

ILLUSTRATED PRODUCT PROPOSAL

Sentinel Assure

Governance, risk, compliance and analysis in permission-controlled workspaces.

Prepared for organisations assessing Sentinel Assure. This is a product overview and proposed implementation approach, not a signed offer or statement of completed deployment.

Sentinel Assure is a governance and analysis application. It does not provide camera monitoring, biometric identification or drone control.

31 October 2026

Generated cover illustration. Product-specific scope and commissioning apply.

Executive overview

Governance, risk, compliance and local data analysis for audit and assurance teams.



Generated illustrative scenario; not a customer deployment.

Intended team

Audit, risk, compliance and revenue-assurance teams

Operational outcome

A traceable view of risks, controls, findings and follow-up actions.

Implementation boundary

Governance, risk, compliance and analysis in permission-controlled workspaces. Requirements depend on the chosen host, inputs, permissions and agreed integration scope.

Decision context

The organisation retains responsibility for authorised use, staff decisions, source data and commissioning. Illustrative scenarios are examples, not customer testimonials.

Users and responsibilities

Clear ownership supports accountable operation.



Generated illustrative scenario; not a customer deployment.

Super administrator

Create staff accounts and grant workspace-creation or external-analysis permissions. Business-record access still requires ownership or sharing.

Workspace owner

Manage membership, assign accountability and review assurance records.

Editor

Maintain records and follow-up actions in the shared workspace.

Viewer

Read and export authorised reports without changing records.

Operational workflow

The product follows its own recorded workflow.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Stage 1

Create a workspace and grant the right access.

Stage 2

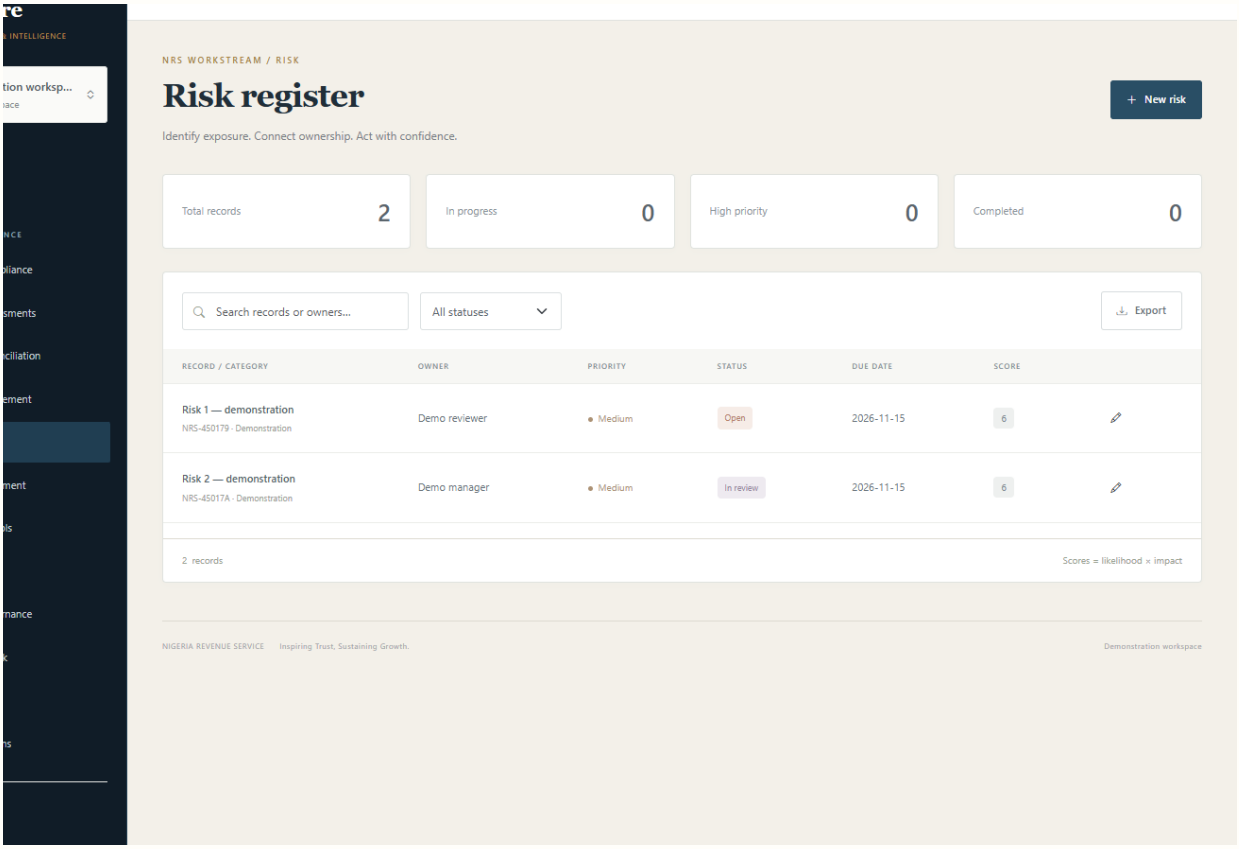
Record the risks, controls and assurance work, or connect an authorised source.

Stage 3

Analyse the evidence, assign follow-up actions and export a reviewable report.

Accountable registers

Track owners, status, priority, deadlines and evidence references for risks, audits, controls, compliance obligations and remediation. Revenue-assurance fields support the configured deployment.



Current application interface captured from the configured test system.

Operating approach

Keep the source evidence and responsible officer together. Review overdue items and record the outcome before producing the final report.

What the team reviews

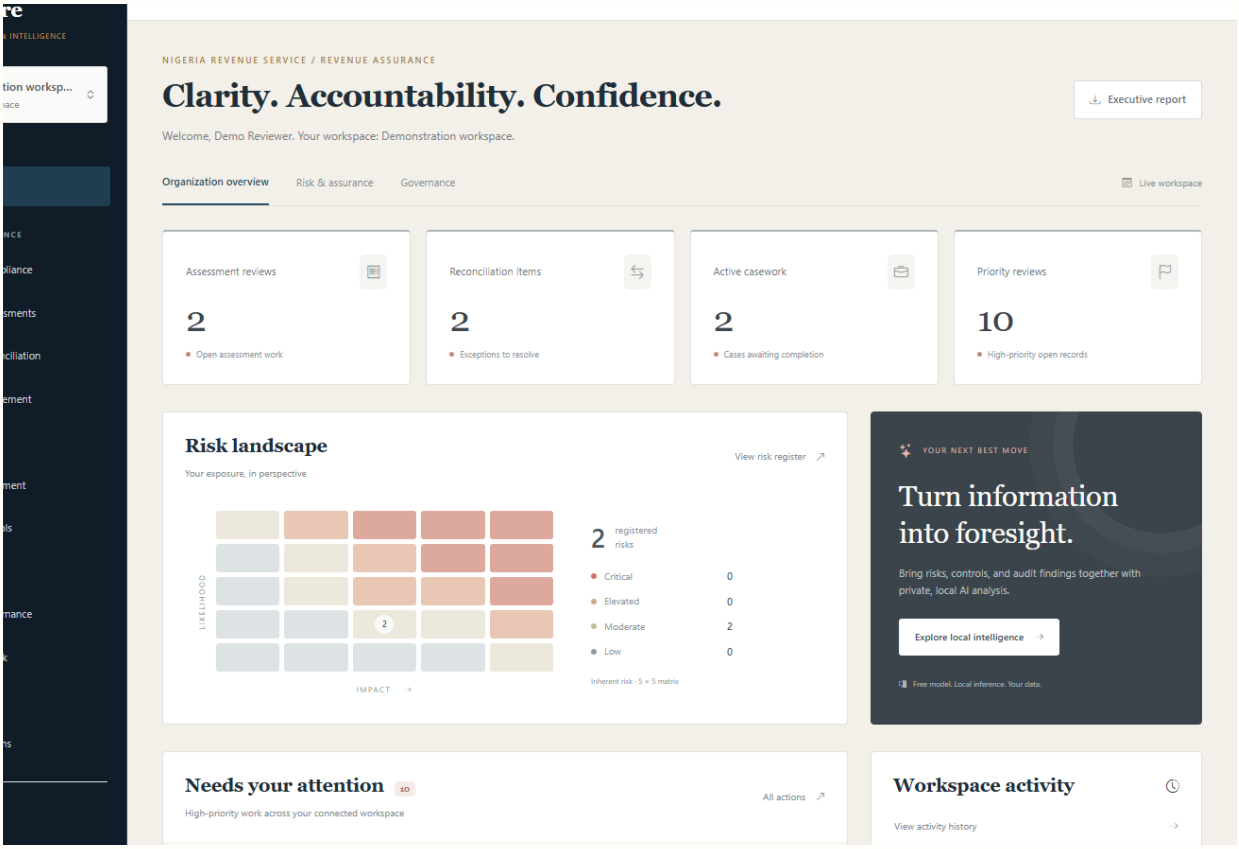
- Risk exposure uses recorded likelihood and impact.
- Remediation actions retain owners and due dates.
- Amounts under review are not independently verified collections.

Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

Workspace privacy

Owners share each workspace with the appropriate Viewer or Editor access. Staff administration does not bypass this business-record boundary.



Current application interface captured from the configured test system.

Operating approach

Workspace selection survives restarts. Server-side checks prevent stale tabs from exporting another workspace accidentally.

What the team reviews

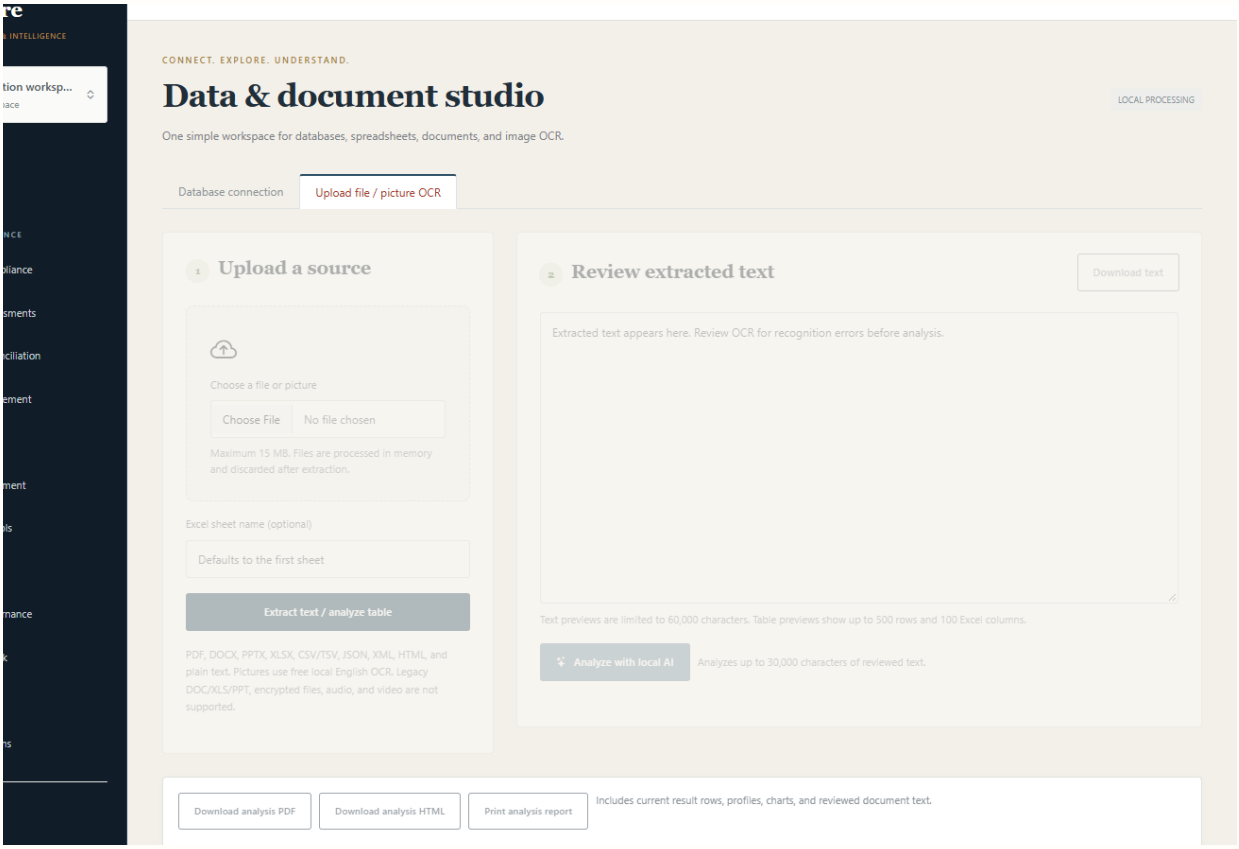
- Grant ownership or explicit membership.
- Review access when responsibilities change.
- Revoke membership when the engagement ends.

Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

Document analysis

The studio extracts supported spreadsheets, text, Office files, PDFs and common images. Image OCR uses local Tesseract resources.



Current application interface captured from the configured test system.

Operating approach

Review extraction quality and the documented size limits before interpreting text or statistics. A poor scan can change the apparent evidence.

What the team reviews

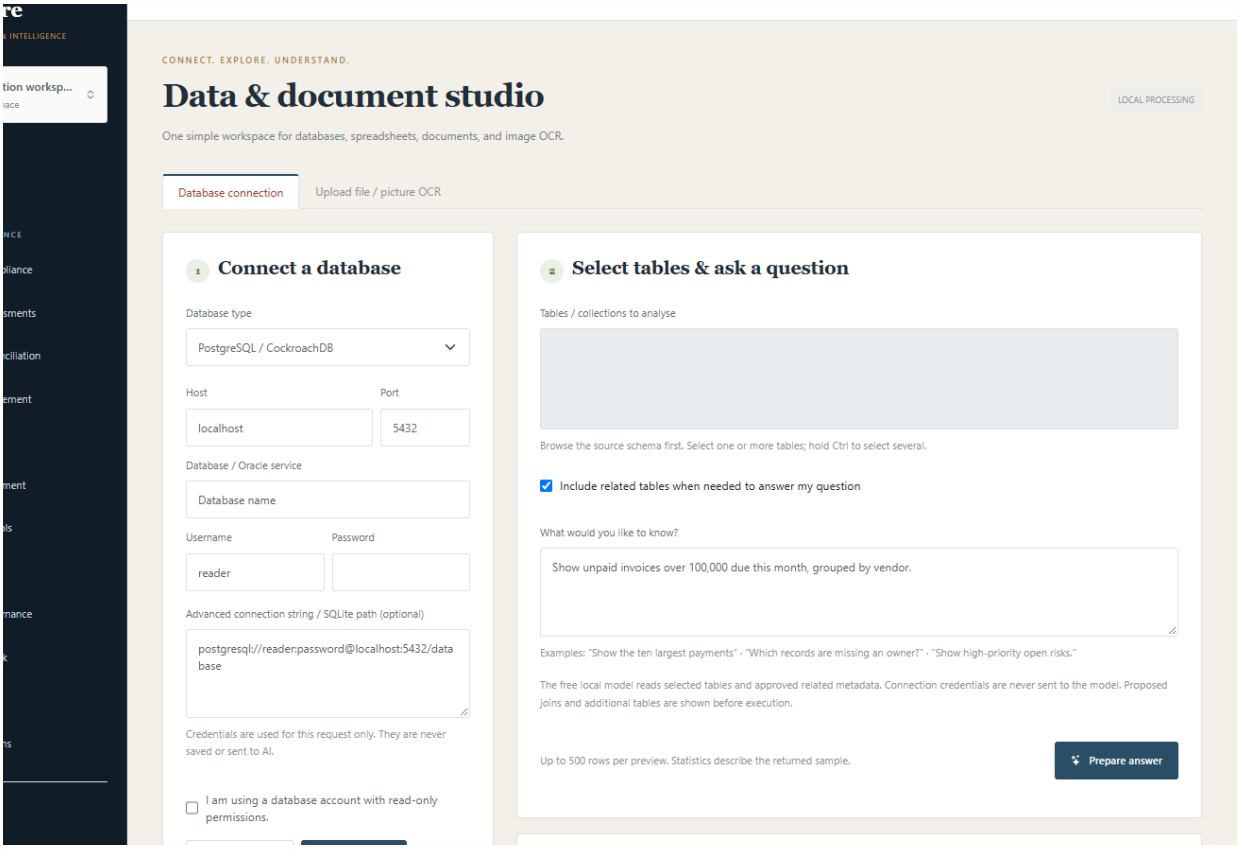
- Use supported formats and bounded samples.
- Check extracted text against the original document.
- Treat sample statistics as sample statistics.

Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

Reviewed data queries

Permitted staff can browse a bounded source schema and prepare a question using the configured database adapters.



Current application interface captured from the configured test system.

Operating approach

Staff review the proposed query before execution. Read-only source grants remain the essential data boundary, even where query validation is available.

What the team reviews

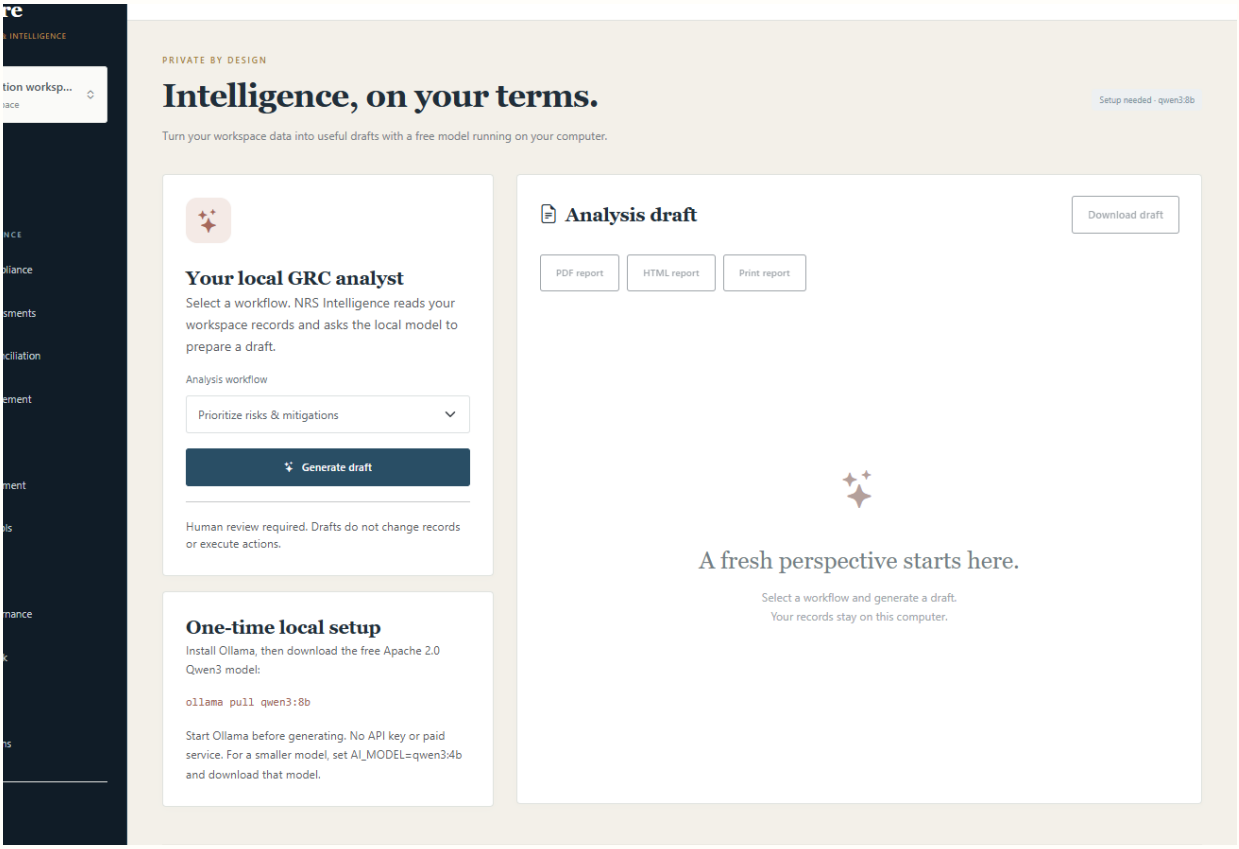
- Review inferred relationships and query intent.
- Keep credentials out of model prompts.
- Test the actual database version and dialect.

Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

Local AI assistance

Configured local Ollama models support query planning and draft observations. The resource manager supports approved model downloads.



Current application interface captured from the configured test system.

Operating approach

The model does not establish a liability, approve enforcement or change source records. Staff retain responsibility for conclusions and source review.

What the team reviews

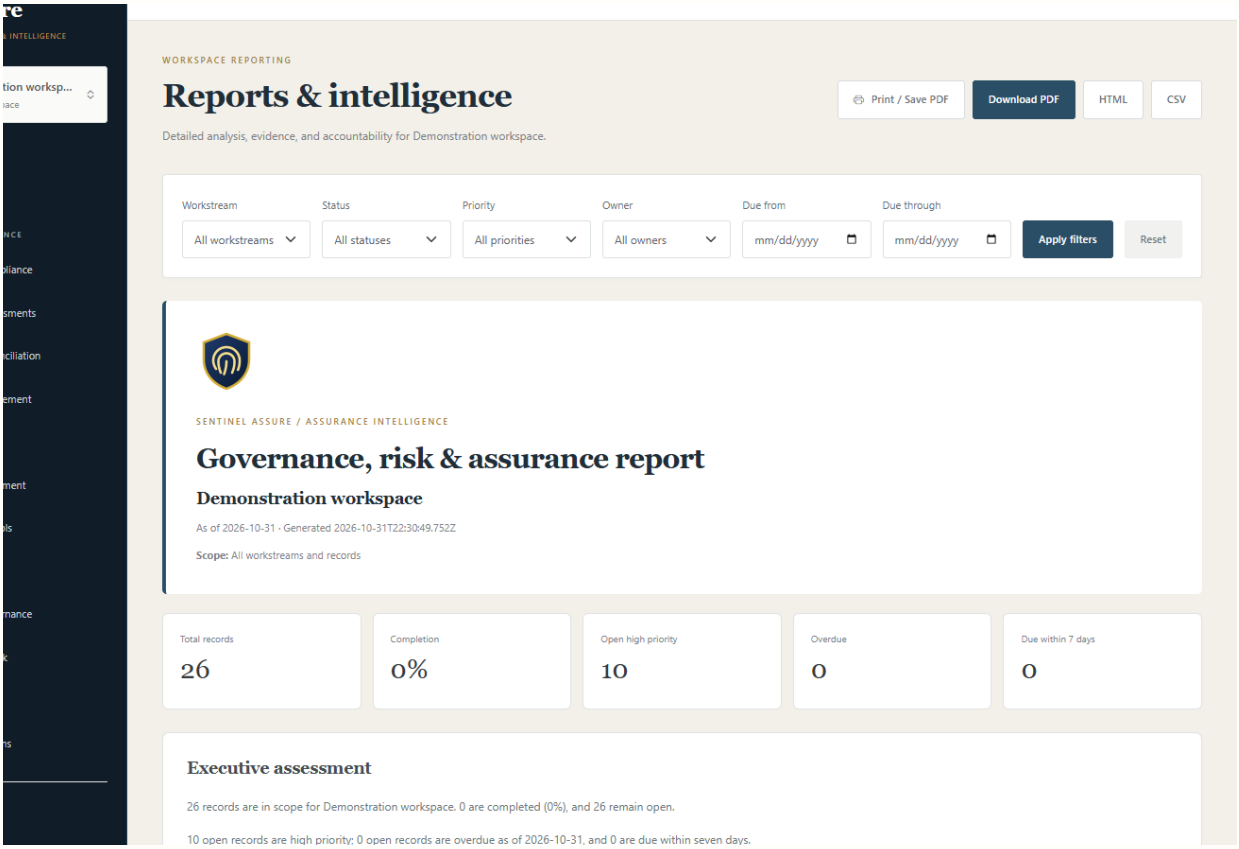
- Choose a model that fits the available host.
- Retain source context for review.
- Confirm local resources before analysis.

Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

Reports and follow-up

Reports show findings, coverage, workload, deadlines and underlying record references. Supported exports include PDF, HTML and CSV.



Current application interface captured from the configured test system.

Operating approach

Charts reflect entered records and schedules. Report readers need the workspace, filters and coverage to interpret the result.

What the team reviews

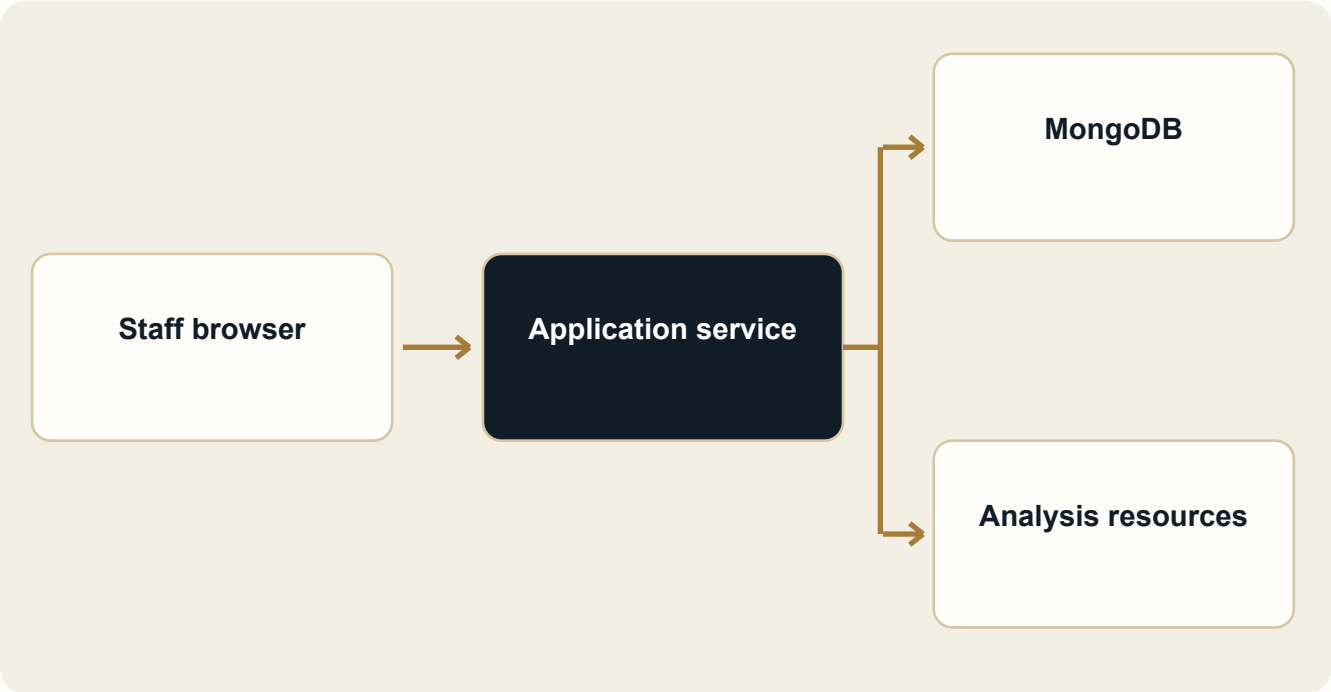
- Filter by workstream, owner and due dates.
- Use protected CSV exports for spreadsheets.
- Review overlapping amounts before summing.

Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

Architecture and information flow

Components and responsibilities for this product.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Staff browser

Authentication and explicit workspace selection.

Application service

Workspace permission checks, validation and reporting.

MongoDB

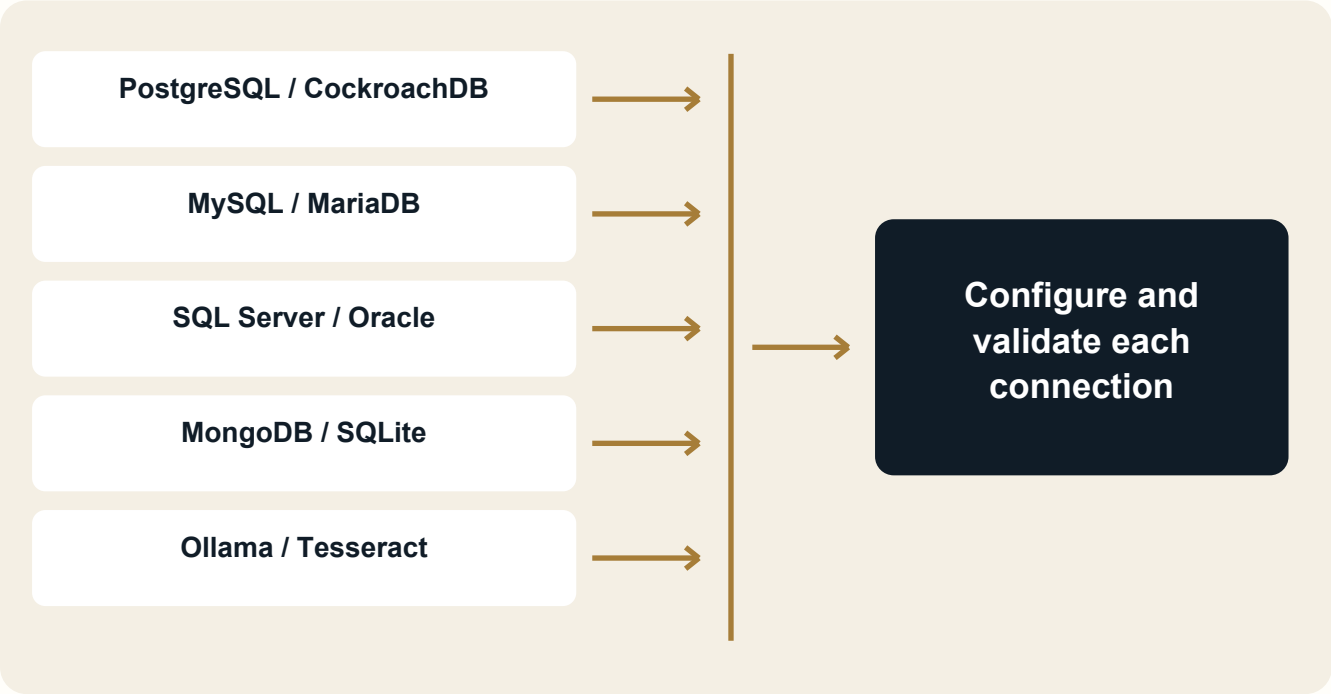
Application accounts, records and workspace membership.

Analysis resources

Approved source accounts, local OCR and configured Ollama models.

Integrations and commissioning

Each connection requires authorised configuration.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

PostgreSQL / CockroachDB

Read-only source account and permitted catalog access. Validate server version, schema scope and relationships.

MySQL / MariaDB

Configured connection and read-only grants. Review schema and query intent before execution.

SQL Server / Oracle

Supported driver and scoped source account. Source permissions and actual dialect testing remain essential.

MongoDB / SQLite

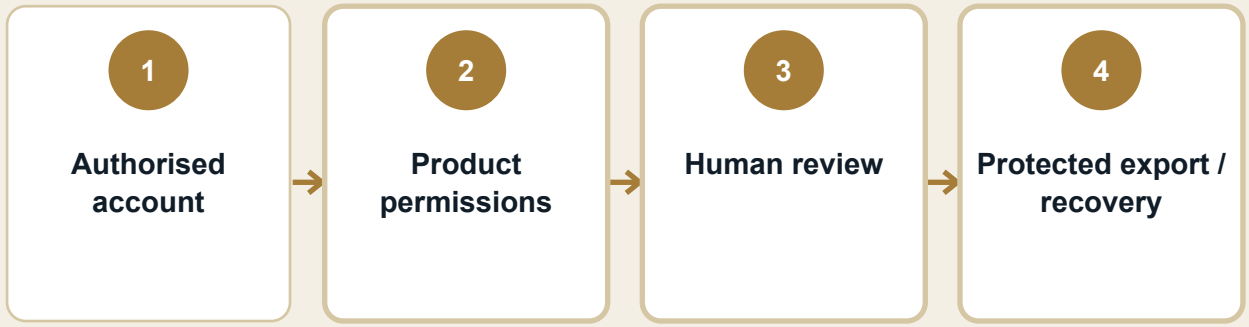
Approved collections or SQLite files within the source root. External MongoDB cannot target the application database.

Ollama / Tesseract

Local runtime, approved model weights and OCR resources. Initial provisioning may need internet; choose suitable host resources.

Security and access boundaries

Security depends on the product controls and the operating environment.



Permissions and review belong to this product's deployment.

Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Business-record boundaries

Workspace ownership and sharing apply on the server, including for administrators.

Account lifecycle

Salted password hashes, required password changes and session revocation after security changes.

Source credentials

Read-only grants and scoped query validation; credentials stay outside model prompts.

Local resources

Configured local models and OCR support controlled processing.

Host controls

Protect source directories, application data, backups and network exposure.

Reports and information handling

Reports should retain source context and operating limits.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Product outputs

- Executive findings and suggested follow-up actions.
- Status, owner workload and overdue or upcoming items.
- Risk exposure derived from recorded likelihood and impact.
- Filtered PDF, HTML and CSV with source context.

Handling responsibilities

Agree who may read, export, share and retain each output. Protect reports and media according to their sensitivity. Review the source records and filters before relying on totals or conclusions.

Illustrative workflows 1

Examples explain use; they do not claim real customer results.



Generated illustrative scenario; not a customer deployment.

An audit finding needs follow-up

An assurance team records a control weakness and supporting references. The review follows the issue to its responsible officer and recorded response.

- Record the finding, priority and evidence.
- Assign a remediation owner and due date.
- Review overdue work and export the filtered report.

Conditions: Staff must maintain source evidence and current record status.

A reconciliation exception needs investigation

An analyst reviews an authorised finance or revenue source. The query result supports an accountable investigation.

- Connect using a scoped source account.
- Prepare and review the proposed query.
- Check source rows before recording a finding.

Conditions: Read-only grants, correct relationships and a supported dialect are required.

Illustrative workflows 2

Examples explain use; they do not claim real customer results.



Local analysis assists the reviewer; it does not approve findings or alter source records.

Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

A restricted workspace needs a reviewer

An owner invites an independent staff reviewer. Read and edit permissions remain explicit.

- Grant Viewer membership.
- Review records and download the report.
- Revoke membership after the engagement.

Conditions: The reviewer needs an active account and the appropriate membership.

A scanned document needs analysis

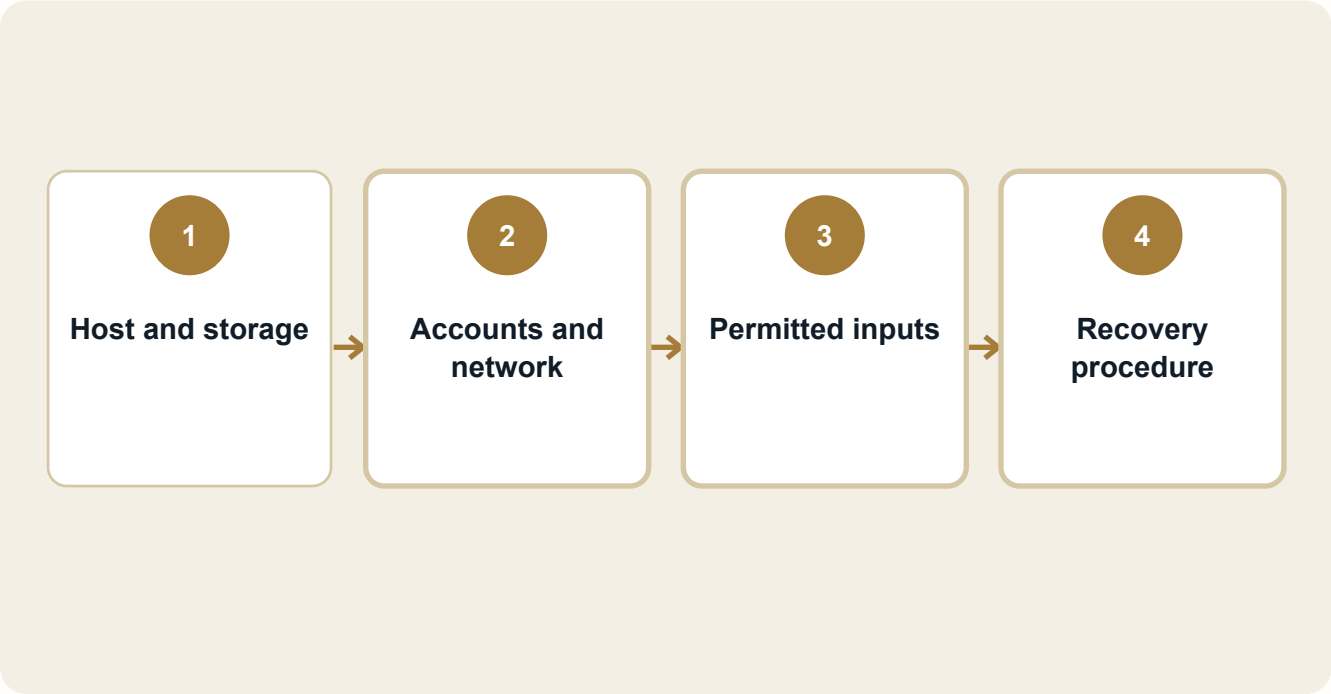
A team receives a supported spreadsheet or scanned page. Findings remain tied to supplied evidence.

- Upload the supported file.
- Review the extracted text or bounded dataset.
- Check local AI observations against the original.

Conditions: OCR quality, supported formats and processing limits apply.

Deployment prerequisites

The deployment plan must name the actual infrastructure and inputs.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Requirements

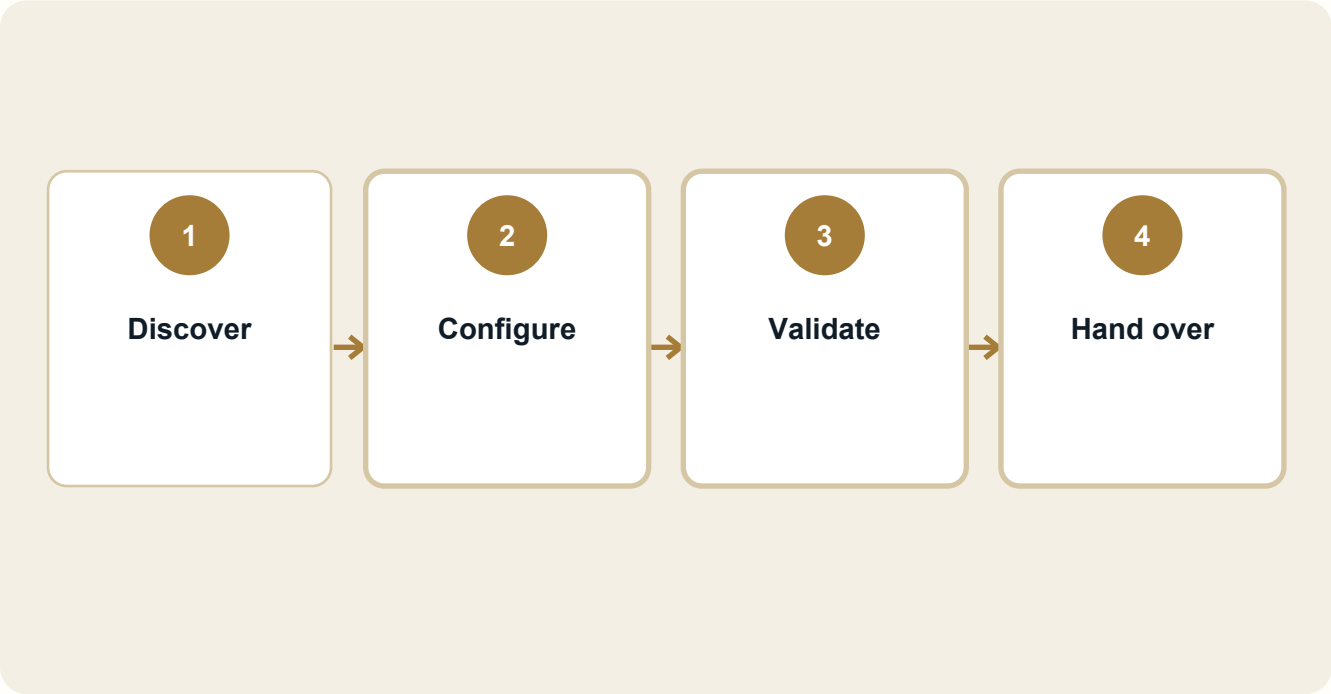
- Supported Node.js host, MongoDB and protected storage.
- Approved Ollama models if AI features are required.
- Scoped read-only accounts and network access to external sources.
- Authorised source-file root and OCR language resources.
- Agreed backup, restore and staff-administration procedures.

Capacity and dependencies

Confirm load, data size, retention, input quality, network behavior and backup needs through representative tests. The product overview does not guarantee throughput or availability.

Pilot and implementation plan

A proposed sequence to agree with the customer.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Discovery

Confirm the intended users, workflows, source systems, integrations and acceptance criteria.

Configuration

Prepare accounts, permissions, infrastructure and the required inputs. Keep any external adapters within the agreed scope.

Pilot

Exercise normal and failure cases with representative authorised data. Record defects and unresolved dependencies.

Handover

Train the responsible staff, review acceptance evidence and agree the support, maintenance and recovery process.

Acceptance and validation

Production approval requires evidence from the intended deployment.



A failed or unresolved check stays with the responsible reviewer.

Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Acceptance checks

- Unshared workspace records remain inaccessible.
- Viewers cannot create, change or delete records.
- Revoked membership and disabled accounts stop access.
- Queries remain read-only and within the approved scope.
- Unsupported files and queries fail clearly.
- Report output matches the reviewed records and filters.
- Backup recovery works on the planned host.

Sign-off record

For each check retain the owner, date, test inputs, expected result and observed result. Resolve critical failures before treating the workflow as commissioned.

Training and handover

Training should follow the roles that will use the installed product.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Administration

Accounts, permissions, source/device configuration and ongoing access reviews.

Daily operation

The product workflow, source review, exception handling and escalation.

Technical handover

Integration responsibilities, protected credentials, backup/restore and host monitoring.

Completion evidence

Record attendance, operating procedures, responsible contacts and any remaining configuration requirements.

Operations and support

Maintain the installation and the human review process.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Operational checklist

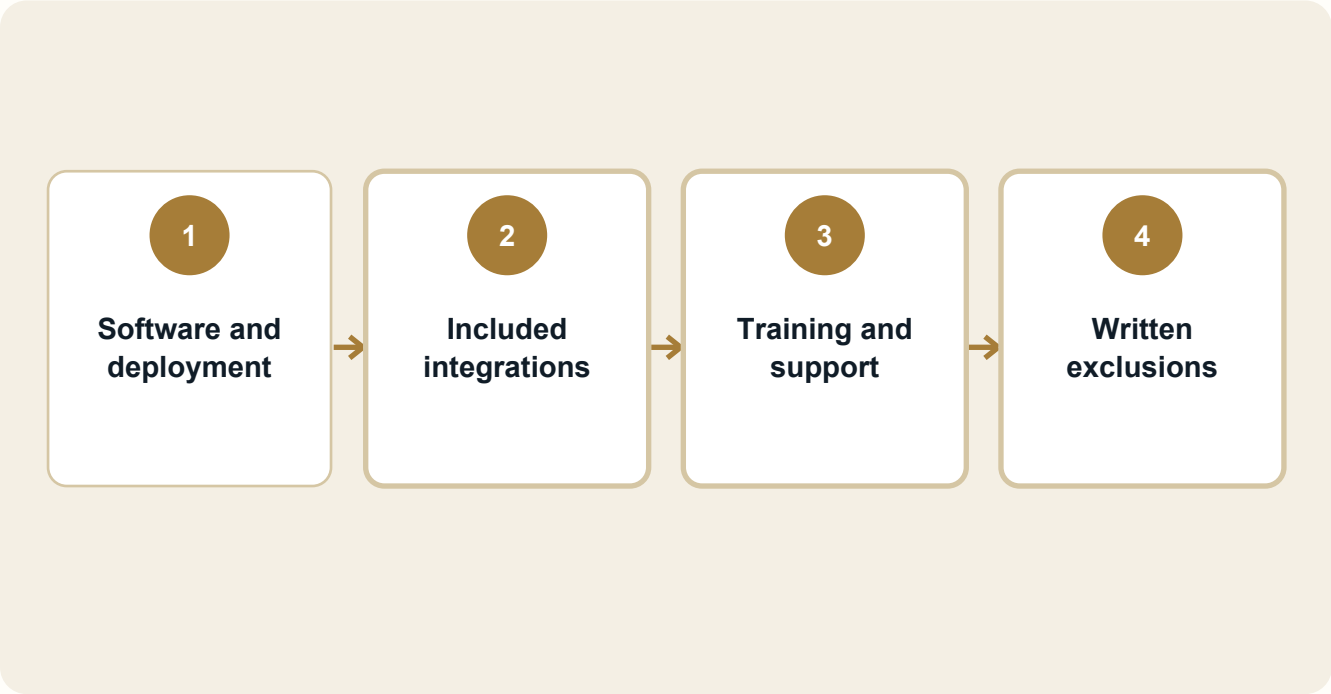
- Review membership and source privileges after staff changes.
- Maintain approved model/OCR resources and host capacity.
- Review extraction failures and rejected queries.
- Test recovery and protect exported reports.

Support agreement

Agree working hours, response targets, escalation contacts, defect/change handling, update responsibilities and any on-site requirements in the commercial agreement. No service-level guarantee is made here.

Commercial scope

A product-specific written quotation defines the offer.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Software and deployment

State the product, permitted deployment, user/usage scope and installation responsibilities.

Integration and hardware

List each included source, device, adapter, third-party licence and specialist service. Identify customer-provided hardware and excluded work.

Training and support

Specify training sessions, handover deliverables, support coverage and renewal arrangements.

Costs and changes

Confirm currency, taxes, payment milestones, travel and infrastructure costs in the quotation. New requirements need written change approval.

Questions and scope boundaries

The product remains separate from the other portfolio applications.

Ask before you deploy

Local analysis assists the reviewer; it does not approve findings or alter source records.

Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Does Sentinel Assure monitor cameras?

No. Sentinel Assure handles assurance workspaces and data analysis. Camera and building access belong to Sentinel SiteGuard.

Does AI make audit or tax decisions?

No. Staff review generated plans, source rows and draft observations.

Can an administrator read every workspace?

No. Ownership or explicit sharing is required for business-record access.

Does every database version work?

Documented adapters still need validation against actual server versions and permitted schemas.

Does document analysis support every file?

Only documented formats and processing limits are supported. OCR output requires review.

How is pricing agreed?

A separate quote covers users, hosting, sources, model resources, deployment, training and support.

Next steps and proposal review

A focused discussion before implementation.



Workflow illustration · Local analysis assists the reviewer; it does not approve findings or alter source records.

Demonstration

Review Sentinel Assure using your intended workflow and representative authorised inputs.

Scope workshop

Agree the users, infrastructure, sources, integrations and operating responsibilities.

Written proposal

Confirm deliverables, acceptance evidence, exclusions, training and commercial terms.

Source basis

Product descriptions reflect the local Sentinel Assure application README and relevant implementation documentation reviewed on 31 October 2026. Optional services and model/hardware performance require validation.

Enquiries

Use the website support form and select Sentinel Assure for a demonstration or quotation.