

PROCUREMENT PACK

Enterprise review, with clear boundaries.

Deployment, data handling, and security review

Stition, Inc. | Winfunc

How to use this pack

A working reference for your procurement, security, and engineering review. It summarizes documented product scope and the decisions to agree for your deployment.

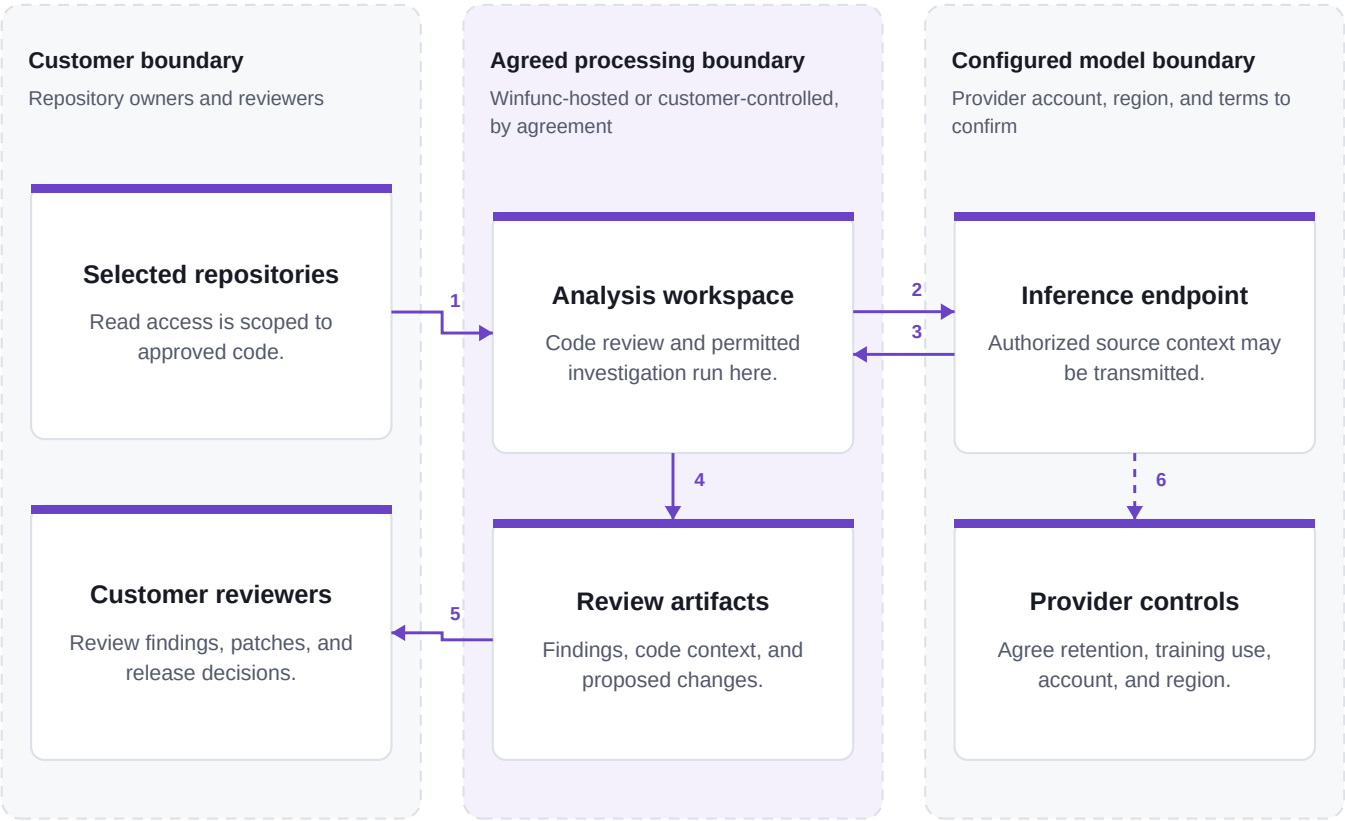
Included	Decision support
Authorize a defined scope	Choose repositories, permitted data, reviewers, test environments, and expected outputs before the pilot.
Make processing boundaries explicit	Analysis can send source context to configured model providers. Customer hosting or customer-owned model keys alone do not establish private inference or zero retention.
Review retention by data category	Working copies, caches, findings, resume state, operational records, backups, and provider data have different purposes and lifecycle requirements.
Keep approval with your team	Treat findings and patches as reviewable evidence. Confirm repository permissions, policy behavior, and verification criteria in the pilot.

Public materials and selected implementation paths were reviewed on October 4, 2026. This is not a production audit, a customer-specific architecture, or a service agreement. Signed service and data-processing terms define the purchased scope.

Prepared for review with your procurement, security, and legal teams. Assurance reports obtained separately remain subject to their access and sharing terms.

Deployment and ownership

Conceptual service flow. Choose the environment, ownership, processing region, and integration permissions in the deployment schedule.



1. Selected code
2. Authorized context
3. Analysis output
4. Review evidence
5. Reports / patches
6. Account-specific controls

Boxes illustrate responsibility boundaries, not a verified network topology or a guaranteed processing region.

Customer-controlled hosting, isolated environments, and customer-owned model credentials are enterprise options scoped by agreement [S1].

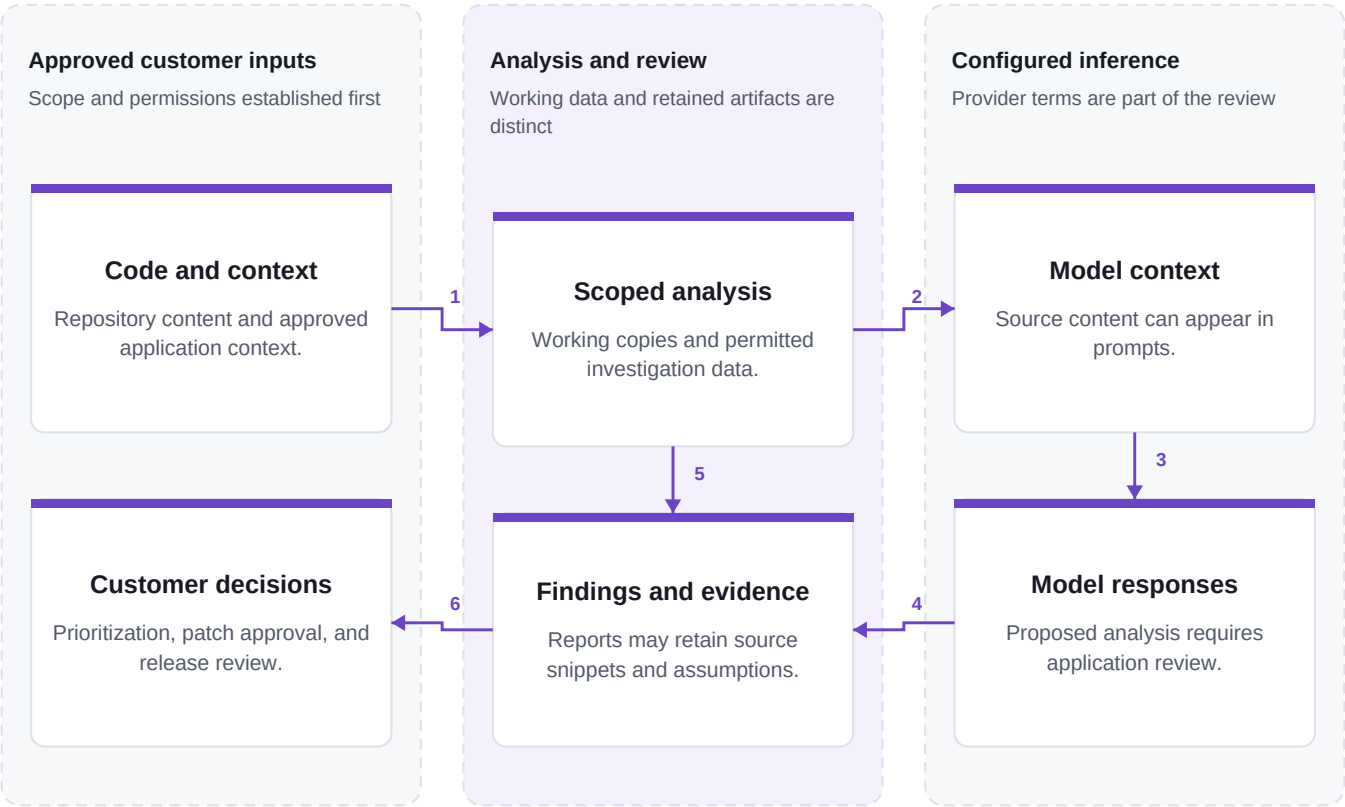
For customer hosting, assign infrastructure, upgrades, access, monitoring, backup, and deletion responsibilities explicitly.

Review any model-provider egress separately. Private hosting and private inference are different deployment decisions.

Optional pull-request and notification integrations require their own approved permissions and availability review [S2].

Data flow and purpose

Review what enters the service, what reaches the model boundary, and which outputs remain available to your reviewers.



1. Approved inputs
2. Scoped context
3. Inference
4. Proposed analysis
5. Evidence
6. Reviewable output

Some operational and resume data persist separately from the working copy. The retention table covers those categories.

Agree whether test credentials or sensitive data are permitted. Use least-privilege, scoped test accounts where credentials are required.

Source inspection corroborates context sent to an external inference service; provider selection and restrictions remain deployment-specific [S7].

Resume state, session traces, API events, and backups are separate data categories with their own access and lifecycle decisions.

Retention and deletion

Data category	Documented position	Confirm for your review
Source working copies and caches	Temporary checkout cleanup exists; source review also identified a repository mirror cache. Do not treat all source storage as transient. [S7]	Agree cache eligibility, deletion timing, failed/cancelled-job cleanup, and any deployment requirement that prohibits caching.
Findings, reports, and code snippets	Findings and reports are retained review artifacts and can contain affected code snippets. [S7] [S1]	Agree access, ownership, export, retention periods, deletion triggers, and downstream integration copies.
Resume state and agent/session traces	Recovery snapshots and local session traces can persist analysis context and transcripts. [S7]	Confirm enabled trace categories, permitted content, access, retention, and removal after completion or cancellation.
Accounts, credentials, jobs, and API events	Account and job records persist. API event metadata is distinct from other logs; encrypted onboarding credentials require configured storage controls. [S7] [S3]	Agree purpose, access, credential revocation, retention, audit export, and deletion exceptions for each record type.
Backups and recovery copies	Backup selection in reviewed source includes application/analysis records and report artifacts; actual deployment policies were not inspected. [S7]	Request backup retention and expiry, deletion propagation, restore-test evidence, RPO/RTO, and responsibility ownership.
Model-provider inputs and outputs	Analysis can transmit source context to the configured provider. Provider credentials do not determine retention or training restrictions. [S1] [S7]	Agree provider and account, subprocessors, processing region, training-use restrictions, retention eligibility, and deletion terms.

04 / SECURITY QUESTIONNAIRE

Answers with source coverage

Supplier and scope

01 Who provides Winfunc and which terms govern the purchase?

Winfunc is offered by Stition, Inc. Confirm the contracting entity and signed service schedule, MSA, and DPA. Website privacy and use terms are public references, not a substitute for service-specific commitments.

By agreement / [S5] [S6]

02 How is repository access scoped?

Repository authorization checks are present in reviewed implementation paths. Agree selected repositories, installation permissions, reviewer access, and how access is revoked before expanding scope.

Implementation evidence / [S2] [S7]

Deployment and models

03 Where will the service run?

Customer-controlled hosting and isolated-environment options are scoped by agreement. Record the selected deployment, infrastructure owner, support and upgrade responsibilities, and permitted integrations.

By agreement / [S1]

04 Can source code be transmitted outside the processing environment?

Yes. Configured model analysis can transmit source content and application context to inference services. Review provider egress, permitted data, account, processing region, and restrictions for the proposed deployment.

Implementation evidence / [S1] [S7]

05 Can we use our own model credentials?

Customer-owned model credentials are an enterprise option by agreement. Confirm supported providers, account ownership, billing, secret handling, and provider restrictions. This alone does not establish private inference or zero retention.

By agreement / [S1]

06 Is customer code used to train models?

Training-use restrictions must be agreed for both Winfunc processing and the selected provider/account. Request written provider terms and applicable controls; source inspection or customer-owned credentials cannot establish those terms.

Confirm in review / [S1] [S7]

07 Which processing regions and subprocessors apply?

Request the current deployment region, approved inference providers, subprocessor list, and data-transfer terms for your purchase. This pack does not establish a universal region or an exhaustive subprocessor inventory.

Confirm in review / [S1] [S5]

Answers with source coverage

Data lifecycle

08 Is all customer data deleted when a scan ends?

No universal immediate-deletion statement is established here. Temporary checkout cleanup differs from source caches, findings, snippets, resume state, session traces, operational records, and backups. Agree each lifecycle using the retention table.

Implementation evidence / [S7]

09 How do we request export or deletion?

Agree export formats, request ownership, deletion triggers and timelines, exceptions, provider copies, and backup expiry in the service schedule/DPA. The website privacy policy describes rights for website personal data, not a complete service deletion schedule.

By agreement / [S5] [S6]

10 What backup and recovery assurances are available?

Reviewed source includes a backup selection path. Request the deployed retention, access/encryption controls, recovery objectives, recent restore evidence, and deletion propagation. This pack does not verify operating effectiveness or a recovery SLA.

Confirm in review / [S7] [S3]

Identity and access

11 How are users authenticated and permissions checked?

GitHub-backed sessions and repository authorization are present in the inspected source paths. Review roles, installation access, administration, session invalidation, and enforcement for your proposed deployment.

Implementation evidence / [S2] [S7]

12 Are SSO and automated provisioning included?

Federated identity and lifecycle options are scoped by agreement. Confirm the identity provider, protocol, provisioning/deprovisioning behavior, and tested deployment. The inspected paths do not establish universally available SAML or SCIM.

By agreement / [S1] [S7]

13 What isolation applies to our repositories and environment?

Repository access checks are implemented in reviewed paths. Dedicated or customer-controlled environments are options by agreement. Review the actual account, network, storage, model, and administrator boundaries; repository authorization is not complete tenant-isolation evidence.

By agreement / [S1] [S7]

Protection and logging

14 How are data and access credentials protected?

Public control summaries describe HTTPS/TLS. Reviewed paths hash read-only MCP keys and support authenticated encryption for onboarding test credentials. Confirm all other token, storage, key-management, and backup protections for the deployment.

Implementation evidence / [S3] [S7]

04 / SECURITY QUESTIONNAIRE / CONTINUED

Answers with source coverage

15 Do logs contain only metadata and provide a complete audit trail?

API event metadata excludes bodies and credential headers in reviewed code, but other agent/session traces can retain transcripts. Event coverage, filtering, saturation behavior, access, retention, and export need review; no universal completeness claim is made.

Implementation evidence / [S3] [S7]

Testing and remediation

16 What authorizes testing and use of test credentials?

Agree repositories, environments, permitted actions, accounts, network boundaries, and exclusions before testing. Confirm the investigation/validation scope and credential lifecycle with your security and application owners.

By agreement / [S1] [S2]

17 Who approves patches and changes?

Winfunc prepares findings and proposed remediation for review. Agree any pull-request creation permissions separately. Your application owner should retain normal change approval, testing, verification, and release controls in the pilot and contract scope.

Documented / [S1] [S2] [S8]

Assurance and contracts

18 How do we review SOC 2 assurance?

Request the current SOC 2 report through the Trust Center and confirm the entity, system scope, audit period, exceptions, and any bridge letter. Public control summaries are not the report; its contents were not reviewed for this pack.

Confirm in review / [S3] [S4]

19 Which NDA, DPA, and regulated-data terms apply?

Confirm required confidentiality, data-processing, subprocessor, and regulated-data terms in your purchase documents. Any BAA/PHI requirements need an explicitly approved processing scope. This pack does not establish suitability for regulated data.

By agreement / [S1] [S5] [S6]

20 What incident notification and support terms apply?

Named support and response terms are contracted. Agree escalation channels, customer contacts, incident-notice obligations, response targets, and reporting expectations. The public website use terms do not establish a service-wide notice period or SLA.

By agreement / [S1] [S6]

05 / REVIEW CHECKLIST

Agree on the evidence to close

Before repository access

Review item / owner	Evidence to request / retain
Pilot confidentiality and processing terms Legal + security + Winfunc	Agree confidentiality, permitted data, provider use, and pilot data-processing terms before any repository access.
Scope and owners Customer + Winfunc	Repository inventory, exclusions, permitted actions, reviewer and application owner.
Architecture and providers Security + infrastructure owners	Approved deployment diagram, regions, provider/account, subprocessors, and egress.
Data lifecycle Privacy + security reviewers	Retention/deletion schedule for all six data categories, including providers and backups.

Before expanding the pilot

Review item / owner	Evidence to request / retain
Identity and access Identity + application owners	Permission review, revocation/deprovisioning walkthrough, isolation and admin boundaries.
Reviewable deliverables Engineering + security	Finding evidence, patch-review workflow, verified closure criteria and exceptions.
Assurance evidence Vendor risk reviewers	Current report scope/period, control exceptions, and required supporting documents.

Before signing and rollout

Review item / owner	Evidence to request / retain
Service and processing terms Legal + procurement	Signed service schedule/MSA/DPA, confidentiality and approved regulated-data scope.
Operations and recovery Operations + vendor owners	Support/escalation/notice terms, backup policy and restore evidence, hosting responsibilities.
Acceptance and ownership Sponsor + procurement	Completed pilot scorecard, acceptance criteria, operating owners, and renewal review date.

06 / EVIDENCE REGISTER

Sources and review coverage

Documented: Supported by public product or security materials; operating effectiveness is not established by this pack.

Implementation evidence: A selected implementation path was inspected; deployed configuration and end-to-end enforcement still require review.

By agreement: Availability, responsibilities, and contractual terms are confirmed for the proposed purchase.

Confirm in review: Request current evidence or agree the deployment-specific answer before granting access.

Document to request	Procurement follow-up
Current assurance report	Obtain through the Trust Center; review scope, period, exceptions, and any bridge letter.
Deployment and responsibility schedule	Confirm hosting, processing/provider boundaries, regions, and customer versus vendor responsibilities.
Data-processing and retention schedule	Record all retained categories, approved subprocessors, training-use restrictions, and deletion/backup expiry.
Access and lifecycle evidence	Review repository permissions, roles, SSO/provisioning scope, revocation, and administrative event coverage.
Pilot scorecard	Use the available blank scorecard with your own accepted findings, reviewer time, and closure evidence.

[S1] Enterprise options and commercial scope

Current public enterprise options are qualified by agreement.

<https://winfunc.com/pricing>

[S2] Integrations and workflow availability

Confirm selected integration status, permissions, and workflow scope.

<https://winfunc.com/integrations>

[S3] Trust Center control summaries

Published summaries; not an independent review of operating effectiveness.

<https://winfunc.trust.site/controls>

Sources and review coverage

[S4] Trust Center assurance access

Request current assurance reports; report contents were not inspected.

<https://winfunc.trust.site/>

[S5] Website privacy policy

Website personal-data practices and rights; service DPA still requires agreement.

<https://winfunc.com/privacy>

[S6] Website terms of use

Website terms; not a complete enterprise service agreement.

<https://winfunc.com/terms>

[S7] Selected implementation evidence

Selected implementation paths at revision 4ff82a8 were inspected read-only on October 4, 2026. Detailed supporting evidence can be reviewed with Winfunc; no production verification was performed.

[S8] Sample audit and pilot materials

Public research example and a blank pilot scorecard; not customer or production verification.

<https://winfunc.com/resources/sample-audit-report>

No customer data, private audit reports, production logs, or credentials are included in this pack.

Source inspection corroborates selected code paths, not deployment, configuration, operational effectiveness, or all execution paths.

Use the current Trust Center and agreed service documents for restricted assurance evidence and binding terms.