and shared-responsibility constraints for every sampled conclusion.
Perspective / access	Read-only cloud configuration reviewer. Assessment requires read-only cloud access, account inventory, representative resources, owners and configuration exports, selected specifically for platform-specific applicability.
Evidence	Evidence records the account, principal, policy, endpoint, network, storage, key, log or workload configuration evidence relevant to platform-specific applicability.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0

Applicability	Applies to Platform-specific applicability when the platform resource and responsibility are included in the read-only review.
Limitations	The conclusion is limited to the sampled platform-specific applicability; findings are vendor-neutral and point-in-time; write actions, live resilience and complete compliance remain outside scope.

Configuration review versus cloud compliance

What is assessed	Damocles distinguishes point-in-time configuration findings from broader governance, operational effectiveness and cloud compliance.
Perspective / access	Workload or service owner where evidence is required. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results; the record names the tested configuration review versus cloud compliance object, path or control and its observed result.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when current configuration evidence and a representative endpoint or device are included in the review.
Limitations	A configuration snapshot cannot prove continuous enforcement across excluded nodes; validation avoids changes unless implementation work is authorised.

Methodologies and standards

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.

ISO/IEC 27001 2022 with Amendment 1:2024 — Provides framework-level context while licensed identifiers remain withheld.

ISO/IEC 27002 2022 — Provides framework-level context while licensed identifiers remain withheld.

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

ISO/IEC 27001 2022 with Amendment 1:2024 — contextual

References: Framework-level mapping

Assessed: The scoped technical behaviour relevant to cloud security review.

Evidence: Scoped observations and coverage status that a qualified assessor may consider.

Applicability: Only when the customer confirms that the framework and environment are applicable.

Limitations: Exact identifiers and licensed text are withheld; this is not certification or a complete framework assessment.

ISO/IEC 27002 2022 — contextual

References: Framework-level mapping

Assessed: The scoped technical behaviour relevant to cloud security review.

Evidence: Scoped observations and coverage status that a qualified assessor may consider.

Applicability: Only when the customer confirms that the framework and environment are applicable.

Limitations: Exact identifiers and licensed text are withheld; this is not certification or a complete framework assessment.

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 Cloud security 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 Cloud security 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 Cloud security 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.

Cloud identity and exposure map

Records cloud identity and exposure map produced from the authorised Cloud security 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.

Cloud configuration evidence

Records cloud configuration evidence produced from the authorised Cloud security 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.

Ownership and remediation matrix

Records ownership and remediation matrix produced from the authorised Cloud security 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.