

Technical Risk & Transaction Impact

Target: Halyard Systems Ltd

Multi-tenant B2B SaaS · Field-operations & project management · NestJS / Next.js / PostgreSQL / AWS

Sample deliverable. “Halyard Systems Ltd” is a fully synthetic target created to demonstrate method and reporting format. All findings, systems, figures and evidence identifiers are fabricated for illustration. No real client, engagement or confidential material is referenced. The same reporting engine renders in two modes — buy-side (shown here) and sell-side readiness — differing only in framing, not in method.

FIELD	DETAIL
Engagement type	Buy-side technical due diligence (sample)
Prepared for	Acquirer / transaction sponsor
Prepared by	Olha Shevchenko — Architecture & Authorization Security Review
Method	Documentation review, configuration inspection, and differential authorization testing against a running staging environment
Access provided	Staging environment + two isolated tenant accounts; read access to the application repository and to cloud configuration
Isolation testing	Section 3 needed only the staging URL and two tenant accounts — no source-code or cloud access
Status	SAMPLE — not a live engagement

1 TECHNICAL RISK & TRANSACTION IMPACT

This section is the whole report in one page. Everything after it is the evidence.

Verdict. The architecture is conventional and survivable, but **tenant isolation is not consistently enforced**: differential testing crossed the tenant boundary on 3 of 24 tenant-scoped routes. Combined with a production database reachable from the public internet, this represents a material pre-close customer-data confidentiality exposure. IP provenance of a core module could not be established and warrants legal attention independent of engineering cost.

The three numbers

DAY-ONE TECHNICAL EXPOSURES (TIER 1) 4	INDICATIVE YEAR-ONE REMEDIATION €120k – €190k	ONE-LINE VERDICT Boring but survivable — authorization needs immediate attention
---	---	--

Estimated at programme level to reflect shared remediation, dependencies and overlapping findings — individual finding bands are not additive. Excludes items that are not engineering-estimable (e.g. IP assignment), tracked separately as they can carry exposure disproportionate to remediation effort.

Findings by tier

TIER	MEANING (TRANSACTION LENS)	COUNT
Tier 1	Material pre-close issue — warrants treatment before or at close	4
Tier 2	Warranty / escrow / disclosure candidate — manageable with protection	5
Tier 3	Post-close remediation backlog — cost and roadmap item	3

One further item (DD-IP-001) is escalated for legal review and sits outside the engineering tier system; it is potentially material to title and valuation.

Top three issues to raise first

- Cross-tenant data leakage on 3 routes (DD-AUTHZ-001/002/003) — verified empirically, not inferred. One customer’s data is retrievable while authenticated as another.
- Production database reachable from the public internet (DD-SEC-001) — confidentiality and availability exposure that exists today, not just at close.
- Unestablished IP ownership of the core routing module (DD-IP-001) — escalated for legal review; not a tiered engineering item, but potentially material to title and valuation.

2 SCOPE, METHOD & CONFIDENCE BASIS

Access model. Tenant-isolation verification (Section 3) used only a staging URL and two isolated tenant accounts. The remainder of the review additionally drew on read access to the application repository and to cloud configuration. Each finding notes its basis accordingly.

What was reviewed

- Public and authenticated application surfaces across three API styles: REST, GraphQL and tRPC.
- Tenant isolation behaviour, exercised empirically using two isolated tenant accounts.
- Cloud configuration reachable from the provided environment: network exposure, IAM posture, secrets handling, backup configuration.
- Delivery and operational posture, from repository metadata and stakeholder interview.
- Third-party dependencies and licensing, and IP provenance of principal modules.

What was not reviewed

- Full source-code audit — out of scope by design; this review is black-box plus configuration and interview.
- Penetration testing beyond authorization-boundary probing; no exploitation beyond proof of access.
- Business, financial, HR and commercial diligence — addressed by other workstreams.

Method — differential authorization testing

Tenant isolation was verified empirically, not inferred from documentation or code review. Authenticated HTTP traffic was recorded as one tenant identity and replayed under a second, isolated tenant identity. For every tenant-scoped route, the review asserts that the second identity cannot observe the first identity’s data. Shared reference data (lookup tables, catalogues) is baselined out so it does not register as a false leak. This produces a route-level pass/fail rather than a subjective judgement.

Why this matters commercially. A generic reviewer writes “authorization middleware appears generally well structured.” This review instead reports: we attempted to cross the tenant boundary 112 times; three attempts succeeded. The difference is the difference between an opinion and evidence a buyer’s counsel can act on.

Confidence basis

Every finding carries a confidence level. This distinguishes what was proven from what was observed or inferred, so the reader can weight each item appropriately and counsel can see exactly where the evidence stands.

CONFIDENCE	MEANING	BASIS
Verified	Reproduced empirically against the running system	Direct test, repeatable
Observed	Directly seen in configuration, data or repository, but not exploited	Primary artefact
Inferred	Concluded from indirect but consistent evidence	Secondary signals + interview
Unverified	Claimed by the target but not confirmable within scope	Assertion pending evidence

A note on treatment language

This report states what a technical fact means for the transaction; it does not prescribe the deal outcome. Wording such as “material pre-close issue” or “escrow consideration” identifies the class of transaction lever a finding may engage. The choice of mechanism — price, warranty, escrow, condition, disclosure — rests with the buyer and their counsel.

3 TENANT ISOLATION VERIFICATION

This is the flagship result and the reason black-box access is sufficient: with only a staging URL and two tenant accounts, tenant isolation can be proven or disproven empirically.

TENANT ISOLATION VERIFICATION — HALYARD SYSTEMS LTD (STAGING)	
Routes discovered	47
Routes exercised	38
Tenant-scoped routes	24
Differential tests	112
Cross-tenant failures	3
Coverage	81%
Result	FAILED

The same defect — a missing tenant-ownership check — was confirmed independently on all three API surfaces. This is not one bug seen three times through a single code path; it is the same omission recurring across REST, GraphQL and tRPC, which indicates tenant isolation is enforced route-by-route rather than as a system-wide invariant.

DD-AUTHZ-001				Direct object reference bypasses tenant scope (REST)		TIER 1			
CONFIDENCE		Verified	EFFORT		Medium	EST. COST €15k – €30k		EXPOSURE Potentially material	
EVIDENCE									
GET /api/projects/:id returned a Tenant B project record when called with a valid Tenant A session. The handler resolves the record by primary key and omits the tenant-ownership check that is present on sibling routes.									
VERIFICATION									
Reproduced across 4/4 attempts using two isolated tenant accounts and non-adjacent object IDs. Confirmed the returned record belonged to the other tenant by cross-referencing a unique field value.									
BUYER CONSEQUENCE									
Tenant isolation is not enforced at the resource boundary for this route. The buyer inherits a customer-data confidentiality exposure that is trivially reachable by any authenticated user who can enumerate or guess identifiers.									
POTENTIAL DEAL RELEVANCE									
Material pre-close issue.									
POSSIBLE TREATMENT									
Pre-close remediation, or specific warranty with escrow consideration pending fix verification.									
Evidence refs AUTHZ-017, AUTHZ-018, HTTP-042-049									

DD-AUTHZ-002				Top-level entity resolver omits the tenant-ownership check (GraphQL)		TIER 1	
CONFIDENCE	Verified	EFFORT	Medium	EST. COST	€10k – €25k	EXPOSURE	Potentially material
EVIDENCE							
The top-level document(id) query applies authentication and role checks, then resolves the document by primary key with no tenant-ownership predicate. A Tenant A session requesting a Tenant B document id received the record — including its filename and parent project reference.							
VERIFICATION							
Reproduced 3/3 using two isolated tenant accounts. The returned filename and project id were confirmed to belong to Tenant B; the same request as Tenant B (the rightful owner) returned the identical record, as a control.							
BUYER CONSEQUENCE							
In GraphQL every resolver enforces authorization independently, so each resolver is a fresh place for the ownership check to be forgotten. Here it was forgotten on a top-level entity that any authenticated user can							

query directly.

POTENTIAL DEAL RELEVANCE

Material pre-close issue.

POSSIBLE TREATMENT

Pre-close remediation; recommend a schema-wide isolation assertion rather than a per-resolver point fix.

Evidence refs AUTHZ-021, AUTHZ-022, GQL-011-013

DD-AUTHZ-003 Authenticated and role-checked, but ownership unverified (tRPC)

TIER 1

CONFIDENCE Verified EFFORT Low EST. COST €8k – €15k EXPOSURE Potentially material

EVIDENCE

The invoice.get procedure applies correct authentication and role middleware, then resolves the invoice by id without confirming it belongs to the caller’s tenant. Middleware presence gives a misleading appearance of protection; the ownership predicate is missing.

VERIFICATION

Reproduced 4/4. Notably, this route passes a naive middleware-coverage check yet still leaks — which is why isolation must be tested by behaviour, not by presence of guards.

BUYER CONSEQUENCE

The buyer cannot rely on “middleware is applied” as evidence of isolation. The correct control (authentication + role) is present but the tenant-ownership control is absent.

POTENTIAL DEAL RELEVANCE

Material pre-close issue.

POSSIBLE TREATMENT

Low-effort pre-close fix; treat as a bellwether for a codebase-wide ownership-check audit.

Evidence refs AUTHZ-024, AUTHZ-025, TRPC-007-010

Reading the coverage box. 81% coverage means 38 of 47 discovered routes were exercised; the 9 unexercised routes require inputs or states not reachable from the two supplied accounts and are listed as open items, not as passes. A FAILED result reflects three confirmed cross-tenant leaks, independent of coverage.

4 FINDINGS BY DOMAIN

4.1 Security posture — cloud, network, identity

DD-SEC-001 Production database reachable from the public internet

TIER 1

CONFIDENCE Verified EFFORT Low EST. COST €5k – €12k EXPOSURE Potentially material

EVIDENCE

The RDS security group permits inbound traffic to port 5432 from 0.0.0.0/0. The database accepted TCP connections from an external host during testing (authentication was not attempted beyond confirming reachability).

VERIFICATION

Reachability confirmed once from an external address; not exploited further by agreement.

BUYER CONSEQUENCE

With the store on the public internet, the network boundary that would normally limit the usefulness of a compromised or weak database credential is absent, and the listener is exposed to internet-wide scanning. This exposure exists today, before any change of control.

POTENTIAL DEAL RELEVANCE

Material pre-close issue; also an immediate operational risk the seller should be told about regardless of deal outcome.

POSSIBLE TREATMENT

Immediate network restriction; pre-close remediation with verification.

Evidence refs SEC-003, NET-011

DD-SEC-002 Long-lived shared IAM credentials, no rotation

TIER 2

CONFIDENCE Observed EFFORT Medium EST. COST €10k – €20k EXPOSURE Limited to moderate

EVIDENCE

A single administrative IAM user with long-lived access keys is shared across deployment tooling; keys show no rotation in available history. No per-engineer roles or short-lived credentials were observed.

BUYER CONSEQUENCE

Attribution and revocation are weak: a departing engineer or leaked key cannot be cleanly contained, and blast radius is account-wide. Standard, well-understood remediation.

POTENTIAL DEAL RELEVANCE

Warranty / disclosure candidate; post-close hardening item.

POSSIBLE TREATMENT

Disclosure and post-close remediation; low deal friction if planned.

Evidence refs IAM-004, IAM-006

DD-SEC-003 Secrets present in repository history

TIER 2

CONFIDENCE Observed EFFORT Medium EST. COST €8k – €18k EXPOSURE Moderate

EVIDENCE

Historic commits contain what appear to be live-format credentials (database URL with password, a third-party API key). Current code uses environment variables, but the historic values remain retrievable from git history.

BUYER CONSEQUENCE

Any credential ever committed must be treated as compromised and rotated. Until rotation is confirmed, the buyer cannot assume current secrets are uncompromised.

POTENTIAL DEAL RELEVANCE

Disclosure candidate; rotation should be a condition or a warranted post-close action.

POSSIBLE TREATMENT

Credential rotation + history remediation; disclosure with warranty.

Evidence refs SEC-009, SEC-010

4.2 Data — backups and restore

DD-DATA-001 Backups are configured; restore has never been exercised

TIER 2

CONFIDENCE Unverified EFFORT Medium EST. COST €8k – €15k EXPOSURE Potentially material

EVIDENCE

Automated daily snapshots are enabled and retained (Observed). However, no record of a restore drill exists and staff confirmed a full restore has never been performed. Recovery time and recovery point objectives are undocumented.

VERIFICATION

Backup existence is Observed; backup effectiveness is Unverified — a backup that has never been restored is an assumption, not a control.

BUYER CONSEQUENCE

The buyer inherits an untested recovery capability. In a real incident, RTO/RPO are unknown and may be unacceptable. This is the gap between a control that exists and a control that is effective.

POTENTIAL DEAL RELEVANCE

Warranty / post-close item; escalates if the business has contractual uptime or recovery commitments.

POSSIBLE TREATMENT

Restore drill during confirmatory diligence or as a post-close first-30-days action.

Evidence refs DATA-002, OPS-014

4.3 Architecture and scalability

DD-ARCH-001 Report generation runs synchronously in the request path

TIER 3

CONFIDENCE Observed EFFORT Medium EST. COST €15k – €30k EXPOSURE Limited

EVIDENCE

Export and reporting endpoints generate output synchronously within the HTTP request, with no job queue (observed in response behaviour and confirmed in interview). Response latency grew with result-set size across the test tenants.

BUYER CONSEQUENCE

The synchronous design has no queue to absorb load, implying a scaling ceiling as tenant data volumes grow. This is an inferred re-architecture cost on the growth path, not a present outage risk.

POTENTIAL DEAL RELEVANCE

Post-close roadmap and cost item.

POSSIBLE TREATMENT

Post-close; introduce asynchronous job processing.

Evidence refs ARCH-005, PERF-003

DD-ARCH-002 Single-AZ database; no tested failover

TIER 3

CONFIDENCE Observed EFFORT Medium EST. COST €10k – €20k EXPOSURE Limited

EVIDENCE

The primary database runs in a single availability zone with no standby replica configured. Application tier is likewise single-region.

BUYER CONSEQUENCE

An availability-zone incident implies downtime. Acceptable for current scale but a gap relative to typical enterprise-customer expectations the buyer may wish to meet.

POTENTIAL DEAL RELEVANCE

Post-close roadmap item; may matter sooner if enterprise SLAs are a growth thesis.

POSSIBLE TREATMENT

Post-close; enable multi-AZ / standby.

Evidence refs ARCH-008

4.4 Delivery and operations

DD-OPS-001 Deployment knowledge concentrated in two individuals

TIER 2

CONFIDENCE Inferred EFFORT Low EST. COST €5k – €10k EXPOSURE Moderate (key-person)

EVIDENCE

Deploy-related commits and configuration changes over the trailing 12 months originate almost entirely from two engineers. No deployment runbook was found; release steps are described as tribal knowledge in interview.

VERIFICATION

Inferred from repository authorship patterns corroborated by interview; not independently drilled.

BUYER CONSEQUENCE

A key-person dependency: loss of either engineer materially raises operational risk during and after transition. Common in companies of this size but relevant to retention and integration planning.

POTENTIAL DEAL RELEVANCE

Integration / retention consideration; supports key-person provisions.

POSSIBLE TREATMENT

Runbook creation and cross-training address the documentation gap — the costed item. The underlying key-person retention exposure is a deal-team matter and is not captured in the cost band.

Evidence refs OPS-001, OPS-002

4.5 Dependencies, licensing and IP

DD-IP-001 IP ownership of the core routing module cannot be established

PRIORITY: LEGAL ESCALATION

CONFIDENCE Inferred EFFORT n/a EST. COST Not estimable EXPOSURE Potentially material

EVIDENCE

The route-optimization module — central to the product — was authored predominantly by an external contractor per repository history. No IP assignment or work-for-hire agreement covering that contractor was made available.

VERIFICATION

Inferred from authorship and the absence of an assignment document; ownership cannot be confirmed within technical scope.

BUYER CONSEQUENCE

The target may not cleanly own a core component of the product it is selling. This is not an engineering defect and cannot be honestly costed as one: formalising an assignment might cost little, or the matter could escalate materially if the contractor is unreachable or disputes ownership.

POTENTIAL DEAL RELEVANCE

Potentially material to title and valuation; a legal matter, not a remediation task. Sits outside the engineering tier system.

POSSIBLE TREATMENT

Legal review; assignment confirmation as a condition, warranty or disclosure per counsel.

Evidence refs IP-001, REP0-014

DD-DEP-001 Copyleft-licensed dependency linked into the distributed service

TIER 2

CONFIDENCE Observed EFFORT Medium EST. COST €5k – €25k EXPOSURE Potentially material

EVIDENCE

A dependency under a strong copyleft licence is compiled into the server-side service. Depending on distribution model and interpretation, this licence family can impose source-availability obligations.

BUYER CONSEQUENCE

Potential licensing obligation or the need to replace the component. Effort ranges from a straightforward swap to a non-trivial re-implementation, hence the wide band.

POTENTIAL DEAL RELEVANCE

Disclosure candidate; warrants legal confirmation of obligation.

POSSIBLE TREATMENT

Legal confirmation, then replace or comply; disclosure meanwhile.

Evidence refs DEP-003, LIC-002

DD-DEP-002 Dependencies carrying published CVEs, unpatched

TIER 3

CONFIDENCE Observed EFFORT Low EST. COST €5k – €12k EXPOSURE Limited

EVIDENCE

Software-composition analysis matched several dependencies to published CVEs, two rated high. Dependency names and versions were confirmed against the lockfile.

VERIFICATION

Presence and versions: Verified against the lockfile. Exploitability and reachability in this codebase: Unverified — no exploitation was attempted, and a published CVE is not a live vulnerability until its reachability in context is

established.

BUYER CONSEQUENCE

Maintenance and patch-cadence debt rather than a demonstrated exploit. The buyer should budget ongoing SCA and upgrade effort; individual CVEs need contextual triage before any is treated as live.

POTENTIAL DEAL RELEVANCE

Post-close backlog item.

POSSIBLE TREATMENT

Post-close dependency upgrade pass and ongoing SCA in CI.

Evidence refs DEP-007, DEP-008, DEP-009

5 RISK REGISTER

All findings, sortable by tier. This is the working table for counsel and the deal team.

ID	DOMAIN	TIER	CONFIDENCE	DEAL RELEVANCE	EFFORT	COST
DD-AUTHZ-001	Authorization	T1	Verified	Material pre-close	Med	€15-30k
DD-AUTHZ-002	Authorization	T1	Verified	Material pre-close	Med	€10-25k
DD-AUTHZ-003	Authorization	T1	Verified	Material pre-close	Low	€8-15k
DD-SEC-001	Security	T1	Verified	Material pre-close	Low	€5-12k
DD-IP-001	IP	Legal	Inferred	Potentially material	n/a	Not estimable
DD-SEC-002	Security	T2	Observed	Warranty / disclosure	Med	€10-20k
DD-SEC-003	Security	T2	Observed	Disclosure	Med	€8-18k
DD-DATA-001	Data	T2	Unverified	Warranty / post-close	Med	€8-15k
DD-OPS-001	Delivery	T2	Inferred	Retention / integration	Low	€5-10k
DD-DEP-001	Licensing	T2	Observed	Disclosure	Med	€5-25k
DD-ARCH-001	Architecture	T3	Observed	Post-close roadmap	Med	€15-30k
DD-ARCH-002	Architecture	T3	Observed	Post-close roadmap	Med	€10-20k
DD-DEP-002	Dependencies	T3	Observed	Post-close backlog	Low	€5-12k

Indicative year-one remediation programme: €120k–€190k. Estimated at programme level — individual finding bands overlap (notably the three authorization findings share one systemic fix) and are not additive. Excludes DD-IP-001 (not estimable) and any legal or licence-replacement cost, tracked separately.

6 REMEDIATION ROADMAP

Sequenced by transaction urgency, then by dependency. In sell-side mode this becomes “fix before the buyer’s diligence”; in buy-side mode, “integration and first-year plan.”

0–30 days — confirm and contain

- Restrict production database network exposure (DD-SEC-001). Immediate; low effort, high urgency.
- Fix the three confirmed tenant-isolation leaks (DD-AUTHZ-001/002/003) and re-run differential tests to confirm closure.
- Rotate any credential present in repository history (DD-SEC-003).
- Legal: open IP-assignment question on the routing module (DD-IP-001) — gates on external counsel, so start now.

31–90 days — harden and prove

- Introduce a codebase-wide tenant-ownership assertion so isolation is a system invariant, not per-route (follows DD-AUTHZ-002/003).
- Perform and document a full restore drill; establish RTO/RPO (DD-DATA-001).
- Move to per-role, short-lived IAM credentials (DD-SEC-002).
- Confirm copyleft-licence obligation and decide comply-or-replace (DD-DEP-001).
- Write the deployment runbook and cross-train beyond the two key engineers (DD-OPS-001).

91-365 days — scale and maintain

- Move report generation to asynchronous processing (DD-ARCH-001).
- Enable multi-AZ / standby for the database (DD-ARCH-002).
- Dependency upgrade pass; add SCA to CI as a standing control (DD-DEP-002).

7 APPENDICES

Appendix A — Confidence definitions

Reproduced here so the register is self-contained.

- Verified — reproduced empirically against the running system; repeatable.
- Observed — directly present in configuration, data or repository, but not exploited.
- Inferred — concluded from indirect but consistent evidence, corroborated where possible by interview.
- Unverified — asserted by the target but not confirmable within the agreed scope; flagged for confirmatory diligence.

Appendix B — Differential authorization testing, in brief

Authenticated traffic is recorded under tenant identity A, then replayed under isolated tenant identity B. For each tenant-scoped route, the test asserts that B cannot observe A's data. Shared reference data is baselined so it does not register as a leak. A route "fails" only when B successfully observes A-owned data. Coverage is the proportion of discovered routes actually exercised; a high coverage figure with zero failures is the target, and any single failure fails the isolation result regardless of coverage.

This is why source-code access is not required: the client provides only a staging URL and two tenant accounts, and the isolation property is proven or disproven behaviourally.

Appendix C — Evidence log (excerpt)

Illustrative format only. In a live engagement each reference resolves to a captured request/response pair, timestamp and hash.

AUTHZ-017	GET /api/projects/8842	as Tenant A	->	200	(record owner: Tenant B)
AUTHZ-018	GET /api/projects/8842	as Tenant B	->	200	(record owner: Tenant B) [control]
AUTHZ-021	query { document(id:"B-D0C-77"){filename project{id}} }	as Tenant A	->	200	(owner: Tenant B)
AUTHZ-022	query { document(id:"B-D0C-77"){filename} }		as Tenant B	->	200 (owner: Tenant B)
	[control]				
AUTHZ-024	trpc invoice.get {id:"B-5590"}	as Tenant A	->	200	(invoice owner: Tenant B)
HTTP-042	replay set projects/ cross-identity	42 requests		4	flagged
NET-011	tcp connect rds:5432 from external host	->	open		

Appendix D — Reliance & limitations (template)

In a live engagement this report is addressed to a named recipient, and reliance is limited to that recipient; no third-party reliance is granted without prior written agreement. The review reflects the systems and information available within a defined window and is not a warranty that no other issues exist. Liability is governed by, and subject to the cap in, the engagement letter. This sample grants no reliance.