

TECHNICAL PRODUCT BRIEF

Network resilience and high availability

Validate that critical network services can recover from failure.

Why customers use this service

Review topology, dependencies and high-availability controls, then validate agreed failure scenarios to expose single points of failure and unsafe recovery assumptions.

What we assess

High-availability design	Redundancy, quorum and dependency assumptions.
Failure paths	Representative device, link and service-loss scenarios.
Routing convergence	Traffic behaviour as paths fail and recover.
State and session handling	Impact on connections and security enforcement.
Dependency resilience	Power, DNS, identity, time and management dependencies.
Monitoring and alerting	Useful status and notifications during degradation.
Recovery operations	Runbooks, authority, rollback and restoration evidence.

Engagement outcome

A resilience report with topology findings, scenario results, observed impact and prioritised recovery improvements.

How the engagement works

How we test or review

Damocles reviews topology, state synchronisation and dependencies and observes only customer-approved failover scenarios during a controlled window. Design evidence cannot prove operational recovery without an exercise, and testing stops at customer rollback criteria.

Testing and review perspectives

Failover observer

Records state, traffic, alerts and recovery during an explicitly approved resilience scenario.

Included when: Used only when live or staged failover observation is authorised.

Access: Scenario, window, success criteria, monitoring and rollback authority.

Limitations: No failover is inferred when only documents are reviewed.

Network or security engineer

Reviews topology, synchronisation, convergence, session and VPN behaviour and controls the exercise.

Included when: Used for design review and technical execution.

Access: Configurations, diagrams, status output and change plan.

Limitations: Design review cannot prove recovery timing.

Dependent service owner

Confirms service dependencies, acceptable interruption and observed business impact.

Included when: Used to interpret end-to-end resilience.

Access: Dependency map, service checks and recovery objectives.

Limitations: Sampled services may not represent every dependency.

Customer access or evidence typically required

Scenario, window, success criteria, monitoring and rollback authority.; Configurations, diagrams, status output and change plan.; Dependency map, service checks and recovery objectives.

What you receive

A resilience report with topology findings, scenario results, observed impact and prioritised recovery improvements.

Detailed technical coverage

High-availability topology

What is assessed	Damocles maps peers, links, failure domains, traffic ownership and single points of failure from diagrams and configuration.
Perspective / access	Network or security engineer. The current HA topology or architecture diagram, peer configuration, interface and link relationships, traffic ownership or active/standby model, routing and upstream or downstream dependencies, expected failure domains, and relevant service ownership.
Evidence	A topology or dependency map, peer and interface configuration or status, traffic-ownership state, identified shared dependency or single point of failure, and the configuration or status evidence supporting each conclusion.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies whenever HA topology is included in design or configuration review, whether or not a live failover scenario is authorised.
Limitations	Topology and configuration review cannot by itself prove live failover behaviour or recovery time; a live result is claimed only where a scenario is separately authorised and observed, and excluded peers, links and dependent services remain outside the conclusion.

Peer state and synchronisation

What is assessed	Damocles compares peer configuration, session and state synchronisation status and records material divergence.
Perspective / access	Failover observer. Assessment requires topology, peer status, configurations, dependencies, scenario plan, monitoring and rollback authority, selected specifically for peer state and synchronisation.
Evidence	Evidence records the configuration, status output, alert, traffic or session observation, timeline and recovery result relevant to peer state and synchronisation.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Peer state and synchronisation when the design review or explicitly approved scenario includes this failure condition.
Limitations	The conclusion is limited to the sampled peer state and synchronisation; no production failover is implied without observation; exercises stop at agreed safety and rollback criteria.

Interface and link failure

What is assessed	Damocles reviews or observes approved interface and link failure scenarios, traffic movement, alerts and recovery.
Perspective / access	Failover observer. Architecture, dependency list, monitoring view, authorised failover window and rollback owner; customer inputs must identify the approved interface and link failure targets and expected behaviour.
Evidence	A timestamped failover observation showing state, convergence, service checks, monitoring and recovery or rollback; the record names the tested interface and link failure object, path or control and its observed result.
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.
--------------------	---

Routing convergence

What is assessed	Damocles reviews or observes route withdrawal and convergence against the selected scenario and success criteria.
Perspective / access	Dependent service owner. 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.

Upstream and downstream dependencies

What is assessed	Damocles traces upstream, downstream, identity, DNS, monitoring and provider dependencies for each resilient service path.
Perspective / access	Dependent service owner. Assessment requires topology, peer status, configurations, dependencies, scenario plan, monitoring and rollback authority, selected specifically for upstream and downstream dependencies.
Evidence	Evidence records the configuration, status output, alert, traffic or session observation, timeline and recovery result relevant to upstream and downstream dependencies.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Upstream and downstream dependencies when the design review or explicitly approved scenario includes this failure condition.
Limitations	The conclusion is limited to the sampled upstream and downstream dependencies; no production failover is implied without observation; exercises stop at agreed safety and rollback criteria.

Stateful session continuity

What is assessed	Damocles assesses expected stateful-session handling and records continuity only when an authorised scenario is observed.
Perspective / access	Network or security engineer. Assessment requires topology, peer status, configurations, dependencies, scenario plan, monitoring and rollback authority, selected specifically for stateful session continuity.
Evidence	Evidence records the configuration, status output, alert, traffic or session observation, timeline and recovery result relevant to stateful session continuity.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Stateful session continuity when the design review or explicitly approved scenario includes this failure condition.
Limitations	The conclusion is limited to the sampled stateful session continuity; no production failover is implied without observation; exercises stop at agreed safety and rollback criteria.

VPN failover

What is assessed	Damocles reviews VPN peer, tunnel, routing and session failover and observes it only in an approved test window.
Perspective / access	Failover 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; the record names the tested vpn failover 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 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.

Power and location dependencies

What is assessed	Damocles reviews evidenced power, rack, site and carrier diversity and records shared dependencies or unverified assumptions.
Perspective / access	Dependent service owner. Assessment requires topology, peer status, configurations, dependencies, scenario plan, monitoring and rollback authority, selected specifically for power and location dependencies.
Evidence	Evidence records the configuration, status output, alert, traffic or session observation, timeline and recovery result relevant to power and location dependencies.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Power and location dependencies when the design review or explicitly approved scenario includes this failure condition.
Limitations	The conclusion is limited to the sampled power and location dependencies; no production failover is implied without observation; exercises stop at agreed safety and rollback criteria.

Monitoring and alerting

What is assessed	Damocles confirms scenario alerts, status signals, escalation paths and recovery notification using supplied monitoring evidence.
Perspective / access	Network or security engineer; Failover observer. The HA monitoring or status view, expected peer, interface, routing and service alerts, notification destinations, a representative existing event or approved scenario where available, and the responsible network or security operations contact.
Evidence	A peer, link or state alert; status-change timestamp; monitoring state before, during and after an approved scenario where performed; notification or recovery alert; and evidence showing whether the expected signal was generated.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Configuration review applies wherever HA monitoring is in scope; live alert validation applies only where a representative event or approved scenario is available.
Limitations	Sampled monitoring evidence does not prove every future failure will generate an alert; no production failure is induced solely to test monitoring unless expressly authorised, and this row does not assess SOC investigation, threat detection or attack-detection coverage.

Capacity and failure domains

What is assessed	Damocles compares capacity assumptions and failure-domain load with current evidence without generating production stress.
Perspective / access	Failover 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; the record names the tested capacity and failure domains object, path or control and its observed result.
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.

Planned validation scenarios

What is assessed	Damocles defines representative failure scenarios, prerequisites, success measures, observers and stopping conditions.
Perspective / access	Failover observer. Assessment requires topology, peer status, configurations, dependencies, scenario plan, monitoring and rollback authority, selected specifically for planned validation scenarios.
Evidence	Evidence records the configuration, status output, alert, traffic or session observation, timeline and recovery result relevant to planned validation scenarios.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Planned validation scenarios when the design review or explicitly approved scenario includes this failure condition.
Limitations	The conclusion is limited to the sampled planned validation scenarios; no production failover is implied without observation; exercises stop at agreed safety and rollback criteria.

Production safety and rollback

What is assessed	Damocles confirms rollback authority, triggers, restoration steps and post-test health checks before any live scenario.
Perspective / access	Failover observer. Assessment requires topology, peer status, configurations, dependencies, scenario plan, monitoring and rollback authority, selected specifically for production safety and rollback.
Evidence	Evidence records the configuration, status output, alert, traffic or session observation, timeline and recovery result relevant to production safety and rollback.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Production safety and rollback when the design review or explicitly approved scenario includes this failure condition.
Limitations	The conclusion is limited to the sampled production safety and rollback; no production failover is implied without observation; exercises stop at agreed safety and rollback criteria.

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.

Standards and control mappings

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — contextual

References: Framework-level mapping

Assessed: The engagement produces point-in-time technical evidence about the configured and observed security behaviour within the authorised Network resilience and high availability scope.

Evidence: Coverage status, procedure results and findings can inform the customer's control assessment and risk treatment records.

Applicability: Framework-level context is provided when the customer uses NIST SP 800-53 to organise its security control program.

Limitations: No individual NIST control is published as verified; organisational implementation, continuous operation, governance and complete catalogue coverage remain outside the engagement.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Network resilience and high availability 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 Network resilience and high availability 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 Network resilience and high availability 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.

Dependency and failure-domain map

Records dependency and failure-domain map produced from the authorised Network resilience and high availability 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.

Failover observation timeline

Records failover observation timeline produced from the authorised Network resilience and high availability 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.

Recovery and rollback record

Records recovery and rollback record produced from the authorised Network resilience and high availability 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.