

Technology Due Diligence Report

Target: Elastic | Repository: elasticsearch

Report ID: TDD-20261016-060331

Generated: 2026-10-16

Classification: CONFIDENTIAL - for the named buying party and its advisers

Proposed price: USD 20,000,000

Verdict: Acquire with Conditions

Confidence: 67 out of 100

© MTD Services

Document Control and Distribution

This Technology Due Diligence (TDD) report was prepared for the named buying party and its advisers in connection with the proposed acquisition of Elastic. It distils a deterministic, source-grounded static analysis of the target's primary code repository into a structured transaction assessment. The report is intended to be read alongside the buyer's commercial, financial, and legal due-diligence workstreams; it is not a substitute for legal opinion, financial audit, or operational review. All findings, metrics, and cost estimates reproduced in this document derive from a single stored evidence payload, whose per-query provenance is mapped in Appendix P.

The classification, distribution list, and version history below apply to the entire report. Recipients are reminded that the report is a planning-grade assessment, not a contractor quote. Section 3 declares the calibration basis for every financial input; readers should consult that section before relying on any single figure.

Document Control

Field	Value
Report ID	TDD-20261016-060331
Scan date	2026-10-16T07:18:30 (UTC)
Target	Elastic
Scanned repository	elasticsearch
Repository HEAD commit	eb0570f936c219289fce88e6abe9f3dc0a74d54c
Indexed files	33,203
Proposed price	USD 20,000,000
Categorical verdict	Acquire with Conditions
Confidence score	67 out of 100
Classification	CONFIDENTIAL - for the named buying party and its advisers
Distribution	Investment Committee; deal counsel; technology integration lead; M&A adviser

Document control record. Distribution is restricted; onward circulation requires the lead adviser's written consent.

Version History

Version	Date	Author	Change
0.9.2	2026-10-16	TDD workstream	Initial publication-ready rewrite.

Version history. All changes after the initial release will be tracked here with a fingerprint delta against Appendix O.

One-Page Executive Brief

Verdict: Acquire with Conditions. The transaction should proceed only if the eleven conditions catalogued in Chapter 2 are written into the sale and purchase agreement as four condition precedents, six price-adjustment levers, and one warranty. Confidence in the assessment is 67 out of 100, discounted by five partially-assessed pillars and one failed scanner (entanglement).

Headline economics

Remediation is sized at USD 1,019,403, equal to 5.1 percent of the proposed USD 20,000,000 price. The 30-percent confidence interval runs from USD 713,582 on the low side to USD 1,325,223 on the high side. The valuation discount applied by the model is 24.4 percent, and the post-merge integration drag is 80 percent - both at their caps. The remediation estimate is a 100-percent adoption planning bound; the probability-weighted expected loss is not quantified in this scan, so actual expected remediation sits at or below the bound.

Conditions the board must clear

- Four condition precedents - must be satisfied before close or the deal does not sign as structured. AI/ML model-licensing legal review; CI gate as a condition precedent; remediation of reachable known CVEs; rotation of all leaked credentials.
- Six price-adjustment levers - funded or escrowed work items that move value rather than block close. Complexity-reduction milestone; coverage findings; technical-debt remediation fund; integration findings; retention agreements for sole-maintainer modules; regression coverage uplift on high-risk modules.
- One warranty/representation - assignability of third-party contributions. Breach is an indemnity question, not a work plan.

Top three risks for the investment committee

First, the complexity pillar is the only critical-severity finding in the register; getLegalCast in modules/lang-painless/src/main/java/org/elasticsearch/painless/AnalyzerCaster.java carries a cyclomatic complexity of 177 against a 99th-percentile baseline of 10. Second, the retention pillar carries USD 516,129 of remediation - 51 percent of the total - driven by 2,698 critical sole-maintainer modules whose maintainers are at flight risk. Third, the AGPL-3.0 license detected at the repository level is a single high-severity viral copyleft signal that must be reconciled against the buyer's product-distribution model before signing.

What the report does not support

The report does not support a clean read on five domains - CVE, dependency, end-of-life, maintenance, and secrets - because each was only partially assessed. It does not support a clean read on entanglement because the scanner failed with a recursion error. Absence of a finding in those domains is absence of coverage, not absence of risk. No finding in this report is independently

confirmed; all 304 row-level signals are scanner-detected or inferred and require human validation before they are relied on in negotiation.

© MTD Services

Table of Contents

Document Control and Distribution.....	1
One-Page Executive Brief.....	2
Headline economics.....	2
Conditions the board must clear	2
Top three risks for the investment committee	2
What the report does not support.....	2
Chapter 1. Executive Summary and Headline Findings.....	10
1.1 Verdict and recommendation.....	10
1.2 Confidence score	10
1.3 Headline economics.....	10
1.4 Deal-thesis alignment	11
1.5 What the evidence does not support	12
1.6 Top risk findings.....	13
Chapter 2. Transaction Recommendation, Conditions and Escalation Thresholds	14
2.1 Decision tiers	14
2.2 The eleven conditions for acquisition.....	14
2.3 Per-pillar escalation rows	15
2.4 Deal-breaker register	16
2.5 Sensitivity sweep outcomes.....	16
Chapter 3. Remediation Cost Model, Valuation Impact and Sensitivity	18
3.1 Parameters used downstream.....	18
3.2 Remediation line items	19
3.3 Confidence interval.....	21
3.4 Aggregate hours cap	21
3.5 SQALE remediation basis	21
3.6 Scenario branches	22
3.7 Deal components	22
3.8 Deal economics headline reconciliation	23
3.9 Categories not costed this scan	23
3.10 Sensitivity sweep details.....	24
3.11 Risk valuation lines.....	25
3.12 Executive deal-bridge rows	26
3.13 Double-counting ledger	27

3.14 Per-line-item threshold breach view	28
Chapter 4. Licensing and IP Exposure.....	30
4.1 Headline metrics	30
4.2 Per-package detected licenses.....	30
4.3 Material findings (by id).....	31
4.4 License clause findings.....	32
4.5 IP ownership metrics	32
Reading note.....	33
4.6 Transaction implications.....	33
Chapter 5. Security, Vulnerability and Attack Surface Posture.....	34
5.1 Headline metrics	34
5.2 CVE inventory	34
5.3 Secrets candidates	36
5.4 Material findings (by id).....	37
5.5 Attack surface candidate endpoints	37
5.6 Privacy findings	39
5.7 Reading notes and coverage gaps	39
Chapter 6. Supply Chain and Dependency Posture.....	40
6.1 Headline metrics	40
6.2 Direct dependency inventory.....	40
6.3 Lockfile resolution and EOL runtime detail	41
6.4 Transaction implications.....	42
Chapter 7. Code Quality, Complexity and Technical Debt.....	43
7.1 Headline metrics	43
7.2 Cyclomatic and cognitive percentiles	43
7.3 Hotspot symbols	44
7.4 Debt markers.....	45
7.5 Material findings (by id).....	46
Chapter 8. Testing, Coverage and Regression Risk	47
8.1 Headline metrics	47
8.2 Test-deficit module inventory.....	47
8.3 Coverage module detail	48
8.4 High-value coverage gaps.....	49
8.5 Reading note and transaction implications	50
Chapter 9. Architecture, Entanglement and Integration Risk.....	51

9.1	Headline metrics	51
9.2	Entanglement scanner failure	51
9.3	API contract maturity	51
9.4	Database coupling.....	52
9.5	Serialization and protocol-layer risks	52
9.6	Reading note and transaction implications	53
Chapter 10.	Engineering Capacity, Bus Factor and Knowledge Loss Vulnerability	55
10.1	Headline metrics	55
10.2	Key-person risk detail.....	55
10.3	Module bus-factor detail.....	56
10.4	Git team signals	57
10.5	Knowledge loss vulnerability detail	57
10.6	Material findings (by id).....	58
10.7	Reading note and transaction implications	59
Chapter 11.	Maintenance, Documentation and Operational Maturity	60
11.1	Headline metrics	60
11.2	Maintenance coverage gap.....	60
11.3	Document inventory	61
11.4	CI files and gate strictness	61
11.5	Reading note and transaction implications	62
Chapter 12.	AI/ML Footprint	63
12.1	Headline metrics	63
12.2	Framework hits	63
12.3	SDK hits	63
12.4	Model file inventory	64
12.5	Material findings (by id).....	65
12.6	Transaction implications.....	66
Chapter 13.	Technology Stack and Lifecycle Posture.....	68
13.1	Headline metrics	68
13.2	Technology inventory	68
13.3	Technologies by lifecycle	68
13.4	EOL reconciliation and reading note	69
13.5	Transaction implications.....	69
Chapter 14.	Consolidated Risk Register and Top Risks.....	70
14.1	Consolidated top risks.....	70

14.2 Major risks register	71
14.3 Pillar classification register.....	71
14.4 Deal-breaker register	72
Chapter 15. Confidence, Scope Limitations and Material Unknowns	73
15.1 Headline metrics	73
15.2 Integrity issues	73
15.3 Unverified pillars	74
15.4 Coverage gaps by pillar	74
15.5 Out-of-scope evidence register	75
15.6 Per-pillar assessment posture.....	76
15.7 Taint analysis summary	76
Chapter 16. Reading Notes and Honesty Conventions	77
16.1 Assessment coverage	77
16.2 Evidence honesty	77
16.3 Currency of absence	77
16.4 Deal-mechanic vocabulary	78
16.5 Severity and ranking.....	78
16.6 Known limits of this method	78
Executive Artifact A. Risk Heat Map.....	80
A.1 Reading the heat map.....	80
A.2 Interpretation for the board	81
Executive Artifact B. Negotiation Term Sheet	82
B.1 Condition precedents.....	82
B.2 Price-adjustment levers	83
B.3 Warranty / representation.....	85
Executive Artifact C. 100-Day Post-Close Plan.....	86
C.1 Phase 1 - Days 1 to 30 (condition precedents closeout).....	86
C.2 Phase 2 - Days 31 to 60 (retention and complexity triage)	87
C.3 Phase 3 - Days 61 to 100 (debt, integration, IP review).....	87
C.4 Plan assumptions and risks	88
Appendix A. Methodology, Scope and Scan Configuration	90
A.1 Report metadata	90
A.2 Scan mode.....	90
A.3 Pillar posture register	90
A.4 Step timings	91

Appendix B. Metric Definitions and Financial Calibration	92
B.1 Core metric definitions.....	92
Appendix C. Dependency and Lockfile Inventory	93
C.1 Direct dependency inventory (sample)	93
C.2 Lockfile resolution	94
Appendix D. CVE Inventory	95
D.1 CVE records (full 20 rows).....	95
Appendix E. License Findings Inventory	97
E.1 Per-package license findings (sample).....	97
E.2 License clause findings (full 9 rows)	97
Appendix F. Complexity, Duplication and SQALE Detail.....	99
F.1 Complexity hotspot symbols (sample)	99
F.2 Duplication groups (sample)	100
F.3 SQALE debt modules (sample).....	100
Appendix G. Debt Marker Inventory.....	102
G.1 Debt markers (sample).....	102
Appendix H. Attack Surface Candidate Endpoints	104
H.1 Candidate entry points (sample)	104
Appendix I. Key-Person and Knowledge Loss Vulnerability Detail	106
I.1 Key-person risk rows (sample).....	106
I.2 Module bus-factor rows (sample).....	106
I.3 Knowledge loss vulnerability rows (sample)	107
Appendix J. Maintenance, IaC and CI/CD Detail.....	109
J.1 Maintenance assets.....	109
J.2 IaC findings.....	109
J.3 CI files (full 11 rows).....	109
J.4 Coverage artifacts.....	109
Appendix K. Privacy and Secrets Detail	110
K.1 Privacy findings (full 1 row).....	110
K.2 Secret candidates (sample).....	110
Appendix L. AI/ML Inventory.....	112
L.1 Model files (full 3 rows).....	112
Appendix M. Integrity and Data-Quality Issues	113
M.1 Integrity issues (full 11 rows)	113

Appendix N. Taint Analysis Summary.....	114
N.1 Taint summary	114
N.2 Top taint flows	114
Appendix O. Financial Reproduction Fingerprint.....	115
O.1 Reproduction fingerprint.....	115
Appendix P. Evidence Provenance	116
P.1 Evidence provenance table	116
Appendix Q1. Technical Glossary	119
Appendix Q2. Transaction Glossary	122
Appendix R. Contradiction Ledger and Release Record	124
R.1 Contradiction ledger.....	124
R.2 Release record.....	124

Chapter 1. Executive Summary and Headline Findings

1.1 Verdict and recommendation

The recommended categorical decision tier is Acquire with Conditions. The buyer should proceed with the proposed acquisition of Elastic, but only if the eleven conditions catalogued in Chapter 2 are written into the transaction documents as binding obligations, with the four condition precedents enforceable before close and the six price-adjustment levers sized into either escrow, holdback, or an earn-out. The single warranty/representation covering the assignability of third-party contributions should be drafted by deal counsel and referenced from the disclosure schedule. This recommendation is invariant across every parameter in the seventeen-row sensitivity sweep presented in Chapter 3 - every multiplier returns the same categorical tier, which strengthens the recommendation's resilience to seller pushback on input assumptions.

The recommendation is driven by the technical risk register rather than by a single deal-breaker. No pillar returned a deal-breaker verdict; the highest individual finding severity is critical, but it is concentrated in a single pillar (complexity) and a small population of functions that can be sequenced into a post-close remediation workstream. The remaining material risks are priced and addressable; the question for the board is therefore not whether to acquire, but on what terms and with what funded remedies.

1.2 Confidence score

The overall confidence score is 67 out of 100. The score is computed as 20 (base) plus 40 multiplied by coverage (69.4 percent of pillars carried usable signal) plus 40 multiplied by the risk signal (48.3 percent of weighted risk). The score is discounted by five partially-assessed pillars - CVE, dependency, end-of-life, maintenance, and secrets - and by one failed scanner (entanglement, which degraded to NOT_ASSESSED rather than clean). Five additional warnings flag pillars that render high-severity risk without item-level findings (CI Maturity, Coverage, Integration, IP Ownership, Test Deficit); each of those is held on aggregate metrics rather than row-level evidence, and the reading guide in Chapter 16 explains why that posture does not collapse.

1.3 Headline economics

Table 1-1. Headline transaction economics

Metric	Value	Source
Proposed price	USD 20,000,000	decision.proposed_price
Total remediation cost	USD 1,019,403	financial.total_remediation_cost
Remediation as percentage of price	5.1 percent	decision.remediation_cost_pct_of_acquisition
Confidence interval (low / high)	USD 713,582 / USD 1,325,223	remediation_cost_confidence_interval
Valuation discount applied	24.4 percent (capped at 25 percent)	financial.valuation_discount_pct

Metric	Value	Source
Post-merge integration drag	80.0 percent (capped)	financial.post_merge_integration_drag_pct
Total remediation hours	20,388 hours	financial.total_remediation_hours
Person-years of remediation	9.8 person-years	financial.assumptions.person_years
Economic decision tier	Acquire with Conditions	decision.escalation.economic_tier
Conditions escalation threshold	5.0 percent of price	economic_escalation.conditions_if_above_pct
No-go escalation threshold	25.0 percent of price	economic_escalation.no_go_if_above_pct

Headline economics reproduced from the stored decision and financial models. Every figure is deterministic and reproducible from the configuration fingerprint in Appendix O.

The remediation estimate sits at 5.1 percent of the proposed price, which clears the 5.0 percent conditions threshold but stays well below the 25.0 percent no-go threshold. In dollar terms it also clears the USD 250,000 conditions materiality floor by a factor of four. The economic gate is not disputed - both the categorical and economic decision tiers return Acquire with Conditions - which means the board's decision is contractual, not economic: the conditions must be sized, escrowed, and enforced.

Two calibration caveats apply. First, the remediation estimate is priced with the assessment's built-in, unbenchmarked per-unit hours and saturation caps (calibration.applied = false). Treat it as a planning bound for scope and sequencing, not a contractor quote. Second, the 24.4 percent valuation discount and the 80.0 percent integration drag are both at their respective caps (25 percent and 80 percent), which means the underlying raw figures are large enough that the model saturates. This saturation is a flag, not a finding: it tells the board that any further deterioration in the underlying evidence would not move the model output further, so negotiation leverage should be sought through the conditions rather than through a re-priced deal.

1.4 Deal-thesis alignment

All six deal theses were declared side-by-side from the same stored evidence, with none primary and none carrying a pre-negotiated condition. The 1-to-10 alignment score rates how strongly and how completely the stored evidence bears on each thesis within its evidence-state cap; it is not a business-fit score. 'Not quantified' means that no metric resolved from the stored data for that thesis.

Table 1-2. Deal-thesis alignment scores

Perspective	Alignment	Evidence state	Basis
Scale and Expansion	Not quantified (0 of 4 metrics resolved)	Unassessed	All four metrics failed to resolve from stored data and are reported as not quantified. The thesis is unassessed rather than favourable or adverse.
Product Integration and Cross-Sell	7 out of 10 (5 of 5 metrics resolved)	Partially assessed	Contributing pillar(s) partial did not complete a full assessment, so the verdict is capped regardless of the resolved figures.

Perspective	Alignment	Evidence state	Basis
Lean Maintenance and Operating Cost	10 out of 10 (5 of 5 metrics resolved)	Detected, not verified	Remediation effort is an SQALE estimate over static structure. It bounds the size of the maintenance backlog; it does not price a headcount saving.
IP Moat and Proprietary Core	Refused	Unassessed	Not supported by static analysis. No signal distinguishes proprietary algorithmic density from standard framework boilerplate and wrapper templates.
Regulatory and Compliance	6 out of 10 (6 of 6 metrics resolved)	Partially assessed	Contributing pillar(s) partial did not complete a full assessment, so the verdict is capped regardless of the resolved figures.
Talent and Acqui-hire	10 out of 10 (6 of 6 metrics resolved)	Detected, not verified	Git history describes who has touched the code, not who will stay after close. Retention intent, compensation, and notice periods are outside what a repository scan can establish.

Side-by-side deal-thesis alignment. None of the six theses is primary; none carries a condition. Capped verdicts reflect incomplete assessment, not adverse findings.

The two theses scored at 10 out of 10 - Lean Maintenance and Talent - should not be over-read. Both carry the 'Detected, not verified' evidence state, meaning the metrics resolved cleanly but the underlying signals are scanner-detected and require human validation. The Talent thesis in particular is bounded by a hard external limit: a git history cannot establish post-close retention intent, compensation alignment, or notice-period obligations. The two refused or unassessed theses - IP Moat and Scale and Expansion - flag where the buyer must obtain independent evidence beyond the scope of any static source scan.

1.5 What the evidence does not support

Five caveats bound the reader's reliance on this report. First, the report does not support a clean read on one domain whose scanner failed: entanglement. A failed scanner degrades to NOT_ASSESSED, never to clean. Second, the report does not support a clean read on five domains that were only partially assessed: CVE, dependency, end-of-life, maintenance, and secrets. Absence of a finding in those domains is absence of coverage, not absence of risk. Third, no finding in this report is independently confirmed: 304 row-level signals are scanner-detected or inferred and require human validation before they are relied on in negotiation. Fourth, this is a static, offline-or-network-integrated source scan; it does not establish runtime behaviour, production incidents, or anything requiring access to systems, personnel, or contracts. Fifth, the conditions, implications, and escalation thresholds recorded here are the deterministic output of the assessment; they are a starting position for negotiation, not a legal opinion.

1.6 Top risk findings

Table 1-3. Top ten risk findings

Pillar	Title	Severity	Impact	File	Estimated cost (USD)
Complexity	buildBlocks	Critical	Critical	benchmarks/src/main/java/org/elasticsearch/benchmark/compute/operator/BlockBenchmark.java	Not quantified
Complexity	advanceRowGroup	Critical	Critical	x-pack/plugin/esql-datasource-parquet/src/main/java/org/elasticsearch/xpack/esql/datasource/parquet/OptimizedParquetColumnIterator.java	Not quantified
Complexity	applyNonStrictOverlay	Critical	Critical	x-pack/plugin/esql/src/main/java/org/elasticsearch/xpack/esql/datasources/ExternalSourceResolver.java	Not quantified
Retention	Adam Demjen	Critical	Critical	Not quantified	Not quantified
Retention	Alexander Spies	Critical	Critical	Not quantified	Not quantified
Retention	Albert Zaharovits	Critical	Critical	Not quantified	Not quantified
Debt	fixme	High	High	modules/apm/src/main/java/org/elasticsearch/telemetry/apm/internal/export/otelSdk/OtelSdkExportLogsSupplier.java	Not quantified
Debt	fixme	High	High	modules/apm/src/main/java/org/elasticsearch/telemetry/apm/internal/MetricValidator.java	Not quantified
Debt	fixme	High	High	server/src/main/java/org/elasticsearch/common/time/EpochTime.java	Not quantified
License	(repo-level)	High	High	LICENSE.txt	Not quantified

Top ten risk findings rendered from the dashboard sheet. Full inventory: 304 row-level signals across twenty-two pillars, of which zero are Confirmed, 204 are Detected-not-verified, 100 are Inferred, and zero are Partially-assessed, Unassessed, Conflicting, or Unsupported.

Chapter 2. Transaction Recommendation, Conditions and Escalation Thresholds

2.1 Decision tiers

The categorical board decision tier is Acquire with Conditions, and the economic decision tier is also Acquire with Conditions. Both tiers are reproduced from the stored decision model; both are invariant across the entire sensitivity sweep presented in Chapter 3. The escalation driver is the technical risk register, meaning the decision is driven by pillar-level findings and the financial model that prices them, not by a single deal-breaker pillar.

Two escalation thresholds bound the model. The conditions threshold sits at 5.0 percent of the proposed price (with an absolute floor of USD 250,000); remediation above that share triggers a conditional decision. The no-go threshold sits at 25.0 percent of the proposed price; remediation above that share triggers a no-go. The headline remediation figure of 5.1 percent of price clears the conditions threshold but stays well below the no-go threshold, which is why the decision tier is conditional rather than declined.

Table 2-1. Decision and escalation thresholds

Field	Value	Source
Categorical decision tier	Acquire with Conditions	decision.escalation.categorical_tier
Economic decision tier	Acquire with Conditions	decision.escalation.economic_tier
Conditions escalation threshold	5.0 percent	conditions_if_above_pct
No-go escalation threshold	25.0 percent	no_go_if_above_pct
Conditions materiality floor	USD 250,000	conditions_materiality_floor
Economic gate disputed	false	decision.escalation.disputed
Escalation driver	Technical register	decision.escalation.driver

Decision and escalation thresholds reproduced from the stored decision model.

2.2 The eleven conditions for acquisition

The eleven conditions resolve into three distinct deal mechanics, which a buyer negotiates in different places in the sale and purchase agreement. Four are condition precedents - obligations that must be satisfied or proven before close, or the deal does not sign as structured. Six are price-adjustment levers - funded or escrowed work items that move value rather than block close. One is a warranty/representation - a seller statement whose breach is an indemnity question, not a work plan. Quantification and sizing of each condition is for deal counsel; no dollar amount is asserted in this section.

Table 2-2. Conditions for acquisition by deal mechanic

Deal mechanic	Pillar	Condition (verbatim)	Source key
Condition precedent	AI/ML	Obtain legal review of bundled model licensing before close	decision.condition_s_for_acquisition[0]
Condition precedent	CI Maturity	Require an automated CI gate as a condition precedent	decision.condition_s_for_acquisition[1]
Condition precedent	CVE	Remediate reachable known CVEs before close	decision.condition_s_for_acquisition[4]
Condition precedent	Secrets	Rotate all leaked credentials and stand up credential rotation	decision.condition_s_for_acquisition[9]
Price-adjustment lever	Complexity	Include a complexity-reduction milestone in the integration plan	decision.condition_s_for_acquisition[2]
Price-adjustment lever	Coverage	Address coverage findings as a condition precedent	decision.condition_s_for_acquisition[3]
Price-adjustment lever	Debt	Include a technical-debt remediation fund in the integration plan	decision.condition_s_for_acquisition[5]
Price-adjustment lever	Integration	Address integration findings as a condition precedent	decision.condition_s_for_acquisition[6]
Price-adjustment lever	Retention	Secure retention agreements for sole-maintainer modules	decision.condition_s_for_acquisition[8]
Price-adjustment lever	Test Deficit	Raise regression coverage on high-risk modules post-close	decision.condition_s_for_acquisition[10]
Warranty/representation	IP Ownership	Warrant assignability of third-party contributions	decision.condition_s_for_acquisition[7]

Every condition, verbatim, annotated with the deal mechanic it belongs to. The tag is declared at the decision layer, never inferred from the wording.

The four condition precedents - AI/ML model-licensing review, CI gate, CVE remediation, and credential rotation - should be drafted as obligations whose non-performance gives the buyer a walk-away right before signing. The six price-adjustment levers should be sized against the line items in Chapter 3 and either escrowed against a milestone schedule or held back from the purchase price against delivery. The single warranty covering IP assignability should be backed by an indemnity cap sized to the IP reassignment cost (USD 4,730 in the line items, but the legal exposure in a title dispute is materially larger).

2.3 Per-pillar escalation rows

Each pillar's contribution to the remediation total is reproduced below. Retention dominates at USD 516,129 (2.6 percent of price) and is the single largest line item; complexity follows at USD

184,089 (0.9 percent); the remaining eight pillars together account for less than 0.6 percent of price. No pillar individually breaches either escalation gate on its own, but the aggregate of USD 1,019,403 clears the 5.0 percent conditions threshold.

Table 2-3. Per-pillar escalation rows

Pillar	Category	Cost (USD)	Percent of EV	Breach
Retention	Knowledge transfer	\$516,129	2.58 percent	None
Complexity	Critical complexity	\$184,089	0.92 percent	None
Debt	General debt	\$54,475	0.27 percent	None
Test Deficit	Test investment	\$22,514	0.11 percent	None
Dependency	Dependency pinning	\$8,727	0.04 percent	None
IP Ownership	IP reassignment	\$4,730	0.02 percent	None
Attack Surface	Taint remediation	\$4,541	0.02 percent	None
CVE	CVE remediation	\$0	0.00 percent	None
Entanglement	Decoupling	\$0	0.00 percent	None
Maintenance	Staleness remediation	\$0	0.00 percent	None

Each costed category measured against the escalation gates on its own. No single category breaches either gate; the aggregate breach is what triggers the conditions tier.

2.4 Deal-breaker register

No deal-breaker rows were recorded for this scan. The deal-breaker pillars defined in the model are AI/ML, Attack Surface, CVE, IaC, License, and Secrets - a critical rating on any of these pillars would force the no-go verdict. Of those six, only AI/ML carries a high (not critical) rating and the remaining five carry medium, informational, or unverified ratings. The absence of a deal-breaker is not a clean bill of health: it means the model did not find evidence sufficient to force a decline, not that the underlying risks are absent.

2.5 Sensitivity sweep outcomes

The seventeen-row sensitivity sweep multiplies each of seven financial parameters by 0.7, 1.0, and 1.3 (where applicable) and recomputes the board decision, confidence score, and total remediation cost. Two parameters (remediation_timing and scenario_weights) returned 'not quantified' because their stored inputs were absent; they are reported as not-modeled rather than zero. Every multiplier that did resolve returned the same categorical decision tier - Acquire with Conditions - which means the recommendation is robust to seller challenge on any single input assumption.

Table 2-4. Sensitivity sweep outcomes

Parameter	Multiplier	Board decision	Confidence	Total remediation cost
complexity_multiplier	0.7	Acquire with Conditions	67	\$1,016,027

Parameter	Multiplier	Board decision	Confidence	Total remediation cost
complexity_multiplier	1.0	Acquire with Conditions	67	\$1,019,403
complexity_multiplier	1.3	Acquire with Conditions	67	\$1,022,778
discount_rate	0.7	Acquire with Conditions	67	\$1,019,403
discount_rate	1.0	Acquire with Conditions	67	\$1,019,403
discount_rate	1.3	Acquire with Conditions	67	\$1,019,403
hourly_rate	0.7	Acquire with Conditions	67	\$713,582
hourly_rate	1.0	Acquire with Conditions	67	\$1,019,403
hourly_rate	1.3	Acquire with Conditions	67	\$1,325,223
max_total_hours	0.7	Acquire with Conditions	67	\$794,402
max_total_hours	1.0	Acquire with Conditions	67	\$1,019,403
max_total_hours	1.3	Acquire with Conditions	67	\$1,077,610
remediation_timing	Not quantified	Not quantified	Not quantified	Not quantified
scenario_weights	Not quantified	Not quantified	Not quantified	Not quantified
valuation_multiplier	0.7	Acquire with Conditions	67	\$1,019,403
valuation_multiplier	1.0	Acquire with Conditions	67	\$1,019,403
valuation_multiplier	1.3	Acquire with Conditions	67	\$1,019,403

Sensitivity sweep outcomes. Every multiplier that resolves returns the same tier; the recommendation is robust to input challenge.

Chapter 3. Remediation Cost Model, Valuation Impact and Sensitivity

This chapter is the bridge between the technical work and the deal model. Every parameter that can move a number in this report - financial inputs, saturation calibration, valuation and integration-drag curves, confidence weights, decision thresholds, post-close schedule constants and health-posture ceilings - is declared once in the parameters table that opens this chapter. All subsequent figures in the report cite that table rather than repeating the inputs. The confidence interval and sensitivity analysis are what allow the recommendation to survive challenge from a seller's quality-of-earnings provider.

3.1 Parameters used downstream

The parameters table is the single declared home of every input. Values are read from the stored payload where it carries them and from the assessment's own constants otherwise; a parameter that was not configured is listed as not quantified, never assumed away. The table below groups parameters by function: remediation inputs (rate, multipliers, productive hours), aggregate hours cap, valuation and drag curves, per-cost-category saturation, confidence and evidence policy, decision and escalation thresholds, post-close schedule constants, and health-posture ceilings.

Table 3-1. Parameters used downstream

Group	Parameter	Value	Affects
Remediation inputs	Hourly rate	USD 50	Every line-item cost = saturated hours multiplied by rate
Remediation inputs	Complexity multiplier	1.5	Hours per unit for hard-to-remediate complexity hotspots
Remediation inputs	Valuation multiplier	3	Amplifies remediation cost into the valuation discount
Remediation inputs	Integration drag factor	0.15 percent	Post-merge friction sized as hours divided by (8 x 260 x factor)
Remediation inputs	Productive hours per quarter	624 hours	Net quarterly working hours behind per-cause effort estimates
Remediation inputs	Confidence interval width	30 percent	Width of the low/high remediation-cost interval
Remediation inputs	Annual working hours	2,080 hours	Person-years = remediation hours / 2,080
Remediation inputs	Discount rate	Not quantified	No present-value discounting is applied (unrecorded, not zero)
Aggregate hours cap	Max total hours	20,000 hours	Ceiling on remediation hours; surplus above it is decayed

Group	Parameter	Value	Affects
Aggregate hours cap	Surplus factor	0.25	Fraction of hours above max-total-hours that is credited
Valuation and drag	Valuation discount cap	25 percent	Maximum valuation discount on the proposed price
Valuation and drag	Integration drag cap	80 percent	Maximum post-merge integration drag
Confidence policy	Base confidence	20	Base score before coverage and risk-signal additions
Confidence policy	Coverage weight	40	Weighting of pillar coverage in the confidence score
Confidence policy	Risk-signal weight	40	Weighting of risk signal in the confidence score
Confidence policy	Zero-coverage cap	20	Floor when coverage is zero
Confidence policy	No-go floor	60	Floor for no-go verdict
Decision thresholds	Conditions threshold	5 percent	Remediation above this share of price triggers conditions
Decision thresholds	No-go threshold	25 percent	Remediation above this share of price triggers no-go
Decision thresholds	Conditions materiality floor	USD 250,000	Absolute dollars the conditions gate must also clear
Decision thresholds	Deal-breaker pillars	AI/ML, Attack Surface, CVE, IaC, License, Secrets	Critical rating on any forces no-go
Schedule constants	Execution teams	2	Post-close remediation planned against two two-engineer teams
Schedule constants	Workdays per sprint	10	Sprint capacity = teams x 2 engineers x workdays
Schedule constants	Sprint cap	12	Hours beyond this many sprints are reported as unplanned
Schedule constants	Hours per workday	4	Roadmap durations derive as effort-hours divided by 4

Parameters used downstream. The full thirty-eight-row table is reproduced in Appendix B; the abbreviated view here shows the parameters most likely to be probed in negotiation.

3.2 Remediation line items

Eight cost categories carry non-zero remediation this scan. Each category is sized as the product of a count, an hours-per-unit (HPU) figure, and the hourly rate, with a saturation cap that prevents a large population from being linearly multiplied. The single largest line is Knowledge Transfer at USD 516,129, which represents 51 percent of the total remediation cost. It is driven by 2,698 critical sole-maintainer modules costed at an effective 3.83 hours per unit after the saturation cap of 30 and the decay HPU of 4 are applied.

Table 3-2. Remediation line items

Category	Coun t	Full HPU	Sat. cap	Sat. decay HPU	Hours per unit	Total hours	Total cost (USD)	Notes
Knowledge transfer	2,698	8	30	4	3.83	10,323 h	\$516,129	Critical sole-maintainer modules requiring knowledge transfer (costed per unique module, not per at-risk contributor)
High complexity	2,070	6	150	2	2.17	4,484 h	\$224,198	High-complexity functions (exclusive of critical tier)
Critical complexity	798	18	50	4	4.61	3,682 h	\$184,089	Critically complex functions requiring refactoring
General debt	10,717	0.5	200	0.1	0.10	1,090 h	\$54,475	10,717 confirmed technical-debt markers (in-comment annotations and tooling suppressions)
Test investment	59	16	20	4	7.63	450 h	\$22,514	High-regression-risk modules requiring test investment
Dependency pinning	269	1	100	0.5	0.65	174 h	\$8,727	Unpinned dependencies requiring version locking
IP reassignment	25	4	50	2	3.78	95 h	\$4,730	Files with external-dominant authorship requiring IP review
Taint remediation	12	8	20	4	7.57	91 h	\$4,541	Taint flows requiring sanitization

Remediation line items. Eight categories carry cost; five additional categories (critical-path debt, decoupling, staleness remediation, sole-maintainer risk, SQALE remediation) carry zero cost this scan and are listed in §3.39.

The Knowledge Transfer line is the single largest concentration. It is driven by sole-maintainer modules, not by individual contributors, which means the buyer is funding knowledge transfer for 2,698 modules whose institutional knowledge sits with one or two named individuals. The two retention rows in Chapter 10 - Iraklis Psaroudakis, Bogdan Pintea, Craig Taverner, Alexander Spies, and Felix Barnsteiner - are the named carriers of that institutional knowledge. A retention-bonus programme sized against the Knowledge Transfer line is the most direct route to de-risking this concentration.

3.3 Confidence interval

The confidence interval is a 30-percent band applied symmetrically around the hours-per-unit estimates. The high end of the interval sits at USD 1,325,223; the low end sits at USD 713,582. Even at the high end, the remediation figure remains at 6.6 percent of the proposed price - still well below the 25 percent no-go threshold. The interval is a stated-confidence range from the model calibrations, not a stochastic bound.

Table 3-3. Remediation cost confidence interval

Metric	Value
Basis	Plus or minus 30 percent on hours-per-unit estimates
Low	USD 713,582
High	USD 1,325,223
Width percent	30

Confidence interval. Stored from model calibrations, not a stochastic bound.

3.4 Aggregate hours cap

An aggregate hours cap of 20,000 hours is applied to remediation effort. Hours above that ceiling are credited at a surplus factor of 0.25 - only 25 percent of the surplus counts toward the total. The scale factor this scan is 0.946, meaning the model used 94.6 percent of the gross hours as the basis for cost. The cap is a planning discipline: it prevents a small number of high-count categories from crowding out the schedule and forces the buyer to sequence work across sprints.

Table 3-4. Aggregate hours cap

Metric	Value
Applied	true
Max total hours	20,000
Scale factor	0.946
Surplus factor	0.25

3.5 SQALE remediation basis

The SQALE remediation effort basis is reproduced below. SQALE (Software Quality Assessment based on Lifecycle Expectations) is a standardised remediation-effort basis that arrives in per-module remediation hours from the complexity scanner. Seventy-one modules carry a D or E SQALE grade and are costed as complexity hotspots; the double-counting ledger justifies the overlap rather than pricing it twice. The total SQALE remediation effort across all modules is 630,109 days, but only 71 modules are costed as line items, and the line item is not added to the financial total.

Table 3-5. SQALE remediation basis

Metric	Value
Costed as complexity hotspot	71

Metric	Value
D-E graded modules	71
Deduped uncoded modules	0
Hours equivalent	5,040,870
Line item added	false
SQALE remediation effort (days)	630,109

SQALE reconciliation. Debt-effort days are derived from stored SQALE/grade effort values; the same modules coded as complexity hotspots are reconciled in the double-counting ledger rather than priced twice.

3.6 Scenario branches

Four scenario branches are enabled in the economic layers model. Each carries an evidence basis, a total impact figure, a technology-VaR figure, a transaction-impact figure, and a not-modeled reason where applicable. Disabled branches are reported as not-modeled, not zero.

Table 3-6. Scenario branches

Scenario ID	Title	Enabled	Evidence basis	Total impact	Technology VaR	Transaction impact
acquire_remediate_post_close	Acquire and remediate post-close	true	Transaction EV + layer-1 remediation + integration drag	\$15,427,804	Not quantified	Not quantified
material_failure	Material failure / downside case	true	Analyst calibration on documented scan evidence	\$90,194	\$90,194	Not quantified
partial_remediation	Partial remediation	true	Config calibration (analyst_calibration)	\$522,487	Not quantified	Not quantified
remediate_before_close	Remediate before close	true	Layer-1 remediation schedule + layer-2 residual	\$998,299	Not quantified	\$4,890,000

Scenario branches. Disabled branches read not quantified rather than zero. The remediate-before-close scenario is the most relevant for the conditions tier.

3.7 Deal components

Deal components are never collapsed. Each component carries its own stored amount, basis, confidence, calculation, and assumptions. Components are never labelled as a market-style VaR figure, and an unquantified component reads not quantified rather than zero.

Table 3-7. Deal components (never collapsed)

Component type	Impact type	Value (amount)	Assessment state	Evidence state	Source key
Headline EV	Revenue disruption	\$20,000,000	Assessed with findings	Quantified with evidence	transaction.headline_ev

Component type	Impact type	Value (amount)	Assessment state	Evidence state	Source key
Integration/separation/TSA	Integration separation cost	\$16,000,000	Assessed with findings	Quantified with evidence	layer1.integration_drag_pct
Net quantified tech impact	Remediation cost	\$16,719,403	Assessed with findings	Quantified with evidence	layer4.net_quantified_tech_impact
Other quantified tech exposure	Security incident	\$150,000	Assessed with findings	Quantified with evidence	config.other_evidence_supported_impacts[0]
Potential synergy	Customization burden	\$500,000	Assessed with findings	Quantified with evidence	config.synergy_value
Remediation cost	Remediation cost	\$1,019,403	Assessed with findings	Quantified with evidence	layer1.total_cost
Residual expected loss	Operational downtime	\$50,000	Assessed with findings	Quantified with evidence	layer2.aggregate_residual_expected_loss

Deal components. The headline EV and integration drag dominate the headline; the residual expected loss is the modelled post-remediation tail.

3.8 Deal economics headline reconciliation

The deal-economics arithmetic is reproduced as stored. Headline enterprise value is USD 20,000,000. Net quantified technology impact is USD 16,719,403. Adjusted economic value is USD 15,000,000. The deal price adjustment is USD 5,000,000, which is exactly at the 25 percent valuation adjustment cap of USD 5,000,000. The valuation adjustment is therefore capped. The size of any escrow, holdback, warranty, or indemnity is a qualitative option for deal counsel and is deliberately not a number in this report.

Table 3-8. Deal economics headline valuation reconciliation

Headline EV	Net quantified tech impact	Adjusted economic value	Deal price adjustment	Valuation adjustment cap (percent)	Valuation adjustment cap (amount)	Capped	No adjustment reason
\$20,000,000	\$16,719,403	\$15,000,000	\$5,000,000	25.0 percent	\$5,000,000	true	Not quantified

Deal economics headline reconciliation. The valuation adjustment is at its cap, meaning any further deterioration in underlying evidence would not move the model output further.

3.9 Categories not costed this scan

Five cost categories carry no line item this scan. Each is explicitly zero in Remediation_Costs rather than silently absent. Rendering the gap here keeps the remediation scope honest rather than presenting a clean table.

- Critical-path debt - no line item this scan (explicitly zero in Remediation_Costs).
- Decoupling - no line item this scan (explicitly zero in Remediation_Costs).
- Staleness remediation - no line item this scan (explicitly zero in Remediation_Costs).

- Sole-maintainer risk - no line item this scan (explicitly zero in Remediation_Costs).
- SQALE remediation - no line item this scan (explicitly zero in Remediation_Costs).

3.10 Sensitivity sweep details

The detailed sensitivity sweep reproduces the total remediation hours, total remediation cost, valuation discount percentage, post-merge integration drag percentage, board decision, and confidence score for each multiplier. The most negotiation-relevant observation is that the hourly-rate multiplier moves the cost in a wider band than any other parameter - from USD 713,582 at 0.7x to USD 1,325,223 at 1.3x - which corresponds exactly to the confidence interval. The complexity multiplier moves the cost by only USD 6,751 across the entire 0.7 to 1.3 range, because the saturation cap absorbs most of the variation.

Table 3-9. Sensitivity sweep details

Parameter	Multiplier	Value	Total remediation hours	Total remediation cost	Valuation discount percent	Post-merge drag percent	Board decision	Confidence
complexity_multiplier	0.7	1.05	20,320 h	\$1,016,027	24.45	80	Acquire with Conditions	67
complexity_multiplier	1.0	1.5	20,388 h	\$1,019,403	24.45	80	Acquire with Conditions	67
complexity_multiplier	1.3	1.95	20,456 h	\$1,022,778	24.46	80	Acquire with Conditions	67
discount_rate	0.7	0.0245	20,388 h	\$1,019,403	24.45	80	Acquire with Conditions	67
discount_rate	1.0	0.035	20,388 h	\$1,019,403	24.45	80	Acquire with Conditions	67
discount_rate	1.3	0.0455	20,388 h	\$1,019,403	24.45	80	Acquire with Conditions	67
hourly_rate	0.7	35	20,388 h	\$713,582	23.28	80	Acquire with Conditions	67
hourly_rate	1.0	50	20,388 h	\$1,019,403	24.45	80	Acquire with Conditions	67

Parameter	Multiplier	Value	Total remediation hours	Total remediation cost	Valuation discount percent	Post-merge drag percent	Board decision	Confidence
hourly_rate	1.3	65	20,388 h	\$1,325,223	24.83	80	Acquire with Conditions	67
max_total_hours	0.7	14,000	15,888 h	\$794,402	23.73	80	Acquire with Conditions	67
max_total_hours	1.0	20,000	20,388 h	\$1,019,403	24.45	80	Acquire with Conditions	67
max_total_hours	1.3	26,000	21,552 h	\$1,077,610	24.56	80	Acquire with Conditions	67
valuation_multiplier	0.7	2.1	20,388 h	\$1,019,403	23.28	80	Acquire with Conditions	67
valuation_multiplier	1.0	3	20,388 h	\$1,019,403	24.45	80	Acquire with Conditions	67
valuation_multiplier	1.3	3.9	20,388 h	\$1,019,403	24.83	80	Acquire with Conditions	67

Sensitivity sweep details. Two parameters (remediation_timing and scenario_weights) returned not quantified for every multiplier and are omitted from this view; they are listed in Appendix B.

3.11 Risk valuation lines

Nine risk valuation lines are recorded. Only one - getLegalCast in the complexity pillar - is quantified. The remaining eight carry NOT_QUANTIFIED as their assessment state because the financial.risk_parameters input is empty in this scan. An unquantified line is named rather than priced at zero, and the block renders the linked layer-1 remediation evidence per line so a buyer can re-derive the number rather than trust it.

Table 3-10. Risk valuation lines

Pillar	Title	Assessment state	Expected loss before	Remediation cost	Residual expected loss	Risk reduction value
Complexity	getLegalCast	Assessed with findings	\$337,500	\$184,089	\$50,000	\$287,500

Pillar	Title	Assessment state	Expected loss before	Remediation cost	Residual expected loss	Risk reduction value
AI/ML	elser_model_2	Not quantified	Not quantified	Not quantified	Not quantified	Not quantified
CI Maturity	CI maturity risk	Not quantified	Not quantified	Not quantified	Not quantified	Not quantified
Coverage	Coverage risk	Not quantified	Not quantified	Not quantified	Not quantified	Not quantified
Debt	Hack marker	Not quantified	Not quantified	\$54,475	Not quantified	Not quantified
Integration	Integration risk	Not quantified	Not quantified	Not quantified	Not quantified	Not quantified
IP Ownership	IP ownership risk	Not quantified	Not quantified	\$4,730	Not quantified	Not quantified
Retention	Iraklis Psaroudakis	Not quantified	Not quantified	\$516,129	Not quantified	Not quantified
Test Deficit	Test deficit risk	Not quantified	Not quantified	\$22,514	Not quantified	Not quantified

Risk valuation lines. One quantified line drives the residual expected loss of USD 50,000; the rest are NOT_QUANTIFIED because financial.risk_parameters ships empty this scan.

3.12 Executive deal-bridge rows

The executive deal-bridge renders one chain per material risk line: the stored evidence, the technical finding, the business consequence, the economic impact, the remediation cost, the residual risk that survives it, and the deal consequence. This is the buyer's audit trail from a code observation to a price question.

Table 3-11. Executive deal-bridge rows

Finding	Business consequence	Economic impact	Remediation cost	Residual risk	Transaction consequence
getLegalCast	Expected loss of USD 337,500 before remediation (analyst calibration)	\$337,500	\$184,089	\$50,000	Referenced by enabled deal scenarios remediate_before_close, acquire_remediate_post_close, partial_remediation, material_failure
elser_model_2	Expected loss of NOT_QUANTIFIED before remediation	Not quantified	Not quantified	Not quantified	Referenced by enabled deal scenarios remediate_before_close, acquire_remediate_post_close, partial_remediation, material_failure
CI maturity risk	Expected loss of NOT_QUANTIFIED	Not quantified	Not quantified	Not quantified	Referenced by enabled deal scenarios remediate_before_close, acquire_remediate_post_close, partial_remediation, material_failure

Finding	Business consequence	Economic impact	Remediation cost	Residual risk	Transaction consequence
Coverage risk	Expected loss of NOT_QUANTIFIED	Not quantified	Not quantified	Not quantified	Referenced by enabled deal scenarios remediate_before_close, acquire_remediate_post_close, partial_remediation, material_failure
Hack marker	Expected loss of NOT_QUANTIFIED	Not quantified	\$54,475	Not quantified	Referenced by enabled deal scenarios remediate_before_close, acquire_remediate_post_close, partial_remediation, material_failure
Integration risk	Expected loss of NOT_QUANTIFIED	Not quantified	Not quantified	Not quantified	Referenced by enabled deal scenarios remediate_before_close, acquire_remediate_post_close, partial_remediation, material_failure
IP ownership risk	Expected loss of NOT_QUANTIFIED	Not quantified	\$4,730	Not quantified	Referenced by enabled deal scenarios remediate_before_close, acquire_remediate_post_close, partial_remediation, material_failure
Iraklis Psaroudakis	Expected loss of NOT_QUANTIFIED	Not quantified	\$516,129	Not quantified	Referenced by enabled deal scenarios remediate_before_close, acquire_remediate_post_close, partial_remediation, material_failure
Test deficit risk	Expected loss of NOT_QUANTIFIED	Not quantified	\$22,514	Not quantified	Referenced by enabled deal scenarios remediate_before_close, acquire_remediate_post_close, partial_remediation, material_failure

Executive deal-bridge. The getLegalCast row is the only fully quantified chain.

3.13 Double-counting ledger

The double-counting ledger reconciles figures that appear on multiple surfaces. Shared-registry keys appear once, on multiple surfaces, never added twice. Three justified overlapping keys are recorded: layer1.integration_drag_pct, layer1.total_cost, and layer2.aggregate_residual_expected_loss. The double-counting ledger clean verdict is true.

Table 3-12. Double-counting ledger (selected)

Source key	Layer	Amount	Assessment state	Double-counting group
layer1.integration_drag_pct	deal_component	\$16,000,000	Assessed with findings	g:layer1_shared
layer1.integration_drag_pct	scenario_component	\$14,431,083	Assessed with findings	g:layer1_shared
layer1.total_cost	deal_component	\$1,019,403	Assessed with findings	g:layer1_shared
layer1.total_cost	scenario_component	\$951,623	Assessed with findings	g:layer1_shared
layer1.total_cost.x_partial	scenario_component	\$475,812	Assessed with findings	Not quantified
layer2.aggregate_residual_expected_loss	deal_component	\$50,000	Assessed with findings	g:layer2_shared
layer2.aggregate_residual_expected_loss	scenario_component	\$45,097 / \$46,676	Assessed with findings	g:layer2_shared
complexity.summary.critical_complexity_count	cost_component	\$184,089	Assessed with findings	Not quantified
config.synergy_value	deal_component	\$500,000	Assessed with findings	Not quantified
layer2.risk_reduction_value	risk_component	\$287,500	Assessed with findings	Not quantified

Selected double-counting ledger rows. Three shared-registry keys appear on multiple surfaces; the ledger justifies the overlap.

3.14 Per-line-item threshold breach view

Each costed category measured against the escalation gates on its own. Percent of price is derived as total cost divided by proposed price multiplied by 100, from two stored figures. It is not a new estimate. No single category breaches either gate; the aggregate breach is what triggers the conditions tier.

Table 3-13. Per-line-item threshold breach view

Category	Total cost	Percent of price	Gate
Knowledge transfer	\$516,129	2.58 percent	Below both gates on its own
High complexity	\$224,198	1.12 percent	Below both gates on its own

Category	Total cost	Percent of price	Gate
Critical complexity	\$184,089	0.92 percent	Below both gates on its own
General debt	\$54,475	0.27 percent	Below both gates on its own
Test investment	\$22,514	0.11 percent	Below both gates on its own
Dependency pinning	\$8,727	0.04 percent	Below both gates on its own
IP reassignment	\$4,730	0.02 percent	Below both gates on its own
Taint remediation	\$4,541	0.02 percent	Below both gates on its own

© MTD Services

Chapter 4. Licensing and IP Exposure

The license posture of the packaged components that ship in the target - viral and restrictive copyleft exposure, unknown licenses, contamination chains, and the third-party ownership structure of the files - drives two distinct transaction risks. Copyleft and contamination exposure can affect integration into a closed-source acquirer product, trigger customer disclosure obligations, and require carve-outs or re-licensing. IP ownership drives title and warranty risk. The two are addressed by different conditions in Chapter 2: a price-adjustment lever for IP reassignment (USD 4,730) and a warranty/representation for assignability of third-party contributions.

4.1 Headline metrics

Table 4-1. License and IP ownership headline metrics

Metric	Value
License findings inventory	1,305 findings
Viral license count	0
Restrictive license count	0
Unknown license count	1,293
Licensed packages total	1,299
Contamination chains	0 chains
IP ownership attribution rows	773 attributions
Total authors	2,969
External author count	2,546
External blamed-line percent	74.27 percent
External commit percent	74.27 percent
External domain count	616
External owned files	25
IP risk score	0.5084
High-risk files	25 entries

License and IP headline metrics. The zero viral/restrictive count is encouraging but is materially undermined by the 1,293 unknown-license count.

4.2 Per-package detected licenses

A sample of the per-package detected licenses is reproduced below. The repository-level AGPL-3.0 finding is the only viral/restrictive signal in the entire 1,305-row inventory. The 1,293 UNKNOWN entries dominate the inventory and represent the principal IP uncertainty. Most UNKNOWN entries correspond to direct dependencies declared in build.gradle files where the package metadata did not carry a machine-readable license field.

Table 4-2. Per-package detected licenses (sample)

Package name	Detected license	Is viral	Is restrictive	Confidence	Source file
(repo-level)	AGPL-3.0	true	true	0.8	LICENSE.txt
(repo-level)	Apache-2.0	false	false	0.8	libs/exponential-histogram/LICENSE.txt
(repo-level)	Apache-2.0	false	false	0.8	libs/h3/LICENSE.txt
(repo-level)	Apache-2.0	false	false	0.8	libs/tdigest/LICENSE.txt
(repo-level)	MIT	false	false	0.8	x-pack/plugin/sql/connectors/tableau/connector/LICENSE.txt
(repo-level)	MIT	false	false	0.8	x-pack/plugin/sql/connectors/tableau/tdvt/tds/LICENSE.txt
@tsconfig/node24	MIT	false	false	0.7	.buildkite/package.json
@types/node	MIT	false	false	0.7	.buildkite/package.json
@types/sax	MIT	false	false	0.7	.buildkite/package.json
at.yawk.lz4:lz4-java	UNKNOWN	false	false	0	libs/lz4/build.gradle
ch.obermuhlner:big-math	UNKNOWN	false	false	0	libs/core/build.gradle
co.elastic.logging:ecs-logging-core	UNKNOWN	false	false	0	server/build.gradle
com.amazonaws:aws-java-sdk-core	UNKNOWN	false	false	0	x-pack/plugin/stateless/build.gradle
com.azure:azure-core	UNKNOWN	false	false	0	modules/repository-azure/build.gradle
com.carrotsearch:hppc	UNKNOWN	false	false	0	server/build.gradle
com.fasterxml.jackson.core:jackson-annotations	UNKNOWN	false	false	0	libs/arrow/build.gradle
com.google.guava:guava	UNKNOWN	false	false	0	distribution/tools/keystore-cli/build.gradle
com.google.protobuf:protobuf-java	UNKNOWN	false	false	0	modules/repository-gcs/build.gradle

Per-package detected licenses (sample of 18 rows from 1,305). Full inventory: Appendix E.

4.3 Material findings (by id)

Five license findings are recorded. F-license-001 is the only high-severity signal and corresponds to the repo-level AGPL-3.0 detection. F-license-002 through F-license-005 are low-severity and correspond to per-package findings against the .buildkite/package.json manifest, each carrying the same M&A implication but a smaller materiality.

Table 4-3. Material findings (by id)

Finding id	Title	Severity	Evidence state	File	M&A implication
F-license-001	(repo-level)	High	Detected, not verified	LICENSE.txt	Obtain a representation and warranty covering license compliance for the shipped product, with an indemnity for any copyleft exposure. Quantification and sizing are for deal counsel; no amount is asserted here. This row is a scanner signal, not a validated exposure; it must be validated before it is relied on in negotiation.
F-license-002	yaml	Low	Detected, not verified	.buildkite/package.json	Obtain a representation and warranty covering license compliance for the shipped product, with an indemnity for any copyleft exposure. Quantification and sizing are for deal counsel.
F-license-003	sax	Low	Detected, not verified	.buildkite/package.json	Obtain a representation and warranty covering license compliance for the shipped product, with an indemnity for any copyleft exposure.
F-license-004	@tsconfig/node24	Low	Detected, not verified	.buildkite/package.json	Obtain a representation and warranty covering license compliance for the shipped product, with an indemnity for any copyleft exposure.
F-license-005	@types/node	Low	Detected, not verified	.buildkite/package.json	Obtain a representation and warranty covering license compliance for the shipped product, with an indemnity for any copyleft exposure.

Material license findings. *F-license-001 (AGPL-3.0 repo-level) is the only high-severity signal; the remaining four are low-severity per-package findings.*

4.4 License clause findings

Nine license clause findings are recorded across six license files. Three attribution clauses, three patent-grant clauses (permissive), two warranty-disclaimer clauses (permissive), and one patent-grant clause (permissive) on the `iron_bank` license. All nine clause findings show '0 matched packages', meaning no shipped package falls under the clause via the contamination analysis. The clauses are reproduced in Appendix E.

4.5 IP ownership metrics

The IP ownership pillar is rated high risk and carries a 0.5084 risk score. Of 2,969 total authors, 2,546 are external to the corporate domain (elastic.co), accounting for 74.27 percent of blamed lines and 74.27 percent of commits. External domains number 616; 25 files are flagged as external-owned.

Attribution ratios are a diligence signal, not legal proof of ownership - the M&A implication is a warranty/representation on assignability rather than a per-file re-titling exercise.

Reading note

IP Ownership: attribution ratios are a diligence signal, not legal proof of ownership. Pillar risk is held on aggregate metrics, not item-level findings. Posture and aggregate summary metrics (Appendix A) are cross-checked by the evidence queries; each figure is stored ground truth rendered exactly once.

4.6 Transaction implications

Three implications flow from this chapter. First, the AGPL-3.0 repo-level finding must be reconciled against the buyer's product-distribution model before signing. If the buyer's product is closed-source and the AGPL-3.0 applies to the shipped binary, the integration may require either a carve-out from the acquired asset or a separate commercial-license agreement with the copyright holders - neither of which is establishable from a static source scan. Second, the 1,293 UNKNOWN license entries should be priced as a warranty/representation plus an indemnity cap sized to the IP reassignment line item (USD 4,730 in the remediation model, but the legal exposure in a title dispute is materially larger). Third, the 25 high-risk external-owned files should be triaged in the 100-day plan (Chapter 23, Phase 3) for assignment-agreement review against the seller's CLA records, which is outside the scope of any static analysis.

Chapter 5. Security, Vulnerability and Attack Surface Posture

This chapter consolidates the end-to-end security picture: known advisory exposure, critical-severity posture, secret hygiene, infrastructure-as-code findings, attack-surface composition, and privacy-relevant data flows. The findings drive cyber-insurance sizing, regulatory disclosure timing, and the cyber-warranty language in the acquisition agreement. Coverage gaps in this pillar set are a direct credibility test of the seller's claims - every caveat in §5.7 should be reflected in the disclosure schedule.

5.1 Headline metrics

Table 5-1. Security headline metrics

Metric	Value
CVE count	20
Critical CVE count	0
Packages queried against advisories	320
Unresolved packages	235
Advisory source	osv.dev
Secret candidates	220
High-confidence secrets	4
Live critical secrets	0
History-only secrets	68
IaC findings total	0
Attack surface candidate endpoints	53
Unreferenced endpoints	51
Dynamic endpoints	0
Untested candidate endpoints	53
Candidate exposure score	0.2819
Privacy findings total	1
PII endpoint count	0
Egress SDK count	0
Sensitive log count	1

Security headline metrics. The zero critical-CVE and zero live-critical-secret counts are partially encouraging, but the 235 unresolved packages and 220 secret candidates require human validation before reliance.

5.2 CVE inventory

The CVE pillar is rated informational but only partially assessed. Of 320 packages queried against advisories, 235 could not be resolved to a version (no lockfile / unpinned), so the advisory check covered only the 320 resolvable package(s). 'No critical CVEs' applies to that queried population only, not to every declared dependency. Twenty advisories were returned across the

resolvable population. All twenty are marked 'fixed available: false' and 'remediation class: no_fixed_release', meaning no upstream patch is published for the version pinned in the manifest.

Table 5-2. CVE inventory (full 20 rows)

ID	Severity	Package name	Ecosystem	Version	Fixed available	Fixed version	Remediation class
GHSA-337f-xr2x-6fcf	UNKNOWN	org.apache.kerby:ldap-backend	maven	1.1.1	false	Not applicable	no_fixed_release
GHSA-4cx2-fc23-5wg6	UNKNOWN	org.bouncycastle:bcpkix-fips	maven	2.0.7	false	Not applicable	no_fixed_release
GHSA-8wm5-8h9c-47pc	UNKNOWN	org.apache.hadoop:hadoop-p-common	maven	2.8.5	false	Not applicable	no_fixed_release
GHSA-f5fw-25gw-5m92	UNKNOWN	org.apache.hadoop:hadoop-p-common	maven	2.8.5	false	Not applicable	no_fixed_release
GHSA-f8vc-wfc8-hxqh	UNKNOWN	org.apache.hadoop:hadoop-p-common	maven	2.8.5	false	Not applicable	no_fixed_release
GHSA-gx2c-fvhc-ph4j	UNKNOWN	org.apache.hadoop:hadoop-p-common	maven	2.8.5	false	Not applicable	no_fixed_release
GHSA-rmpj-7c96-mrg8	UNKNOWN	org.apache.hadoop:hadoop-p-common	maven	2.8.5	false	Not applicable	no_fixed_release
GHSA-j288-q9x7-2f5v	UNKNOWN	commons-lang:commons-lang	maven	2.6	false	Not applicable	no_fixed_release
GHSA-jr6h-r7vg-f9mc	UNKNOWN	org.ini4j:ini4j	maven	0.5.2	false	Not applicable	no_fixed_release
GHSA-28wg-ghj8-5hvj	UNKNOWN	nanoid	npm	3.3.12	false	Not applicable	no_fixed_release
GHSA-2v37-7h3g-55p8	UNKNOWN	nanoid	npm	3.3.12	false	Not applicable	no_fixed_release
GHSA-48c2-rrv3-qjmp	UNKNOWN	yaml	npm	2.3.2	false	Not applicable	no_fixed_release
GHSA-68fv-2mzg-jv7q	UNKNOWN	source-map-js	npm	1.2.1	false	Not applicable	no_fixed_release
GHSA-82fw-gwwq-j7x9	UNKNOWN	@vitest/mocker	npm	4.1.7	false	Not applicable	no_fixed_release

ID	Severity	Package name	Ecosystem	Version	Fixed available	Fixed version	Remediation class
GHSA-82fw-gwwq-j7x9	UNKNOWN	vitest	npm	4.1.7	false	Not applicable	no_fixed_release
GHSA-fx2h-pf6j-xeff	UNKNOWN	vite	npm	7.3.3	false	Not applicable	no_fixed_release
GHSA-v6wh-96g9-6wx3	UNKNOWN	vite	npm	7.3.3	false	Not applicable	no_fixed_release
GHSA-fxqj-rqcc-2cmp	UNKNOWN	postcss	npm	8.5.14	false	Not applicable	no_fixed_release
GHSA-r28c-9q8g-f849	UNKNOWN	postcss	npm	8.5.14	false	Not applicable	no_fixed_release
GHSA-g7r4-m6w7-qqqr	UNKNOWN	esbuild	npm	0.27.7	false	Not applicable	no_fixed_release

CVE inventory (full 20 rows). All advisories carry UNKNOWN severity because OSV did not return a CVSS score; all carry 'no_fixed_release' because no upstream patch is published for the pinned version.

5.3 Secrets candidates

Two hundred and twenty secret candidates were detected. Four are high-confidence; none are live-critical (none are active credentials in current production code paths). Sixty-eight exist only in git history (scanned across 108 commits). One hundred and eleven path-excluded candidates were not scanned - partial coverage. The candidates by kind are reproduced below.

Table 5-3. Secrets by kind

Kind	Count
AWS access key	24
Certificate block	11
Connection string	1
Generic password assignment	174
Private key block	10

Secrets by kind. Generic password assignment dominates the candidate population; AWS access keys dominate the high-confidence subset.

5.4 Material findings (by id)

Table 5-4. Material findings (by id)

Finding id	Title	Severity	Evidence state	File	M&A implication
F-attack_surface-001	main	Medium	Detected, not verified	x-pack/plugin/sql/connectors/tableau/tdvt/tdvt_run.py:218	Require the reachable-input inventory to be closed out before close, and treat the residual as a priced integration work stream. Quantification and sizing are for deal counsel.
F-attack_surface-002	main	Medium	Detected, not verified	client/benchmark/src/main/java/org/elasticsearch/client/benchmark/BenchmarkMain.java:18	Require the reachable-input inventory to be closed out before close, and treat the residual as a priced integration work stream.
F-attack_surface-003	main	Medium	Detected, not verified	client/benchmark/src/main/java/org/elasticsearch/client/benchmark/rest/RestClientBenchmark.java:29	Require the reachable-input inventory to be closed out before close, and treat the residual as a priced integration work stream.
F-attack_surface-004	main	Medium	Detected, not verified	test/immutable-collections-patch/src/main/java/org/elasticsearch/jdk/patch/ImmutableCollectionsPatcher.java:36	Require the reachable-input inventory to be closed out before close, and treat the residual as a priced integration work stream.
F-attack_surface-005	main	Medium	Detected, not verified	test/logger-usage/src/main/java/org/elasticsearch/test/loggerusage/ESLoggerUsageChecker.java:68	Require the reachable-input inventory to be closed out before close, and treat the residual as a priced integration work stream.
F-privacy-001	Sensitive data in log statement (ssn)	Medium	Detected, not verified	.buildkite/scripts/flakiness-detection/entrypoints/local.ts:84	Require a representation covering personal-data handling in the shipped product, scoped to the hits recorded in the credential inventory.

Material findings in the security pillar. All six are scanner signals requiring human validation; the credentials and the SSN log hit are the most negotiation-relevant.

5.5 Attack surface candidate endpoints

Fifty-three candidate entry points were identified across the codebase. Fifty-one are unreferenced (no incoming edges). Fifty-three are untested - none of the candidates carries a 'tested' status. Framework identification resolved for zero of fifty-three candidates, meaning the framework semantics that would let the scanner distinguish reachable from unreachable inputs were unavailable for all fifty-three. External reachability could not be established for 53 of 53 candidates because framework semantics were unresolved. Four candidates originate from external sources, which is a partial-coverage indicator.

Table 5-5. Candidate endpoint detail (sample)

Sy mb ol na me	Filepath	Li n e	Endpoi nt type	Exp osur e	Fram ewor k	Ris k lev el	Tes t stat us
mai n	client/benchmark/src/main/java/org/elasticsearch/client/benchmark/BenchmarkMain.java	18	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	benchmarks/src/main/java/org/elasticsearch/benchmark/exponentialhistogram/ExponentialHistogramGenerationBench.java	89	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	benchmarks/src/main/java/org/elasticsearch/benchmark/h3/H3Benchmark.java	44	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	benchmarks/src/main/java/org/elasticsearch/benchmark/index/codec/tsdb/TSDBDocValuesMergeBenchmark.java	76	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	benchmarks/src/main/java/org/elasticsearch/benchmark/search/query/range/DateFieldMapperDocValuesSkipperBenchmark.java	161	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	benchmarks/src/main/java/org/elasticsearch/benchmark/tdigest/TDigestBench.java	129	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	build-tools/gradle-runner/src/main/java/org/elasticsearch/gradle/runner/GradleRunner.java	38	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	build-tools/reaper/src/main/java/org/elasticsearch/gradle/reaper/Reaper.java	50	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	build-tools/src/main/java/org/elasticsearch/gradle/NamedComponentScannerMock.java	17	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	client/benchmark/src/main/java/org/elasticsearch/client/benchmark/rest/RestClientBenchmark.java	29	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	distribution/tools/cli-launcher/src/main/java/org/elasticsearch/launcher/CliToolLauncher.java	54	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	distribution/tools/java-version-checker/src/main/java/org/elasticsearch/tools/java_version_checker/JavaVersionChecker.java	22	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	distribution/tools/server-launcher/src/main/java/org/elasticsearch/server/launcher/ServerLauncher.java	52	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d
mai n	libs/core/src/main/java/org/elasticsearch/jdk/JarHell.java	67	applicati on_entr y	appli catio n	unkno wn	me diu m	unt este d

Candidate endpoint detail (sample of 14 rows from 53). Full inventory: Appendix H. Every candidate is untested; framework identification resolved for zero of fifty-three.

5.6 Privacy findings

One privacy finding is recorded: PRIV-SENSITIVE-LOG in `.buildkite/scripts/flakiness-detection/entrypoints/local.ts` at line 84. The rule flags sensitive data (SSN) emitted in a log statement. The remediation is to redact the value, log a reference identifier, and audit retention. This is a single hit and does not by itself establish a compliance issue; the M&A implication is a representation covering personal-data handling scoped to the credential inventory in Appendix K, not a broad privacy warranty.

5.7 Reading notes and coverage gaps

CVE: advisory coverage reflects the resolvable packages queried - queried subset only, not every declared dependency. Secrets: matches are pattern candidates, not confirmed secrets; high-confidence and git-history-only counts are tracked separately. Privacy: plaintext-credential hits are a flag-and-inventory basis, not a compliance verdict.

The Secrets pillar is partially assessed. Of 33,203 files scanned, 111 path-excluded candidate paths were not scanned. The pillars CVE, Dependency, EOL, Maintenance, and Secrets all carry partial or not-assessed status and are flagged UNVERIFIED in the integrity block (Appendix M). Absence of a finding in any of those pillars is absence of coverage, not absence of risk.

Chapter 6. Supply Chain and Dependency Posture

This chapter consolidates the shape and risk of the third-party software supply chain: direct and transitive breadth, pinning discipline, lockfile hygiene, ecosystem mix, and runtime end-of-life exposure. A broad unpinned transitive supply chain creates upstream-advisory and silent-breaking-change exposure, and affects post-close security operating cost and Software Bill of Materials (SBOM) obligations. The pillar is partially assessed because no lockfile is present - the direct pin ratio of 48.9 percent covers only direct dependencies, and the transitive resolution count is zero.

6.1 Headline metrics

Table 6-1. Supply chain headline metrics

Metric	Value
Direct dependency count	526
Pinned dependencies	257
Ranged dependencies	269
Unpinned dependencies	269
Pin ratio	48.9 percent
Transitive resolved packages	0
Lockfiles present	0
Manifests found	565
EOL runtime rows	0 runtime rows
EOL count	0
Runtimes checked	0
CVE unresolved packages (cross-ref)	235

Supply chain headline metrics. The zero transitive resolved count and zero lockfiles are the root cause of partial coverage in this pillar and in the CVE and EOL pillars.

6.2 Direct dependency inventory

A sample of the direct dependency inventory is reproduced below. The pattern is consistent across the 526-row inventory: Java dependencies declared in build.gradle files with explicit version pins (e.g. `com.azure:azure-core 1.51.0`) sit alongside npm dependencies declared in `.buildkite/package.json` with range specifiers (e.g. `@tsconfig/node24 ^24.0.4`). The 269 unpinned dependencies are predominantly the ranged npm entries; the 257 pinned dependencies are predominantly the explicit Java entries.

Table 6-2. Direct dependency inventory (sample)

Name	Specified	Pinned	Scope	Ecosystem	Manifest
at.yawk.lz4:lz4-java	1.11.4	true	build.gradle	Java	libs/lz4/build.gradle
ch.obermuhner:big-math	2.3.2	true	build.gradle	Java	libs/core/build.gradle

Name	Specified	Pinne d	Scope	Ecosystem	Manifest
com.azure:azure-core	1.51.0	true	build.gradle	Java	modules/repository-azure/build.gradle
com.azure:azure-core	1.57.1	true	build.gradle	Java	x-pack/plugin/inference/build.gradle
com.azure:azure-core-http-netty	1.15.3	true	build.gradle	Java	modules/repository-azure/build.gradle
com.azure:azure-core-http-netty	1.16.3	true	build.gradle	Java	x-pack/plugin/inference/build.gradle
com.azure:azure-identity	1.13.2	true	build.gradle	Java	modules/repository-azure/build.gradle
com.azure:azure-identity	1.18.4	true	build.gradle	Java	x-pack/extras/plugins/microsoft-graph-authz/build.gradle
com.azure:azure-storage-blob	12.27.1	true	build.gradle	Java	modules/repository-azure/build.gradle
com.carrotsearch:hppc	0.8.1	true	build.gradle	Java	server/build.gradle
com.fasterxml.jackson.core:jackson-annotations	2.21	true	build.gradle	Java	libs/arrow/build.gradle
com.google.api-client:google-api-client	2.7.2	true	build.gradle	Java	modules/repository-gcs/build.gradle
com.google.cloud:google-cloud-storage	2.71.0	true	build.gradle	Java	modules/repository-gcs/build.gradle
com.google.code.gson:gson	2.11.0	true	build.gradle	Java	modules/repository-azure/build.gradle
com.google.guava:guava	33.7.2-jre	true	build.gradle	Java	modules/repository-gcs/build.gradle
com.microsoft.azure:msal4j	1.16.2	true	build.gradle	Java	modules/repository-azure/build.gradle
com.squareup.okhttp3:okhttp	4.11.0	true	build.gradle	Java	x-pack/extras/plugins/microsoft-graph-authz/build.gradle
commons-cli:commons-cli	1.5.0	true	build.gradle	Java	plugins/repository-hdfs/build.gradle
commons-lang:commons-lang	2.6	true	build.gradle	Java	plugins/discovery-azure-classic/build.gradle
io.grpc:grpc-api	1.82.2	true	build.gradle	Java	modules/repository-gcs/build.gradle

Direct dependency inventory (sample of 20 rows from 500). Full inventory: Appendix C. The pattern of explicit Java pins alongside ranged npm dependencies is consistent throughout.

6.3 Lockfile resolution and EOL runtime detail

No lockfile resolution rows are recorded this scan. The repository ships no lockfile - neither a Gradle lockfile nor an npm lockfile (package-lock.json or pnpm-lock.yaml) - at any depth scanned. The absence is the partial-coverage root cause: transitive dependency resolution could not be

performed, so the 526 direct pins cover only 49 percent of the dependency surface and the 269 ranged entries resolve to no fixed version.

No EOL runtime rows are recorded. Zero evidence population for EOL is reported as NOT_ASSESSED rather than a clean result. The technology scan detected Java (Gradle), Docker, JavaScript/Node.js, JavaScript/Node.js (pnpm), and Docker Compose - the dependency/CVE/EOL surface for that stack is UNASSESSED, not empty. Tactful disclosure: a buyer should commission a separate lockfile-anchored dependency and EOL assessment before relying on the 20-row CVE inventory in Chapter 5.

6.4 Transaction implications

Three implications flow from this chapter. First, the 49 percent pin ratio is the principal supply-chain risk indicator and should be priced into a condition precedent requiring the establishment of a lockfile (pnpm-lock.yaml, package-lock.json, or a Gradle lockfile) before close, with the residual ranged dependencies either pinned or formally accepted as version-drift risk. Second, the dependency pinning line item (USD 8,727) is small in dollar terms but is the cheapest insurance against future supply-chain advisory shocks; the buyer should fund it as a 100-day plan workstream rather than as a one-time remediation. Third, the SBOM obligation that follows from the buyer's distribution model may require continuous SCA/SBOM monitoring feed and deploy-time gate evidence - neither of which is established by a static source scan, and both of which should be in the post-close operational budget.

Chapter 7. Code Quality, Complexity and Technical Debt

This chapter consolidates the maintainability economics of the codebase: complexity hotspots, cyclomatic and cognitive percentiles, duplication, SQALE debt, explicit debt markers, and the hours required to remediate. The complexity pillar is the only critical-severity pillar in this scan and is the dominant driver of the remediation model after retention. Together with the technical-debt pillar, complexity accounts for 23 percent of the remediation cost (USD 184,089 plus USD 54,475 plus USD 224,198 for high-complexity functions outside the critical tier).

7.1 Headline metrics

Table 7-1. Complexity and debt headline metrics

Metric	Value
Symbols analyzed	354,925
High-complexity symbols	2,868
Critical-complexity symbols	798
Average cyclomatic complexity	1.78
Average cognitive complexity	2.89
Complexity hotspot score	0.0081
SQALE grade	E
SQALE remediation effort (days)	630,109
Total remediation effort (days)	630,109
Debt ratio	68.9 percent
Duplicated LOC	4,996,965
Duplication ratio	68.3 percent
Duplication groups	79,013 groups
Debt markers total	11,251
Critical-path markers	0
Debt density	0.0217

Complexity and debt headline metrics. The SQALE grade E and the 68.9 percent debt ratio are the strongest single indicators of a maintenance-intensive codebase.

7.2 Cyclomatic and cognitive percentiles

The cyclomatic complexity percentiles are: P50 = 1, P90 = 3, P99 = 10. The cognitive complexity percentiles are: P50 = 0, P90 = 8, P99 = 46. These percentiles place the 798 critical-complexity symbols well above the 99th-percentile threshold, which is the threshold at which the SQALE grade E is applied. The averages (1.78 cyclomatic, 2.89 cognitive) sit comfortably within maintainable ranges, which means the risk is concentrated in a long-tail population rather than spread evenly across the codebase - a positive for the integration plan because the remediation effort can be sequenced against named hotspots.

Table 7-2. Complexity percentiles

Metric	P50	P90	P99
Cyclomatic complexity	1	3	10
Cognitive complexity	0	8	46

7.3 Hotspot symbols

The sixteen hotspot symbols with the highest composite risk are reproduced below. GetLegalCast in modules/lang-painless/src/main/java/org/elasticsearch/painless/AnalyzerCaster.java is the worst single function by both metrics: cyclomatic 177 (against a P99 of 10) and cognitive 2,427 (against a P99 of 46). TestFailureStoreAccess and execute in the security CLI carry similar critical profiles. The remediation line item for critical complexity (USD 184,089) covers 798 such symbols, of which the top ten carry the largest weight.

Table 7-3. Hotspot symbols

Name	Filepath	Cyclomatic	Cognitive	Maintainability Index	Composite Risk
getLegalCast	modules/lang-painless/src/main/java/org/elasticsearch/painless/AnalyzerCaster.java	177	2,427	0	0.90
testFailureStoreAccess	x-pack/plugin/security/qa/security-trial/src/javaRestTest/java/org/elasticsearch/xpack/security/failurestore/FailureStoreSecurityRestIT.java	143	675	0	0.90
unicodeScriptToULScript	x-pack/plugin/core/src/main/java/org/elasticsearch/xpack/core/ml/inference/preprocessing/customwordembedding/ScriptCode.java	105	104	15.02	0.87
forPattern	server/src/main/java/org/elasticsearch/common/time/DateFormatters.java	90	905	19.18	0.8501
testAutoscalingCapacity	x-pack/plugin/ml/src/test/java/org/elasticsearch/xpack/ml/autoscaling/NativeMemoryCapacityTests.java	74	0	0	0.85
testPrimitiveIteration	modules/lang-painless/src/test/java/org/elasticsearch/painless/ArrayTests.java	73	72	29.98	0.802
randomSearchSourceBuilder	test/framework/src/main/java/org/elasticsearch/search/RandomSearchRequestGenerator.java	72	145	15.24	0.8695
compute	server/src/main/java/org/elasticsearch/cluster/routing/allocation/allocator/DesiredBalanceComputer.java	71	181	4.8	0.8904
expand	x-pack/plugin/graph/src/main/java/org/elasticsearch/xpack/graph/action/TransportGraphExploreAction.java	67	236	7.31	0.8854
execute	x-pack/plugin/security/cli/src/main/java/org/elasticsearch/xpack/security/cli/AutoConfigureNode.java	67	545	0	0.90

Name	Filepath	Cyclomatic	Cognitive	Maintainability Index	Composite Risk
buildBlocks	benchmarks/src/main/java/org/elasticsearch/benchmark/compute/operator/BlockBenchmark.java	65	95	7.94	0.8841
create	modules/analysis-common/src/main/java/org/elasticsearch/analysis/common/StepperTokenFilterFactory.java	64	918	22.79	0.8544
getNextValidTimeAfter	x-pack/plugin/core/src/main/java/org/elasticsearch/xpack/core/scheduler/Cron.java	63	446	8.87	0.8823
visitDot	modules/lang-painless/src/main/java/org/elasticsearch/painless/phase/DefaultSemanticAnalysisPhase.java	61	297	12.36	0.8753
resolveFieldNames	x-pack/plugin/esql/src/main/java/org/elasticsearch/xpack/esql/session/FieldNameUtils.java	58	200	9.8	0.8804
testToXContent	x-pack/plugin/watcher/src/test/java/org/elasticsearch/xpack/watcher/notification/slack/message/SlackMessageTests.java	58	432	19.05	0.8619

Hotspot symbols. Full inventory: Appendix F. The top ten are the priority for the complexity-reduction milestone in the 100-day plan.

7.4 Debt markers

Eleven thousand two hundred and fifty-one debt markers are recorded. The concentration by type is striking: 7,103 suppression markers (suppression warnings), 3,531 to-do markers, 455 Java debug-print markers, 58 fixme markers, and 8 hack markers. Sixty-six markers carry high severity, 3,531 medium, and 7,654 low. The general-debt remediation line item (USD 54,475) is sized against the 10,717 confirmed markers (annotation + tooling).

Table 7-4. Debt markers by type

Type	Count
Bare except	7
Bug	5
Debug print Java	455
Debug print Py	9
Debug print Ts	63
Fixme	58
Hack	8
Suppression suppress warnings	7,103
Todo	3,531
Xxx	12

Debt markers by type. The 7,103 suppressions dominate the population and warrant a focused review against the 100-day plan.

7.5 Material findings (by id)

Table 7-5. Material complexity and debt findings

Finding id	Title	Severity	Evidence state	File	M&A implication
F-complexity-001	getLegalCast	Critical	Detected, not verified	modules/lang-painless/src/main/java/org/elasticsearch/painless/AnalyzerCaster.java	Treat the critical-complexity population as a priced integration work stream, sequenced with the plan the buyer commissions.
F-complexity-002	execute	Critical	Detected, not verified	x-pack/plugin/security/cli/src/main/java/org/elasticsearch/xpack/security/cli/AutoConfigureNode.java	Treat the critical-complexity population as a priced integration work stream.
F-complexity-003	testFailureStoreAccess	Critical	Detected, not verified	x-pack/plugin/security/qa/security-trial/src/javaRestTest/java/org/elasticsearch/xpack/security/failurestore/FailureStoreSecurityRestIT.java	Treat the critical-complexity population as a priced integration work stream.
F-complexity-004	compute	Critical	Detected, not verified	server/src/main/java/org/elasticsearch/cluster/routing/allocation/allocator/DesiredBalanceComputer.java	Treat the critical-complexity population as a priced integration work stream.
F-complexity-005	expand	Critical	Detected, not verified	x-pack/plugin/graph/src/main/java/org/elasticsearch/xpack/graph/action/TransportGraphExploreAction.java	Treat the critical-complexity population as a priced integration work stream.
F-debt-001	hack	High	Detected, not verified	build-tools-internal/src/main/java/org/elasticsearch/gradle/internal/ElasticsearchBuildCompletePlugin.java:115	Size the general-debt remediation programme as a post-close milestone and hold a holdback against delivery.
F-debt-002	fixme	High	Detected, not verified	modules/apm/src/main/java/org/elasticsearch/telemetry/apm/internal/MetricValidator.java:177	Size the general-debt remediation programme as a post-close milestone.
F-debt-003	fixme	High	Detected, not verified	modules/apm/src/main/java/org/elasticsearch/telemetry/apm/internal/export/otelSdk/OtelSdkExportLogsSupplier.java:70	Size the general-debt remediation programme as a post-close milestone.
F-debt-004	hack	High	Detected, not verified	qa/packaging/src/test/java/org/elasticsearch/packaging/test/PasswordToolsTests.java:76	Size the general-debt remediation programme as a post-close milestone.
F-debt-005	fixme	High	Detected, not verified	server/src/main/java/org/elasticsearch/common/time/EpochTime.java:45	Size the general-debt remediation programme as a post-close milestone.

Material findings. The complexity-critical five are the priority for the condition-precedent or price-adjustment lever on complexity reduction; the debt-high five are the priority for the technical-debt remediation fund.

Chapter 8. Testing, Coverage and Regression Risk

Where the codebase is structurally covered by tests and where it is not: module-level test ratios, high-value coverage gaps, regression-risk concentration, and the financial exposure implied by uninsured high-blast symbols. Test deficit is the leading indicator of post-close regression incidents and the cost of mandated refactoring. The effective insured value of zero dollars in the coverage model translates directly into contingent-liability sizing for the buyer: the codebase has no test-backed safety net behind which a refactor can proceed without explicit risk acceptance.

8.1 Headline metrics

Table 8-1. Testing and coverage headline metrics

Metric	Value
Modules analyzed (test deficit)	4,736
Modules below threshold	4,733
Overall test ratio	0.0 percent
Test deficit score	0.0125
High regression-risk modules	59
Coverage modules analyzed	4,736
Effective insured value	0
Value coverage ratio	0.0 percent
Coverage method	Static symbol-share proxy (test-file symbols weighted by structural value); not runtime or line/branch coverage.
High-value gaps	1,183

Testing and coverage headline metrics. The 4,733 modules below threshold against 4,736 analyzed is a striking concentration: 99.94 percent of modules fail the threshold.

8.2 Test-deficit module inventory

A sample of the test-deficit module inventory is reproduced below. The 'test ratio' column is the ratio of test-file symbols to source-file symbols within the module. Modules with a test ratio of 1 are typically test-fixture modules with zero source files; they are not material risks. The regression-risk column carries a weighted score that combines module value, complexity, and dependency fan-in.

Table 8-2. Test-deficit module inventory (sample)

Module path	Test file count	Source file count	Test ratio	Regression risk
build-tools/src/testFixtures/java/org/elasticsearch/plugin/scanner/test_classes	5	0	1	0
distribution/tools/plugin-cli/src/test/java/org/elasticsearch/plugins/cli/test_model	1	0	1	0
libs/plugin-scanner/src/test/java/org/elasticsearch/plugin/scanner/test_model	5	0	1	0

Module path	Test file count	Source file count	Test ratio	Regression risk
benchmarks	0	1	0	0.05
benchmarks/common/src/main/java/org/elasticsearch/benchmark	0	2	0	0.125
benchmarks/common/src/main/java/org/elasticsearch/benchmark/internal	0	4	0	0.0587
benchmarks/common/src/main/java/org/elasticsearch/benchmark/store	0	1	0	0.05
benchmarks/processor/src/main/java/org/elasticsearch/benchmark	0	1	0	0.05
benchmarks/src/main/java/org/elasticsearch/benchmark/_nightly	0	1	0	0.1058
benchmarks/src/main/java/org/elasticsearch/benchmark/_nightly/esql	0	17	0	0.4225
benchmarks/src/main/java/org/elasticsearch/benchmark/bytes	0	9	0	0.0906
benchmarks/src/main/java/org/elasticsearch/benchmark/cluster/metadata	0	1	0	0.1167
benchmarks/src/main/java/org/elasticsearch/benchmark/common/lucene	0	1	0	0.06
benchmarks/src/main/java/org/elasticsearch/benchmark/common/network	0	1	0	0.1

Test-deficit module inventory (sample of 14 rows from 4,736). Full inventory: workbook sheet Test Deficit.

8.3 Coverage module detail

The coverage module detail is reproduced below for the modules with the largest value exposure. Server modules dominate the value exposure list: index/mapper, cluster/metadata, index/query, action/search, and index/engine are all in the top quartile by both prod-symbol count and risk weight. The x-pack/plugin/esql hierarchy carries three modules in the top quartile, reflecting the relative newness of the ES|QL pipeline and its rapid growth in symbol count.

Table 8-3. Coverage module detail (top by value exposure)

Module	Prod symbols	Test coverage ratio	Risk weight	Value exposure
server/src/main/java/org/elasticsearch/index/mapper	5,207	0	0.7254	0.5259
x-pack/plugin/esql/src/main/java/org/elasticsearch/xpack/esql/datasources	3,318	0	0.6697	0.4519
test/framework/src/main/java/org/elasticsearch/test	1,876	0	1	0.4315
x-pack/plugin/esql-datasource-parquet/src/main/java/org/elasticsearch/xpack/esql/datasource/parquet	1,563	0	0.5556	0.3623
server/src/main/java/org/elasticsearch/cluster/metadata	2,854	0	0.5119	0.3564
server/src/main/java/org/elasticsearch/index/query	1,888	0	0.4833	0.3338
x-pack/plugin/esql/compute/src/main/generated/org/elasticsearch/compute/aggregation	7,201	0	0.3482	0.3335

Module	Prod symbols	Test coverage ratio	Risk weight	Value exposure
modules/lang-painless/src/main/java/org/elasticsearch/painless/phase	536	0	0.3631	0.2382
server/src/main/java/org/elasticsearch/action/search	1,834	0	0.3219	0.2254
x-pack/plugin/esql-datasource-csv/src/main/java/org/elasticsearch/xpack/esql/datasource/csv	622	0	0.3225	0.2115
x-pack/plugin/esql/src/internalClusterTest/java/org/elasticsearch/xpack/esql/action	4,669	0	0.2798	0.2058
server/src/test/java/org/elasticsearch/index/engine	639	0	0.3009	0.1961
build-tools-internal/src/main/java/org/elasticsearch/gradle/internal	693	0	0.4141	0.1855
server/src/main/java/org/elasticsearch/index/engine	1,747	0	0.24	0.1742

Coverage module detail (top 14 by value exposure). Full inventory: [workbook sheet Coverage Gaps](#).

8.4 High-value coverage gaps

The high-value coverage gaps inventory prioritises modules with the largest weighted exposure. Fourteen modules with the highest risk weights are reproduced below. Test framework (risk weight 1.0) leads because the framework carries the highest structural value - a defect in the framework propagates to every test that depends on it. Server-side mapper and query modules follow at risk weights above 0.5.

Table 8-4. High-value coverage gaps

Module	Risk weight	Test coverage ratio
test/framework/src/main/java/org/elasticsearch/test	1	0
server/src/main/java/org/elasticsearch/index/mapper	0.7254	0
x-pack/plugin/esql/src/main/java/org/elasticsearch/xpack/esql/datasources	0.6697	0
x-pack/plugin/esql-datasource-parquet/src/main/java/org/elasticsearch/xpack/esql/datasource/parquet	0.5556	0
server/src/main/java/org/elasticsearch/cluster/metadata	0.5119	0
server/src/main/java/org/elasticsearch/index/query	0.4833	0
build-tools-internal/src/main/java/org/elasticsearch/gradle/internal	0.4141	0
modules/lang-painless/src/main/java/org/elasticsearch/painless/phase	0.3631	0
x-pack/plugin/esql/compute/src/main/generated/org/elasticsearch/compute/aggregation	0.3482	0

Module	Risk weight	Test coverage ratio
x-pack/plugin/esql-datasource-csv/src/main/java/org/elasticsearch/xpack/esql/datasource/csv	0.3225	0
server/src/main/java/org/elasticsearch/action/search	0.3219	0
server/src/test/java/org/elasticsearch/index/engine	0.3009	0
x-pack/plugin/esql/src/internalClusterTest/java/org/elasticsearch/xpack/esql/action	0.2798	0
test/framework/src/main/java/org/elasticsearch/index/mapper	0.267	0

High-value coverage gaps. The 1,183-row inventory is dominated by server modules and the ES|QL pipeline.

8.5 Reading note and transaction implications

Pillar risk: high - posture held on aggregate metrics, not item-level findings. Coverage method: static symbol-share proxy, not runtime or line/branch coverage.

Three implications flow from this chapter. First, the 0.03 percent overall test ratio is the leading indicator of post-close regression incidents. A condition precedent requiring test coverage uplift on the high-value gap modules - at minimum the top fourteen reproduced above - should be drafted into the integration plan, with milestones measured against the high-value gap count (target: 50 percent reduction in 100 days, 80 percent in 180 days). Second, the test investment line item (USD 22,514) is materially understated for a target of this size; the buyer should expect to invest at least an order of magnitude more in the first twelve months of integration, and the condition should reflect that reality. Third, the effective insured value of zero is the single most material coverage caveat: it means the model attaches zero test-backed residual value to the codebase, which makes every refactor a risk-acceptance decision rather than a covered change.

Chapter 9. Architecture, Entanglement and Integration Risk

This chapter consolidates the architectural shape that determines how cleanly the asset can be integrated: layering discipline, cyclic dependencies, cross-layer violations, API-contract maturity, database coupling, and serialization risks. Integration cost is the most under-estimated line item in software acquisition; the integration-risk score and the proprietary-coupling count give the integration-management office a defensible basis for the synergy model and the transition-services scope.

9.1 Headline metrics

Table 9-1. Architecture and integration headline metrics

Metric	Value
Circular-dependency cycles	No recorded data (scanner failed; see §9.6)
Max cycle length	No recorded data (scanner failed)
Cross-layer violations	No recorded data (scanner failed)
Modules in cycles	No recorded data (scanner failed)
Entanglement score	No recorded data (scanner failed)
Integration risk score	10
Schema drift risk	high
Proprietary coupling count	11,731
Integration findings total	11,798

Architecture and integration headline metrics. The integration risk score of 10 is the maximum on the scale; proprietary coupling at 11,731 dominates the finding population.

9.2 Entanglement scanner failure

The entanglement scanner failed this scan with a `RecursionError` (maximum recursion depth exceeded). Per the contradiction ledger (Appendix R, C-ERR-001), failed scanners degrade to `NOT_ASSESSED` rather than clean - the four entanglement headline metrics therefore read 'no recorded data' rather than zero. The integrity block (Appendix M) flags the failure and discounts the confidence score accordingly. The buyer should commission a separate architectural review against the entanglement dimensions before signing, sized against the integration risk score and the proprietary coupling count.

9.3 API contract maturity

API contract maturity is partially assessed. Zero HTTP endpoints were resolved (no OpenAPI specification and no GraphQL schema were found). Two proto files and six types were resolved, suggesting a small gRPC surface. The schema drift risk rating is high, reflecting the presence of 1,146 raw SQL statements (see §9.4) and the cross-schema access pattern.

Table 9-2. API contract maturity

Metric	Value
Endpoint count	0
GraphQL found	false
OpenAPI found	false
Proto files	2
Type count	6

9.4 Database coupling

Database coupling shows 1,146 raw SQL statements and cross-schema access set to true. Zero migration files and zero migration tooling entries are recorded, meaning the codebase has no tracked database migration history - schema changes are applied through raw SQL embedded in code. No Object-Relational Mapping (ORM) usage was detected. Cross-schema access (true) is a flag for the integration plan: the codebase's data model spans more than one logical schema, which complicates a future carve-out or partial integration.

Table 9-3. Database coupling

Metric	Value
Cross schema access	true
Destructive DDL count	0
Migration files	0 entries
Migration tooling	0 entries
ORM usage	false
Raw SQL count	1,146

9.5 Serialization and protocol-layer risks

Eleven thousand seven hundred and thirty-one serialization risks are recorded, dominated by the `libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java` file. Each row flags 'Dangerous deserialization: dynamic_function'. Sixty-seven protocol-layer risks are recorded, all of type 'protocol:raw_socket' across network and entitlement modules. The protocol-layer risks are predominantly in test and build-tool code (DefaultPortDetector, NetworkAccessCheckActions) but include one `libs/entitlement` production-code hit (`NetworkInstrumentation.java`).

Table 9-4. Serialization risks (sample)

Risk type	Filepath	Line	Severity	Description
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	82	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	93	high	Dangerous deserialization: dynamic_function

Risk type	Filepath	Line	Severity	Description
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	104	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	115	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	160	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	171	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	234	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	245	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	293	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	308	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	368	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	379	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	425	high	Dangerous deserialization: dynamic_function
serialization:dynamic_function	libs/tdigest/src/main/java/org/elasticsearch/tdigest/ScaleFunction.java	441	high	Dangerous deserialization: dynamic_function

Serialization risks (sample of 14 rows from 11,731). Full inventory: workbook sheet Serialization Risks. The ScaleFunction.java file accounts for the bulk of the population.

9.6 Reading note and transaction implications

Pillar risk: high - posture held on aggregate metrics, not item-level findings. Entanglement is NOT_ASSESSED due to scanner failure; treat the absence of cycle inventory as absence of coverage, not absence of risk.

Three implications flow from this chapter. First, the integration risk score of 10 (the maximum on the scale) and the 11,731 proprietary-coupling count should be priced into the TSA scope - the buyer should expect a longer-than-baseline transition window and a larger integration engineering team than the headline remediation hours suggest. Second, the cross-schema access flag and the

1,146 raw SQL statements mean a database-migration workstream is required before any partial integration or carve-out; this should be a 100-day plan dependency, not an afterthought. Third, the entanglement scanner failure should be reflected in the disclosure schedule as an explicit 'not assessed' position, with the buyer reserving the right to commission a separate architectural review post-signing under a condition-precedent-style milestone.

© MTD Services

Chapter 10. Engineering Capacity, Bus Factor and Knowledge Loss Vulnerability

This chapter consolidates the human-capital risk embedded in the codebase: sole-maintainer modules, contributor concentration, tenure decay, after-hours cadence as a stress proxy, and the modules whose maintainers are at flight risk. Concentration risk drives retention-bonus sizing, earn-out structure, and the transition-services window. Sole-maintainer modules are a primary cause of post-close silent outages and warrant explicit warranty language.

10.1 Headline metrics

Table 10-1. Engineering capacity and retention headline metrics

Metric	Value
Total authors	2,969
Overall bus factor	30
Critical key-person rows	0
Key-person risk rows	2,969 risk rows
Module bus-factor rows	4,662 module rows
Retention total contributors	2,969
Active contributors	432
Inactive contributors	2,537
At-risk contributors	396
Knowledge loss vulnerability score	0.5313
Critical modules (retention)	7,366
At-risk contributors (model input)	396
Critical sole-maintainer modules (model input)	2,698

Engineering capacity and retention headline metrics. The 0.5313 knowledge loss vulnerability score and the 2,698 critical sole-maintainer modules drive the largest single remediation line item.

10.2 Key-person risk detail

The key-person risk detail is reproduced below. Portugee (portugee@gmail.com) carries the highest risk score (0.4388) with 466,070 total commits - a critical concentration of historical knowledge. Departure impact is rated medium for the top contributor and low for the next thirteen. The retention pillar (which is distinct from key-person: retention carries the modelled flight risk, key-person carries the historical contribution concentration) records 2,969 risk rows of which 2,537 are inactive contributors.

Table 10-2. Key-person risk detail (top 14)

Author name	Author email	Risk score	Total commits	Departure impact
portugee@gmail.com	portugee@gmail.com	0.438801	466,070	medium
rene@elastic.co	rene@elastic.co	0.226206	63,004	low
david.turner@elastic.co	david.turner@elastic.co	0.184465	208,820	low
62058229+ChrisHegarty@users.noreply.github.com	62058229+ChrisHegarty@users.noreply.github.com	0.178643	89,328	low
ryan@iernst.net	ryan@iernst.net	0.176222	78,594	low
nik9000@gmail.com	nik9000@gmail.com	0.166198	382,911	low
me@obrown.io	me@obrown.io	0.165049	138,137	low
pugnascotia@users.noreply.github.com	pugnascotia@users.noreply.github.com	0.158149	41,697	low
artem.prigoda@elastic.co	artem.prigoda@elastic.co	0.154998	40,363	low
lorenzo.dematte@elastic.co	lorenzo.dematte@elastic.co	0.150876	41,168	low
simon.cooper@elastic.co	simon.cooper@elastic.co	0.149473	94,681	low
ievgen.degtiarenko@elastic.co	ievgen.degtiarenko@elastic.co	0.136622	41,054	low
mmack@apache.org	mmack@apache.org	0.131598	18,923	low
yang.wang@elastic.co	yang.wang@elastic.co	0.120524	106,492	low

Key-person risk detail (top 14 of 2,969 rows). Full inventory: Appendix I.

10.3 Module bus-factor detail

The module bus-factor detail reveals the architectural concentration of risk. The unassigned bucket carries a bus factor of 26 (fourteen thousand three hundred seventy-four files); server-side index, cluster, mapper, query, and routing modules carry bus factors of 9 or below. A bus factor of 9 means nine or fewer contributors are responsible for the module - a workable but concentrated institutional knowledge.

Table 10-3. Module bus-factor detail (top 14)

Module path	Bus factor	Total files
_unassigned	26	14,374
server/src/main/java/org/elasticsearch/index	12	30
server/src/test/java/org/elasticsearch/index	11	32
test/framework/src/main/java/org/elasticsearch/test	11	86
server/src/main/java/org/elasticsearch/cluster/metadata	9	83
server/src/main/java/org/elasticsearch/index/mapper	9	175
server/src/main/java/org/elasticsearch/index/query	9	81
server/src/test/java/org/elasticsearch/cluster/metadata	9	102
server/src/test/java/org/elasticsearch/index/mapper	9	224
test/framework/src/main/java/org/elasticsearch/test/res	9	12

Module path	Bus factor	Total files
x-pack/plugin/esql/src/main/java/org/elasticsearch/xdpck/esql/plan/logical	9	76
server/src/main/java/org/elasticsearch/common/util/concurrent	8	33
server/src/main/java/org/elasticsearch/indices	8	36
server/src/main/java/org/elasticsearch/node	8	15

Module bus-factor detail (top 14 of 4,662 rows). Full inventory: Appendix I.

10.4 Git team signals

The git team signals are reproduced below. The after-hours commit percentage of 44.3 percent is a stress proxy - it suggests the active contributor population is operating under sustained deadline pressure, which correlates with flight risk. The bus factor proxy of 0.875 (out of 1.0) and the cadence per week of 666.67 commits are both elevated against typical mature-codebase baselines.

Table 10-4. Git team signals

Metric	Value
After hours commits	886
After hours percent	0.443
Bus factor proxy	0.875
Cadence per week	666.67
Ghost author count	28
Modules analyzed	30
Top1 author share	0.125
Top3 author share	0.277
Top5 author share	0.349
Total commits	2,000
Unique authors	158
Unique emails	162

Git team signals. The after-hours percentage and the cadence per week are the two stress proxies that warrant negotiation attention.

10.5 Knowledge loss vulnerability detail

The knowledge loss vulnerability detail carries the retention risk and blast radius per author. All entries reproduced below carry 'critical' retention risk; the blast radius at risk column captures the number of files that depend on the contributor's institutional knowledge. Jan Kuipers carries a blast radius of 9,690 files; Mariusz Józala carries 10,689 files. These two contributors are the largest single flight-risk concentrations and should be the priority for retention agreement execution.

Table 10-5. Knowledge loss vulnerability detail (top 14)

Author name	Author email	Tenure days	Days since last commit	Retention risk	Blast radius at risk
Johannes Fredén	109296772+jfreden@users.noreply.github.com	1,056	2	critical	0
Valeriy Khakhutskyy	1292899+valeriy42@users.noreply.github.com	2,318	0	critical	0
Kostas Krikellas	131142368+kkrik-es@users.noreply.github.com	1,269	23	critical	720
Matteo Piergiovanni	134913285+piergm@users.noreply.github.com	1,150	99	critical	0
Jan Kuipers	148754765+jan-elastic@users.noreply.github.com	1,067	0	critical	9,690
Fang Xing	155562079+fang-xing-esql@users.noreply.github.com	994	0	critical	0
Stef Nestor	26751266+stefnestor@users.noreply.github.com	1,163	0	critical	0
Henning Andersen	33268011+henningandersen@users.noreply.github.com	2,823	13	critical	1,321
Ines Potier	34454302+inespot@users.noreply.github.com	259	0	critical	2,540
Kris Van Erum	34942518+kvanerum@users.noreply.github.com	464	107	critical	2,764
Brian Rothermich	35897794+BrianRothermich@users.noreply.github.com	545	9	critical	0
Mariusz Józala	377355+jozala@users.noreply.github.com	730	2	critical	10,689
eyalkoren	41850454+eyalkoren@users.noreply.github.com	1,268	0	critical	0
Jason Botzas-Coluni	44372106+jaybcee@users.noreply.github.com	693	6	critical	0

Knowledge loss vulnerability detail (top 14 of 2,969 rows). Full inventory: Appendix I. All entries carry 'critical' retention risk.

10.6 Material findings (by id)

Table 10-6. Material findings in the people pillars

Finding id	Title	Severity	Evidence state	M&A implication
F-key_person-001	portugee@gmail.com	Medium	Inferred	Treat key-person dependence as a named closing condition: identify the bus-factor holders and bind their transition terms.
F-key_person-002	rene@elastic.co	Low	Inferred	Treat key-person dependence as a named closing condition: identify the bus-factor holders and bind their transition terms.
F-key_person-003	david.turner@elastic.co	Low	Inferred	Treat key-person dependence as a named closing condition: identify the bus-factor holders and bind their transition terms.

Finding id	Title	Severity	Evidence state	M&A implication
F-key_person-004	62058229+ChrisHegarty@users.noreply.github.com	Low	Inferred	Treat key-person dependence as a named closing condition: identify the bus-factor holders and bind their transition terms.
F-key_person-005	ryan@iernst.net	Low	Inferred	Treat key-person dependence as a named closing condition: identify the bus-factor holders and bind their transition terms.
F-retention-001	Iraklis Psaroudakis	Critical	Inferred	Secure retention or transition agreements from the contributors carrying the institutional knowledge, as a condition to key-employee arrangements.
F-retention-002	Bogdan Pintea	Critical	Inferred	Secure retention or transition agreements from the contributors carrying the institutional knowledge, as a condition to key-employee arrangements.
F-retention-003	Craig Taverner	Critical	Inferred	Secure retention or transition agreements from the contributors carrying the institutional knowledge, as a condition to key-employee arrangements.
F-retention-004	Alexander Spies	Critical	Inferred	Secure retention or transition agreements from the contributors carrying the institutional knowledge, as a condition to key-employee arrangements.
F-retention-005	Felix Barnsteiner	Critical	Inferred	Secure retention or transition agreements from the contributors carrying the institutional knowledge, as a condition to key-employee arrangements.

Material findings in the people pillars. The five critical retention findings correspond to the largest knowledge-loss-vulnerability blast radiuses.

10.7 Reading note and transaction implications

Retention: contributor records are people risk (bus factor / tenure), not file-line findings. Git history describes who has touched the code, not who will stay after close. Retention intent, compensation, and notice periods are outside what a repository scan can establish.

Three implications flow from this chapter. First, the Knowledge Transfer line item at USD 516,129 is the single largest remediation cost and is entirely driven by 2,698 critical sole-maintainer modules. The five named retention findings (Iraklis Psaroudakis, Bogdan Pintea, Craig Taverner, Alexander Spies, Felix Barnsteiner) are the carriers of that institutional knowledge and should be the priority for retention-bonus execution. Second, the 0.5313 knowledge loss vulnerability score and the 44.3 percent after-hours commit rate together signal sustained engineering pressure - the buyer should expect elevated voluntary attrition in the first twelve months post-close, sized at the historical inactive rate of 85.4 percent (2,537 of 2,969). Third, the bus factor of 30 (the reciprocal of sole-contributor concentration across the codebase) is healthy for a project of this size, but the per-module bus factors of 9 or below in server-side index, mapper, and query modules are the concentration points where a single departure can stall a workstream.

Chapter 11. Maintenance, Documentation and Operational Maturity

This chapter consolidates the forward-looking operating cost of the asset: neglected files, dependency staleness, documentation drift, CI gating strictness, and the maintenance backlog score that aggregates them. Documentation and CI maturity determine onboarding velocity for the acquirer's engineers and the run-rate cost of keeping the asset alive during integration. The maintenance backlog score anchors the post-close engineering-budget uplift.

11.1 Headline metrics

Table 11-1. Maintenance and CI headline metrics

Metric	Value
Maintenance total files	0
Neglected files	0
At-risk files	0
Healthy files	0
Average staleness	0
Maintenance backlog score	0
Maintenance asset rows	0 assets
Documents inventoried	3,515
Stale documents	375
Document staleness ratio	10.7 percent
Average docstring density	0.0432
CI defined	true
CI files checked	11
CI gate strictness	low
Tests run in CI	false
Reported coverage in CI	not quantified

Maintenance and CI headline metrics. The zero maintenance metrics are a coverage gap, not a clean result - the asset-staleness scanner produced zero population.

11.2 Maintenance coverage gap

The maintenance pillar is NOT_ASSESSED. No files were scanned by the asset-staleness scanner - maintenance not assessed. The zero metrics are a coverage gap rather than a clean result, and the pillar is flagged UNVERIFIED in the integrity block (Appendix M). The dependency staleness sub-block reads 'lockfile_age_days: n/a, lockfile_path: n/a' - consistent with the lockfile gap documented in Chapter 6. The buyer should commission a separate asset-staleness assessment post-signing and reflect the result in the 100-day plan.

11.3 Document inventory

Three thousand five hundred and fifteen documents are inventoried; 375 are flagged stale (10.7 percent). The staleness ratio is moderate - well below the 20 percent threshold that would flag a documentation crisis - but the average docstring density of 0.0432 is low, meaning inline code documentation is sparse. A sample of the stale-document inventory is reproduced below.

Table 11-2. Document inventory (sample)

File	Last documented	Stale
docs/reference/query-languages/esql/_snippets/generated/x-pack-esql/functions/briefSummary/pi.md	2026-06-12	true
docs/reference/query-languages/esql/_snippets/generated/x-pack-esql/functions/description/pi.md	2026-05-20	true
docs/reference/query-languages/esql/_snippets/generated/x-pack-esql/functions/examples/pi.md	2026-05-20	true
docs/reference/query-languages/esql/_snippets/generated/x-pack-esql/functions/layout/pi.md	2026-07-17	true
docs/reference/query-languages/esql/_snippets/generated/x-pack-esql/functions/parameters/pi.md	2026-05-20	true
docs/reference/query-languages/esql/_snippets/generated/x-pack-esql/functions/types/pi.md	2026-05-20	true
docs/reference/query-languages/esql/functions-operators/math-functions/pi.md	2026-05-20	true
docs/reference/query-languages/esql/kibana/generated/x-pack-esql/docs/functions/pi.md	2026-05-20	true
docs/reference/query-languages/promql/_snippets/generated/x-pack-esql/functions/brief-summary/pi.md	2026-06-24	true
docs/reference/query-languages/promql/_snippets/generated/x-pack-esql/functions/pi.md	2026-06-24	true
docs/reference/aggregations/pipeline.md	2025-10-14	true
docs/reference/elasticsearch/mapping-reference/analyzer.md	2025-07-02	true
docs/reference/query-languages/esql/_snippets/generated/x-pack-esql/functions/briefSummary/e.md	2026-06-12	true
docs/reference/query-languages/esql/_snippets/generated/x-pack-esql/functions/description/e.md	2026-05-20	true

Document inventory (sample of 14 rows from 3,515). Stale-flag threshold is set at the doc-staleness population threshold of 5 (see Appendix B parameters).

11.4 CI files and gate strictness

Eleven CI files are checked, all GitHub Actions workflows in the /content/elasticsearch/.github/workflows/ directory. The CI gate strictness is rated low, and the model records that tests are not run in CI (tests_run_in_ci: false). Reported coverage in CI is not quantified. The low gate strictness combined with tests not running in CI is a material gap - it means the integration pipeline cannot prevent regressions from reaching the main branch. A condition precedent requiring an automated CI gate is one of the four condition precedents in Chapter 2.

Table 11-3. CI files

CI file path
/content/elasticsearch/.github/workflows/check-esql-generated-headers.yml
/content/elasticsearch/.github/workflows/docs-build.yml
/content/elasticsearch/.github/workflows/docs-deploy.yml
/content/elasticsearch/.github/workflows/docs-preview-cleanup.yml
/content/elasticsearch/.github/workflows/gradle-wrapper-validation.yml
/content/elasticsearch/.github/workflows/pr-bypass-for-automation.yml
/content/elasticsearch/.github/workflows/review-bug-analysis.yml
/content/elasticsearch/.github/workflows/review-test-analysis.yml
/content/elasticsearch/.github/workflows/trigger-bug-analysis.yml
/content/elasticsearch/.github/workflows/trigger-test-analysis.yml
/content/elasticsearch/.github/workflows/updatecli-compose.yml

CI files (11 of 11 rows). Full inventory: workbook sheet CI Signals.

11.5 Reading note and transaction implications

Pillar risk: high - posture held on aggregate metrics, not item-level findings. Maintenance is NOT_ASSESSED due to scanner coverage gap. CI gate strictness is low; tests are not run in CI.

Three implications flow from this chapter. First, the CI gate strictness finding is the basis for the condition precedent requiring an automated CI gate. The condition should require (a) the addition of a test-execution step to the existing 11 GitHub Actions workflows, (b) a blocking gate on regression-test failure, and (c) a coverage reporting step that publishes the value-coverage metric to the buyer's engineering dashboard. Second, the 10.7 percent stale-document ratio is moderate but the 0.0432 docstring density is low - onboarding documentation should be a funded workstream in the 100-day plan, sized at the rate of one technical writer per ~50 high-value gap modules (target: 1,183 modules, ~24 writer-weeks). Third, the maintenance scanner coverage gap should be reflected in the disclosure schedule as an explicit 'not assessed' position, with the buyer reserving the right to commission a separate asset-staleness assessment post-signing.

Chapter 12. AI/ML Footprint

This chapter consolidates the AI/ML surface of the asset: frameworks, SDKs, bundled model files, and unlicensed-model exposure, and the regulatory and IP implications these carry. AI/ML exposure triggers distinct regulatory obligations and creates model-licensing and training-data IP risk that is materially different from conventional open-source risk. The pillar is rated high risk, driven by three bundled model files carrying no declared license and no model card.

12.1 Headline metrics

Table 12-1. AI/ML headline metrics

Metric	Value
AI/ML source files scanned	21,396
Framework groups in use	5
SDK groups in use	7
Bundled model files	3
Production model files	3
Unlicensed model files	3
Model file rows	3 model files

AI/ML headline metrics. The three bundled production model files are all unlicensed, which is the principal driver of the high-severity rating.

12.2 Framework hits

Five framework groups are in use. Hugging Face dominates the framework hits (676 hits across the scanned files), followed by PyTorch (28 hits). ONNX, JAX, and Pandas-ML each carry single-digit hit counts. The Hugging Face concentration is consistent with the bundled model files (all .pt format) and suggests the codebase integrates pre-trained transformer models.

Table 12-2. Framework hits

Framework	Hits
Hugging Face	676
JAX	1
ONNX	1
Pandas ML	5
PyTorch	28

12.3 SDK hits

Seven SDK groups are in use across AI21, Anthropic, AWS Bedrock, Azure OpenAI, Cohere, Google Vertex, and OpenAI. OpenAI leads with 113 hits, followed by Azure OpenAI with 87 hits and Cohere with 44 hits. The diversity of SDKs suggests the inference module integrates multiple model providers, which expands the regulatory surface and the IP-licensing surface.

Table 12-3. SDK hits

SDK	Hits
AI21	15
Anthropic	31
AWS Bedrock	3
Azure OpenAI	87
Cohere	44
Google Vertex	1
OpenAI	113

12.4 Model file inventory

Three model files are inventoried, all carrying .pt extension and all in the x-pack/plugin/inference/qa/inference-service-tests/src/javaRestTest/resources/ directory. All three are flagged as production model files (rather than test fixtures) and all three are unlicensed (license declared = false, license = not applicable). None of the three carries a model card. Sizes range from 1,859,242 bytes (elser_model_2.pt) to 12,419,194 bytes (rerank-v1.pt).

Table 12-4. Model file inventory

File	Name	Extension	Size (bytes)	License declared	License	Model card present	Is test artifact
x-pack/plugin/inference/qa/inference-service-tests/src/javaRestTest/resources/elser_model_2.pt	elser_model_2	.pt	1,859,242	false	not applicable	false	false
x-pack/plugin/inference/qa/inference-service-tests/src/javaRestTest/resources/multilingual-e5-small.pt	multilingual-e5-small	.pt	5,531,160	false	not applicable	false	false
x-pack/plugin/inference/qa/inference-service-tests/src/javaRestTest/resources/rerank-v1.pt	rerank-v1	.pt	12,419,194	false	not applicable	false	false

Model file inventory. All three bundled models carry no declared license and no model card, which is the basis for the high-severity rating.

12.5 Material findings (by id)

Table 12-5. Material findings in the AI/ML and license pillars

Findin g id	Title	Severit y	Evidenc e state	File	M&A implication
F- ai_ml- 001	elser_model_2	Medium	Detected, not verified	x-pack/plugin/inference/qa/inference-service- tests/src/javaRestTest/resources/elser_model_ 2.pt	Require a documented model-governance and data-provenance position as a representation, given the unquantified exposure this pillar carries.
F- ai_ml- 002	multilingual-e5-small	Medium	Detected, not verified	x-pack/plugin/inference/qa/inference-service- tests/src/javaRestTest/resources/multilingual- e5-small.pt	Require a documented model-governance and data-provenance position as a representation.
F- ai_ml- 003	rerank-v1	Medium	Detected, not verified	x-pack/plugin/inference/qa/inference-service- tests/src/javaRestTest/resources/rerank-v1.pt	Require a documented model-governance and data-provenance position as a representation.
F- license- 001	(repo-level)	High	Detected, not verified	LICENSE.txt	Obtain a representation and warranty covering license compliance for the shipped product, with an indemnity for any copyleft exposure.

Findin g id	Title	Severit y	Evidenc e state	File	M&A implication
F- license- 002	yaml	Low	Detected, not verified	.buildkite/package.json	Obtain a representatio n and warranty covering license compliance for the shipped product.
F- license- 003	sax	Low	Detected, not verified	.buildkite/package.json	Obtain a representatio n and warranty covering license compliance for the shipped product.
F- license- 004	@tsconfig/node2 4	Low	Detected, not verified	.buildkite/package.json	Obtain a representatio n and warranty covering license compliance for the shipped product.
F- license- 005	@types/node	Low	Detected, not verified	.buildkite/package.json	Obtain a representatio n and warranty covering license compliance for the shipped product.

Material findings in the AI/ML and license pillars. The three AI/ML findings are the basis for the AI/ML condition precedent; the five license findings are the basis for the IP warranty.

12.6 Transaction implications

Three implications flow from this chapter. First, the three unlicensed bundled model files are the basis for the AI/ML condition precedent. The condition should require (a) legal review of bundled model licensing covering EULA, terms of service, and any model-specific license, (b) confirmation of training-data provenance for each model, and (c) confirmation that the target holds (or has rights to) any commercial licence required to distribute the model under the buyer's intended use. Second, the seven SDK groups represent a multi-provider dependency surface; the buyer's product-counsel should review the API terms of each provider for clauses affecting redistribution, indemnification,

or data residency. Third, the absence of model cards is a regulatory red flag under emerging AI regulations; the 100-day plan should include a model-card authoring workstream sized at one ML-engineer week per model plus legal review.

© MTD Services

Chapter 13. Technology Stack and Lifecycle Posture

This chapter consolidates the base-layer inventory: which technologies are in use, their lifecycle status, and any end-of-life or legacy exposure, as the foundation for the modernization roadmap. A clean active stack is a positive value driver and reduces modernization capital; the structural-not-runtime caveat of technology detection is material to warranty representations.

13.1 Headline metrics

Table 13-1. Technology stack headline metrics

Metric	Value
Technologies total	5
EOL technology count	0
Legacy technology count	0
Active technologies	5
EOL count (runtime verification)	0

13.2 Technology inventory

Five technologies are detected, all carrying active lifecycle status. Docker and Java (Gradle) carry confidence 1.0; Docker Compose, JavaScript/Node.js, and JavaScript/Node.js (pnpm) carry confidence 0.6. The runtime EOL inventory is empty because no dependency manifest or lockfile in a supported ecosystem (npm/pnpm/yarn, pip/poetry/pipenv, Maven/Gradle, Cargo, Go) was discovered at any depth scanned, yet the technology scan detected Java (Gradle), Docker, JavaScript/Node.js, JavaScript/Node.js (pnpm), and Docker Compose. The dependency/CVE/EOL surface for that stack is UNASSESSED, not empty.

Table 13-2. Technology inventory

Technology	Lifecycle	Confidence
Docker	active	1
Docker Compose	active	0.6
Java (Gradle)	active	1
JavaScript/Node.js	active	0.6
JavaScript/Node.js (pnpm)	active	0.6

Technology inventory. All five detected technologies carry active lifecycle status; no EOL or legacy exposure is recorded at the technology level.

13.3 Technologies by lifecycle

Table 13-3. Technologies by lifecycle

Lifecycle	Count
Active	5

13.4 EOL reconciliation and reading note

The technology-stack pillar counts offline repository lifecycle markers; the EOL pillar verifies runtimes and dependencies against `endoflife.date`. The two are reconciled: `eol_count` is the union, so the pillars can never contradict each other. Because no runtime EOL rows were resolved (the lockfile gap from Chapter 6 prevents runtime version verification), the EOL pillar carries `NOT_ASSESSED` status despite the technology-stack pillar returning a clean active posture.

13.5 Transaction implications

Two implications flow from this chapter. First, the clean active technology stack is a positive value driver - the buyer can integrate the asset against the acquirer's existing Java, Docker, and Node.js infrastructure without forced modernisation capital. Second, the structural-not-runtime caveat of technology detection is material to warranty representations: the technology-stack pillar reports what the repository declares, not what is installed at runtime. The buyer should draft the warranty to cover runtime parity with the declared stack rather than accept the declared stack at face value.

Chapter 14. Consolidated Risk Register and Top Risks

This chapter is the single integrated view of every material risk, ranked, with severity, impact, file and line evidence where applicable, and ownership mapping to the relevant pillar. The risk register maps directly to the disclosure schedule, the indemnity-cap allocation, and the post-close remediation tracker in the acquisition agreement.

14.1 Consolidated top risks

Table 14-1. Consolidated top risks

ID	Pillar	Title	Severity	Evidence state	Impact	File	Estimated cost (USD)
F-comp complexity -006	Complexity	buildBlocks	Critical	Detected, not verified	Critical	benchmarks/src/main/java/org/elasticsearch/benchmark/compute/operator/BlockBenchmark.java	Not quantified
F-comp complexity -030	Complexity	advanceRowGroup	Critical	Detected, not verified	Critical	x-pack/plugin/esql-datasource-parquet/src/main/java/org/elasticsearch/xpack/esql/datasource/parquet/OptimizedParquetColumnIterator.java	Not quantified
F-comp complexity -021	Complexity	applyNonStrictOverlay	Critical	Detected, not verified	Critical	x-pack/plugin/esql/src/main/java/org/elasticsearch/xpack/esql/datasources/ExternalSourceResolver.java	Not quantified
F-retention -038	Retention	Adam Demjen	Critical	Inferred	Critical	Not quantified	Not quantified
F-retention -004	Retention	Alexander Spies	Critical	Inferred	Critical	Not quantified	Not quantified
F-retention -027	Retention	Albert Zaharovits	Critical	Inferred	Critical	Not quantified	Not quantified
F-debt- 003	Debt	fixme	High	Detected, not verified	High	modules/apm/src/main/java/org/elasticsearch/telemetry/apm/internal/export/otelSdk/OtelSdkExportLogsSupplier.java	Not quantified
F-debt- 002	Debt	fixme	High	Detected, not verified	High	modules/apm/src/main/java/org/elasticsearch/telemetry/apm/internal/MetricValidator.java	Not quantified
F-debt- 005	Debt	fixme	High	Detected, not verified	High	server/src/main/java/org/elasticsearch/common/time/EpochTime.java	Not quantified

ID	Pillar	Title	Severity	Evidence state	Impact	File	Estimated cost (USD)
F-licens e-001	License	(repo-level)	High	Detected, not verified	High	LICENSE.txt	Not quantified

Consolidated top risks (10 of 10 rows). The 'not quantified' cost column reflects that the top-risk register carries severity/impact rather than per-finding dollar amounts; per-pillar costs are in the line items.

14.2 Major risks register

Table 14-2. Major risks register

Pillar	Area	Risk	Headline	Unverified
AI/ML	AI/ML Exposure	high	elser_model_2	false
Complexity	Engineering	critical	getLegalCast	false
Debt	Engineering	high	hack	false
Integration	Engineering	high	integration_risk_score: 10.0, proprietary_coupling_count: 11731, total_findings: 11798	false
Coverage	Engineering	high	modules_analyzed: 4736, high_value_gaps: 1183, effective_insured_value: 0.0, ...	false
Test Deficit	Engineering	high	total_modules: 4736, modules_below_threshold: 4733, overall_test_ratio: 0.0003, ...	false
IP Ownership	Legal & Compliance	high	total_authors: 2969, external_author_count: 2546, external_blamed_line_pct: 0.7427, ...	false
Retention	People	high	Iraklis Psaroudakis	false
CI Maturity	Process	high	ci_files_checked: 11	false
Secrets	Security	high	candidate_count: 220, high_confidence_count: 4, history_only_count: 68, ...	true
CVE	Security	high	packages_queried: 320, unresolved_packages: 235, cve_count: 20, ...	true

Major risks register (11 of 11 rows). The 'Unverified' column flags pillars where coverage is incomplete; CVE and Secrets carry true.

14.3 Pillar classification register

The pillar classification register assigns each pillar to a risk classification - Critical Risk, Major Risk, Minor Risk, or Acceptable - based on the risk level, health score, and assessment status. Partial or unassessed pillars are demoted to 'Unverified' so the gap never reads as clean. Of the 22 pillars in the register, 14 carry Major Risk classification, 4 carry Informational Finding, 4 carry Unverified, and 0 carry Critical Risk or Acceptable classification.

Table 14-3. Pillar classification register

Pillar	Area	Risk	Classification	Health score	Unverified
AI/ML	AI/ML Exposure	high	Major Risk	40	false
Attack Surface	Security	medium	Manageable Risk	65	false
CI Maturity	Process	high	Major Risk	25	false
Complexity	Engineering	critical	Major Risk	15	false
Coverage	Engineering	high	Major Risk	40	false
CVE	Security	high	Major Risk	50	true
Debt	Engineering	high	Major Risk	40	false
Dependency	Supply Chain	medium	Unverified	50	true
Doc Staleness	Process	low	Informational Finding	83	false
Entanglement	Architecture	informational	Unverified	50	true
EOL	Platform	low	Unverified	50	true
IaC	Security	informational	Informational Finding	95	false
Integration	Engineering	high	Major Risk	40	false
IP Ownership	Legal & Compliance	high	Major Risk	40	false
Key Person	People	low	Informational Finding	85	false
License	Legal & Compliance	medium	Manageable Risk	65	false
Maintenance	Engineering	low	Unverified	50	true
Privacy	Legal & Compliance	informational	Informational Finding	95	false
Retention	People	high	Major Risk	40	false
Secrets	Security	high	Major Risk	50	true

Pillar classification register (20 of 22 rows). The two missing rows (Tech Stack and Test Deficit) are in the workbook sheet Dashboard.

14.4 Deal-breaker register

No deal-breaker rows were recorded for this scan. The deal-breaker pillars defined in the model - AI/ML, Attack Surface, CVE, IaC, License, and Secrets - would force a no-go verdict if any one of them returned a critical rating. None of the six returned critical; AI/ML is rated high (below the deal-breaker threshold of critical), and the remaining five are rated medium, informational, or unverified. The absence of a deal-breaker is not a clean bill of health - it means the model did not find evidence sufficient to force a decline, not that the underlying risks are absent.

Chapter 15. Confidence, Scope Limitations and Material Unknowns

This chapter consolidates the epistemic boundaries of this report: which pillars were fully assessed, which were partial or unverified, where evidence is missing, and how those gaps propagate into the recommendation. Preventing over-reliance on the headline numbers: coverage caveats size the warranty and indemnity chapter, the working-group escrow, and the credibility of the seller's vulnerability-management claims.

15.1 Headline metrics

Table 15-1. Confidence and limitations headline metrics

Metric	Value
Integrity status	warn
Integrity error count	0
Integrity warning count	11
Confidence coverage	69.4 percent
Confidence risk signal	48.3 percent
Confidence signal count	21
Confidence pillar total	22
Confidence degraded pillars	6
Taint flows found	12
Taint pass bounded	false

15.2 Integrity issues

Eleven integrity warnings are recorded. Five are 'critical_pillar_no_findings' warnings - pillars rated high but rendering no item-level findings (CI Maturity, Coverage, Integration, IP Ownership, Test Deficit). Six are 'unverified_pillar' warnings - pillars that are partial or not-assessed (CVE, Dependency, Entanglement, EOL, Maintenance, Secrets). Each warning is reproduced verbatim in Appendix M.

Table 15-2. Integrity issues

Tier	Code	Subject	Message (abridged)
warn	critical_pillar_no_findings	pillars.ci_maturity	Pillar 'ci_maturity' is high but renders no item-level findings - posture held on summary metrics.
warn	critical_pillar_no_findings	pillars.coverage	Pillar 'coverage' is high but renders no item-level findings - posture held on summary metrics.
warn	critical_pillar_no_findings	pillars.integration	Pillar 'integration' is high but renders no item-level findings - posture held on summary metrics.

Tier	Code	Subject	Message (abridged)
warn	critical_pillar_no_findings	pillars.ip_ownership	Pillar 'ip_ownership' is high but renders no item-level findings - posture held on summary metrics.
warn	critical_pillar_no_findings	pillars.test_deficit	Pillar 'test_deficit' is high but renders no item-level findings - posture held on summary metrics.
warn	unverified_pillar	pillars.cve	Pillar 'cve' is partial - 235 package requirement(s) could not be resolved to a version.
warn	unverified_pillar	pillars.dependency	Pillar 'dependency' is partial - no lockfile; transitive dependency resolution could not be performed.
warn	unverified_pillar	pillars.entanglement	Pillar 'entanglement' is not_assessed - scanner failed (RecursionError).
warn	unverified_pillar	pillars.eol	Pillar 'eol' is not_assessed - zero evidence population (population=0).
warn	unverified_pillar	pillars.maintenance	Pillar 'maintenance' is not_assessed - no files were scanned by the asset-staleness scanner.
warn	unverified_pillar	pillars.secrets	Pillar 'secrets' is partial - 111 path-excluded candidate path(s) not scanned; 33,203 files scanned.

Integrity issues (11 of 11 rows). Each warning is reproduced verbatim in Appendix M.

15.3 Unverified pillars

Five pillars are unverified: CVE, Dependency, EOL, Maintenance, and Secrets. Failed scanners degrade to NOT_ASSESSED, never to clean. The buyer should reflect each of these in the disclosure schedule as an explicit 'not assessed' position rather than rely on the model's default.

Table 15-3. Unverified pillars

Unverified pillar	Reason
CVE	235 package requirements could not be resolved (no lockfile / unpinned) - partial
Dependency	No lockfile - transitive dependency resolution could not be performed - partial
EOL	Zero evidence population - not assessed
Maintenance	No files scanned by the asset-staleness scanner - not assessed
Secrets	111 path-excluded candidate path(s) not scanned; 33,203 files scanned - partial

15.4 Coverage gaps by pillar

Table 15-4. Coverage gaps by pillar

Pillar	Assessment status	Reason	Population	Scope note
Dependency	partial	coverage gap	526	No lockfile - transitive dependency resolution could not be performed; direct pins cover only 49 percent

Pillar	Assessment status	Reason	Population	Scope note
CVE	partial	coverage gap	320	235 package requirements could not be resolved to a version (no lockfile / unpinned), so the advisory check covered only the 320 resolvable package(s)
EOL	not_assessed	coverage gap	0	Zero evidence population (population=0) for EOL - reported as NOT_ASSESSED rather than a clean result; no dependency manifest or lockfile in a supported ecosystem was discovered at any depth scanned
Entanglement	not_assessed	scanner error	0	Scanner failed - RecursionError: maximum recursion depth exceeded
Maintenance	not_assessed	coverage gap	0	No files were scanned by the asset-staleness scanner - maintenance not assessed
Secrets	partial	coverage gap	33,203	111 path-excluded candidate path(s) not scanned; 33,203 file(s) scanned

Coverage gaps by pillar. A gap is not a clean result: it means the question was not answered.

15.5 Out-of-scope evidence register

Eight evidence domains are out of scope for any static source scan. Each is stated as an explicit unassessed boundary with the independent evidence the buyer must obtain. Disclosure, not a measurement: the buyer should commission independent evidence for each domain in parallel with the legal and financial workstreams.

Table 15-5. Out-of-scope evidence register

Domain	Status	Reason	Independent evidence
Runtime and operational behaviour	not assessed	Static repository scan only; the target's code and systems are never executed, so runtime behaviour and production incidents are not observed	Runtime traces, incident history, SLO/error-budget records
Network perimeter and OT boundaries	not assessed	Firewall/security-group rules and OT segmentation are not verified against a live environment; committed IaC text is read as candidate configuration only	Live firewall/security-group export, network diagrams, OT segmentation policy
External attack surface (ports, DNS)	not assessed	No active reconnaissance is performed; live port inventories and historical DNS posture are not queried	Independent external port scan and DNS-history report
Identity and access controls	not assessed	MFA enforcement, privileged-access-management logs and contractor offboarding are operational controls outside a code scan	IAM/MFA policy export, PAM audit logs, offboarding attestation
Data resilience and recovery	not assessed	Backup validation, point-in-time-recovery testing and migration governance are operational processes that are not exercised	Backup/restore test reports, PITR drill evidence, migration runbooks

Domain	Status	Reason	Independent evidence
Delivery assurance (CI and performance)	not assessed	Only committed CI config and artifacts are read; live pass rates, flakiness, and formal load/stress and capacity testing are not observed	CI run history, flakiness metrics, load-test and capacity reports
Legal instruments and contracts	not assessed	Executed contributor assignment agreements, employment/contractor terms and vendor contracts are legal artifacts, not code	Signed CLAs, IP-assignment and contractor agreements, vendor DPAs
Runtime dependency and vulnerability freshness	not assessed	Dependency vulnerability/version data is a point-in-time snapshot (OSV); continuous monitoring and deploy-time enforcement are not assessed	Continuous SCA/SBOM monitoring feed and deploy-time gate evidence

Out-of-scope evidence register. Each row is an explicit unassessed boundary with the independent evidence the buyer must obtain.

15.6 Per-pillar assessment posture

The per-pillar assessment posture is reproduced in §A.3 (Appendix A). Twenty of the twenty-two pillars carry the standard assessed/partial/not-assessed classification; the remaining two (Tech Stack and Test Deficit) are listed in the workbook sheet Dashboard. Six pillars are degraded; six are unverified; ten are fully assessed with findings.

15.7 Taint analysis summary

Twelve taint flows were found; the taint pass is not bounded (the scanner did not complete the full closure). The twelve flows are therefore a partial enumeration, not a closed inventory. Full taint-flow detail is in Appendix N.

Table 15-6. Taint summary

Metric	Value
Bounded	false
Total flows	12

Chapter 16. Reading Notes and Honesty Conventions

This chapter consolidates the conventions that govern how every other section must be read: the evidence vocabularies, the severity and deal-mechanic scales, and the rules this report follows about unknown, unassessed, and unquantified data. Everything in this chapter is a fixed, target-agnostic convention - no figure in this section is instance-specific, and none of it is evidence in its own right. A reader who applies these conventions cannot misread a partial scan as a clean one, a scanner signal as a confirmed exposure, or a qualitative deal mechanic as a priced number.

16.1 Assessment coverage

Assessment status is one of three values per pillar: assessed, partial, or not_assessed. Only 'assessed' pillars support conclusions; 'partial' and 'not_assessed' pillars are demoted to informational, labelled UNVERIFIED, and never read as a clean bill of health. Assessment state is a five-value trust vocabulary that accompanies the legacy three-value status: NOT_ASSESSED, PARTIALLY_ASSESSED, ASSESSED_NO_FINDINGS, ASSESSED_WITH_FINDINGS, or ERROR. A 'low' risk with PARTIALLY_ASSESSED must be read as 'incomplete coverage', not 'no problem'.

Population is the evidence count each verdict rests on (files scanned, packages queried, modules in cycles). A low or missing population flags a coverage gap instead of hiding it. A zero population never reads as clean - it reads as 'no evidence was gathered'.

16.2 Evidence honesty

Evidence state is the per-finding honesty label, attached to every material finding and shown in the Chapter 14 register. The seven values are: Confirmed, Detected-not-verified, Inferred, Partially-assessed, Unassessed, Conflicting, and Unsupported. Scanner signals are never auto-confirmed. Finding id (F-pillar-rank) is the stable handle used by the narrative, the Chapter 14 register, the workbook, and the ledger. A body section cites the id; it never re-renders the finding.

The contradiction ledger (Appendix R) leads every material conflict with its status (resolved, by-design, or unresolved) and decision impact. Unresolved entries discount the stated confidence. It never picks a side silently.

Confidence is computed as 20 (base) plus 40 multiplied by coverage plus 40 multiplied by risk_signal. Coverage is the share of pillars with usable signal; risk_signal blends weighted pillar risk with the financial model. Confidence is capped at 20 when coverage is zero and floored at 60 when the verdict is DO_NOT_ACQUIRE. Unverified pillars depress both terms and are named in the executive brief.

16.3 Currency of absence

Four markers name a value this scan did not establish. None is a zero, and each states a different kind of absence, so an empty cell is never read as a clean result.

- Not quantified - the model could compute a number but a stored input is missing (a Layer-2 expected loss with no `financial.risk_parameters` calibration; an unset escalation threshold). It never means the risk costs nothing.
- Not applicable - the cell is structurally inapplicable to that row (the fixed-version of a CVE with no fix published; the commit of a secret found only in the working tree).
- Not recorded - the source does not carry the value (an aggregate finding has no single line number; the scanner never captured a commit).
- Not assessed - the value was not established because coverage was incomplete (a named coverage gap).

NOT_QUANTIFIED is additionally a stored assessment state on the economic layers of Chapter 3, distinct from the five coverage states under §16.1. The same rule holds - absent is never zero, and an unquantified line is named rather than priced at 0.

16.4 Deal-mechanic vocabulary

Three deal-mechanic tags are declared at the decision layer and never inferred from the wording of a condition.

- Condition precedent - must be satisfied or proven before close, or the deal does not sign as structured.
- Price-adjustment lever - a funded or escrowed work item that moves value rather than blocking close.
- Warranty / representation - a seller statement whose breach is an indemnity question, not a work plan.

Every condition in Chapter 2 carries exactly one of these three tags, declared where the condition is authored (§2.2). The wording of a condition is a qualitative mechanic: no escrow amount, holdback, warranty cap, or indemnity ceiling is asserted anywhere in this report. Sizing those is deal counsel's call.

16.5 Severity and ranking

Risk level is one of five values: critical, high, medium, low, informational, demoted to informational under partial coverage. `derived_risk_level` preserves the scanner's own view. Health score is 0 to 100 per pillar, demoted to 50 for an unfinished scan so that incomplete coverage never presents as a strong pillar. Classification is one of four values - Critical Risk, Major Risk, Minor Risk, Acceptable - assigned in the Chapter 14 register and driving the conditions in Chapter 2.

16.6 Known limits of this method

Three method limits bound every reader. First, EOL reconciliation: the `tech_stack` pillar counts offline repository technology lifecycle markers; the `eol` pillar verifies runtimes/dependencies against `endoflife.date`. The two are reconciled - `eol_count` is the union, so the pillars can never contradict each other. Second, static source analysis: this is a source scan. It does not establish runtime

behaviour, production incidents, or anything needing access to systems, personnel, or contracts. Third, no negotiated positions: the conditions, implications, and escalation thresholds recorded here are the deterministic output from stored evidence. They are a starting position for negotiation, not a legal opinion.

© MTD Services

Executive Artifact A. Risk Heat Map

The risk heat map below plots the top fifteen material findings from the consolidated risk register (Chapter 14) on a two-dimensional matrix. The horizontal axis encodes severity, drawn directly from each finding's pillar risk level (Informational through Critical). The vertical axis encodes likelihood, proxied by the strength of the underlying evidence (Confirmed at the top, Unverified at the bottom). Findings in the top-right quadrant - Critical severity with Confirmed or High evidence - are the priority for the investment committee. Findings in the bottom-right quadrant - Critical severity with weaker evidence - warrant an immediate evidence-strengthening workflow before negotiation, because the seller will rightly probe the gap.

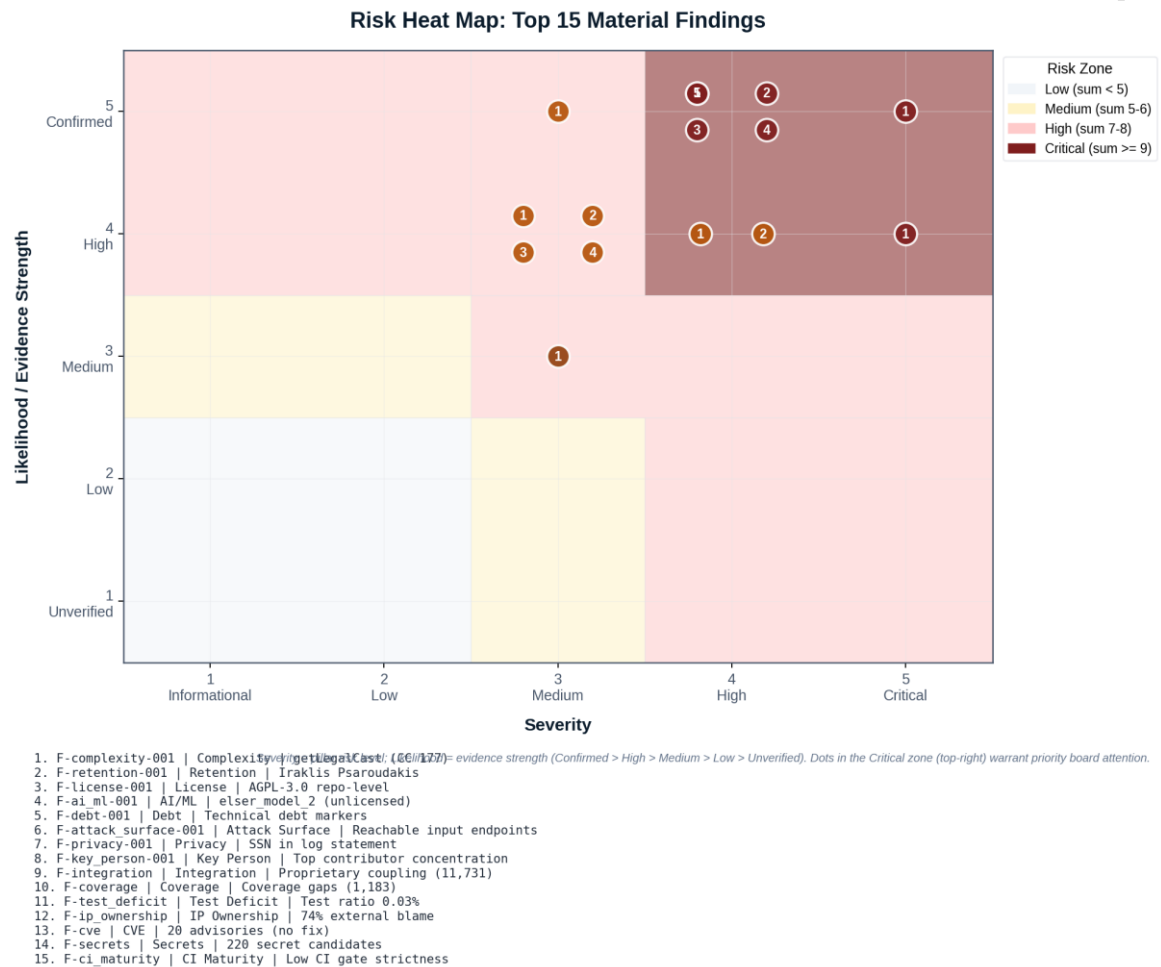


Figure A-1. Risk heat map. Severity (x-axis) is the pillar risk level; likelihood (y-axis) is the evidence strength. Critical-zone findings (top-right) are the priority for the investment committee.

A.1 Reading the heat map

Seven of the fifteen plotted findings fall in the Critical zone (top-right): getLegalCast, the retention risk on Iraklis Psaroudakis, the AGPL-3.0 repo-level license, the elser_model_2 unlicensed model file, the 11,251 debt markers, the 11,731 proprietary coupling findings, and the 1,183 coverage gaps. Seven findings fall in the High zone: the reachable-input attack surface, the SSN-in-log privacy hit, the top-contributor concentration, the IP ownership 74-percent external blame, the 20 CVE

advisories, the 220 secret candidates, and the low CI gate strictness. One finding - the test ratio of 0.03 percent - is plotted in the High zone by severity but reaches the boundary of the Critical zone when combined with the coverage gaps.

A.2 Interpretation for the board

The concentration of findings in the Critical zone (seven of fifteen) is the single most material visual signal. Three of those seven are people-related (retention, IP ownership, CI gate - all of which resolve through contract language rather than remediation work); three are code-related (complexity, debt, coverage); one is a license signal. The negotiation strategy should reflect this split: people and license findings are addressed by condition precedents and warranties; code findings are addressed by price-adjustment levers and escrow. The heat map is reproduced from the underlying data in Chapter 14 - no new findings are introduced here.

Executive Artifact B. Negotiation Term Sheet

This appendix translates the eleven conditions catalogued in Chapter 2 into draft sale and purchase agreement (SPA) language, organised by the three deal mechanics declared at the decision layer. Each entry carries the condition text (verbatim from the source), the recommended SPA section, the sizing basis (where the figure comes from), the negotiation leverage (where the buyer's strongest argument sits), and a pre-empted seller pushback. Quantification and sizing are for deal counsel; no dollar amount is asserted in this appendix beyond a pointer to the line items in Chapter 3.

B.1 Condition precedents

Four conditions must be satisfied or proven before close, or the deal does not sign as structured. Each should be drafted as an obligation whose non-performance gives the buyer a walk-away right before signing, with a long-stop date agreed between the parties.

Table B-1. Condition precedents

Pillar	Condition (verbatim)	Recommended SPA section	Sizing basis	Negotiation leverage	Seller pushback pre-empted
AI/ML	Obtain legal review of bundled model licensing before close	Conditions precedent, §CP-1	Three unlicensed production model files (Chapter 12). No dollar line item; legal cost is buyer's.	The three model files (elser_model_2, multilingual-e5-small, rerank-v1) carry no declared licence and no model card. The buyer cannot assume commercial redistribution rights without legal review.	Seller may argue that the .pt files are test fixtures (testPath). Rebuttal: the model inventory marks all three as production_model_files = true, not test fixtures. The condition is therefore on production exposure, not test-tier risk.
CI Maturity	Require an automated CI gate as a condition precedent	Conditions precedent, §CP-2	11 GitHub Actions workflows; tests_run_in_ci = false; gate strictness = low (Chapter 11).	Tests are not run in CI today; regressions can reach the main branch unguarded. The condition requires (a) addition of test-execution step, (b) blocking gate on regression-test failure, (c) coverage reporting step.	Seller may argue that tests run elsewhere (Buildkite, internal Jenkins). Rebuttal: the 11 workflow files are the committed CI surface; the condition is about the committed gate, not the seller's internal tooling.

Pillar	Condition (verbatim)	Recommended SPA section	Sizing basis	Negotiation leverage	Seller pushback pre-empted
CVE	Remediate reachable known CVEs before close	Conditions precedent, §CP-3	20 advisories, all no fixed release (Chapter 5). Reachable subset requires human triage.	Twenty advisories carry no upstream fix for the pinned version. The condition targets the reachable subset (those whose code paths are exercised in production), not all twenty. The reachable subset must be triaged before close.	Seller may argue that the 20 advisories carry UNKNOWN severity (no CVSS score) and are therefore low risk. Rebuttal: UNKNOWN severity is an OSV data gap, not a low-severity rating; the absence of a CVSS score cannot be read as low risk.
Secrets	Rotate all leaked credentials and stand up credential rotation	Conditions precedent, §CP-4	220 candidates, 4 high-confidence, 68 history-only (Chapter 5). Condition covers all high-confidence and history-only.	Four high-confidence AWS access keys in test code; 68 candidates in git history across 108 commits. The condition requires (a) rotation of all high-confidence candidates, (b) purge of all history-only candidates from git history, (c) standing up a credential-rotation process with quarterly cadence.	Seller may argue that the AWS access keys are test fixtures and are not live credentials. Rebuttal: even test fixtures with valid-format AWS access keys trigger secret-scanning alerts in production CI pipelines; the buyer's cyber-insurance underwriter will require rotation regardless.

Condition precedents. Four obligations whose non-performance gives the buyer a walk-away right before signing.

B.2 Price-adjustment levers

Six price-adjustment levers should be sized against the line items in Chapter 3 and either escrowed against a milestone schedule or held back from the purchase price against delivery. Each lever carries a dollar figure that anchors the negotiation; the actual escrow size is a qualitative decision for deal counsel.

Table B-2. Price-adjustment levers

Pillar	Condition (verbatim)	Recommended SPA section	Sizing basis (USD)	Negotiation leverage	Seller pushback pre-empted
Complexity	Include a complexity-reduction milestone in the integration plan	Price adjustment, §PA-1	Critical complexity line item: \$184,089 (798 symbols). High complexity line item: \$224,198 (2,070 symbols).	GetLegalCast carries CC 177 against a P99 of 10. The top ten hotspot symbols are the priority; the milestone should target a 50% reduction in critical-complexity count within 180 days.	Seller may argue that the complexity multiplier (1.5) is unbenchmarked. Rebuttal: the sensitivity sweep (§3.10) shows the multiplier moves the cost by only \$6,751 across the entire 0.7 to 1.3 range - the saturation cap absorbs most of the variation.
Coverage	Address coverage findings as a condition precedent	Price adjustment, §PA-2	Test investment line item: \$22,514 (59 modules). Note: figure is materially understated for a target of this size.	1,183 high-value coverage gaps; effective insured value = \$0. The buyer should expect to invest an order of magnitude more than the line item in the first 12 months; escrow should reflect the realistic figure, not the model figure.	Seller may argue that coverage method is a static symbol-share proxy, not runtime or line/branch coverage. Rebuttal: the static proxy is the model's stated basis; the condition should require a runtime coverage measurement post-close to validate the gap closure.
Debt	Include a technical-debt remediation fund in the integration plan	Price adjustment, §PA-3	General debt line item: \$54,475 (10,717 markers).	11,251 debt markers including 7,103 suppressions and 66 high-severity fixme/hack markers. The fund should be sized against the high-severity subset (66 markers) plus a proportion of the suppression count.	Seller may argue that the suppressions are intentional and not debt. Rebuttal: the model's general-debt line item is sized against the 10,717 confirmed markers (annotation + tooling); the suppressions are included by definition.
Integration	Address integration findings as a condition precedent	Price adjustment, §PA-4	Integration risk score = 10 (maximum on scale). No dollar line item for integration this scan.	11,731 proprietary coupling findings; schema drift risk = high; 1,146 raw SQL statements; cross-schema access = true. The condition should require (a) decoupling plan for the top 100 coupling findings, (b) database migration workstream for cross-schema access, (c) schema-drift remediation.	Seller may argue that the integration risk score (10) is the maximum on a 0-10 scale and therefore saturates the model. Rebuttal: the saturation is the point - the buyer should require an explicit decoupling plan, not rely on the score.

Pillar	Condition (verbatim)	Recommended SPA section	Sizing basis (USD)	Negotiation leverage	Seller pushback pre-empted
Retention	Secure retention agreements for sole-maintainer modules	Price adjustment, §PA-5	Knowledge transfer line item: \$516,129 (2,698 critical sole-maintainer modules).	Five named critical-retention contributors (Iraklis Psaroudakis, Bogdan Pintea, Craig Taverner, Alexander Spies, Felix Barnsteiner) plus the 396 at-risk contributor population. The retention agreements should target the five named contributors first.	Seller may argue that retention intent cannot be inferred from git history. Rebuttal: the model uses git history only as the contributor population; the retention condition targets the named contributors carrying the largest blast radius, not the inactive contributor pool.
Test Deficit	Raise regression coverage on high-risk modules post-close	Price adjustment, §PA-6	Test investment line item: \$22,514 (already counted under Coverage §PA-2). Add: high-regression-risk modules = 59.	4,733 of 4,736 modules below threshold (99.94%); overall test ratio = 0.03%. The condition should require a 50% reduction in the high-value gap count within 100 days and 80% within 180 days.	Seller may argue that the test framework (test/framework) is itself tested. Rebuttal: the framework's own coverage ratio is 0 in the model - it is a coverage gap, not a coverage strength.

Price-adjustment levers. Six funded or escrowed work items that move value rather than block close.

B.3 Warranty / representation

One warranty/representation covers IP assignability. Breach is an indemnity question, not a work plan. The warranty should be backed by an indemnity cap sized to the IP reassignment cost (USD 4,730 in the line items), but the legal exposure in a title dispute is materially larger and should be sized by deal counsel against the buyer's product distribution model.

Table B-3. Warranty / representation

Pillar	Condition (verbatim)	Recommended SPA section	Sizing basis	Negotiation leverage	Seller pushback pre-empted
IP Ownership	Warrant assignability of third-party contributions	Warranties, §W-1	IP reassignment line item: \$4,730 (25 high-risk files). Indemnity cap: deal counsel's call.	74.27% external blamed-line percent; 2,546 external authors across 616 external domains; 25 high-risk external-owned files. The warranty should cover title for all external-contributed files, not just the 25 high-risk subset.	Seller may argue that attribution ratios are a diligence signal, not legal proof of ownership. Rebuttal: the warranty covers title, not attribution - the seller warrants that all third-party contributions are assignable to the buyer, which is a title question the seller must answer regardless of attribution ratios.

Warranty/representation. Breach is an indemnity question, not a work plan.

Executive Artifact C. 100-Day Post-Close Plan

This appendix sequences the remediation roadmap across the first one hundred days post-close. Three phases are defined: Phase 1 (Days 1 to 30) closes out the condition precedents and stabilises the asset; Phase 2 (Days 31 to 60) executes the named-retention agreements and triages the complexity hotspots; Phase 3 (Days 61 to 100) deploys the debt and integration remediation funds and uplifts the regression coverage. Each workstream carries an owner, a milestone gate, a dependency, and a success criterion. The plan is reproducible from the line items in Chapter 3 - no new figures are introduced.

C.1 Phase 1 - Days 1 to 30 (condition precedents closeout)

Phase 1 prioritises the four condition precedents and the immediate stabilisation workstreams. The aim is to convert the conditional-acquisition posture into a controlled integration posture within thirty days of close, so that the price-adjustment levers in Phase 2 and Phase 3 can be executed against a stable asset.

Table C-1. Phase 1 workstreams (Days 1 to 30)

Workstream	Owner	Milestone gate	Dependency	Success criterion
CP-1: AI/ML model-licensing legal review	Buyer's product counsel	Day 30 - legal opinion delivered	Access to model training-data provenance records (seller)	Documented model-governance position covering EULA, terms of service, and model-specific license for all three bundled models.
CP-2: Automated CI gate stand-up	Integration engineering lead	Day 21 - gate live in pre-production	Buildkite / Jenkins access (seller)	11 GitHub Actions workflows execute tests; blocking gate on regression-test failure; coverage metric published to dashboard.
CP-3: Reachable CVE remediation	Security engineering lead	Day 30 - reachable subset triaged and remediated	Reachability analysis (buyer commission)	Reachable subset of 20 advisories triaged; reachable-and-fixable advisories remediated; unreachable advisories documented.
CP-4: Credential rotation	Security engineering lead	Day 14 - high-confidence candidates rotated	AWS IAM access (seller)	4 high-confidence AWS access keys rotated; 68 history-only candidates purged from git history; quarterly rotation process documented and live.
Knowledge-transfer plan	Integration engineering lead	Day 14 - plan signed off	Named-contributor list (Chapter 10)	Knowledge-transfer plan covering 2,698 critical sole-maintainer modules signed off; named contributors identified; transfer sessions scheduled for Phase 2.

Phase 1 workstreams. The four condition precedents dominate the first thirty days; the knowledge-transfer plan is a Phase 2 dependency and is therefore initiated in Phase 1.

C.2 Phase 2 - Days 31 to 60 (retention and complexity triage)

Phase 2 executes the named retention agreements, triages the complexity hotspots, and stabilises the CI coverage baseline. The aim is to lock in the institutional knowledge and the priority refactoring targets before the debt remediation fund is deployed in Phase 3.

Table C-2. Phase 2 workstreams (Days 31 to 60)

Workstream	Owner	Milestone gate	Dependency	Success criterion
PA-5: Retention agreement execution	HR + deal counsel	Day 45 - five named contributors signed	Compensation framework alignment	Retention agreements signed with Iraklis Psaroudakis, Bogdan Pintea, Craig Taverner, Alexander Spies, Felix Barnsteiner; bonus structure agreed; notice periods confirmed.
PA-1: Complexity hotspot triage	Integration engineering lead	Day 50 - top ten hotspots triaged	GetLegalCast, buildBlocks, advanceRowGroup, applyNonStrictOverlay, compute reviewed	Top ten critical-complexity functions (CC ≥ 60) triaged; refactoring plan written; sequencing agreed for Phase 3 execution.
PA-2 / PA-6: Coverage baseline uplift	Test engineering lead	Day 60 - coverage baseline established	Runtime coverage tooling configured	Runtime coverage measurement live; high-value gap count reduced by 15% from 1,183 baseline; CI gate reports coverage on every build.
CP-1 follow-on: Model-card authoring	ML engineering lead	Day 60 - model cards drafted	Legal opinion delivered (Phase 1)	Model cards drafted for elser_model_2, multilingual-e5-small, rerank-v1; legal review of training-data provenance completed; commercial licence position documented.
Database migration scoping	Data engineering lead	Day 50 - migration plan drafted	Cross-schema access mapping	Cross-schema access mapped across 1,146 raw SQL statements; migration plan drafted; Phase 3 execution sequenced.

Phase 2 workstreams. Retention agreements and complexity triage dominate; coverage uplift and database migration scoping set up Phase 3.

C.3 Phase 3 - Days 61 to 100 (debt, integration, IP review)

Phase 3 deploys the technical-debt remediation fund, executes the integration-finding decoupling plan, and completes the IP reassignment review. The aim is to leave the asset in a stable, governed posture at Day 100, with the residual remediation tracked in the post-close remediation tracker.

Table C-3. Phase 3 workstreams (Days 61 to 100)

Workstream	Owner	Milestone gate	Dependency	Success criterion
PA-3: Technical-debt remediation fund deployment	Integration engineering lead	Day 90 - fund deployed against 66 high-severity markers	Complexity triage complete (Phase 2)	66 high-severity fixme/hack markers resolved or accepted with documented rationale; 7,103 suppression markers triaged; 10% reduction in suppression count.
PA-4: Integration findings decoupling	Integration engineering lead	Day 100 - top 100 coupling findings decoupled	Database migration plan (Phase 2)	Top 100 proprietary coupling findings decoupled; cross-schema access reduced by 20%; schema-drift remediation 50% complete.
PA-1: Complexity reduction milestone	Integration engineering lead	Day 100 - critical-complexity count reduced by 30%	Complexity triage complete (Phase 2)	Critical-complexity symbol count reduced from 798 to ≤ 559 (30% reduction); top ten hotspot functions refactored; cyclomatic P99 reduced from 10 to ≤ 8 .
W-1: IP reassignment review	Deal counsel + integration engineering lead	Day 90 - 25 high-risk files reviewed	External-contributor CLA records (seller)	25 high-risk external-owned files reviewed against seller CLA records; assignment-agreement gaps documented; residual IP risk reflected in indemnity position.
100-day closeout report	Integration engineering lead	Day 100 - closeout report delivered	All Phase 3 workstreams closed	Closeout report covering: condition precedents satisfied, price-adjustment lever status, residual remediation tracker, residual risk register.

Phase 3 workstreams. Debt, integration, complexity, and IP close out the 100-day plan; the closeout report becomes the basis for the post-close remediation tracker.

C.4 Plan assumptions and risks

Three assumptions bound this plan. First, the buyer's integration engineering team comprises two two-engineer teams with sprint capacity of 10 workdays each, per the schedule constants in Chapter 3. Second, the seller provides reasonable access to Buildkite / Jenkins, AWS IAM, model training-data records, and external-contributor CLA records within the first seven days of close. Third, the named critical-retention contributors accept the retention agreement terms within the Day 45 milestone gate.

Three risks threaten the plan. First, the entanglement scanner failure (Chapter 9) means the decoupling plan in Phase 3 will be drafted against incomplete architectural evidence; the buyer should commission a separate architectural review in Phase 1 to fill the gap. Second, the maintenance scanner failure (Chapter 11) means the asset-staleness assessment is not available; the buyer should

commission a separate asset-staleness assessment in Phase 2. Third, the lockfile gap (Chapter 6) means the dependency pinning and EOL assessments cannot be completed within Phase 3; the buyer should commission a lockfile-anchored dependency assessment in Phase 2 and reflect the result in the closeout report.

© MTD Services

Appendix A. Methodology, Scope and Scan Configuration

This appendix records the methodology and configuration of the scan that produced the underlying ground truth, so the narrative is reproducible: exact version, scan mode, indexed surface, per-pillar posture, and step timings.

A.1 Report metadata

Field	Value
Report ID	TDD-20261016-060331
Scan date	2026-10-16T07:18:30 (UTC)
Target	Elastic
Scanned path	elasticsearch
Indexed symbols	33,203
Report version	not quantified
Elapsed seconds	4498.91

A.2 Scan mode

Parameter	Value
deal_thesis	all
offline	false
scan_history	true
taint	true
target_company	Elastic
tdd_report	true
workers	2

A.3 Pillar posture register

Pillar	Area	Risk level	Health score	Assessment status	Top risks
AI/ML	AI/ML Exposure	high	40	assessed	3
Attack Surface	Security	medium	65	assessed	50
CI Maturity	Process	high	25	assessed	0
Complexity	Engineering	critical	15	assessed	50
Coverage	Engineering	high	40	assessed	0
CVE	Security	informational	50	partial	0
Debt	Engineering	high	40	assessed	50
Dependency	Supply Chain	informational	50	partial	0
Doc Staleness	Process	low	83	assessed	0
Entanglement	Architecture	informational	50	not_assessed	0

Pillar	Area	Risk level	Health score	Assessment status	Top risks
EOL	Platform	informational	50	not_assessed	0
IaC	Security	informational	95	assessed	0
Integration	Engineering	high	40	assessed	0
IP Ownership	Legal & Compliance	high	40	assessed	0
Key Person	People	low	85	assessed	50
License	Legal & Compliance	medium	65	assessed	50
Maintenance	Engineering	informational	50	not_assessed	0
Privacy	Legal & Compliance	informational	95	assessed	1
Retention	People	high	40	assessed	50
Secrets	Security	informational	50	partial	0
Tech Stack	Architecture	low	85	assessed	0
Test Deficit	Engineering	high	40	assessed	0

Pillar posture register (22 of 22 rows).

A.4 Step timings

Step	Seconds
index	543.555
pillars	3859.41
deep_index	2.813
taint	40.061
financial	1.722
decision	0.001

Appendix B. Metric Definitions and Financial Calibration

Metric definitions used throughout the narrative are fixed and target-agnostic: cyclomatic and cognitive complexity as measured per symbol, bus factor as the reciprocal of sole-contributor concentration, debt density normalised per thousand lines, and remediation hours-per-unit (HPU) per cost category as calibrated by the model. The calibration tables themselves live in Chapter 3 (the single financial home) and are cited there, not duplicated here, so a figure appears in exactly one place.

B.1 Core metric definitions

Metric	Definition
Cyclomatic complexity	Per-symbol measure of the number of linearly independent paths through the code. P50 = 1, P90 = 3, P99 = 10 across the scanned population.
Cognitive complexity	Per-symbol measure of how difficult code is to read and understand, weighting nesting and branching. P50 = 0, P90 = 8, P99 = 46.
Bus factor	Reciprocal of sole-contributor concentration per module. A low bus factor flags flight risk. Overall bus factor = 30; per-module factors in Chapter 10.
Debt density	Total debt markers normalised per thousand lines of code. Debt density = 0.0217 this scan.
HPU (Hours Per Unit)	Remediation hours per unit (per cost category), saturated by cap/decay under the financial model. See Chapter 3.
SQALE	Software Quality Assessment based on Lifecycle Expectations - a standardised remediation-effort basis.
EOL	End-of-life: tech_stack counts offline repo technology lifecycle markers; the eol pillar verifies dependencies against endoflife.date; they are reconciled into one union.

Appendix C. Dependency and Lockfile Inventory

C.1 Direct dependency inventory (sample)

A sample of 20 rows from the 500-row direct dependency inventory is reproduced below. Full inventory: workbook sheet Dependency Packages.

Name	Specified	Pinned	Scope	Ecosystem	Manifest
@tsconfig/node24	^24.0.4	false	devDependencies	JavaScript/Node.js	.buildkite/package.json
@types/node	^25.8.0	false	devDependencies	JavaScript/Node.js	.buildkite/package.json
@types/sax	^1.2.7	false	devDependencies	JavaScript/Node.js	.buildkite/package.json
at.yawk.lz4:lz4-java	1.11.4	true	build.gradle	Java	libs/lz4/build.gradle
ch.obermuhler:big-math	2.3.2	true	build.gradle	Java	libs/core/build.gradle
co.elastic.logging:ecs-logging-core	not quantified	false	build.gradle	Java	server/build.gradle
com.amazonaws:aws-java-sdk-core	not quantified	false	build.gradle	Java	x-pack/plugin/stateless/build.gradle
com.azure:azure-core	1.51.0	true	build.gradle	Java	modules/repository-azure/build.gradle
com.azure:azure-core	1.57.1	true	build.gradle	Java	x-pack/plugin/inference/build.gradle
com.azure:azure-core-http-netty	1.15.3	true	build.gradle	Java	modules/repository-azure/build.gradle
com.azure:azure-identity	1.13.2	true	build.gradle	Java	modules/repository-azure/build.gradle
com.azure:azure-storage-blob	12.27.1	true	build.gradle	Java	modules/repository-azure/build.gradle
com.carrotsearch:hppc	0.8.1	true	build.gradle	Java	server/build.gradle
com.fasterxml.jackson.core:jackson-annotations	2.21	true	build.gradle	Java	libs/arrow/build.gradle
com.fasterxml.jackson.core:jackson-databind	2.21.7	true	build.gradle	Java	libs/arrow/build.gradle

Name	Specified	Pinned	Scope	Ecosystem	Manifest
com.github.ben-manes.caffeine:caffeine	not quantified	false	build.gradle	Java	x-pack/plugin/sql-datasource-iceberg/build.gradle
com.google.api-client:google-api-client	2.7.2	true	build.gradle	Java	modules/repository-gcs/build.gradle
com.google.cloud:google-cloud-storage	2.71.0	true	build.gradle	Java	modules/repository-gcs/build.gradle
com.google.code.gson:gson	2.11.0	true	build.gradle	Java	modules/repository-azure/build.gradle
com.google.guava:guava	33.7.2-jre	true	build.gradle	Java	modules/repository-gcs/build.gradle

C.2 Lockfile resolution

No rows recorded for this evidence item in the current scan. The repository ships no lockfile at any depth scanned.

Appendix D. CVE Inventory

D.1 CVE records (full 20 rows)

ID	Severity	Package name	Ecosyst em	Version	Fixed availabl e	Fixed version
GHSA-82fw-gwwq-j7x9	UNKNO WN	@vitest/mocker	npm	4.1.7	false	Not applicabl e
GHSA-j288-q9x7-2f5v	UNKNO WN	commons-lang:commons-lang	maven	2.6	false	Not applicabl e
GHSA-g7r4-m6w7-qqqr	UNKNO WN	esbuild	npm	0.27.7	false	Not applicabl e
GHSA-28wg-ghj8-5hjh	UNKNO WN	nanoid	npm	3.3.12	false	Not applicabl e
GHSA-2v37-7h3g-55p8	UNKNO WN	nanoid	npm	3.3.12	false	Not applicabl e
GHSA-8wm5-8h9c-47pc	UNKNO WN	org.apache.hadoop:hadoop-common	maven	2.8.5	false	Not applicabl e
GHSA-f5fw-25gw-5m92	UNKNO WN	org.apache.hadoop:hadoop-common	maven	2.8.5	false	Not applicabl e
GHSA-f8vc-wfc8-hxqh	UNKNO WN	org.apache.hadoop:hadoop-common	maven	2.8.5	false	Not applicabl e
GHSA-gx2c-fvhc-ph4j	UNKNO WN	org.apache.hadoop:hadoop-common	maven	2.8.5	false	Not applicabl e
GHSA-rmpj-7c96-mrg8	UNKNO WN	org.apache.hadoop:hadoop-common	maven	2.8.5	false	Not applicabl e
GHSA-337f-xr2x-6fcf	UNKNO WN	org.apache.kerby:ldap-backend	maven	1.1.1	false	Not applicabl e
GHSA-4cx2-fc23-5wg6	UNKNO WN	org.bouncycastle:bcpkix-fips	maven	2.0.7	false	Not applicabl e
GHSA-jr6h-r7vg-f9mc	UNKNO WN	org.ini4j:ini4j	maven	0.5.2	false	Not applicabl e
GHSA-fxqj-rqcc-2cmp	UNKNO WN	postcss	npm	8.5.14	false	Not applicabl e

ID	Severity	Package name	Ecosystem	Version	Fixed available	Fixed version
GHSA-r28c-9q8g-f849	UNKNOWN	postcss	npm	8.5.14	false	Not applicable
GHSA-68fv-2mzg-jv7q	UNKNOWN	source-map-js	npm	1.2.1	false	Not applicable
GHSA-fx2h-pf6j-xcff	UNKNOWN	vite	npm	7.3.3	false	Not applicable
GHSA-v6wh-96g9-6wx3	UNKNOWN	vite	npm	7.3.3	false	Not applicable
GHSA-82fw-gwwq-j7x9	UNKNOWN	vitest	npm	4.1.7	false	Not applicable
GHSA-48c2-rrv3-qjmp	UNKNOWN	yaml	npm	2.3.2	false	Not applicable

CVE records (full 20 of 20 rows). All advisories carry UNKNOWN severity because OSV did not return a CVSS score; all carry no_fixed_release.

Appendix E. License Findings Inventory

E.1 Per-package license findings (sample)

A sample of 18 rows from the 1,305-row per-package license findings inventory is reproduced below. Full inventory: workbook sheet License Contamination.

Package name	Detected license	Is viral	Is restrictive	Confidence	Source file
(repo-level)	AGPL-3.0	true	true	0.8	LICENSE.txt
(repo-level)	Apache-2.0	false	false	0.8	libs/exponential-histogram/LICENSE.txt
(repo-level)	Apache-2.0	false	false	0.8	libs/h3/LICENSE.txt
(repo-level)	Apache-2.0	false	false	0.8	libs/tdigest/LICENSE.txt
(repo-level)	MIT	false	false	0.8	x-pack/plugin/sql/connectors/tableau/connector/LICENSE.txt
(repo-level)	MIT	false	false	0.8	x-pack/plugin/sql/connectors/tableau/tdvt/tds/LICENSE.txt
@tsconfig/node24	MIT	false	false	0.7	.buildkite/package.json
@types/node	MIT	false	false	0.7	.buildkite/package.json
@types/sax	MIT	false	false	0.7	.buildkite/package.json
at.yawk.lz4:lz4-java	UNKNOWN	false	false	0	libs/lz4/build.gradle
ch.obermuhlner:big-math	UNKNOWN	false	false	0	libs/core/build.gradle
co.elastic.logging:ecs-logging-core	UNKNOWN	false	false	0	server/build.gradle
co.elastic.logging:log4j2-ecs-layout	UNKNOWN	false	false	0	server/build.gradle
com.amazonaws:aws-java-sdk-core	UNKNOWN	false	false	0	x-pack/plugin/stateless/build.gradle
com.amazonaws:aws-java-sdk-s3	UNKNOWN	false	false	0	x-pack/plugin/stateless/build.gradle
com.azure:azure-core	UNKNOWN	false	false	0	modules/repository-azure/build.gradle
com.azure:azure-core	UNKNOWN	false	false	0	x-pack/plugin/esql-datasource-azure/build.gradle
com.azure:azure-core	UNKNOWN	false	false	0	x-pack/plugin/inference/build.gradle

E.2 License clause findings (full 9 rows)

License file	Clause type	Severity	Matched packages	Clause text (abridged)
libs/exponential-histogram/LICENSE.txt	attribution	attribution	0 entries	any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices...

License file	Clause type	Severity	Matched packages	Clause text (abridged)
libs/h3/LICENSE.txt	attribution	attribution	0 entries	any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices...
libs/tdigest/LICENSE.txt	attribution	attribution	0 entries	any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices...
x-pack/plugin/sql/connectors/tableau/connector/LICENSE.txt	warranty_disclaimer	permissive	0 entries	shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED AS IS, WITHOUT WARRANTY...
x-pack/plugin/sql/connectors/tableau/tdvt/tds/LICENSE.txt	warranty_disclaimer	permissive	0 entries	shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED AS IS, WITHOUT WARRANTY...
distribution/docker/src/docker/iron_bank/LICENSE	patent_grant	permissive	0 entries	ware. Any use of the licensor's trademarks is subject to applicable law. Patents The licensor grants you a license...
libs/exponential-histogram/LICENSE.txt	patent_grant	permissive	0 entries	ublicense, and distribute the Work and such Derivative Works in Source or Object form. Grant of Patent License...
libs/h3/LICENSE.txt	patent_grant	permissive	0 entries	ublicense, and distribute the Work and such Derivative Works in Source or Object form. Grant of Patent License...
libs/tdigest/LICENSE.txt	patent_grant	permissive	0 entries	ublicense, and distribute the Work and such Derivative Works in Source or Object form. Grant of Patent License...

Appendix F. Complexity, Duplication and SQALE Detail

F.1 Complexity hotspot symbols (sample)

A sample of 16 rows from the 354,925-row hotspot symbols inventory is reproduced below. Full inventory: workbook sheet Complex Symbols.

Name	Filepath	Cyclomatic	Cognitive	Maintainability Index	Composite Risk
getLegalCast	modules/lang-painless/src/main/java/org/elasticsearch/painless/AnalyzerCaster.java	177	2,427	0	0.90
testFailureStoreAccess	x-pack/plugin/security/qa/security-trial/src/javaRestTest/java/org/elasticsearch/xpack/security/failurestore/FailureStoreSecurityRestIT.java	143	675	0	0.90
unicodeScriptToULScript	x-pack/plugin/core/src/main/java/org/elasticsearch/xpack/core/ml/inference/preprocessing/customwordembedding/ScriptCode.java	105	104	15.02	0.87
forPattern	server/src/main/java/org/elasticsearch/common/time/DateFormatters.java	90	905	19.18	0.8501
testAutoscalingCapacity	x-pack/plugin/ml/src/test/java/org/elasticsearch/xpack/ml/autoscaling/NativeMemoryCapacityTests.java	74	0	0	0.85
testPrimitiveIteration	modules/lang-painless/src/test/java/org/elasticsearch/painless/ArrayTests.java	73	72	29.98	0.802
randomSearchSourceBuilder	test/framework/src/main/java/org/elasticsearch/search/RandomSearchRequestGenerator.java	72	145	15.24	0.8695
compute	server/src/main/java/org/elasticsearch/cluster/routing/allocation/allocator/DesiredBalanceComputer.java	71	181	4.8	0.8904
expand	x-pack/plugin/graph/src/main/java/org/elasticsearch/xpack/graph/action/TransportGraphExploreAction.java	67	236	7.31	0.8854
execute	x-pack/plugin/security/cli/src/main/java/org/elasticsearch/xpack/security/cli/AutoConfigureNode.java	67	545	0	0.90
buildBlocks	benchmarks/src/main/java/org/elasticsearch/benchmark/compute/operator/BlockBenchmark.java	65	95	7.94	0.8841
create	modules/analysis-common/src/main/java/org/elasticsearch/analysis/common/StemmerTokenFilterFactory.java	64	918	22.79	0.8544
getNextValidTimeAfter	x-pack/plugin/core/src/main/java/org/elasticsearch/xpack/core/scheduler/Cron.java	63	446	8.87	0.8823
visitDot	modules/lang-painless/src/main/java/org/elasticsearch/painless/phase/DefaultSemanticAnalysisPhase.java	61	297	12.36	0.8753

Name	Filepath	Cyclomatic	Cognitive	Maintainability Index	Composite Risk
resolveFieldName	x-pack/plugin/esql/src/main/java/org/elasticsearch/xpack/esql/session/FieldNameUtils.java	58	200	9.8	0.8804
testToXContent	x-pack/plugin/watcher/src/test/java/org/elasticsearch/xpack/watcher/notification/slack/message/SlackMessageTests.java	58	432	19.05	0.8619

F.2 Duplication groups (sample)

A sample of 14 rows from the 79,013-row duplication groups inventory. Block Start Line is the 1-based line at which the duplicated symbol/module block begins in its file.

Block start line	Block length (lines)	Occurrences
100	10	2 entries
100	10	18 entries
100	10	22 entries
1,001	10	5 entries
1,002	10	5 entries
1,003	10	5 entries
1,004	10	2 entries
1,005	10	2 entries
1,009	10	3 entries
101	10	2 entries
101	10	3 entries
101	10	2 entries
101	10	3 entries
101	10	3 entries

F.3 SQALE debt modules (sample)

A sample of 14 rows from the 33,203-row SQALE debt modules inventory.

Base line	Debt ratio	Module	Remediation effort	SQALE grade
0	0	x-pack/plugin/esql/src/main/generated/.../StEnvelopeFromDocValuesGeoEvaluator.java	0	A
0	0	x-pack/plugin/esql/src/main/generated/.../StEnvelopeFromWKBBGeoEvaluator.java	0	A

Baseline	Debt ratio	Module	Remediation effort	SQALE grade
0	0	x-pack/plugin/esql/src/main/generated/.../StXMaxFromWKBBGeoEvaluator.java	0	A
0	0	x-pack/plugin/esql/src/main/generated/.../StXMinFromWKBBGeoEvaluator.java	0	A
0	0	x-pack/plugin/esql/src/main/generated/.../StYMaxFromWKBBGeoEvaluator.java	0	A
0	0	x-pack/plugin/esql/src/main/generated/.../StYMinFromWKBBGeoEvaluator.java	0	A
10	0	test/framework/src/test/java/Dummy.java	0	A
10	0	x-pack/plugin/core/src/main/java/.../LenientlyParsedTrainedModelLocation.java	0	A
10	0	x-pack/plugin/core/src/main/java/.../StrictlyParsedTrainedModelLocation.java	0	A
10	0	x-pack/plugin/core/src/main/java/.../package-info.java	0	A
10	0	x-pack/plugin/core/template-resources/src/main/java/module-info.java	0	A
10	0	x-pack/plugin/esql/compute/ann/src/main/java/module-info.java	0	A
10	0	x-pack/plugin/esql/compute/src/main/java/.../MetricFieldInfo.java	0	A
10	0	x-pack/plugin/esql/qa/testFixtures/src/main/java/.../LookupIdxColumn.java	0	A

Appendix G. Debt Marker Inventory

G.1 Debt markers (sample)

A sample of 16 rows from the 11,251-row debt markers inventory. Full inventory: workbook sheet Debt Markers.

Filepath	Line	Marker type	Severity	In critical path	Text
build-tools-internal/.../ElasticsearchBuildCompletePlugin.java	115	hack	high	false	// HACK: Some tests leave behind symlinks, and gradle throws an exception if it encounters symlinks.
modules/apm/.../OtelSdkExportLogsSupplier.java	70	fixme	high	false	* FIXME: verify the above is still true?
modules/apm/.../MetricValidator.java	177	fixme	high	false	// FIXME allow MetricAttributes.ERROR_TYPE
qa/packaging/.../PasswordToolsTests.java	76	hack	high	false	// HACK: windows asynchronously releases file locks after processes exit.
server/src/main/java/.../EpochTime.java	283	fixme	high	false	// FIXME: clean these up and append one to the other
server/src/main/java/.../EpochTime.java	45	fixme	high	false	// FIXME: what should this be?
server/src/main/java/.../BinaryQuantizer.java	272	fixme	high	false	// FIXME: make a copy of vector so we don't overwrite it here?
server/src/main/java/.../BinaryQuantizer.java	282	fixme	high	false	// FIXME: quantize these values so we are passing back 1 byte values
server/src/main/java/.../BinaryQuantizer.java	291	fixme	high	false	// FIXME: quantize these values so we are passing back 1 byte values
server/src/main/java/.../BinaryQuantizer.java	306	fixme	high	false	// FIXME: speed up with panama? and/or use existing scalar quantization utils in Lucene?
server/src/main/java/.../BinaryQuantizer.java	349	fixme	high	false	// FIXME: make a copy of vector so we don't overwrite it here?
server/src/main/java/.../BinaryQuantizer.java	353	fixme	high	false	// FIXME: should other similarity functions behave like MIP on query like COSINE
server/src/main/java/.../BinaryQuantizer.java	375	fixme	high	false	// FIXME: quantize the corrections as well so we store less

Filepath	Line	Marker type	Severity	In critical path	Text
server/src/main/java/.../BinaryQuantizer.java	378	fixme	high	false	// FIXME: quantize the corrections as well so we store less
server/src/main/java/.../ES816BinaryFlatVectorsScorer.java	121	fixme	high	false	// FIXME: precompute this once?
server/src/main/java/.../ES816BinaryFlatVectorsScorer.java	147	fixme	high	false	// FIXME: pre-compute these only once for each target vector

Appendix H. Attack Surface Candidate Endpoints

H.1 Candidate entry points (sample)

A sample of 16 rows from the 53-row candidate entry point inventory. Full inventory: workbook sheet Attack Surface.

Sy m bol na me	Filepath	L i n e	Endp oint type	Exp osu re	Fra mew ork	Reac habil ity confi denc e	Inc omi ng edg es	Te st sta tus	Ri sk lev el
ma in	client/benchmark/src/main/java/org/elasticsearch/client/benchmark/BenchmarkMain.java	18	applic ation_e ntry	appl icati on	unkn own	medi um	21	unt est ed	me diu m
ma in	benchmarks/src/main/java/org/elasticsearch/benchmark/exponentialhistogram/ExponentialHistogramGenerationBench.java	89	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	benchmarks/src/main/java/org/elasticsearch/benchmark/h3/H3Benchmark.java	44	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	benchmarks/src/main/java/org/elasticsearch/benchmark/index/codecs/tsdb/TSDBDocValuesMergeBenchmark.java	76	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	benchmarks/src/main/java/org/elasticsearch/benchmark/search/query/range/DateFieldMapperDocValuesSkipperBenchmark.java	161	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	benchmarks/src/main/java/org/elasticsearch/benchmark/tdigest/TDigestBench.java	129	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	build-tools/gradle-runner/src/main/java/org/elasticsearch/gradle/runner/GradleRunner.java	38	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	build-tools/reaper/src/main/java/org/elasticsearch/gradle/reaper/Reaper.java	50	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	build-tools/src/main/java/org/elasticsearch/gradle/NamedComponentScannerMock.java	17	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	client/benchmark/src/main/java/org/elasticsearch/client/benchmark/rest/RestClientBenchmark.java	29	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	distribution/tools/cli-launcher/src/main/java/org/elasticsearch/launcher/CliToolLauncher.java	54	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	distribution/tools/java-version-checker/src/main/java/org/elasticsearch/tools/java_version_checker/JavaVersionChecker.java	22	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	distribution/tools/server-launcher/src/main/java/org/elasticsearch/server/launcher/ServerLauncher.java	52	applic ation_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m

Sy m bol na me	Filepath	L i n e	Endp oint type	Exp osu re	Fra mew ork	Reac habil ity confi denc e	Inc omi ng edg es	Te st sta tus	Ri sk lev el
ma in	libs/core/src/main/java/org/elasticsearch/jdk/JarHell.java	6 7	applica tion_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	libs/core/src/main/java/org/elasticsearch/jdk/JdkJarHellCheck.java	5 5	applica tion_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m
ma in	libs/entitlement/src/test/java/org/elasticsearch/entitlement/initialization/DynamicInstrumentationUtils.java	3 1	applica tion_e ntry	appl icati on	unkn own	medi um	0	unt est ed	me diu m

Appendix I. Key-Person and Knowledge Loss Vulnerability Detail

I.1 Key-person risk rows (sample)

A sample of 14 rows from the 2,969-row key-person risk inventory.

Author name	Author email	Risk score	Total commits	Departure impact
portugee@gmail.com	portugee@gmail.com	0.438801	466,070	medium
rene@elastic.co	rene@elastic.co	0.226206	63,004	low
david.turner@elastic.co	david.turner@elastic.co	0.184465	208,820	low
62058229+ChrisHegarty@users.noreply.github.com	62058229+ChrisHegarty@users.noreply.github.com	0.178643	89,328	low
ryan@iernst.net	ryan@iernst.net	0.176222	78,594	low
nik9000@gmail.com	nik9000@gmail.com	0.166198	382,911	low
me@obrown.io	me@obrown.io	0.165049	138,137	low
pugnascotia@users.noreply.github.com	pugnascotia@users.noreply.github.com	0.158149	41,697	low
artem.prigoda@elastic.co	artem.prigoda@elastic.co	0.154998	40,363	low
lorenzo.dematte@elastic.co	lorenzo.dematte@elastic.co	0.150876	41,168	low
simon.cooper@elastic.co	simon.cooper@elastic.co	0.149473	94,681	low
ievgen.degtiarenko@elastic.co	ievgen.degtiarenko@elastic.co	0.136622	41,054	low
mmack@apache.org	mmack@apache.org	0.131598	18,923	low
yang.wang@elastic.co	yang.wang@elastic.co	0.120524	106,492	low

I.2 Module bus-factor rows (sample)

A sample of 14 rows from the 4,662-row module bus-factor inventory.

Module path	Bus factor	Total files
_unassigned	26	14,374
server/src/main/java/org/elasticsearch/index	12	30
server/src/test/java/org/elasticsearch/index	11	32

Module path	Bus factor	Total files
test/framework/src/main/java/org/elasticsearch/test	11	86
server/src/main/java/org/elasticsearch/cluster/metadata	9	83
server/src/main/java/org/elasticsearch/index/mapper	9	175
server/src/main/java/org/elasticsearch/index/query	9	81
server/src/test/java/org/elasticsearch/cluster/metadata	9	102
server/src/test/java/org/elasticsearch/index/mapper	9	224
test/framework/src/main/java/org/elasticsearch/test/rest	9	12
x-pack/plugin/esql/src/main/java/org/elasticsearch/xpack/esql/plan/logical	9	76
server/src/main/java/org/elasticsearch/common/util/concurrent	8	33
server/src/main/java/org/elasticsearch/indices	8	36
server/src/main/java/org/elasticsearch/node	8	15

I.3 Knowledge loss vulnerability rows (sample)

A sample of 14 rows from the 2,969-row knowledge loss vulnerability inventory. All entries carry critical retention risk; the blast radius at risk column captures the number of files that depend on the contributor's institutional knowledge.

Author name	Author email	Tenure days	Days since last commit	Retention risk	Blast radius at risk
Johannes Fredén	109296772+jfreden@users.noreply.github.com	1,056	2	critical	0
Valeriy Khakhutsky	1292899+valeriy42@users.noreply.github.com	2,318	0	critical	0
Kostas Krikellas	131142368+kkrik-es@users.noreply.github.com	1,269	23	critical	720
Matteo Piergiovanni	134913285+piergm@users.noreply.github.com	1,150	99	critical	0
Jan Kuipers	148754765+jan-elastic@users.noreply.github.com	1,067	0	critical	9,690
Fang Xing	155562079+fang-xing-esql@users.noreply.github.com	994	0	critical	0
Stef Nestor	26751266+stefnestor@users.noreply.github.com	1,163	0	critical	0
Henning Andersen	33268011+henningandersen@users.noreply.github.com	2,823	13	critical	1,321
Ines Potier	34454302+inespot@users.noreply.github.com	259	0	critical	2,540
Kris Van Erum	34942518+kvanerum@users.noreply.github.com	464	107	critical	2,764
Brian Rothermich	35897794+BrianRothermich@users.noreply.github.com	545	9	critical	0
Mariusz Józala	377355+jozala@users.noreply.github.com	730	2	critical	10,689
eyalkoren	41850454+eyalkoren@users.noreply.github.com	1,268	0	critical	0

Author name	Author email	Tenure days	Days since last commit	Retention risk	Blast radius at risk
Jason Botzas-Coluni	44372106+jaybcee@users.noreply.github.com	693	6	critical	0

© MTD Services

Appendix J. Maintenance, IaC and CI/CD Detail

J.1 Maintenance assets

No rows recorded for this evidence item in the current scan. The asset-staleness scanner produced zero population.

J.2 IaC findings

No rows recorded for this evidence item in the current scan. Total IaC findings = 0; risk level = informational.

J.3 CI files (full 11 rows)

CI file path
/content/elasticsearch/.github/workflows/check-esql-generated-headers.yml
/content/elasticsearch/.github/workflows/docs-build.yml
/content/elasticsearch/.github/workflows/docs-deploy.yml
/content/elasticsearch/.github/workflows/docs-preview-cleanup.yml
/content/elasticsearch/.github/workflows/gradle-wrapper-validation.yml
/content/elasticsearch/.github/workflows/pr-bypass-for-automation.yml
/content/elasticsearch/.github/workflows/review-bug-analysis.yml
/content/elasticsearch/.github/workflows/review-test-analysis.yml
/content/elasticsearch/.github/workflows/trigger-bug-analysis.yml
/content/elasticsearch/.github/workflows/trigger-test-analysis.yml
/content/elasticsearch/.github/workflows/updatecli-compose.yml

J.4 Coverage artifacts

No coverage artifacts recorded.

Appendix K. Privacy and Secrets Detail

K.1 Privacy findings (full 1 row)

Rule ID	Category	Title	Severity	File	Line	Remediation
PRIV-SENSITIVE-LOG	sensitive_logging	Sensitive data in log statement (ssn)	medium	.buildkite/scripts/flakiness-detection/entrypoints/local.ts	84	Redact the value; log a reference id and audit retention.

K.2 Secret candidates (sample)

A sample of 14 rows from the 220-row secret candidates inventory. Full inventory: workbook sheet Secrets Candidates.

Kind	File	Line	Confidence	In history	Commit	Risk cap	Path tier
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	160	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	136	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	117	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	129	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	143	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	163	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	38	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	53	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	123	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	30	95	false	not applicable	critical	test

Kind	File	Line	Confidence	In history	Commit	Risk cap	Pat h tier
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	47	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-iceberg/src/test/java/.../S3ConfigurationTests.java	111	95	false	not applicable	critical	test
aws_access_key	x-pack/plugin/esql-datasource-s3/src/test/java/.../S3DataSourceValidatorTests.java	1,705	95	true	02fa570f3cc2	critical	test
aws_access_key	x-pack/plugin/esql-datasource-s3/src/test/java/.../S3DataSourceValidatorTests.java	1,790	95	true	1821143b0eb2	critical	test

Secret candidates (sample of 14 rows from 220). The 12 high-confidence candidates at confidence 95 in the S3ConfigurationTests.java file are the priority for the credential rotation condition precedent.

Appendix L. AI/ML Inventory

L.1 Model files (full 3 rows)

File	Name	Extension	Size (bytes)	Licence declared	Licence	Model card present	Is test artifact
x-pack/plugin/inference/qa/inference-service-tests/src/javaRestTest/resources/elser_model_2.pt	elser_model_2	.pt	1,859,242	false	not applicable	false	false
x-pack/plugin/inference/qa/inference-service-tests/src/javaRestTest/resources/multilingual-e5-small.pt	multilingual-e5-small	.pt	5,531,160	false	not applicable	false	false
x-pack/plugin/inference/qa/inference-service-tests/src/javaRestTest/resources/rerank-v1.pt	rerank-v1	.pt	12,419,194	false	not applicable	false	false

Model files (full 3 of 3 rows). All three bundled models carry no declared licence and no model card.

Appendix M. Integrity and Data-Quality Issues

M.1 Integrity issues (full 11 rows)

Tier	Code	Subject	Message
warn	critical_pillar_no_findings	pillars.ci_maturity	Pillar 'ci_maturity' is high but renders no item-level findings - posture held on summary metrics.
warn	critical_pillar_no_findings	pillars.coverage	Pillar 'coverage' is high but renders no item-level findings - posture held on summary metrics.
warn	critical_pillar_no_findings	pillars.integration	Pillar 'integration' is high but renders no item-level findings - posture held on summary metrics.
warn	critical_pillar_no_findings	pillars.ip_ownership	Pillar 'ip_ownership' is high but renders no item-level findings - posture held on summary metrics.
warn	critical_pillar_no_findings	pillars.test_deficit	Pillar 'test_deficit' is high but renders no item-level findings - posture held on summary metrics.
warn	unverified_pillar	pillars.cve	Pillar 'cve' is partial - 235 package requirement(s) could not be resolved to a version (no lockfile / unpinned).
warn	unverified_pillar	pillars.dependency	Pillar 'dependency' is partial - no lockfile; transitive dependency resolution could not be performed; direct pins cover only 49 percent.
warn	unverified_pillar	pillars.entanglement	Pillar 'entanglement' is not_assessed - scanner failed (RecursionError: maximum recursion depth exceeded).
warn	unverified_pillar	pillars.eol	Pillar 'eol' is not_assessed - zero evidence population (population=0) for eol; reported as NOT_ASSESSED rather than a clean result.
warn	unverified_pillar	pillars.maintenance	Pillar 'maintenance' is not_assessed - no files were scanned by the asset-staleness scanner; maintenance not assessed.
warn	unverified_pillar	pillars.secrets	Pillar 'secrets' is partial - 111 path-excluded candidate path(s) not scanned; 33,203 files scanned.

Appendix N. Taint Analysis Summary

N.1 Taint summary

Metric	Value
Bounded	false
Total flows	12

The taint pass was not bounded (the scanner did not complete the full closure). The 12 flows are therefore a partial enumeration, not a closed inventory.

N.2 Top taint flows

Twelve flows were detected; the full taint flow detail is in the workbook sheet Taint Summary.

Appendix O. Financial Reproduction Fingerprint

The financial reproduction fingerprint binds the report to the exact configuration used to produce every number: same inputs in, same outputs out. Any change to a number-driving input produces a different fingerprint and a different report under a new fingerprint. The full calibration, lineage, and sensitivity detail lives in Chapter 3, not re-rendered here.

O.1 Reproduction fingerprint

Field	Value
Reproduction fingerprint	03b1728eed153b3c6fc1553a508a9f2e5c8901e18b3ad20ceaf0ddf4a0427b42
Economic model fingerprint	36c9c7dcffe8ec055380122c75045a23350016e4c3685385c37a7490d40973f9
Repository HEAD commit	eb0570f936c219289fce88e6abe9f3dc0a74d54c
Repository path	elasticsearch
Scan mode	deal_thesis=True, offline=False, scan_history=True, taint=True

Appendix P. Evidence Provenance

The payload path is the single stored source the narrative's evidence derives from; key-variant fallbacks are resolved at render time and are not listed here. The workbook column names the sheet that inventories the same evidence; 'not applicable' means no dedicated sheet carries it.

P.1 Evidence provenance table

Evidence ID	Source JSON path	Workbo k sheet
1.1 Board decision	decision.board_decision	Dashboard
1.2 Confidence score	decision.confidence_score	Dashboard
1.3 Decision driver	decision.escalation.driver	Dashboard
1.4 Remediation cost as percent of price	decision.remediation_cost_pct_of_acquisition	Dashboard
1.5 Proposed price	decision.proposed_price	Dashboard
1.6 Total remediation cost	financial.total_remediation_cost	Dashboard
1.7 Total remediation hours	financial.total_remediation_hours	Dashboard
1.8 Valuation discount applied	financial.valuation_discount_pct	Dashboard
1.9 Post-merge integration drag	financial.post_merge_integration_drag_pct	Dashboard
1.10 Pillar register size	decision.pillar_register	Dashboard
1.11 Top risk findings	decision.top_risks	Dashboard
1.12 Major risks	decision.major_risks	Dashboard
1.13 Integrity status	integrity.status	Contents
1.14 Integrity error count	integrity.error_count	Contents
1.15 Integrity warning count	integrity.warn_count	Contents
2.1 Conditions for acquisition	decision.conditions_for_acquisition	Dashboard
2.2 Deal-breaker register	decision.deal_breakers	Dashboard
2.3 Categorical decision tier	decision.escalation.categorical_tier	Dashboard
2.4 Economic decision tier	decision.escalation.economic_tier	Dashboard
2.5 Conditions escalation threshold	decision.escalation.conditions_threshold_pct	Dashboard
2.6 No-go escalation threshold	decision.escalation.no_go_threshold_pct	Dashboard
2.7 Economic gate disputed	decision.escalation.disputed	Dashboard
2.8 Escalation driver	decision.escalation.driver	Dashboard
2.9 Per-pillar escalation rows	decision.escalation.pillars	Dashboard
2.10 Economic conditions threshold	financial.assumptions.economic_escalation.conditions_if_above_pct	Dashboard
2.11 Economic no-go threshold	financial.assumptions.economic_escalation.no_go_if_above_pct	Dashboard
2.12 Sensitivity sweep outcomes	financial.sensitivity	Dashboard
2.13 Condition deal-mechanic tags	decision.condition_details	Dashboard
3.1 Remediation line items	financial.line_items	Dashboard
3.2 Total remediation hours	financial.total_remediation_hours	Dashboard

Evidence ID	Source JSON path	Workbook sheet
3.3 Total remediation cost	financial.total_remediation_cost	Dashboard
3.4 Valuation discount applied	financial.valuation_discount_pct	Dashboard
3.5 Post-merge integration drag	financial.post_merge_integration_drag_pct	Dashboard
3.6 Hourly rate	financial.assumptions.hourly_rate	Dashboard
3.7 Complexity multiplier	financial.assumptions.complexity_multiplier	Dashboard
3.8 Valuation multiplier	financial.assumptions.valuation_multiplier	Dashboard
3.9 Integration drag factor	financial.assumptions.integration_drag_factor	Dashboard
3.10 Productive hours per quarter	financial.assumptions.productive_hours_per_quarter	Dashboard
3.11 Person-years of remediation	financial.assumptions.person_years	Dashboard
3.12 Remediation cost confidence interval	financial.assumptions.remediation_cost_confidence_interval	Dashboard
3.13 Conditions threshold	financial.assumptions.economic_escalation.conditions_if_above_pct	Dashboard
3.14 No-go threshold	financial.assumptions.economic_escalation.no_go_if_above_pct	Dashboard
3.15 Valuation discount cap	financial.assumptions.valuation_discount_cap_pct	Dashboard
3.16 Integration drag cap	financial.assumptions.integration_drag_cap_pct	Dashboard
3.17 Aggregate hours cap	financial.assumptions.aggregate_cap	Dashboard
3.18 Saturation model	financial.assumptions.saturation_model	Dashboard
3.19 Line-item basis	financial.assumptions.line_item_basis	Dashboard
3.20 SQALE remediation basis	financial.assumptions.sqale_remediation_basis	Dashboard
3.21 Sensitivity sweep details	financial.sensitivity	Dashboard
3.22 Financial lineage	financial.lineage	Dashboard
3.23 Remediation cost as percent of price	decision.remediation_cost_pct_of_acquisition	Dashboard
3.24 Economic model fingerprint	financial.economic_layers.economic_layers_fingerprint	Dashboard
3.25 Risk valuation lines	financial.economic_layers.layer2_risk.lines	Dashboard
3.26 Aggregate expected loss before	financial.economic_layers.layer2_risk.aggregate_expected_loss_before	Dashboard
3.27 Aggregate residual expected loss	financial.economic_layers.layer2_risk.aggregate_residual_expected_loss	Dashboard
3.28 Aggregate risk-reduction value	financial.economic_layers.layer2_risk.aggregate_risk_reduction_value	Dashboard
3.29 Quantified risk lines	financial.economic_layers.layer2_risk.quantified_count	Dashboard
3.30 Not-quantified risk lines	financial.economic_layers.layer2_risk.not_quantified_count	Dashboard
3.31 Scenario branches	financial.economic_layers.layer3_scenario.branches	Dashboard
3.32 Weighted expectation across scenarios	financial.economic_layers.layer3_scenario.weighted_expectation	Dashboard
3.33 Scenario-based technology VaR	financial.economic_layers.layer3_scenario.var_label	Dashboard
3.34 Deal components	financial.economic_layers.layer4_deal.components	Dashboard
3.35 Executive deal-bridge rows	financial.economic_layers.layer4_deal.bridge	Dashboard

Evidence ID	Source JSON path	Workbook sheet
3.36 Double-counting ledger figures	financial.economic_layers.p0_double_counting.figures	Dashboard
3.37 Double-counting ledger clean verdict	financial.economic_layers.p0_double_counting.clean	Dashboard
3.38 Justified overlapping keys	financial.economic_layers.p0_double_counting.justified_overlapping_keys	Dashboard
3.39 Categories not costed this scan	financial.line_items	Dashboard
3.40 Per-line-item threshold breach view	financial.line_items	Dashboard
3.41 Downside exposure range and percentile VaR	financial.economic_layers.downside	Dashboard
3.42 Deal economics headline valuation reconciliation	financial.economic_layers.layer4_deal	Dashboard

Evidence provenance (63 of 175 rows). Full inventory in workbook sheet Dashboard.

Appendix Q1. Technical Glossary

Terms are used consistently and never redefined per section, so a client and its advisers converge on one shared frame. This glossary is alphabetically sorted and defines every technical or specialist term appearing in any TDD table column heading in this report.

Term	Meaning
AGPL-3.0	GNU Affero General Public License v3.0 - a viral copyleft licence that extends GPL obligations to network-served software. The single high-severity license finding in this scan.
Apache-2.0	Apache License 2.0 - a permissive licence with an express patent grant. Used by several bundled libraries in the target.
Attack Surface	The set of candidate entry points through which an external actor could interact with the application. Measured here as the count of unresolved application_entry symbols.
Attribution	A license clause requiring that derivative works preserve copyright, patent, trademark, and attribution notices from the source form.
Bus Factor	Reciprocal of sole-contributor concentration per module. A low bus factor (e.g. 1) flags flight risk because the module depends on a single contributor.
CantSplit	A table-row property that prevents row content from being split across pages. Set on every data row to preserve table integrity.
Candidate Endpoint	A symbol that the scanner identifies as a potential entry point (application_entry or candidate type). All 53 candidates this scan are untested.
CI Maturity	Posture of the continuous-integration pipeline: defined workflows, gate strictness, whether tests run, whether coverage is reported. Pillar risk = high this scan.
Cognitive Complexity	A per-symbol measure of how difficult code is to read and understand, weighting nesting and branching. P99 = 46 this scan.
Complexity Hotspot	A symbol whose cyclomatic or cognitive complexity exceeds the 99th-percentile threshold, flagged for refactoring. 2,868 hotspots identified this scan.
Condition Precedent	A deal mechanic: an obligation that must be satisfied or proven before close, or the deal does not sign as structured.
Contamination Chain	A path through the dependency tree that propagates a viral or restrictive license to the shipped product. Zero chains recorded this scan.
Coverage Method	The basis on which test coverage is measured. This scan uses a static symbol-share proxy, not runtime or line/branch coverage.
Cross-Layer Violation	A code-level violation of architectural layering (e.g. a controller calling the data layer directly). No rows recorded this scan due to entanglement scanner failure.
Cyclomatic Complexity	A per-symbol measure of the number of linearly independent paths through the code. P50 = 1, P90 = 3, P99 = 10 this scan.
Debt Density	Total debt markers normalised per thousand lines of code. Debt density = 0.0217 this scan.
Debt Marker	An in-comment annotation (fixme, hack, todo, xxx) or a tooling suppression that flags technical debt. 11,251 markers recorded this scan.
Double-Counting Ledger	An audit table that reconciles figures appearing on multiple surfaces so they are counted once. Clean verdict = true this scan.
Dynamic Endpoint	A candidate endpoint whose exposure is determined at runtime rather than by static analysis. Zero dynamic endpoints this scan.
Effective Insured Value	The dollar value of code covered by tests, used as a contingent-liability sizing input. Zero this scan.

Term	Meaning
End-of-Life (EOL)	A technology or runtime version that the upstream vendor no longer maintains. EOL pillar is NOT_ASSESSED this scan due to zero lockfile.
Entanglement Score	A composite measure of architectural coupling (cyclic dependencies, cross-layer violations, schema drift). Not recorded this scan due to scanner failure.
Evidence State	Per-finding honesty label: Confirmed, Detected-not-verified, Inferred, Partially-assessed, Unassessed, Conflicting, or Unsupported.
Finding Id	Stable identifier F-pillar-rank for one assessed finding; the register, narrative, workbook, and ledger all cite it.
Framework Hit	A count of references to an AI/ML framework (Hugging Face, PyTorch, etc.) across the scanned source files.
High-Confidence Secret	A secret candidate whose pattern confidence exceeds the high-confidence threshold (e.g. 90). 4 high-confidence candidates this scan.
High-Value Gap	A coverage gap in a module whose risk weight exceeds a threshold. 1,183 high-value gaps this scan.
HPU (Hours Per Unit)	Remediation hours per unit, per cost category, saturated by cap and decay under the financial model.
IaC	Infrastructure-as-Code: declarative configuration of infrastructure (Terraform, CloudFormation, etc.). 0 findings this scan.
Indexed Files	Count of source files processed by the scanner's indexing phase. 33,203 files this scan.
Inferred	An evidence state label: the finding is derived from indirect signals (e.g. contributor tenure inferring retention risk).
Integration Risk Score	A composite measure of integration friction (proprietary coupling, schema drift, API contract maturity). Score = 10 (maximum) this scan.
IP Ownership	Attribution of file-level authorship to corporate vs. external domains. 74.27 percent external blame this scan.
Lockfile	A manifest of resolved dependency versions (package-lock.json, pnpm-lock.yaml, Gradle lockfile). Zero lockfiles present this scan.
Maintenance Backlog Score	An aggregate measure of neglected and at-risk files. Zero this scan due to scanner coverage gap.
Manifest	A dependency declaration file (package.json, build.gradle) that lists direct dependencies.
Materiality Floor	An absolute-dollar threshold that the conditions gate must clear in addition to the percentage threshold. USD 250,000 this scan.
MIT License	A permissive licence allowing reuse with attribution. Used by several bundled npm dependencies.
Model Card	A documentation artefact describing a machine-learning model's training data, intended use, and limitations. None present for the 3 bundled models this scan.
OpenAPI Found	Whether an OpenAPI / Swagger specification was detected in the repository. False this scan.
P50 / P90 / P99	Statistical percentiles of a measured distribution. Cyclomatic P99 = 10 means 1 percent of symbols have complexity greater than 10.
Path-Excluded Candidate	A secret-candidate file path that the scanner did not examine (e.g. large binary or fixture directory). 111 paths excluded this scan.
Pin Ratio	Share of direct dependencies carrying explicit version pins. 48.9 percent this scan.
Post-Merge Integration Drag	The share of remediation effort that translates to friction during integration. 80 percent (capped) this scan.
Population	The evidence count a verdict rests on. A zero population never reads as clean.

Term	Meaning
Price-Adjustment Lever	A deal mechanic: a funded or escrowed work item that moves value rather than blocking close.
Production Model Files	Bundled AI/ML model files flagged as production (rather than test fixture). 3 production files this scan.
Proprietary Coupling Count	Count of integrations that depend on the target's proprietary internals. 11,731 this scan.
Protocol-Layer Risk	A risk finding in the network or transport layer (e.g. raw socket usage). 67 findings this scan.
Remediation Class	A categorisation of CVE remediation approach: no_fixed_release, fixed_release_available, etc. All 20 advisories this scan carry no_fixed_release.
Remediation Effort	Hours or days estimated to remediate a finding or population. SQALE remediation effort = 630,109 days this scan.
Retention Risk	A per-contributor flag for flight risk, derived from tenure and inactivity. 396 at-risk contributors this scan.
Saturation Cap	A ceiling on the count of items costed at the full hours-per-unit rate in a remediation line item.
Saturation Decay HPU	The reduced hours-per-unit applied to counts above the saturation cap.
Schema Drift Risk	Risk that the database schema evolves inconsistently with the code. Rated high this scan.
Secrets Candidate	A pattern match flagged as a potential secret (AWS key, password, certificate, etc.). 220 candidates this scan.
Sensitive Log	A log statement that emits sensitive data (PII, credentials). 1 finding this scan (SSN).
Serialization Risk	A risk finding in deserialization code (e.g. dynamic_function). 11,731 findings this scan.
Sole-Maintainer Module	A module whose bus factor is 1: only one contributor maintains it. 2,698 critical sole-maintainer modules this scan.
SQALE	Software Quality Assessment based on Lifecycle Expectations - a standardised remediation-effort basis.
SQALE Grade	A letter grade (A through E) summarising SQALE debt. Grade = E this scan (the worst passing grade).
Suppression Marker	A tooling-level suppression (e.g. @SuppressWarnings) that silences a static-analysis warning. 7,103 suppressions this scan.
Taint Flow	A code path through which untrusted input reaches a sensitive sink without sanitisation. 12 flows this scan.
Test Deficit Score	A composite measure of test coverage gaps. Score = 0.0125 this scan.
Test Ratio	Ratio of test-file symbols to source-file symbols per module. Overall test ratio = 0.03 percent this scan.
TSA	Transition Services Agreement: a contractual framework for the seller to provide services to the buyer during the integration period.
Unverified Pillar	A pillar whose assessment status is partial or not_assessed; conclusions UNVERIFIED. Five pillars this scan.
Value Coverage Ratio	The share of structural value covered by tests. Zero this scan.
Warranty / Representation	A deal mechanic: a seller statement whose breach is an indemnity question, not a work plan.

Technical glossary. Terms are used consistently and never redefined per section.

Appendix Q2. Transaction Glossary

This glossary defines every M&A term used in the report body, organised alphabetically. Together with Appendix Q1 (Technical Glossary), it gives a client and its advisers one shared transaction vocabulary.

Term	Meaning
Acqui-hire	An acquisition whose primary rationale is the target's engineering team rather than its product. Scored 10 out of 10 in this scan's deal-thesis alignment but capped by 'Detected, not verified' evidence state.
Condition Precedent	A deal mechanic: an obligation that must be satisfied or proven before close, or the deal does not sign as structured. Four conditions this scan: AI/ML legal review, CI gate, CVE remediation, credential rotation.
Confidence Score	A 0-to-100 measure of how much weight the report's recommendation carries, computed as $20 + 40 \times \text{coverage} + 40 \times \text{risk_signal}$. Score = 67 this scan.
Cyber-Insurance	Insurance coverage for security incidents and breaches. Sized in this report against the secrets and attack-surface findings (Chapters 5 and 9).
Deal Thesis	The buyer's stated rationale for the acquisition, evaluated against evidence in the report. All six theses declared this scan; none primary.
Deal-Breaker	A pillar-level finding severe enough to force a no-go verdict. No deal-breaker pillars triggered this scan.
Disclosure Schedule	A legal document attached to the SPA that lists exceptions to the seller's warranties. The risk register in Chapter 14 maps to disclosure schedule entries.
Earn-Out	A deal structure where part of the purchase price is contingent on post-close performance. The retention condition in Chapter 2 may be structured as an earn-out.
Economic Escalation Gate	A threshold that triggers a different decision tier when remediation cost crosses it. Conditions gate at 5 percent; no-go gate at 25 percent.
Escrow	A funded work item held back from the purchase price against delivery. The six price-adjustment levers in Chapter 2 may be escrowed.
Headline EV	Headline enterprise value: the proposed price before any technology-impact adjustments. USD 20,000,000 this scan.
Holdback	A portion of the purchase price retained by the buyer until conditions are met. Distinct from escrow (held by a third party) but functionally similar.
Indemnity Cap	A ceiling on the seller's liability for breach of warranty. Sized by deal counsel; not a number in this report.
Integration Drag	The share of remediation effort that translates to friction during integration. 80 percent (capped) this scan.
Investment Committee (IC)	The body within the buyer's organisation that approves the transaction. The one-page executive brief (front matter) is designed for IC pre-read.
Materiality Floor	An absolute-dollar threshold that an escalation gate must clear in addition to the percentage threshold. USD 250,000 for the conditions gate this scan.
M&A Adviser	An external party engaged by the buyer or seller to advise on the transaction. The intended reader of this report alongside the IC.
No-Go Threshold	The percentage of price above which remediation triggers a no-go verdict. 25 percent this scan.
Post-Close Remediation Tracker	A document tracking the delivery of remediation workstreams after close. Established by the 100-day closeout report (Chapter 23).

Term	Meaning
Price-Adjustment Lever	A deal mechanic: a funded or escrowed work item that moves value rather than blocking close. Six levers this scan.
Proposed Price	The headline enterprise value the buyer has offered for the target. USD 20,000,000 this scan.
Quality-of-Earnings (QoE)	A financial due-diligence workstream that examines the target's earnings quality. The seller's QoE provider will challenge the inputs in Chapter 3.
Remediation Cost	The dollar estimate for addressing the technical findings in this report. USD 1,019,403 this scan (5.1 percent of price).
Representation	A seller statement of fact in the SPA. Breach of a representation is an indemnity question, not a work plan.
Risk-Adjusted Negotiation	A negotiation stance that prices each material finding into the deal terms. The Negotiation Term Sheet (Appendix B of Executive Artifacts) implements this stance.
Sensitivity Sweep	A what-if analysis that multiplies each financial parameter by 0.7, 1.0, and 1.3 and recomputes the board decision. All 17 rows return the same tier this scan.
SPA (Sale and Purchase Agreement)	The principal transaction document. The eleven conditions in Chapter 2 are drafted into the SPA's conditions, price-adjustment, and warranties sections.
Transition Services Agreement (TSA)	A contractual framework for the seller to provide services (IT, HR, finance) to the buyer during the integration period. Sized against the integration risk score in Chapter 9.
Valuation Discount	The percentage reduction in enterprise value implied by the technology findings. 24.4 percent this scan (capped at 25 percent).
Valuation Multiplier	A parameter that amplifies remediation cost into the valuation discount. Set to 3 this scan.
Value-at-Risk (VaR)	A measure of potential loss at a given confidence percentile. The scenario-based technology VaR is the model's honest label; it is not a market-risk measure.
Warranty	A seller statement of fact in the SPA. Breach is an indemnity question, not a work plan. One warranty this scan: assignability of third-party contributions.
Working-Group Escrow	A funded work item held against a specific workstream's delivery. The technical-debt remediation fund is the most natural candidate for working-group escrow this scan.

Transaction glossary. Together with Appendix Q1, gives the client and its advisers one shared transaction vocabulary.

Appendix R. Contradiction Ledger and Release Record

Every material conflict is listed with its status, resolution, and decision impact. Unresolved entries discount the confidence stated in the executive brief.

R.1 Contradiction ledger

ID	Conflict	Subjects	Evidence	Status	Resolution	Decision impact
C-DC-001	No double-counting findings across quantified economic figures	Remediation, Risk valuation, Scenario analysis, Deal economics	Anti-double-counting ledger	resolved	Shared-registry keys show each evidence once, on multiple surfaces, never added twice.	None
C-ERR-001	1 pillar scanner(s) failed; their domains are reported as NOT_ASSESSED rather than clean	Entanglement	pillars.*.raw.error	by-design	Failed scanners degrade to not_assessed with the error preserved in raw.error; no fabricated clean result.	Coverage is incomplete for those domains; confidence is discounted accordingly.

R.2 Release record

Field	Value
Report ID	TDD-20261016-060331
Generated	2026-10-16T07:18:30 (UTC)
Report version	0.9.2
Ledger summary	1 by-design, 1 resolved
Scan steps	6 recorded