

TECHNICAL PRODUCT BRIEF

Secure code review

Find security weaknesses in the code paths that matter.

Why customers use this service

Review architecture and source code to trace trust boundaries, sensitive data and security-critical functions that runtime testing may not fully expose.

What we assess

Architecture and trust	Entry points, components, identities and data flows.
Authentication and authorisation	Implementation of identity, roles and access decisions.
Input and output	Validation, injection, parsing and encoding weaknesses.
Secrets and cryptography	Credential handling, key use and security-sensitive algorithms.
Data protection	Sensitive-data storage, logging and lifecycle decisions.
Dependencies	Third-party component use and unsafe integration patterns.
Error and concurrency handling	Failure paths, race conditions and unsafe state changes.
Security observability	Events and context available for investigation and audit.

Engagement outcome

A code-referenced report with affected files or functions, practical impact, remediation guidance and validation results.

How the engagement works

How we test or review

Damocles traces security decisions through the named repositories, branches, files, functions and data flows, recording exact code locations and design assumptions. Runtime confirmation is performed only when separately included; generated code and excluded dependencies are not represented as reviewed.

Testing and review perspectives

Source-code reviewer

Traces security-relevant data and control flow through named files, functions, classes and modules.

Included when: Used for all repositories and commits included in source review.

Access: Read access to the exact repositories, branches, commits, build instructions and language context.

Limitations: Cannot establish runtime deployment or configuration that is absent from the reviewed source.

Architecture and repository reviewer

Reconciles repository boundaries and implementation with diagrams, trust assumptions, generated code and dependency ownership.

Included when: Used to define review coverage and interpret cross-component design decisions.

Access: Architecture diagrams, repository inventory, commit boundary, dependency manifests and exclusions.

Limitations: Design evidence may be stale and excluded repositories or generated artefacts remain unassessed.

Runtime-assisted reviewer where separately included

Executes narrowly scoped runtime checks to confirm selected source-level hypotheses.

Included when: Used only when runtime-assisted review is expressly authorised.

Access: A test deployment, accounts, representative data and a written list of permitted checks.

Limitations: Runtime confirmation is not implicit in source review and covers only the selected hypotheses.

Customer access or evidence typically required

Read access to the exact repositories, branches, commits, build instructions and language context.; Architecture diagrams, repository inventory, commit boundary, dependency manifests and exclusions.; A test deployment, accounts, representative data and a written list of permitted checks.

What you receive

A code-referenced report with affected files or functions, practical impact, remediation guidance and validation results.

Detailed technical coverage

Repositories, branches and commits

What is assessed	Damocles fixes the review boundary to named repositories, branches and commits and records generated, vendored and excluded content.
Perspective / access	Source-code reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for repositories, branches and commits.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to repositories, branches and commits.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Repositories, branches and commits when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled repositories, branches and commits; source review cannot prove deployment or runtime behaviour unless separately validated.

Architecture and trust boundaries

What is assessed	Damocles traces trust boundaries and data flows from architecture evidence into the files, modules and calls that implement them.
Perspective / access	Architecture and repository reviewer; Source-code reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for architecture and trust boundaries.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to architecture and trust boundaries.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Architecture and trust boundaries when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled architecture and trust boundaries; source review cannot prove deployment or runtime behaviour unless separately validated.

Authentication implementation

What is assessed	Damocles follows credential verification, MFA, recovery and session creation through the responsible functions and configuration paths.
Perspective / access	Architecture and repository reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for authentication implementation.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to authentication implementation.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Authentication implementation when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled authentication implementation; source review cannot prove deployment or runtime behaviour unless separately validated.

Authorisation enforcement

What is assessed	Damocles traces role, object and tenant checks from entry points to data access and identifies missing or client-only enforcement.
Perspective / access	Architecture and repository reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for authorisation enforcement.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to authorisation enforcement.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Authorisation enforcement when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled authorisation enforcement; source review cannot prove deployment or runtime behaviour unless separately validated.

Input validation

What is assessed	Damocles follows untrusted data through parsing, validation, canonicalisation and interpreter or query sinks.
Perspective / access	Source-code reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for input validation.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to input validation.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Input validation when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled input validation; source review cannot prove deployment or runtime behaviour unless separately validated.

Output encoding

What is assessed	Damocles traces untrusted values to HTML, URL, command, document or other output contexts and reviews the selected encoding routines.
Perspective / access	Source-code reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for output encoding.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to output encoding.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Output encoding when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled output encoding; source review cannot prove deployment or runtime behaviour unless separately validated.

Cryptographic use

What is assessed	Damocles reviews cryptographic algorithms, modes, randomness, key derivation, key custody and call-site error handling in source.
Perspective / access	Source-code reviewer. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Evidence cites the repository, commit, file, function and cryptographic API call or unsafe source-code logic.
References	Application Security Verification Standard 5.0.0
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.

Secrets handling

What is assessed	Damocles searches authorised source and configuration for embedded secrets and traces secret loading, use, rotation and logging paths.
Perspective / access	Source-code reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for secrets handling.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to secrets handling.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Secrets handling when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled secrets handling; source review cannot prove deployment or runtime behaviour unless separately validated.

Dependency use

What is assessed	Damocles reviews dependency manifests, lockfiles and security-sensitive library use and distinguishes direct code defects from dependency risk.
Perspective / access	Source-code reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for dependency use.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to dependency use.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Dependency use when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled dependency use; source review cannot prove deployment or runtime behaviour unless separately validated.

Error handling

What is assessed	Damocles follows exceptional paths to determine whether failures expose sensitive detail, bypass cleanup or create unsafe default behaviour.
-------------------------	--

Perspective / access	Source-code reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for error handling.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to error handling.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Error handling when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled error handling; source review cannot prove deployment or runtime behaviour unless separately validated.

Security logging

What is assessed	Damocles traces security event creation, sensitive-field filtering, correlation identifiers and audit integrity through logging calls.
Perspective / access	Runtime-assisted reviewer where separately included. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for security logging.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to security logging.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Security logging when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled security logging; source review cannot prove deployment or runtime behaviour unless separately validated.

Concurrency and state

What is assessed	Damocles examines shared state, locking, transactions, ordering and retry code for races, duplicate processing and inconsistent authorisation.
Perspective / access	Source-code reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for concurrency and state.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to concurrency and state.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Concurrency and state when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled concurrency and state; source review cannot prove deployment or runtime behaviour unless separately validated.

Business logic

What is assessed	Damocles traces business prerequisites, state transitions, limits and approval decisions through the functions that enforce them.
Perspective / access	Source-code reviewer. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for business logic.

Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to business logic.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Business logic when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled business logic; source review cannot prove deployment or runtime behaviour unless separately validated.

Generated code and excluded dependencies

What is assessed	Damocles records generated code and excluded dependency boundaries and checks whether reviewed source safely invokes those opaque components.
Perspective / access	Runtime-assisted reviewer where separately included. Assessment requires named repositories, branches and commits, build context, architecture evidence and explicit exclusions, selected specifically for generated code and excluded dependencies.
Evidence	Evidence records the repository, commit, file, function, class, module, data flow or call-path citation relevant to generated code and excluded dependencies.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to Generated code and excluded dependencies when the implementing source is present in the agreed commit boundary.
Limitations	The conclusion is limited to the sampled generated code and excluded dependencies; source review cannot prove deployment or runtime behaviour unless separately validated.

Source review versus runtime validation

What is assessed	Damocles distinguishes conclusions supported by repository, file and function review from hypotheses requiring separately authorised runtime validation.
Perspective / access	Runtime-assisted reviewer where separately included. The exact repository and commit boundary plus a test deployment and accounts only when selected runtime hypotheses are separately authorised.
Evidence	The finding cites the source-code location and marks runtime behaviour as observed, separately validated or not validated.
References	Application Security Verification Standard 5.0.0
Applicability	Applies to every source-review conclusion that depends on deployment state or behaviour unavailable in the reviewed code.
Limitations	Source evidence and runtime evidence are labelled separately; unexecuted code paths and excluded deployments remain unvalidated.

Methodologies and standards

Application Security Verification Standard 5.0.0 — Supports requirement-level verification only when exact ASVS 5.0.0 requirements are agreed and recorded in the statement of work and coverage matrix.

Common Weakness Enumeration 4.20 — Classifies confirmed weakness types using CWE 4.20.

Guidelines for Software Development June 2026 — Provides secure-development guidance relevant to the software procedure in scope.

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 Secure code review 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 Secure code 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 Secure code 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 Secure code 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.

Repository and branch coverage

Records repository and branch coverage produced from the authorised Secure code 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.

File and code-location findings

Records file and code-location findings produced from the authorised Secure code 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.

Design and implementation trace

Records design and implementation trace produced from the authorised Secure code 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.