

Pre-Investment Technical Assessment

A European B2B logistics and field-services SaaS. Founded 2016. Revenue in the €4–6M band. Twenty-eight staff, nine of them engineers, with an offshore engineering team. One technical founder, departing at close.

PREPARED FOR

The Buyer

INVESTMENT COMMITTEE

PREPARED BY

Harivansh

REDSHIFT LTD, MAURITIUS

ENGAGEMENT

Ten working days

REMOTE

RECOMMENDATION

Proceed, with a price adjustment and protections in the agreement.

Contents

	SECTION	SHEET
1	Scope, method and limitations	3
2	Executive summary	4
3	Technology scorecard	6
4	The system as it stands	7
5	Findings	9
6	Risk register	18
7	Remediation and transaction treatment	20
8	Appendices	22

Sections 2, 3 and 6 carry the decision. Section 5 carries the evidence behind them, and Section 7 states where each finding belongs: in the price, in the agreement, in the first hundred days, or in the backlog.

Scope, method and limitations

Engagement. Ten working days, conducted remotely, with three days of scheduled interviews.

What I examined. The full application repository and its commit history since inception. The infrastructure definitions and deployment pipelines. The production database schema, its migration history, and a read replica populated with production data. The dependency manifests for every deployable component. The issue tracker for the preceding eighteen months. Whatever internal documentation exists. Interviews with the technical founder, the two most senior engineers, the engineer responsible for deployments, the newest engineering hire, the offshore engineering lead, the head of customer operations, and the chief executive.

How I examined it. I built and ran the system from a clean machine before reading any of it, and recorded what that took. I traced two business-critical paths end to end: a job from dispatch to completion, and a billing period from usage capture to invoice. I ran dependency, licence, secret-scanning and static analysis tooling, listed in Appendix A, and treated every result as a question rather than a finding. Everything reported here was confirmed by reading the code or by interview.

LIMITATIONS

What I did not examine, and what this report cannot tell you.

I did not perform a penetration test, and nothing here should be read as assurance that the Target's systems cannot be breached. I did not audit the Target's cloud spend or verify its infrastructure costs. I did not review customer contracts, and where I refer to commercial obligations I am reporting what the Target's staff told me. I saw production data in a replica and did not observe the live production environment under load. I have not tested the Target's disaster recovery, because it has not been tested.

Three limits are worth stating plainly. First, ten days is enough to find what is systematically wrong with a codebase of this size and not enough to find everything wrong with it. Second, I assessed the software as it exists, not the roadmap, and a plan is not evidence. Third, and most importantly, a technical review can establish what a system does and cannot establish what a business earns. Where those two questions meet, at DAT-01, I have said so explicitly and referred it to the financial diligence team rather than resolving it here.

Executive summary

Recommendation: proceed, with a price adjustment and protections in the agreement.

The Target is a competently built business with two problems that belong in the transaction rather than in the backlog, and one that belongs in your first hundred days.

The software does what the Target says it does. Its architecture is unremarkable in the way working systems usually are, the engineering team is better than the codebase suggests, and I found nothing that would prevent this business from operating and growing under new ownership. The concerns below are specific and priceable. None of them is a reason to stop.

The three findings that affect the decision:

1. Usage and billing records cannot be reconciled to reported revenue.

DAT-01 • CRITICAL

The Target bills on consumption, but the system does not retain an immutable record of the events it charges for. Usage is aggregated nightly and the source events are discarded after thirty days. For any period older than a month, there is no technical means of demonstrating that an invoice was correct. This does not mean revenue is overstated. It means it cannot be substantiated from the system, and your quality-of-earnings work should be told so before it relies on platform data. Rebuilding the billing event trail is possible and costed in Section 7. The historical gap cannot be recovered.

2. A copyleft-licensed component sits inside the core product.

IPL-01 • CRITICAL

The routing engine, which is central to the Target's principal commercial claim, incorporates an AGPL-3.0 library. The Target distributes the product as a hosted service, which engages the network clause. On a plain reading, the obligation to offer corresponding source extends to the service as delivered. The Target's management were not aware of this. It is resolvable, by replacement or by licence negotiation, but it is a matter for the agreement rather than the roadmap.

3. One departing person holds the billing and integration knowledge.

TEA-01 • HIGH

The technical founder, who is leaving at close, is the only individual with working knowledge of the billing pipeline and four of the seven customer integrations. Documentation for these areas is absent rather than poor. This is the most time-sensitive item in this report: the window to extract that knowledge closes on the day he leaves.

What I looked at and did not find: no evidence of undisclosed security incidents, no personal data held outside the stated jurisdictions other than the disclosure gap at SEC-02, no unlicensed commercial software, and no dependency on a single cloud vendor that would prevent migration.

Remediation: €495,000 to €865,000 over twelve months, of which €215,000 to €345,000 falls in the first hundred days.

Suggested transaction treatment: a price adjustment of €500,000; an indemnity covering the licensing exposure at IPL-01; a warranty on revenue substantiation covering the period since the last audited accounts; a representation on IP ownership addressing IPL-02; and a retention tied to a documented knowledge transfer from the departing founder.

Technology scorecard

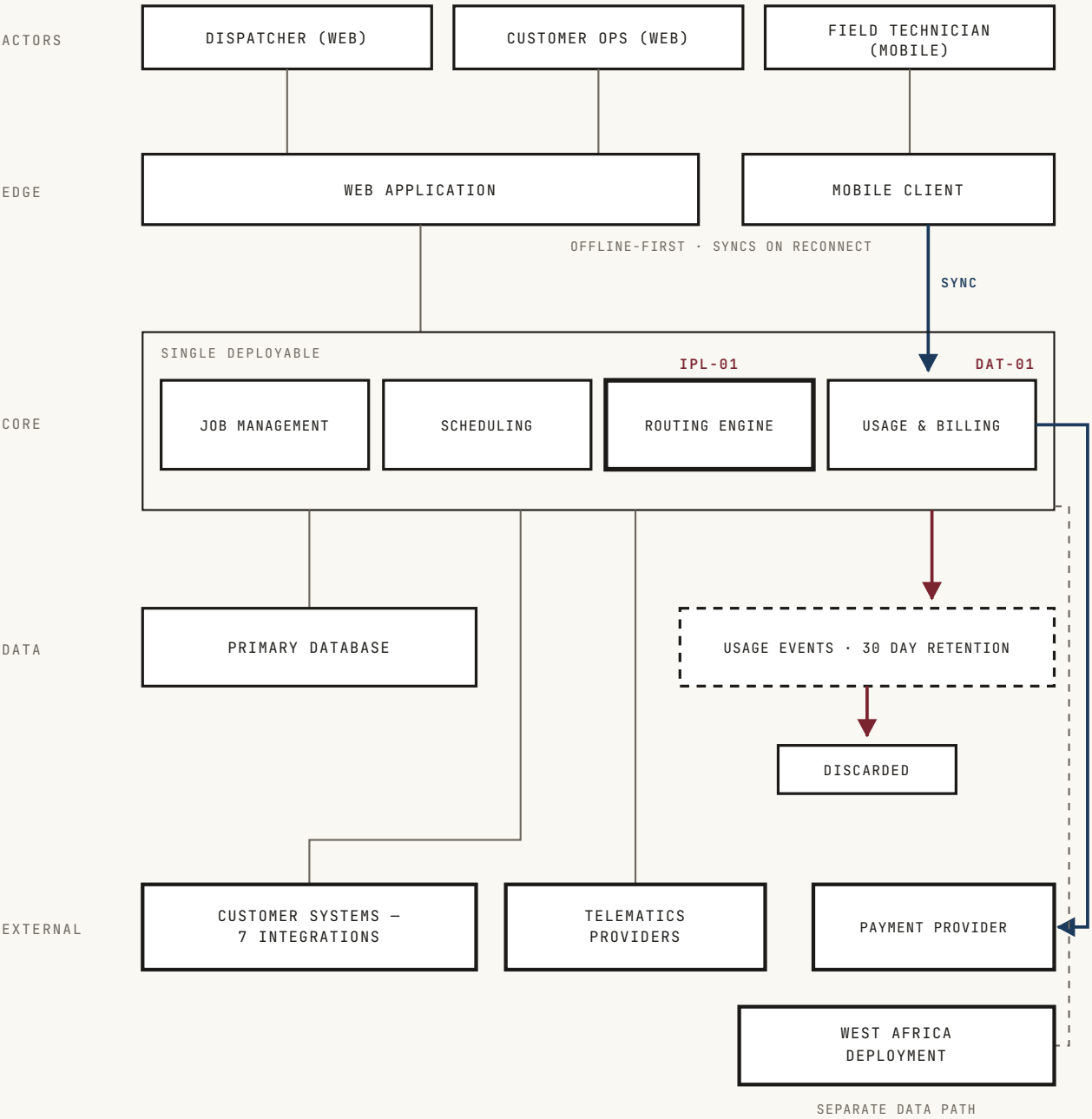
Eight dimensions, rated against what I would expect of a business at this revenue and stage, not against an ideal. A red rating means something must be resolved in the transaction. A half-filled square means it must be funded. An open square means it is not your problem.

DIMENSION	RATING	RATIONALE
ARCHITECTURE		Boundaries are real and enforced. Two localised breaches. No re-platform required or advisable.
DATA MODEL & INTEGRITY		Billing events are discarded before they can be audited. Deletion semantics are inconsistent across core tables.
SECURITY		Access control and secrets handling are strong. Three high-severity dependencies, personal data in logs, one disclosure gap.
TEST & QUALITY		Core paths are meaningfully covered. Integration coverage is thin and the suite is slow enough that engineers avoid it.
DELIVERY & OPERATIONS		Deployment and rollback are exemplary. Disaster recovery is untested; monitoring watches machines, not outcomes.
SCALABILITY & PERFORMANCE		Comfortable headroom at current and projected volumes. Single region is a resilience constraint, not capacity.
TEAM & KNOWLEDGE		Critical systems are held by one departing individual. No onboarding path for replacements.
IP & LICENSING		A copyleft component sits in the core product. Offshore contributor agreements assign ownership ambiguously.
 RESOLVE IN THE TRANSACTION  FUND IT  NOT YOUR PROBLEM		

EXHIBIT B • THE CODE IS IN BETTER CONDITION THAN THE ARRANGEMENTS AROUND IT.

Three red, three amber, two open. The pattern is worth naming: the code is in better condition than the arrangements around it. The engineering is sound. What is unresolved is who owns it, who understands it, and what the system can prove about itself.

The system as it stands



FLAGS REFERENCE FINDINGS IN SECTION 5.

EXHIBIT A • THE TWO FINDINGS THAT DRIVE THIS REPORT SIT IN THE SAME HALF OF THE DRAWING.

The Target sells scheduling, dispatch and proof-of-service software to companies that send people to sites. Its customers are mid-sized field-services and last-mile operators in six European markets, plus one customer operating in West Africa.

The system is a single application with an accompanying mobile client. A dispatcher plans a day in the browser. The routing engine sequences the day's jobs. The mobile client receives the resulting schedule, works offline, and syncs proof of service, photographs, signatures and timestamps on reconnection. Those events feed the usage record, which produces the invoice. Seven customer integrations push and pull work orders against the customers' own systems.

Four observations about that shape matter to this transaction.

The routing engine is the product. Everything else the Target sells is competently built and broadly replicable. The scheduling quality is the reason customers stay, and it is also where the licensing exposure at IPL-01 sits. The component carrying the Target's commercial differentiation is the one component it may not be entitled to distribute as it currently does. These two facts sit in the same box on Exhibit A, and that is the single most important thing on the drawing.

The offline mobile client is harder than it looks and works. Conflict resolution on reconnection is the sort of problem that is usually solved badly. Here it is solved with a defined merge policy and it holds under the failure cases I tried. This is real engineering value and it would be expensive to rebuild.

Billing sits at the edge of the system, not the centre. The usage pipeline was added after the product had customers, and it shows in the topology. It reads from an aggregate rather than from the event stream, which is the mechanism behind DAT-01. It is also the area with the highest knowledge concentration, per TEA-01. The two findings share a cause.

The West African integration is architecturally separate, and correctly so. It carries its own connectivity assumptions, its own retry behaviour, and a different data path. Isolating it was a good decision. The concern it raises is not architectural: data flows to a jurisdiction that the Target's published privacy notice does not mention, which is recorded at SEC-02.

On the whole: this is a system built by people who understood their domain, under commercial pressure, without the time to go back and tidy. That is the normal condition of software at this revenue, and it is not a reason for alarm. The concerns worth transacting on are specific and are listed in Section 5.

Findings

Findings are grouped by domain and ordered by severity within each. Severity is stated in transaction terms rather than engineering terms.

CRITICAL	Affects whether to proceed, or requires a change to price or structure.
HIGH	Carries material remediation cost and belongs in the price or in warranties.
MEDIUM	Should be planned and funded within twelve months.
LOW	Hygiene: noted, not actioned.

Findings are numbered within their domain in order of presentation.

Twenty-one findings follow: two Critical, five High, nine Medium, five Low. Alongside them I record one concern examined and dismissed, and two findings that are genuinely reassuring.

	CRITICAL	HIGH	MEDIUM	LOW	TOTAL
ARCHITECTURE & CODE			2	2	4
DATA & SCHEMA	1	1	2		4
SECURITY & COMPLIANCE		1	1	1	3
DELIVERY & OPERATIONS		1	2	1	4
TEAM & KNOWLEDGE		1	2		3
IP & LICENSING	1	1		1	3
TOTAL	2	5	9	5	21

EXHIBIT C • SEVERITY CONCENTRATES IN DATA AND IN LICENSING, NOT IN THE CODE.

5.1 Architecture and code

ARC-00

The monolith is not the problem · NOT A FINDING

Management flagged their monolithic architecture as a concern, and I examined it on that basis. I do not consider it a risk to this transaction, and I want to record why, because the obvious objection deserves an answer rather than a silence.

The application is a single deployable, but its internal boundaries are real: domain modules own their tables, cross-module access goes through explicit interfaces, and I found only two places where that discipline is broken. Deploys run several times a week without ceremony. The team of nine is well within the range a codebase of this shape supports comfortably. The architecture that would replace it, on this team at this revenue, would cost eighteen months and buy very little.

There is a version of this report that lists monolithic architecture as a finding, assigns it a remediation budget, and looks thorough. It would be wrong, and it would cost you a seven-figure programme to solve a problem you do not have. If the business doubles headcount, revisit the boundaries at that point. Not now.

BELONGS NOWHERE	TIMING CLOSED
--------------------	------------------

Recorded so the question is closed.

ARC-01

Two modules read another module's tables directly · MEDIUM

Reporting and the notification service both query job tables without going through the owning module. Everything else respects the boundary. Left alone, these become the seams that make future change expensive.

REMEDIATION €15-25K	BELONGS IN THE PRICE	TIMING 12 MONTHS
------------------------	-------------------------	---------------------

ARC-02

Deployment and rollback are routine · REASSURING

Deployments run from a pipeline on every merge to main, average four to six per week, and roll back through a documented and rehearsed path. Two engineers performed a rollback for me on request, from a cold start, in under twelve minutes. This is better than the codebase's cosmetic condition would suggest, and it is the single strongest indicator in this review that the team can operate what they have built.

ARC-03

Business rules duplicated between web and mobile clients · MEDIUM

Validation for job state transitions exists twice, in two languages, and the two have already diverged in one case I could demonstrate. The divergence is currently harmless. It will not stay that way.

REMEDIATION	BELONGS	TIMING
€20-30K	IN THE PRICE	12 MONTHS

ARC-04

No record of architectural decisions · LOW

Nothing explains why the system is shaped as it is. The people who know are the people leaving. Cheap to start, impossible to backfill later.

REMEDIATION	BELONGS	TIMING
€5-8K	BACKLOG	AS CONVENIENT

ARC-05

The test suite takes forty minutes and is routinely skipped · LOW

Engineers push and wait for the pipeline instead of running tests locally. This is a productivity tax rather than a risk, but it compounds with TEA-02 for any new joiner.

REMEDIATION	BELONGS	TIMING
€10-15K	BACKLOG	AS CONVENIENT

5.2 Data and schema

DAT-01	Usage events are discarded before they can be audited · CRITICAL
EVIDENCE	Consumption events are written to a queue, aggregated into <code>billing_period_totals</code> by a nightly job, and deleted from source after thirty days by a retention task. The aggregate table carries totals only. There is no event archive, no cold storage, and no signed record. Invoices are generated from the aggregate. I re-ran the aggregation for three sample periods and could not reproduce two of the three published totals from surviving data.
IMPACT	For any billing period older than thirty days, the Target cannot demonstrate from its own systems that an invoice was correct. This is exposure in three directions at once: a customer dispute cannot be answered with evidence, a revenue warranty cannot be supported by platform data, and the quality-of-earnings analysis is relying on a source that cannot be independently verified. I want to be precise about what I am and am not saying. I found no indication that revenue is misstated. I found that the system cannot prove it either way.
REMEDIATION	Retain raw usage events immutably with a defined retention horizon; make invoice generation reproducible from retained events; reconcile forward from the date of change. Historical periods cannot be reconstructed.

EFFORT	REMEDIATION	BELONGS	TIMING
8-12 ENG-WEEKS	€70-110K	IN THE PRICE	IMMEDIATE

Referred to the financial diligence team as a limitation on platform-sourced revenue evidence.

DAT-02	Soft deletion applied inconsistently · MEDIUM
	Some tables soft-delete, some hard-delete, and three tables do both depending on the code path. Reporting reads across all of them. Historical figures move depending on which query produced them.

REMEDIATION	BELONGS	TIMING
€20-35K	IN THE PRICE	6 MONTHS

DAT-03	No retention policy outside the usage tables · MEDIUM
	Job history, photographs and audit tables have never been pruned. Storage growth is not yet a cost problem and will be within roughly two years. Note the asymmetry with DAT-01: the one dataset with a retention rule is the one that needed to be kept.

REMEDIATION	BELONGS	TIMING
€15-25K	IN THE PRICE	12 MONTHS

DAT-04

Personal data present in application logs · HIGH

Error traces capture request payloads, which include customer contact details and, in the mobile sync path, technician location. Logs are retained for fourteen days and are accessible to the full engineering team including offshore contributors. This is a straightforward data protection exposure for a business selling into six European markets.

REMEDIATION €25-40K	BELONGS FIRST 100 DAYS	TIMING 60 DAYS
------------------------	---------------------------	-------------------

5.3 Security and compliance

SEC-01

Three high-severity dependency vulnerabilities · MEDIUM

All three have published fixes and clear upgrade paths. None is currently exploitable in the Target's configuration as deployed. This is catch-up, not alarm.

REMEDIATION €25-40K	BELONGS IN THE PRICE	TIMING 90 DAYS
------------------------	-------------------------	-------------------

SEC-02

West Africa data path outside the published privacy notice · HIGH

Job and technician data for the West African deployment transits and rests in a jurisdiction the Target's privacy notice does not name. The architecture is sound. The disclosure is missing. This is a documentation and consent problem with a regulatory consequence, and it is fixable in weeks.

REMEDIATION €30-45K	BELONGS FIRST 100 DAYS	TIMING 30 DAYS
------------------------	---------------------------	-------------------

SEC-03

Access control and secrets handling are sound · REASSURING

Secrets are held in a managed store with rotation in place, and I found none in version control history across the full repository. Access to production is role-based, individually attributed, and reviewed quarterly with records retained. Customer data access by staff is logged. For a company of this size, this is above what I typically encounter and materially reduces the security remediation I would otherwise expect to recommend here.

SEC-04

No incident response runbook · LOW

The team has handled incidents competently and improvisationally. Nothing is written down, which means the competence leaves with the people.

REMEDIATION €8-12K	BELONGS BACKLOG	TIMING AS CONVENIENT
-----------------------	--------------------	-------------------------

5.4 Delivery and operations

OPS-01

Disaster recovery untested for eighteen months · HIGH

Backups run and restore has been verified at the database level. A full recovery of the running system has never been rehearsed, so the recovery time objective is an assumption rather than a measurement.

REMEDIATION
€35-55K

BELONGS
IN THE PRICE

TIMING
FIRST 100 DAYS

OPS-02

Monitoring watches infrastructure, not outcomes · MEDIUM

Alerts fire on CPU, memory and error rates. Nothing alerts on jobs not dispatched, syncs not completing, or invoices not generated. The team learns about business-level failures from customers.

REMEDIATION
€25-40K

BELONGS
FIRST 100 DAYS

TIMING
90 DAYS

OPS-03

Single region, no documented failover · MEDIUM

Adequate for the current customer base and their contractual commitments. Becomes a procurement obstacle with larger customers, which is a growth constraint rather than a present risk.

REMEDIATION
€40-60K

BELONGS
IN THE PRICE

TIMING
12 MONTHS

OPS-04

Log retention of fourteen days · LOW

Too short to investigate a billing dispute, which is the dispute this business actually has. Compounds DAT-01 directly.

REMEDIATION
€5-10K

BELONGS
BACKLOG

TIMING
AS CONVENIENT

5.5 Team and knowledge concentration

TEA-01	Single-person knowledge over billing and four integrations • HIGH
EVIDENCE	Commit history over three years shows one contributor accounting for the substantial majority of changes to the billing pipeline and to four of the seven customer integrations (the D–G group in Exhibit D). Two other engineers described those areas as his. No design documentation, runbooks, or integration specifications exist for them. That contributor is the technical founder, who departs at close. Exhibit D maps this across the estate.
IMPACT	These are the systems that produce invoices and connect the Target’s largest customers. On his departure the buyer inherits systems that work, until they do not, with nobody able to explain why. The cost of this finding rises every week it is deferred and becomes unrecoverable at his exit date.
REMEDIATION	A structured knowledge transfer with written outputs, run before departure, not a series of handover calls. Hire or assign a named owner for billing in month one. Reconstruct integration specifications from behaviour where documentation does not exist.

EFFORT	REMEDIATION	BELONGS	TIMING
6-10 ENG-WEEKS	€50-85K	FIRST 100 DAYS	BEFORE EXIT DATE

Effort includes the founder’s own time. Pair with a retention arrangement tied to defined knowledge-transfer deliverables.

SUBSYSTEM	FDR	E2	E3	E4	E5	E6	E7	E8	E9	OS
JOB MANAGEMENT	■	■	■	■						
SCHEDULING		■	■				■			
ROUTING ENGINE	■	■								
USAGE & BILLING	■									BUS FACTOR 1
MOBILE CLIENT								■	■	■
CUSTOMER INTEGRATIONS A-C				■	■	■				
CUSTOMER INTEGRATIONS D-G	■									BUS FACTOR 1 • 4 OF 7
INFRASTRUCTURE					■	■				
WEST AFRICA DEPLOYMENT		■								BUS FACTOR 1

■ MEANINGFUL AUTHORSHIP • FDR FOUNDER • E2-E9 ENGINEERS • OS OFFSHORE TEAM
BUS FACTOR 1 ONE OWNER, DEPARTING AT CLOSE • BUS FACTOR 1 ONE OWNER, REMAINING
THE SEVEN CUSTOMER INTEGRATIONS ARE ANONYMISED A THROUGH G AND GROUPED BY OWNERSHIP. FOUR OF THE SEVEN ARE HELD SOLELY BY THE DEPARTING FOUNDER.

EXHIBIT D • USAGE & BILLING AND FOUR OF SEVEN CUSTOMER INTEGRATIONS HAVE ONE OWNER. HE LEAVES ON COMPLETION.

TEA-02

No onboarding documentation · MEDIUM

The most recent hire reached first meaningful commit in three weeks, entirely through pairing. With TEA-01 requiring new owners for billing and integrations, this is on the critical path rather than a nicety.

REMEDIATION €15-25K	BELONGS FIRST 100 DAYS	TIMING 90 DAYS
------------------------	---------------------------	-------------------

TEA-03

Two hours of overlap with the offshore team · MEDIUM

Review latency runs to a full day on mobile changes. The arrangement works and is not a reason to change it. It is a reason not to assume the mobile client can be accelerated simply by asking. Codify the asynchronous review protocol and stagger one engineer's hours during transition periods.

REMEDIATION €10-20K	BELONGS BACKLOG	TIMING AS CONVENIENT
------------------------	--------------------	-------------------------

5.6 IP and licensing

IPL-01

AGPL-3.0 component embedded in the core routing engine · CRITICAL

EVIDENCE

The optimisation library at the centre of the routing engine is AGPL-3.0. It is compiled into the same service as proprietary code and called directly rather than through a process boundary. The dependency manifest records it accurately; nobody had read it. The Target's counsel had not been asked.

IMPACT

The Target offers the product as a hosted service. The AGPL network clause is engaged by providing users with access over a network, and on a plain reading the obligation to offer corresponding source extends to the service as delivered. The exposure attaches to the component that supports the Target's principal commercial differentiator, which means it is not a candidate for quiet removal. I am flagging a technical fact with legal consequences; the legal conclusion belongs to your counsel, and they should have this before signing.

REMEDIATION

Three routes, in ascending cost: replace with a permissively-licensed equivalent and accept a documented loss of solution quality; isolate behind a process boundary, which mitigates but does not eliminate the argument; or negotiate a commercial licence with the copyright holder.

EFFORT 6-16 ENG-WEEKS	REMEDIATION €55-150K	BELONGS IN THE AGREEMENT	TIMING PRE-SIGNING
--------------------------	-------------------------	-----------------------------	-----------------------

Effort varies with the route chosen and excludes any licence fee. Belongs in the agreement as an indemnity, not on the roadmap.

IPL-02

Offshore contributor agreements assign ownership ambiguously · HIGH

The contracts covering three offshore engineers, who wrote the majority of the mobile client, contain no explicit present assignment of intellectual property and are governed by a jurisdiction where work-for-hire does not apply by default. The Target believes it owns this code. The paperwork does not clearly say so.

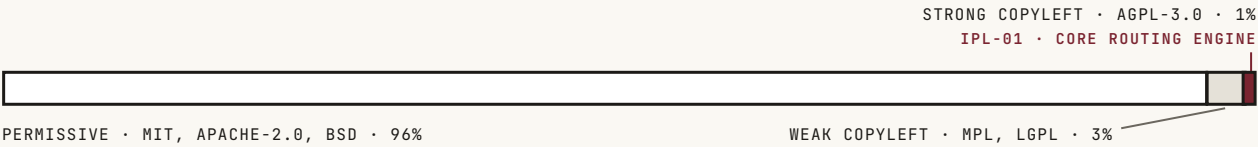
REMEDIATION €15-30K	BELONGS IN THE AGREEMENT	TIMING PRE-SIGNING
------------------------	-----------------------------	-----------------------

IPL-03

Open source attribution not maintained · LOW

No NOTICE file, and several permissive licences require attribution the Target does not provide. Low consequence, trivially fixed, and worth fixing at the same time as IPL-01.

REMEDIATION €3-5K	BELONGS BACKLOG	TIMING AS CONVENIENT
----------------------	--------------------	-------------------------



DIRECT DEPENDENCIES	214
TRANSITIVE	C. 1,900
TWO OR MORE MAJOR VERSIONS BEHIND	31
NO RELEASE IN 24 MONTHS	4, ONE IN THE CRITICAL PATH
KNOWN VULNERABILITIES	3 HIGH, 11 MODERATE

EXHIBIT E · ONE PER CENT OF THE DEPENDENCY TREE CARRIES THE ONLY LICENSING EXPOSURE THAT MATTERS.

Risk register

Every finding, grouped by severity. This is the page to take into an investment committee.

CRITICAL • 2

ID	FINDING	BELONGS	TIMING
DAT-01	Usage events discarded before they can be audited	In the price	Immediate
IPL-01	AGPL-3.0 component in the core routing engine	In the agreement	Pre-signing

HIGH • 5

ID	FINDING	BELONGS	TIMING
DAT-04	Personal data present in application logs	First 100 days	60 days
IPL-02	Offshore contractor agreements assign IP ambiguously	In the agreement	Pre-signing
OPS-01	Disaster recovery untested for eighteen months	In the price	First 100 days
SEC-02	West Africa data path outside the published privacy notice	First 100 days	30 days
TEA-01	Billing and four integrations held by one departing person	First 100 days	Before exit date

MEDIUM • 9

ID	FINDING	BELONGS	TIMING
ARC-01	Two modules breach the internal boundary discipline	In the price	12 months
ARC-03	Business rules duplicated between web and mobile clients	In the price	12 months
DAT-02	Soft deletion applied inconsistently across core tables	In the price	6 months
DAT-03	No retention policy outside the usage tables	In the price	12 months
OPS-02	Monitoring covers infrastructure, not business outcomes	First 100 days	90 days
OPS-03	Single region, no documented failover	In the price	12 months
SEC-01	Three high-severity dependency vulnerabilities	In the price	90 days
TEA-02	No onboarding documentation; three weeks to first commit	First 100 days	90 days
TEA-03	Two hours of overlap with the offshore team	Backlog	As convenient

LOW · 5

ID	FINDING	BELONGS	TIMING
ARC-04	No record of architectural decisions	Backlog	As convenient
ARC-05	Test suite takes forty minutes and is routinely skipped	Backlog	As convenient
IPL-03	Open source attribution not maintained	Backlog	As convenient
OPS-04	Log retention of fourteen days	Backlog	As convenient
SEC-04	No incident response runbook	Backlog	As convenient

EXAMINED AND CLOSED

ID	FINDING	BELONGS	TIMING
ARC-00	Monolithic architecture, examined and dismissed	Nowhere	Closed

REASSURING · 2

ID	FINDING	BELONGS	TIMING
ARC-02	Deployment and rollback are routine	—	—
SEC-03	Access control and secrets handling are sound	—	—

Remediation, and where each finding belongs

A finding is only useful once you know what to do with it. Everything in this report goes to one of four places, and the distinction matters more than the engineering detail.

In the price • €240–380K

Work the buyer will fund after close, quantified so it can be argued over now. The billing event trail at DAT-01 is the largest single item. The rest is ordinary catch-up: disaster recovery, dependency upgrades, deletion consistency, resilience, and the two boundary breaches.

In the agreement • €70–180K of exposure

Matters that should be resolved between the parties before signing, not inherited. IPL-01 warrants an indemnity, because the exposure is open-ended and attaches to the component the valuation rests on. IPL-02 warrants a representation that the Target owns what it sells, with the offshore agreements remediated as a condition. Neither of these is a roadmap item, and neither should be traded away for a discount. A discount does not extinguish a licensing obligation.

I would also seek a warranty on revenue substantiation for the period since the last audited accounts, arising from DAT-01. That is a matter for your counsel and your financial advisers; I am supplying the technical basis for it.

First hundred days • €145–235K

Work that is cheap now and expensive later, or that cannot be done at all once the window closes. TEA-01 is the whole reason this category exists in this transaction. The knowledge transfer has a hard deadline set by someone else's resignation date, and no amount of budget recovers it afterwards. SEC-02 and DAT-04 are here because a privacy notice that does not describe where data goes, and logs that leak personal data, are problems measured in days, not quarters.

Backlog • €40–70K

Real, worth doing, and not deal-relevant. Recorded so that nobody spends diligence attention on it, and so that the incoming team inherits the list rather than rediscovering it.

Totals and phasing

Total remediation of €495,000 to €865,000 over twelve months. Of that, €215,000 to €345,000 is spent within the first hundred days, which is more than the first-hundred-days category above, because DAT-01 and OPS-01 both begin immediately even though their cost sits in the price.

Against a deal in the low-to-mid twenties of millions, total remediation is between two and four per cent of enterprise value. That is an ordinary outcome for a technical review of a business at this stage. I mention it because the number in isolation can look alarming, and it should not.

Recommended price adjustment: €500,000. This reflects the billing event trail, the operational catch-up, and the cost of the knowledge transfer. It deliberately excludes the licensing exposure, which belongs in the indemnity rather than in the price.

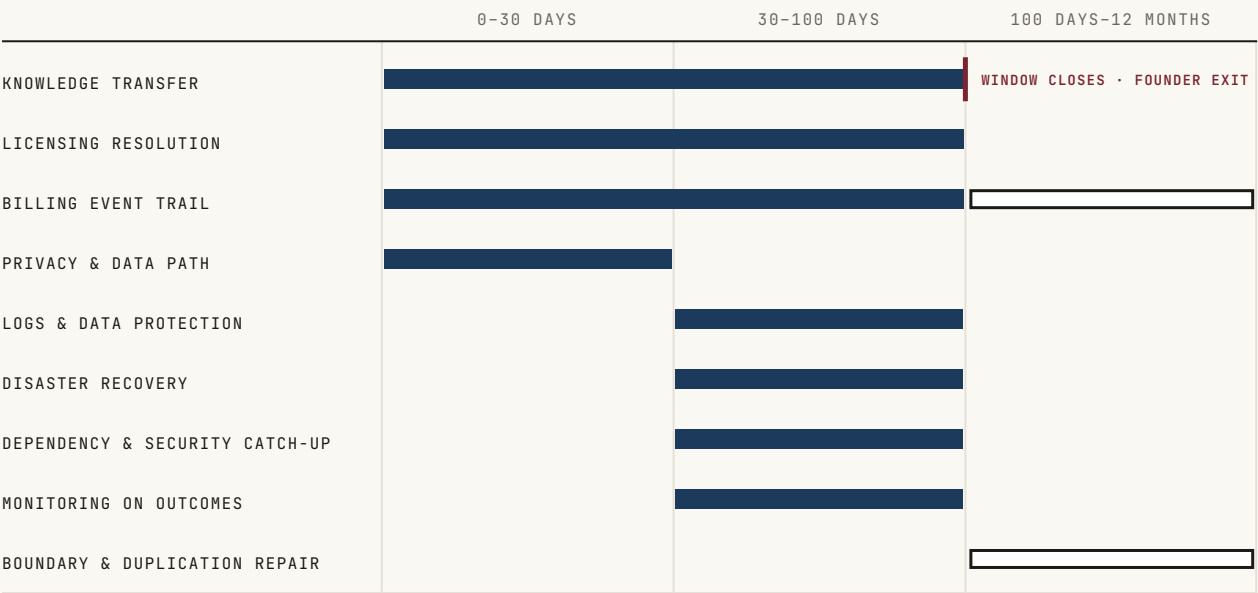


EXHIBIT F · ONE OF THESE WORKSTREAMS HAS A DEADLINE SET BY SOMEBODY ELSE.

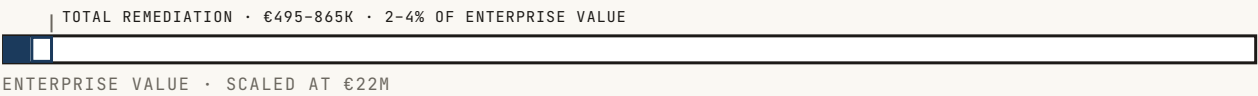
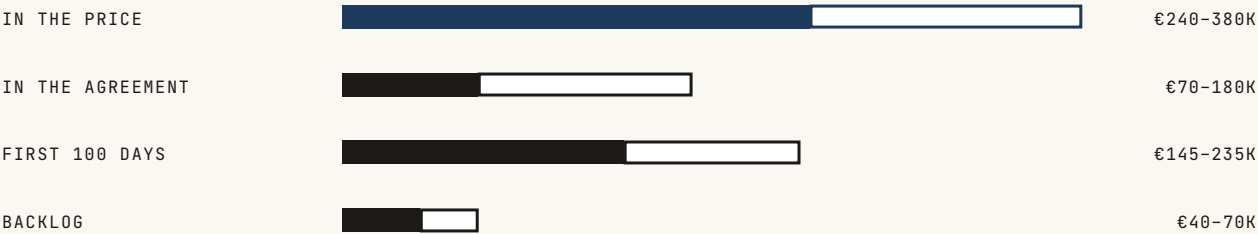


EXHIBIT G · REMEDIATION AGAINST DEAL VALUE. THE PROPORTION IS THE POINT.

Appendices

APPENDIX A • TOOLS RUN

Recorded so that findings can be reproduced and so that the boundary between tooling output and judgment is visible. Every result below was treated as a question to investigate, not as a finding in itself.

PURPOSE	TOOL
Software bill of materials	syft
Dependency vulnerabilities	osv-scanner, gype
Licence identification	syft licence output, verified manually against source headers
Secrets in history	gitleaks, trufflehog
Static analysis	semgrep, with the language rulesets for the stack in use
Codebase shape and volume	tokei
Change concentration and hotspots	code-maat, over full commit history
Coverage	The Target's own suite, shape only
Build reproducibility	Clean-machine container build, timed

Every licence identification at IPL-01 and IPL-03 was confirmed by reading the source headers and the upstream project's own statements. I do not report a licensing finding on scanner output alone.

APPENDIX B • INTERVIEWS

Nine conversations across three days: the technical founder, twice; the two most senior engineers; the engineer responsible for deployments; the most recent engineering hire; the offshore engineering lead; the head of customer operations; and the chief executive. Two engineers were asked separately to define the Target's core domain terms. Their answers agreed, which is recorded here because it is a favourable finding and an unusual one.

APPENDIX C • DOCUMENTS AND SYSTEMS REVIEWED

Application repository and full commit history. Infrastructure repository. Deployment pipeline configuration. Production schema and migration history. Read replica of production data. Dependency manifests and lockfiles for all deployable components. Issue tracker, eighteen months. Such internal documentation as exists, comprising a README, two runbooks and a partial API reference. Published privacy notice and terms of service. Offshore contributor agreements, three, reviewed for IP assignment language only and not otherwise.

Bus factor. The number of people who would have to be unavailable before a system can no longer be maintained. A bus factor of one means one person.

Copyleft. A class of open source licence that conditions use on making source code available. The AGPL extends this obligation to software offered over a network, not only software distributed as files.

Referential integrity. Database rules ensuring that related records stay consistent: an invoice cannot reference a customer that does not exist.

Soft deletion. Marking a record as deleted rather than removing it, so history is preserved. Mixing soft and hard deletion makes historical figures unstable.

Recovery time objective. How long restoring service is allowed to take after a failure. Untested, it is an aspiration rather than an objective.

Transitive dependency. A software component pulled in indirectly by something the Target chose. The Target is responsible for its behaviour and licence all the same.

Static analysis. Examining source code with tooling, without running it, to surface classes of defect for human review.