



WORKED EXAMPLE / OCTOBER 2026

Technical & Product Due Diligence

How evidence becomes decisions for investors, acquirers and boards

BUSINESS CONTEXT

A B2B workflow software business preparing for enterprise expansion

The example investment thesis is enterprise expansion through a more capable workflow product. This report shows how evidence about technology, delivery and product choices can be translated into decisions, ownership and a practical operating plan.

About this worked example

This report demonstrates FoundationState's assessment approach. The company, evidence and findings have been created for illustration; they do not describe a client engagement.

Inside the report

Where to start

A concise commercial readout

Executive view - page 2

Scope, evidence and calibrated confidence

Assessment basis - page 3

Findings across technology and product operations

Risk register and analysis - pages 4-11

Owners, dependencies and closure evidence

Action plan and decisions - pages 12-13

How to commission and use an assessment

Using the report - page 14

Prepared by FoundationState | Independent technical and product assessment

foundationstate.com



01 / EXECUTIVE VIEW

A credible product direction; an operating plan to prove

The enterprise growth thesis, its dependencies and the decisions required

In this scenario, a hosted workflow platform serves existing business users while management proposes expansion into larger accounts. The architecture is understandable and a substantial rebuild is not justified by the evidence presented. The main uncertainty is whether operational control and delivery capacity can support the proposed expansion.

Decision for the deal team

Continue the assessment, but do not treat the growth roadmap or recovery assumptions as established. Obtain proof of company-controlled administration and a witnessed restore exercise before relying on operational continuity. Rebaseline the enterprise roadmap against observed delivery capacity.

What supports the thesis

- A shared application platform and versioned configuration offer a plausible basis for consistent deployments. The repository extract shows a repeatable build process.
- The proposed enterprise feature set responds to named buyer needs in the discovery notes. Product priorities can be tested without replacing the entire platform.

What could impair it

- **Control:** one route to cloud administration depends on an individual account; company-controlled recovery has not been demonstrated (F01).
- **Continuity:** backup jobs are recorded, but a representative restore and service recovery have not been evidenced (F02).
- **Execution:** roadmap estimates assume capacity that support and release work also consume (F04).

Immediate leadership decisions

Assign accountable owners for access and recovery; make evidence completion a visible decision point; choose which enterprise commitments remain provisional. Counsel and the buyer should determine any contractual response after the facts are established.

Confidence: moderate in the operating-model observations; limited in recovery, isolation and future delivery claims. Evidence gaps are not proof of a breach, outage or inability to deliver. See page 3 for the review boundaries.



02 / ASSESSMENT BASIS

Scope and evidence come first

The basis for each finding and the limits of the review

The assumed scope covers product strategy, architecture, operational control, delivery capacity, release quality, migration readiness and external dependencies. It demonstrates document review, role-based interviews and selected technical walkthroughs. The evidence below is illustrative; no client interviews, tests or system access are represented.

Evidence item	Review result	Supports
E01 - platform overview and deployment walkthrough	Architecture understood at component level; throughput not validated.	F02, F03
E02 - administrative access export	Ownership and recovery path partially evidenced.	F01
E03 - backup job log and recovery runbook	Job success visible; no end-to-end restore result supplied.	F02
E04 - tenancy design and sampled access tests	Selected API checks present; background jobs and exports not covered.	F03
E05 - roadmap, backlog and delivery records	Priorities stated; interruptions not reflected consistently in plans.	F04
E06 - supplier handover and repository access pack	Access available; independent deployment not demonstrated.	F05
E07 - release checklist and defect log	Build pipeline present; closure and escape data incomplete.	F06
E08 - interviews with functional owners	Context for observations; statements require corroboration.	F01-F06

Explicit exclusions

No penetration test, exhaustive code audit, full load test, legal opinion on IP or contracts, certification audit, financial valuation, or independent verification of every management assertion is assumed. Source-code and access samples cannot establish the absence of defects across an estate.

Confidence language: higher confidence means the stated observation has more direct support in the evidence presented, not that the business is safe. Limited confidence identifies an evidence gap requiring further work. Each action specifies what would change the conclusion.



03 / RISK REGISTER

Six findings; different decisions

Ratings describe priority in this scenario, not a universal scoring formula

Finding	Rating / impact / likelihood	Decision and owner
F01 - Administration depends on an individual account. E02, E08. Confidence: moderate.	RED Impact: high. Likelihood: plausible; not measured.	Before completion: demonstrate company-controlled access and recovery. Owner: CTO.
F02 - Recovery assumptions lack a restore exercise. E01, E03. Confidence: high in the evidence gap.	RED Impact: high. Likelihood: undetermined.	Before completion: witness a representative restore and service recovery. Owner: Engineering lead.
F03 - Tenant isolation assurance is incomplete. E01, E04. Confidence: limited in overall isolation.	AMBER Impact: high. Likelihood: undetermined.	Before enterprise expansion: verify API, job and export boundaries. Owner: Security / engineering lead.
F04 - Roadmap capacity excludes recurring interruptions. E05, E08. Confidence: moderate.	AMBER Impact: medium. Likelihood: likely under current planning.	First 30 days: baseline demand and replan commitments. Owner: Product lead.
F05 - Supplier handover has not been exercised. E06, E08. Confidence: moderate.	AMBER Impact: medium. Likelihood: plausible.	Before renewal / transition: rehearse independent operation. Owner: CTO + commercial lead.
F06 - Release evidence does not cover key failure paths. E07, E08. Confidence: moderate.	AMBER Impact: medium. Likelihood: plausible.	Before material release: require risk-based tests and named sign-off. Owner: Engineering lead.

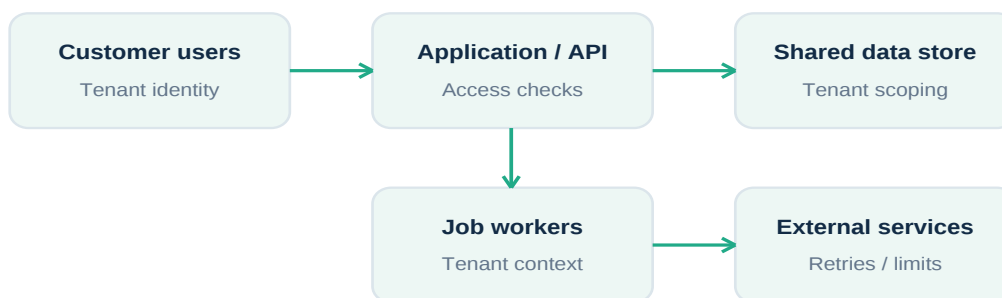
Red: resolve or explicitly accept a material control/continuity uncertainty before relying on it. **Amber:** manageable with a visible plan; escalate if new evidence increases impact. **Green:** no material issue found within the reviewed scope; not a blanket assurance. This report does not assign a single overall score that could obscure evidence gaps.



04 / ARCHITECTURE AND RESILIENCE

Keep the platform; prove the recovery path

F02 | E01, E03 | Engineering lead



Illustrative logical view only. Supporting infrastructure and security controls are intentionally omitted. The review question is whether these components can be restored into a working service, not merely whether their data is backed up.

Observation and interpretation

The backup log records completed jobs. The runbook describes restoring the database, but does not demonstrate reconstruction of application configuration, credentials, queued work or external connections. A job marked successful provides useful evidence of backup execution; it does not establish recovery time or data loss in a service incident.

Commercial implication

Enterprise commitments could be made against an untested recovery assumption. The concern is interruption and uncertain restoration effort, not an evidenced outage. Availability promises and incident communications should reflect what has actually been demonstrated.

Recommended treatment

Agree recovery objectives with product and commercial owners. Restore a representative dataset into an isolated environment, rebuild dependencies and verify critical journeys. Capture timings, data reconciliation, failures and operator steps. Have a second engineer execute the runbook rather than relying on its author.

Evidence of closure

A witnessed exercise restores the service within the agreed recovery objectives, reconciles data, records unresolved exceptions and proves a company-controlled operator can repeat the process. If the exercise fails, revise the rating and operating commitments before scaling adoption.

Architecture trade-off: maintain the shared platform unless tested limits justify a change. A new hosting model would add migration and operating costs without, by itself, proving resilience.



05 / SECURITY AND CONTROL

Make ownership and boundaries demonstrable

F01 and F03 | E02, E04, E08 | CTO and security / engineering lead

F01 - Company-controlled administration

In the access export, a primary administrative route belongs to an individual account. Management describes a recovery route, but no exercise or independently accessible company-owned route is supplied. This creates a continuity concern if that person becomes unavailable; it does not establish misuse or a compromised account.

Action: inventory privileged roles and recovery dependencies, establish individually accountable company-controlled access, enforce appropriate authentication, and test recovery with a second authorised operator. Preserve auditability; avoid replacing personal dependency with a shared unrestricted credential.

Closure: company ownership, access assignments and recovery evidence are documented; access revocation and recovery are exercised without interrupting the service. Accountability remains with the CTO even if an administrator performs the work.

F03 - Tenant isolation assurance

The API samples check tenant identity for selected requests. The evidence does not cover background processing, report exports or privileged support access. The observation is incomplete assurance, not a demonstrated cross-tenant exposure.

Action: map every path that reads or writes tenant data. Add negative tests for access from another tenant, queued jobs, exports and support tooling. Review how tenant identity is established and propagated; do not rely on a user-supplied identifier alone.

Escalation trigger

A reproduced isolation defect, excessive support access or incorrect export changes the decision: contain the issue, assess affected data and involve the appropriate incident and legal owners. Missing tests alone should not be presented as evidence that customer information was exposed.

Closure: an approved boundary map, risk-based test results and a documented review of privileged access. Where enterprise contracts require stronger assurance, commission the relevant specialist work before making that commitment.



06 / PRODUCT AND ROADMAP

Test the growth plan against customer value and capacity

F04 | E05, E08 | Product lead, supported by engineering and commercial owners

The roadmap groups enterprise requests into reporting, access control and integration capabilities. The business has an understandable direction, but the backlog combines customer-specific requests with reusable product work. Delivery dates assume that the same engineers will absorb support, implementation and release work without an explicit capacity allowance.

What the buyer should establish

- Which capabilities are prerequisites for a target segment, and which are requests from a single prospect? Identify the evidence for buyer demand without assuming forecast revenue is committed.
- Which commitments have already been made? Reconcile roadmap wording, sales conversations and customer obligations before treating dates as flexible.
- What is the dependency chain? Isolation assurance, recovery and release discipline may constrain expansion before a feature does.

A proportionate product decision

Prioritise one coherent enterprise adoption path over several parallel feature packages. Define its user outcome, acceptance criteria and technical prerequisites. Keep customer-specific exceptions visible and decide whether to productise, price, defer or decline them.

Planning horizon	Evidence and decision
First 30 days	Classify demand and commitments; baseline capacity; select the next product outcome.
Days 31-60	Test the proposed capability with representative users; review engineering dependencies and size remaining uncertainty.
Days 61-90	Commit the next release only after capacity and acceptance evidence support it; update customer-facing expectations.

Evidence of closure

A prioritised roadmap links outcomes to demand evidence, owners, dependency gates and available capacity. Forecasts state assumptions and confidence. A change in support load or discovery findings triggers replanning rather than an invisible deadline slip.



07 / DELIVERY AND ORGANISATION

Recover capacity before adding commitments

F04 | E05, E08 | Product lead and engineering lead

The delivery records show planned work being interrupted by operational requests. Functional interviews disagree about how much time those requests consume. The discrepancy is itself useful: the team lacks a shared baseline, so a precise annual productivity saving or immediate hiring case would overstate the evidence.

Measure the demand, not individual busyness

For a short observation period, classify work as planned product delivery, operational support, customer-specific work or rework. Use ticket and release records alongside team explanations. Capture queue age, interruptions and outcomes rather than demanding exhaustive personal time sheets.

Change the operating model in small steps

- **Intake:** give requests one visible route, with severity-based escalation and a named decision maker for commercial exceptions.
- **Coverage:** nominate a support rotation and protected product capacity. Ensure critical incidents can still override the plan explicitly.
- **Knowledge:** pair a second operator on access recovery, deployments and supplier handover. A document alone does not prove operational coverage.
- **Responsibility:** distinguish accountable product decisions from engineering execution; use functional owners even where one person temporarily holds both roles.

How to size an intervention

Estimate the recurring workload from the baseline, then compare routing improvements, automation, targeted contractor support and a hire. Include management time and handover cost. Treat any benefit estimate as a scenario until the change has been observed; avoid adding overlapping savings together.

Evidence of closure

The next two planning cycles show visible operational demand, explicit capacity allocation and fewer unexplained interruptions. Leadership can see what was displaced and why. This demonstrates planning control; it does not promise an automatic productivity increase.



08 / QUALITY AND RELEASE

Release confidence needs observable evidence

F06 | E07, E08 | Engineering lead

The build pipeline is a strength: it provides a repeatable way to produce releases. The release checklist, however, records approval without consistently linking it to tests of permissions, imports and data changes. The defect log does not reliably distinguish defects found before release from defects reaching customers.

Retain what works; close the material gaps

Keep the existing pipeline and engineering review practice. Add a compact checklist covering affected user journeys, tenancy and permissions, migration behaviour, external dependencies, monitoring and the recovery response. Depth should match the change, rather than imposing the same ceremony on every small correction.

Release gate	What makes the gate meaningful
Scope and acceptance	Product and engineering agree the outcome, material changes and unresolved exceptions.
Risk-based tests	Critical and negative paths have results tied to the release; failed checks remain visible.
Rollout and recovery	Owners know cohort order, health signals, stop conditions and how to respond to data-changing failures.
Named go / no-go	A responsible person records acceptance of residual risk and confirms operational readiness.
Post-release review	Customer-impacting defects and rollout failures feed back into tests and planning.

Measure quality without claiming certainty

Track customer-impacting defects, failed changes and time to restore service using consistent definitions. Explain the denominator and observation window. Tool adoption, more tests or a lower raw bug count do not alone establish better customer outcomes.

Evidence of closure

A material release has traceable acceptance and test results, documented exceptions, named sign-off and a completed post-release review. No unresolved critical finding is hidden by changing the gate or excluding a failed check.

09 / MIGRATION AND CHANGE

A deployment rollback is not a data recovery strategy

F02, F06 | E03, E07 | Engineering lead

The proposed enterprise capability introduces a revised workflow data model. The application can be redeployed to an earlier build, but that does not establish that data written under the new model remains readable by the old version. Change readiness must cover both code and data.

Treat the change as a controlled programme

Stage	Required decision or evidence
1. Bound the change	Inventory schema, permissions, integration and workflow changes. Define acceptable service interruption and data reconciliation.
2. Rehearse both directions	Use representative, appropriately protected data in isolation. Prove forward migration and recovery, including new writes and external side effects.
3. Approve a small cohort	Choose representative users with agreed communication and support coverage. Avoid a cohort that excludes the difficult cases the wider rollout must handle.
4. Observe before expanding	Compare critical journeys and error signals against the baseline. Assign a person who can stop the rollout against explicit thresholds.
5. Close deliberately	Record reconciliation, outstanding exceptions, customer impact and operational acceptance before retiring fallback arrangements.

The rollback decision must be explicit

Once new writes occur, restoring an earlier backup can lose data and cause divergence from external systems. The plan must state when rollback remains safe, when roll-forward repair is preferable, and how affected writes will be reconciled. Never describe a backup as an automatic zero-loss fallback.

Evidence of closure

A rehearsal records recoverability at each stage, data-loss exposure, reconciliation steps and operator responsibilities. Product and commercial owners accept the operational consequences before committing the wider cohort.

This section illustrates migration readiness. A detailed engineering migration design and production execution would require a separately agreed scope.

10 / EXTERNAL DEPENDENCIES

A helpful supplier can still be an operating dependency

F05 | E06, E08 | CTO and commercial lead

The handover pack gives the business repository access to an integration maintained by an external partner. The service is working and the relationship appears constructive. No exercise shows an internal engineer rebuilding, deploying or troubleshooting it without the supplier. Access is an asset; independent operability remains unproven.

Separate the questions

- **Operational:** can the company build, deploy, diagnose and restore the component? Identify tool access, credentials, documentation and skills needed.
- **Commercial:** what service levels, availability, notice periods and transition support have been agreed? Separate informal goodwill from contractual commitments.
- **Ownership:** what rights exist to code, configuration, deliverables and third-party components? Have counsel resolve the legal position; repository possession alone is not proof of rights.

Compare proportionate options

Option	Trade-off to evaluate
Retain the supplier with a tested handover	Preserves knowledge and continuity; requires agreed evidence, responsibilities and transition support.
Bring routine operation in-house	Improves control if the team has capacity; creates training and maintenance obligations.
Transition to another provider	May improve coverage or capability; adds discovery, transfer and dual-running risk.

Recommended sequence

Rehearse independent operation and clarify the agreement before choosing a structural change. Use the resulting gap list to compare options. Do not replace a functioning partner solely to create the appearance of control.

Closure: an internal operator completes a witnessed build and deployment, unresolved dependencies have owners, and commercial/legal reviewers record the agreed rights and transition terms. No named vendor or real supplier arrangement is represented here.



11 / PRIORITISED ACTION PLAN

Sequence the work; make closure inspectable

Target horizons - recalibrate after evidence and capacity are established

When / action	Accountable owner / dependency	Closure evidence
Before completion A01: establish administrative control (F01).	CTO. Inventory and authorised access to the estate.	Company ownership and a second-operator recovery exercise.
Before completion A02: prove service recovery (F02).	Engineering lead. A01; agreed recovery objectives.	Witnessed restore, service checks, timings and reconciled data.
Day 1 A03: confirm operational handover (F01, F02, F05).	CTO. A01/A02; supplier contacts and incident ownership.	Access, escalation and recovery owners acknowledged; exceptions visible.
Days 1-30 A04: rebaseline roadmap capacity (F04).	Product lead. Operational demand baseline and customer commitments.	Priorities, capacity allowance and provisional dates approved.
Days 1-30 A05: define release gates (F06).	Engineering lead. Critical journeys and change-risk map.	Checklist used on the next material release with test evidence and exceptions.
Days 31-60 A06: strengthen tenant assurance (F03).	Security / engineering lead. Boundary map and access to relevant code/tests.	Negative-path results; privileged support access review; remediation tracked.
Days 31-60 A07: exercise supplier handover (F05).	CTO + commercial lead. Supplier participation and rights review.	Independent deployment and a written transition gap list.
Days 61-90 A08: validate expansion readiness (F02-F06).	Product lead + CTO. Relevant gates A02, A04-A07.	Leadership accepts evidence, residual risk and a capacity-backed rollout plan.

Horizons identify intended order, not a delivery guarantee. A failed control, recovery or isolation exercise can pull an action forward or change the expansion decision. Effort and cost estimates should be agreed with the operators after discovery; costs should be scoped once the required work and capacity are understood.



12 / LEADERSHIP DECISIONS

What remains unresolved

Questions that change confidence, sequencing or scope

Question	Owner / decision point	Evidence that resolves it
What continuity commitments can the business support today?	CTO + commercial lead. Before relying on enterprise availability claims.	Recovery exercise compared with agreed objectives and contract commitments.
Which capabilities are essential to the enterprise adoption path?	Product lead. Before reissuing roadmap commitments.	Buyer need, acceptance criteria, dependencies and observed capacity.
Does tenant assurance need specialist expansion?	Security / engineering lead. Before material enterprise adoption.	Boundary tests, code review limits and customer assurance requirements.
Can the company operate the supplier-maintained component independently?	CTO + commercial lead. Before renewal or transition.	Rehearsed handover, gap list and counsel-reviewed rights.
Can the proposed data change be recovered safely after new writes?	Engineering lead. Before migration approval.	Rehearsal, reconciliation design and explicit stop / recovery decisions.

A short governance rhythm

Hold a weekly review of material actions during the initial period. Each owner reports evidence completed, dependencies blocked and the next decision needed. Use one action register rather than parallel lists across product, engineering and commercial teams.

Acceptance is a decision, not disappearance

If leadership accepts a residual risk, record the rationale, accountable owner, affected commitments and review date. Keep the finding visible. Missing evidence should remain labelled missing; an optimistic explanation does not close it.

What a real readout should leave behind

A shared view of the thesis, the uncertainties that could change it, the evidence still required and the owners of the next actions. A fuller engagement can supply separate workstream papers where operators need more detail.



13 / USING THE REPORT

From evidence to decisions

How to use this report when scoping an engagement

Start with the decision you need to make

An investment, acquisition, growth programme and product recovery have different evidence needs. Define the decision deadline, target context, critical assumptions and the level of technical depth before agreeing the review scope.

Request traceability, not a document count

Ask how conclusions connect to artefacts and interviews, how missing evidence is handled, how management can correct factual errors, and how actions will pass to operators. A concise report can be useful when the evidence is clear; a larger pack is appropriate when detailed workstreams need their own treatment.

Use the workstream depth that the situation needs

Decision-level output	Optional supporting depth
Executive view and risk register	Architecture and resilience assessment; targeted security or source-code review.
Product and delivery assessment	Roadmap feasibility, delivery demand, operating model and resourcing options.
Transition and dependency assessment	Migration readiness, external partner options, rights questions for counsel.
Prioritised operating plan	Named owners, dependencies, evidence of closure and leadership readout.

Discuss an independent assessment

FoundationState provides technical and product due diligence for investors, acquirers and boards. Share the decision to be made, available evidence and deadline so the scope and deliverables can be matched to the business.

foundationstate.com/contact/

About this worked example: the company, evidence and findings have been created for illustration. It demonstrates the reporting approach and does not represent a client assessment. Engagement scope and evidence access determine the depth of a commissioned report.