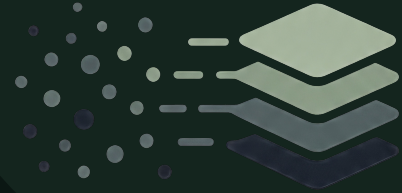


REPRESENTATIVE FINAL REPORT

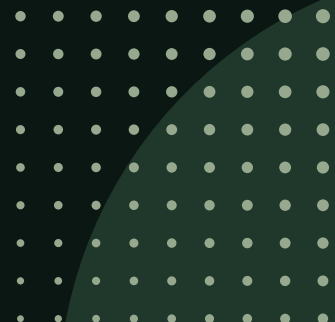


Client Handover, Training & Operating Runbook

A plain-language ownership pack explaining what the client receives, how the operating workflow is run and governed, and how access, knowledge, and responsibility are transferred.

Prepared for	Representative Construction Client
Prepared by	StructuredLayer
Workflow	Representative RFQ-to-Bid Operating Path
Document	Version 1.0 20 July 2026
Status	Illustrative client-ready sample

Illustrative records, roles, systems, dates, and procedures are used throughout. A client-issued pack contains approved environments, named owners, real access boundaries, operating instructions, evidence, open items, and signed transfer decisions.



01 / START HERE

What this handover means

Handover is the point at which the client can operate, inspect, recover, change, export, and govern the implemented workflow without relying on undocumented knowledge held by the implementation team.

Plain-language rule

The system is not fully handed over because a dashboard works. Handover is complete when the client controls the accounts and information, understands normal and exceptional operation, can remove provider access, and has the documentation required to continue safely.

Ownership

Client-controlled systems, repositories, data, documentation, access, and decision rights.

Capability

Named client roles can operate the workflow and resolve routine exceptions using the runbook.

Portability

Another qualified team can understand the architecture, records, controls, and outstanding work.

What handover does not mean

- Third-party platforms, licences, and model providers do not become client property; their own terms still apply.
- An implemented workflow does not authorise untested additions, broader AI autonomy, or changes outside the approved scope.
- Handover does not eliminate the need for monitoring, source changes, credential renewal, maintenance, or future decisions.

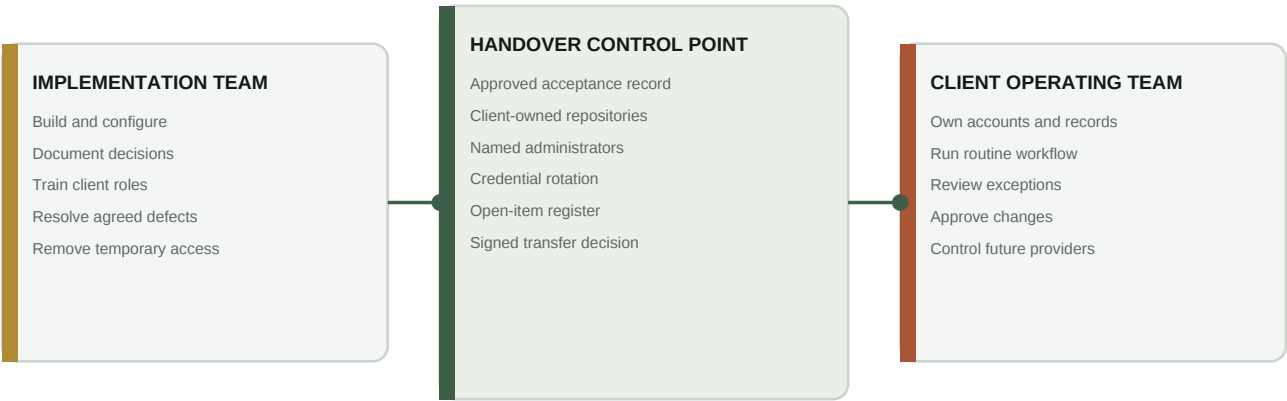
Support and maintenance after stabilisation apply only where separately agreed.

The final boundary is defined by the signed agreement, approved architecture, provider accounts, licences, security policy, and acceptance record.

02 / EXECUTIVE SUMMARY

The ownership transfer in one page

The representative implementation is transferred through an approved acceptance record, client-owned operating assets, named administrator and operator roles, training completion, open-item transfer, credential review, and removal of temporary implementation access.



Ownership is transferred through evidence, access, training, and an explicit client decision.

Transfer area	Client receives or controls	Completion evidence
Business records	Database, stable IDs, relationships, source links, exports	Client administrator access and verified export
Workflow	Stages, rules, schedules, approvals, queues, notifications	Named operators complete agreed scenarios
Integrations	Register, environments, credentials ownership, limits, disable path	Connections reviewed and ownership confirmed
Documentation	Architecture, dictionary, runbook, exceptions, tests, decisions	Issued pack stored in client repository
Security	Users, service accounts, roles, secrets process, revocation	Temporary access removed and rotation confirmed
Open work	Defects, accepted limitations, improvements, owners, dates	Signed open-item register

Executive decision

Approve final ownership transfer when the client can operate the tested scope, recover from agreed failures, control access, understand open conditions, and revoke StructuredLayer or other temporary implementation access.

03 / HANDOVER CONTENTS

The complete ownership pack

Each item has an accountable client owner and a controlled storage location. The issued pack should not depend on personal folders, temporary links, or implementation accounts.

Deliverable	Representative handover content	Client owner
Architecture record	Systems, environments, data flow, IDs, write boundaries, dependencies	Technical owner
Workflow runbook	Stages, roles, transitions, schedules, manual actions, escalation	Workflow owner
Data dictionary	Records, fields, types, authority, validation, retention, permissions	Data owner
Source-of-truth map	Approved authority, correction path, cross-system ownership	Business/data owners
Integration register	Connections, credential owner, limits, monitoring, renewal, disable procedure	IT/system owner
Exception catalogue	Failure states, queue rules, severity, owners, release conditions	Operations owner
Acceptance record	Requirements, tests, results, defects, limitations, approvals	Project sponsor
Training record	Audience, materials, attendance, exercises, questions, follow-up	Adoption owner
Open-item register	Remaining work, risk, workaround, owner, date, decision	Business sponsor
Access closure record	Accounts, roles, credential actions, revoked temporary access	Security owner

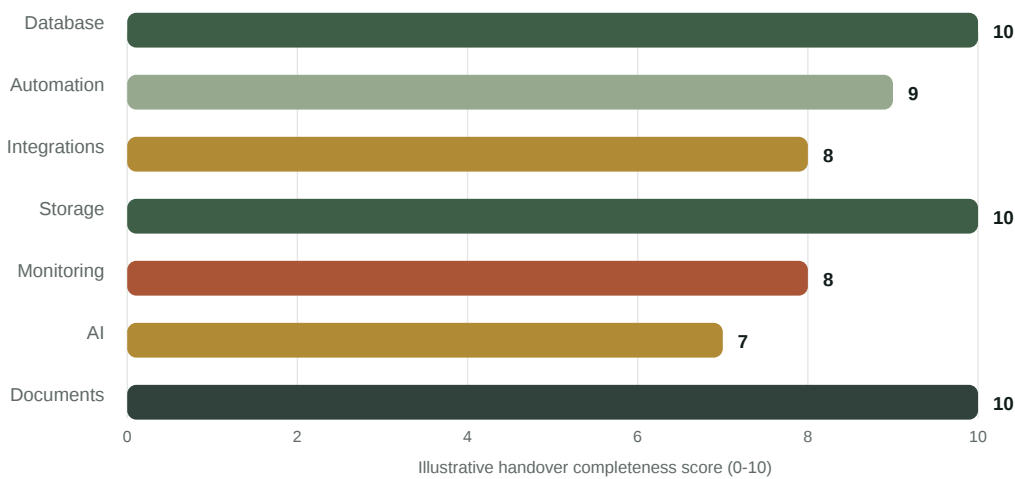
Issued PDF Readable approved record for sign-off, audit, and reference.	Editable source Client-maintainable records, registers, diagrams, and procedures.	Machine-readable export Schemas, mappings, configuration, and data exports where applicable.
---	---	--

04 / SYSTEM & ASSET INVENTORY

Know what exists, where it lives, and who controls it

The inventory separates business ownership, technical administration, provider ownership, billing responsibility, credentials, environments, data location, and the ability to export or disable the service.

Asset	Purpose and content	Client control	Handover verification
Operating database	Connected records, IDs, states, evidence, queues	Admin role and billing	Login, backup/export, restore path
Automation environment	Schedules, rules, scripts, jobs, deployment	Repository/environment owner	Run, pause, rollback, redeploy
Integration accounts	API/webhook/browser/email/file connections	Named account and credential owner	Test, rotate, revoke, disable
Document storage	Downloaded and generated files, source evidence	Storage administrator	Permissions, retention, version, export
Monitoring	Run health, failures, usage, queue alerts	Notification and dashboard owner	Trigger test and escalation
AI providers	Approved extraction, classification, retrieval, drafting	Account, keys, spend controls	Model list, limits, disable path
Documentation repository	Issued pack, editable sources, decisions, recordings	Client repository owner	Access, retention, future edit process



Illustrative readiness values only. A client pack uses verified inventory and evidence.

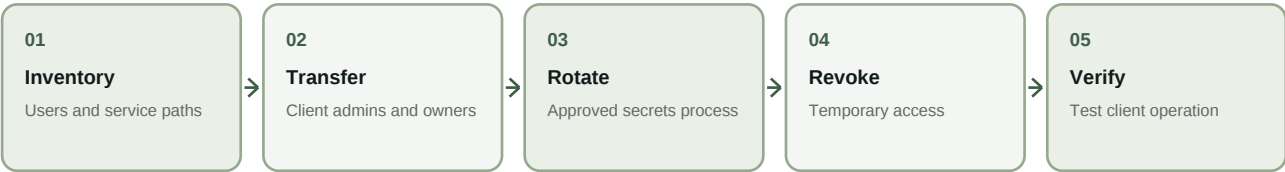
05 / ACCESS & SECURITY TRANSFER

Transfer control without exchanging credentials in documents

The handover record names account owners and required actions. Passwords, API keys, MFA codes, tokens, cookies, recovery codes, and other secrets stay inside approved credential or secret-management processes, never inside the PDF.

Control	Transfer action	Evidence retained
Named accounts	Replace shared or personal implementation identities where practical	Account list, owner, role, effective date
Administrator roles	Assign primary and alternate client administrators	Successful role test and approval
Service accounts	Confirm purpose, scope, owner, rotation, and disable process	Register entry and access test
Secrets	Move to approved vault/environment and rotate where required	Rotation confirmation, not secret value
MFA and recovery	Confirm client-controlled recovery and alternate owner	Recovery test or approved record
Temporary access	Remove implementation users, tokens, sessions, and permissions	Revocation evidence and re-test
Third-party providers	Confirm account, billing, data, region, retention, and terms	Approved provider register
Incident contacts	Name business, technical, security, and provider escalation	Current contact and response path

Access closure sequence



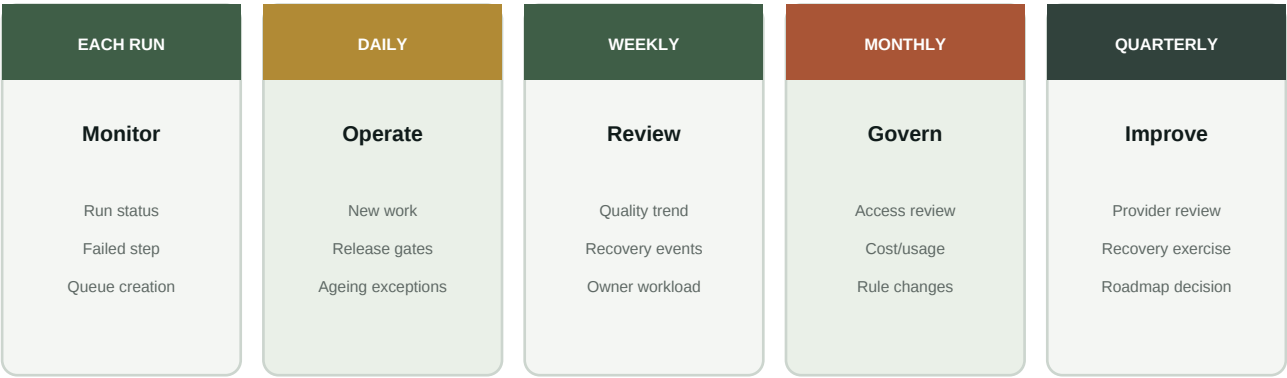
Security boundary

The handover document records ownership and completed control actions. It must never contain operational passwords, API keys, MFA secrets, unrestricted tokens, or live session information.

06 / OPERATING CADENCE

What the client team does after launch

The runbook turns system operation into a repeatable business routine. It states what should be checked, who owns the review, what normal looks like, and when an issue becomes an exception or escalation.



The client runbook defines what is checked, by whom, and what evidence is retained.

Cadence	Representative operating task	Evidence or outcome
Each scheduled run	Confirm start, completion, records processed, failures, and queue creation	Run record and exception links
Daily	Review new records, release gates, urgent deadlines, unowned and ageing items	Assigned actions and decisions
Weekly	Review data quality, recovery events, unresolved exceptions, user questions	Trend review and improvement actions
Monthly	Review access, provider usage/cost, integration limits, rule/model changes	Governance decision log
Quarterly	Test export/restore/recovery, review providers and roadmap	Exercise result and approved changes
On source change	Assess API, portal, document, email, or workflow change	Impact decision and controlled release

Operational source of truth

Notifications may arrive through email, Teams, Slack, Discord, SMS, or another approved channel. The operating database, queue, and decision history remain the governed status record.

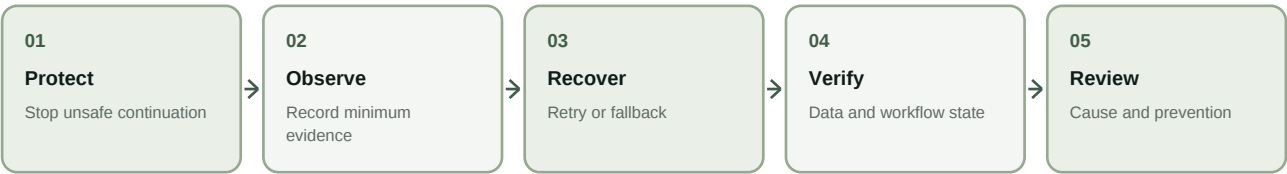
07 / EXCEPTIONS, INCIDENTS & RECOVERY

Know when to retry, continue manually, escalate, or stop

Routine exceptions remain part of normal operation. An incident is a material event involving unavailable service, repeated failure, data loss or exposure risk, unauthorised action, missed consequential deadline, or an inability to continue safely.

Condition	Immediate response	Owner and evidence
Single recoverable failure	Use bounded retry and verify result	System owner; run and recovery result
Repeated source failure	Stop after threshold; preserve state; use approved fallback	System owner; attempts, stop reason, fallback
Data conflict or uncertainty	Create review exception; do not guess controlling value	Data owner; sources and decision
Approval or permission failure	Block consequential action and notify named authority	Business/security owner; denied event
Possible data exposure	Stop affected path, preserve minimum evidence, follow client incident policy	Security owner; incident record
Missed deadline risk	Escalate workflow owner and use controlled manual continuation	Business owner; decision and action
Provider outage	Assess scope, switch approved fallback if available, communicate status	Technical owner; provider evidence
Unrecoverable full stop	Pause affected workflow and call support/escalation route	Named incident owner; timeline and decision

Recovery sequence



A recovered run is not complete until the resulting records, files, notifications, and downstream workflow state have been verified.

08 / CHANGE & RELEASE CONTROL

Future changes should not silently break the operating layer

Tools, APIs, portals, models, documents, teams, and business rules change. The client runbook defines how a proposed change is assessed, tested, approved, released, monitored, and reversed.

Change type	Impact review	Minimum release evidence
Field or status	Dictionary, validation, reports, automations, history	Approved definition, migration, tests
Workflow rule	Owners, transitions, deadlines, exceptions, approvals	Before/after map and acceptance cases
Integration or source	Identity, permissions, limits, fields, failure handling	Sandbox/test result, recovery, monitoring
Browser path	Authorised navigation, selectors, page state, downloads	Representative run, failure and fallback tests
AI model or prompt	Quality, citations, safety boundary, cost, latency, data handling	Versioned evaluation and approval
Provider or hosting	Data location, export, retention, security, billing, recovery	Migration, rollback, access, acceptance
Role or permission	Least privilege, segregation, audit, revocation	Positive/negative access tests



Scope boundary

A handover enables the client to govern future change. It does not guarantee that every future platform, portal, model, provider, or business change will work without analysis, testing, or implementation effort.

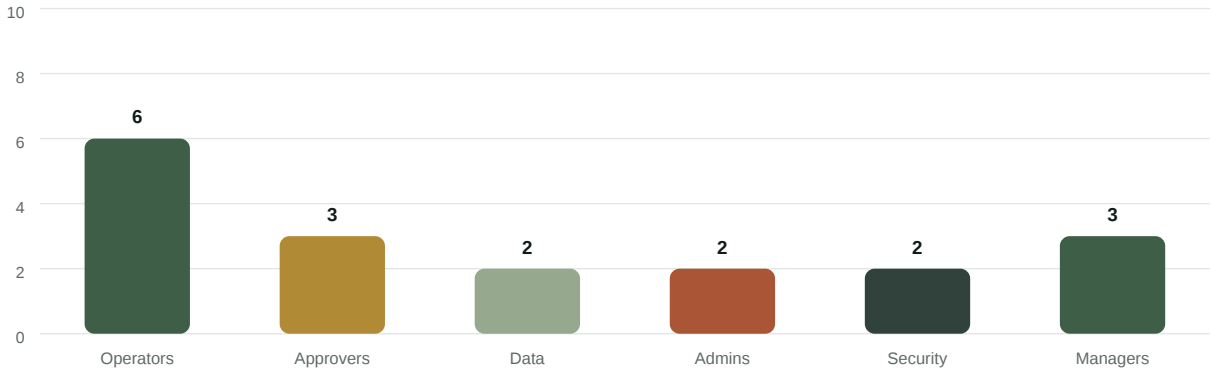
09 / ROLE-BASED TRAINING

Train people on decisions and exceptions, not only buttons

Training is complete when each role can perform the agreed scenarios, explain its authority boundary, recognise abnormal conditions, and use the runbook to recover or escalate.

Audience	Required capability	Representative exercise	Completion evidence
Workflow operator	Run daily work, assign ownership, monitor deadlines	Process an RFQ and resolve a routine exception	Observed scenario and questions
Business approver	Review evidence and make consequential decisions	Approve/reject submission and record reason	Signed approval exercise
Data owner	Correct authority values and resolve identity conflicts	Resolve duplicate and conflicting source	Decision history reviewed
System administrator	Control users, integrations, runs, recovery, export	Revoke account and recover failed run	Technical exercise result
Security/IT owner	Review providers, access, secrets, incidents	Test unauthorised action and access removal	Control review signed
Manager	Interpret dashboards, ageing, quality, exceptions, outcomes	Review weekly operating summary	Management scenario completed

Illustrative trained users by role



Illustrative attendance only. A client pack records named participants and actual completion.

Training record

Retain date, audience, materials, attendance, exercises, result, questions, unresolved topics, follow-up owner, and any recording retention decision.

10 / 30-DAY STABILISATION

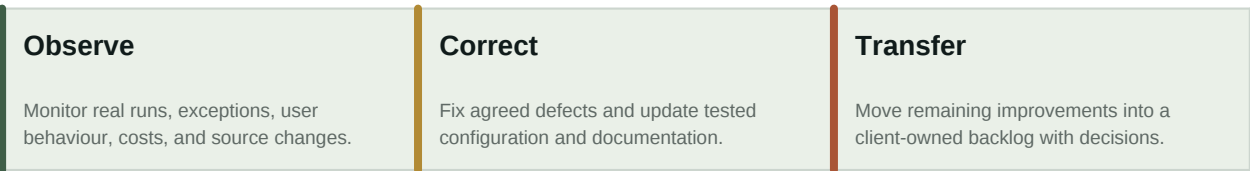
Move from implementation support to client operation

The stabilisation period confirms that the tested workflow remains operable under real use and that client owners can resolve routine work. Exact duration and support terms depend on the engagement agreement.



Stabilisation ends with explicit transfer of remaining work, not the disappearance of every minor issue.

Period	Primary focus	Exit evidence
Before launch	Role-based walkthroughs, acceptance exercises, admin transfer	Named users complete agreed scenarios
Days 1-7	Run monitoring, queue review, permission issues, urgent defects	Critical workflow path remains operable
Days 8-21	Exception trends, data quality, adoption questions, minor corrections	Owners resolve routine issues using runbook
Days 22-30	Final review, access closure, documentation update, open-item handoff	Every open item has owner, decision, and date



Stabilisation is not an indefinite managed service. Continued monitoring, maintenance, enhancements, or operational support require a separately agreed arrangement.

11 / FINAL TRANSFER & SIGN-OFF

What must be true before handover is complete

Final sign-off confirms that the client has received the agreed assets, understands the tested operating scope and limitations, controls access, and accepts the remaining work and support boundary.

Completion gate	Required evidence	Approval role
Acceptance	Signed test record and approved conditional items	Business sponsor
Documentation	Issued and editable pack stored in client repository	Workflow owner
Asset ownership	Databases, repositories, environments, accounts, billing, exports confirmed	System owner
Access transfer	Client admins active; temporary implementation access removed	Security/IT owner
Training	Named roles complete agreed scenarios and know escalation path	Adoption owner
Operations	Monitoring, queues, recovery, change, and incident process understood	Operations owner
Open work	Limitations, defects, improvements, risk, owner, date, and decision retained	Business sponsor
Support boundary	Stabilisation end, exclusions, maintenance, and future support clarified	Commercial owner

Final handover package

Operate Runbook, queues, schedules, approvals, notifications, recovery, and incidents.	Govern Architecture, dictionary, ownership, access, providers, changes, and decisions.	Continue Exports, editable sources, open-item register, roadmap, and provider portability.
--	--	--

Final principle

A successful handover leaves the client with more than a working automation. It leaves the client with ownership, understanding, evidence, operating capability, and the freedom to continue with its own team or another qualified provider.

Representative sign-off

Role	Name	Decision	Date
Business sponsor	_____	Accept / revise	_____
Workflow owner	_____	Accept / revise	_____
Security or IT owner	_____	Accept / revise	_____
Client system owner	_____	Accept / revise	_____