01 / EXECUTIVE SCORECARD

Argus assessment Results and remediation

81
ASSESSMENT CASES
8 review areas

92.6%
CASE COVERAGE
75 scored / 81 planned

88.0%
CASE ACCEPTANCE
66 pass / 75 scored

3
UNIQUE FINDINGS
9 failed cases / 3 issues

2
HIGH-PRIORITY ISSUES
1 medium / 0 critical

6
PENDING CASES
Cost and data handling



66 pass 9 fail 6 pending

Disposition: remediation and retest

The scorecard contains two high-priority findings and six unresolved cases. The proposed response is to resolve the high-priority issues and complete the missing checks before approving the assessed workflow.

Priority	Recommended action
High / F-02	Restrict cross-customer report access. Two of ten isolation cases fail.
High / F-01	Expose incomplete collection. Four of ten scan-completeness cases report an incorrect status.
Medium / F-03	Investigate three missed public-access fixtures. Five of eight seeded violations are detected.

Coverage = 75 / 81. Acceptance = 66 / 75. Pending cases remain outside the acceptance denominator and visible in coverage.

02 / SCOPE AND COVERAGE

Where the numbers come from

Proposed assessment unit: one Argus build, two synthetic customer tenants, approved AWS test accounts, and an agreed service/region inventory. Actual build, execution dates, environments, and access remain pending.

Test area	Cases	Pass	Fail	Pending	Coverage
AWS access	10	10	0	0	10/10
Customer isolation	10	8	2	0	10/10
Finding accuracy	12	9	3	0	12/12
Scan completeness	10	6	4	0	10/10
Drift reporting	10	10	0	0	10/10
Cost reporting	9	7	0	2	7/9
Data handling	10	6	0	4	6/10
Traceability	10	10	0	0	10/10
TOTAL	81	66	9	6	75/81

Read each measure against its denominator

Measure	Value	Interpretation
Case coverage	75 / 81 = 92.6%	Cases with a supplied outcome and reviewer verdict.
Case acceptance	66 / 75 = 88.0%	Scored cases that meet their defined expectation.
Violation detection	5 / 8 = 62.5%	Seeded violations detected in the eight positive fixtures.
False alarms	0 / 4 controls	Compliant reference cases with an incorrect finding.
Cost variance	USD 0.00 in 7 cases	Absolute difference against matching reference totals. Two billing cases are pending.

Scoring and evidence

Each case has one verdict. Nine failures map to three findings: four scan-status failures, two export-isolation failures, and three missed public-access fixtures. Production findings would retain the input, expected result, raw output, configuration, evidence hash, execution time, and reviewer.

03 / FINDINGS REGISTER

Three issues. Ranked by impact.

Severity distribution

Critical	High	Medium	Low	Total
0	2	1	0	3

ID / priority	Issue and impact	Cases
F-01 / High	An unreadable or interrupted scan is shown as clear or complete. A partner could act on a misleading assessment summary.	T04-01, 02, 04, 05
F-02 / High	A report export returns another customer's record. A user with access to one tenant could receive another tenant's information.	T02-03, 05
F-03 / Medium	A configured check misses three seeded public-access fixtures. The partner would need an additional review to identify the issue.	T03-03, 05, 06

Severity rationale

High reflects customer-data exposure or a failed collection path that can mislead a consequential decision. Medium reflects a missed check in this bounded fixture. Actual severity would depend on affected data, prerequisites, reachability, and demonstrated impact.

Open evidence gaps

Pending case	Missing evidence	Consequence for the opinion
T06-03, 09	Credits and amortized cost references	Seven of nine billing fixtures can be reconciled.
T07-02, 09	Backup and replica deletion evidence	Long-lived copies remain outside verified deletion coverage.
T07-03, 10	Subprocessor inventory and retention settings	Third-party handling and retention remain unassessed.

All three findings are open. Fix verification and reviewer sign-off remain pending. Production acceptance criteria must retain unresolved issues and missing evidence.

04 / EVIDENCE WALKTHROUGH / F-01

A finding an engineer can reproduce

Expected and supplied behavior

Case	Expected result	Response	Verdict
T04-01	IAM status incomplete after AccessDenied.	IAM status clear; finding count 0.	Fail
T04-02	Scan incomplete after collection stops early.	Scan status complete.	Fail
T04-03	Scan complete after every required check finishes.	Scan status complete.	Pass

E-T04-01 / Minimal synthetic trace

```
tenant: demo-client-a
check: iam-inventory
collector_result: AccessDenied
required_check_completed: false
summary_status: clear
finding_count: 0
```

Impact and quantified exposure

The three cases above describe the failure path. Across all ten completeness cases, four fail and six pass. The failed paths involve denied reads, interruption, exhausted retries, and regional timeout. The defect concerns how missing evidence reaches the summary, which requires a different fix from changing an individual detection rule.

Reproduction in the agreed test environment

Deny one required read in a disposable account, trigger a normal scan, and compare the collector error with the check and scan summaries. Repeat with an interrupted job and a successful collection control. Record the exact role, rule version, run ID, timestamps, and raw responses.

Fix and closure target

Propagate collection status into the summary and available exports. Proposed retest target: 10 / 10 cases pass, all four failed collection paths stay visibly incomplete, and successful controls remain complete. Live retest results are pending.

05 / CASE LEDGER / 1 OF 7

Cases 1-12

Each case supplies one verdict to the executive scorecard. Finding IDs connect failed cases to the remediation register.

Case / input	Output or observation	Verdict
T01-01 Valid role and external ID	Read permitted for the correct customer role.	PASS
T01-02 Incorrect external ID	AssumeRole request denied.	PASS
T01-03 Unapproved write operation	Write denied on a disposable test resource.	PASS
T01-04 Missing external ID	Role assumption denied.	PASS
T01-05 Customer B external ID on A role	Mismatched customer context denied.	PASS
T01-06 Expired temporary credentials	Read rejected after credential expiry.	PASS
T01-07 Trust policy removes scanner principal	New role session denied.	PASS
T01-08 Read outside approved resource scope	Out-of-scope resource denied.	PASS
T01-09 Successful session refresh	Approved read resumes with new session.	PASS
T01-10 Unapproved delete operation	Delete denied on disposable resource.	PASS
T02-01 Customer A lists its findings	Only customer A records returned.	PASS
T02-02 Customer A requests B detail	Request denied with no B record returned.	PASS

Subtotal: 12 cases, 12 pass, 0 fail, 0 pending.

06 / CASE LEDGER / 2 OF 7

Cases 13-24

Each case supplies one verdict to the executive scorecard. Finding IDs connect failed cases to the remediation register.

Case / input	Output or observation	Verdict
T02-03 Customer A opens B export	Export contains one synthetic B record.	FAIL F-02
T02-04 Customer A requests B cached view	No B data served from the cache.	PASS
T02-05 Customer A downloads B report file	Download contains one synthetic B record.	FAIL F-02
T02-06 Unauthenticated findings request	Authentication required.	PASS
T02-07 Alter tenant ID in list request	Server retains authorized tenant scope.	PASS
T02-08 Use an expired export link	Expired link rejected.	PASS
T02-09 Revoked user requests findings	Session loses access after revocation.	PASS
T02-10 Viewer requests admin-only action	Privilege escalation denied.	PASS
T03-01 Seeded broad IAM policy	Known violation correctly flagged.	PASS
T03-02 Compliant reference configuration	Completed check reports clear.	PASS
T03-03 Seeded public-access violation	Completed check reports no finding.	FAIL F-03
T03-04 Private storage control	No public-access finding reported.	PASS

Subtotal: 12 cases, 9 pass, 3 fail, 0 pending.

07 / CASE LEDGER / 3 OF 7

Cases 25-36

Each case supplies one verdict to the executive scorecard. Finding IDs connect failed cases to the remediation register.

Case / input	Output or observation	Verdict
T03-05 Seeded conditional public policy	Known public-access violation missed.	FAIL F-03
T03-06 Seeded public ACL violation	Known public-access violation missed.	FAIL F-03
T03-07 Seeded broad trust policy	Trust-policy violation flagged.	PASS
T03-08 Seeded exposed admin port	Exposure flagged with matching resource.	PASS
T03-09 Required audit logging disabled	Disabled-logging violation flagged.	PASS
T03-10 Required encryption disabled	Encryption violation flagged.	PASS
T03-11 Restricted admin-port control	No exposure finding reported.	PASS
T03-12 Compliant encryption control	No encryption finding reported.	PASS
T04-01 IAM collection gets AccessDenied	Summary incorrectly reports clear.	FAIL F-01
T04-02 Collection interrupted mid-run	Summary incorrectly reports complete.	FAIL F-01
T04-03 Normal full collection	Successful collection reports complete.	PASS
T04-04 Retries exhausted after throttling	Failed check incorrectly reports clear.	FAIL F-01

Subtotal: 12 cases, 7 pass, 5 fail, 0 pending.

08 / CASE LEDGER / 4 OF 7

Cases 37-48

Each case supplies one verdict to the executive scorecard. Finding IDs connect failed cases to the remediation register.

Case / input	Output or observation	Verdict
T04-05 One required region times out	Multi-region summary reports complete.	FAIL F-01
T04-06 Required pagination page missing	Check correctly reports incomplete.	PASS
T04-07 Transient failure then full recovery	Recovered collection reports complete.	PASS
T04-08 Explicitly excluded service	Exclusion visible in coverage summary.	PASS
T04-09 Successful empty resource inventory	Complete empty result retains evidence.	PASS
T04-10 User cancels an active scan	Cancelled status shown explicitly.	PASS
T05-01 One approved configuration change	Correct resource and change identified.	PASS
T05-02 Unchanged configuration control	No difference reported.	PASS
T05-03 Snapshot older than agreed limit	Report clearly marks stale evidence.	PASS
T05-04 Approved resource created	Creation and correct resource recorded.	PASS
T05-05 Approved resource deleted	Deletion retained in scan comparison.	PASS
T05-06 Permission policy modified	Changed policy fields identified.	PASS

Subtotal: 12 cases, 11 pass, 1 fail, 0 pending.

09 / CASE LEDGER / 5 OF 7

Cases 49-60

Each case supplies one verdict to the executive scorecard. Finding IDs connect failed cases to the remediation register.

Case / input	Output or observation	Verdict
T05-07 Configuration reverted to baseline	Reversion recorded against prior scan.	PASS
T05-08 List order changes without state change	No false configuration drift reported.	PASS
T05-09 Change in a second approved region	Region and resource attribution retained.	PASS
T05-10 Compare snapshots out of time order	Collection times remain explicit.	PASS
T06-01 USD 1,000.00 reference total	Report USD 1,000.00; variance USD 0.00.	PASS
T06-02 USD 1,250.00 reference total	Report USD 1,250.00; variance USD 0.00.	PASS
T06-03 Credit-adjusted billing period	Credit-adjusted source data unavailable.	PENDING
T06-04 USD 0.00 reference period	Report USD 0.00; variance USD 0.00.	PASS
T06-05 USD 99.99 resource subtotal	Report USD 99.99; variance USD 0.00.	PASS
T06-06 USD 432.10 service subtotal	Report USD 432.10; variance USD 0.00.	PASS
T06-07 USD 2,000.00 account subtotal	Report USD 2,000.00; variance USD 0.00.	PASS
T06-08 USD 3,782.09 aggregate reference	Report USD 3,782.09; variance USD 0.00.	PASS

Subtotal: 12 cases, 11 pass, 0 fail, 1 pending.

10 / CASE LEDGER / 6 OF 7

Cases 61-72

Each case supplies one verdict to the executive scorecard. Finding IDs connect failed cases to the remediation register.

Case / input	Output or observation	Verdict
T06-09 Amortized commitment allocation	Allocation reference data unavailable.	PENDING
T07-01 Delete a synthetic canary record	Record absent from primary store after deletion.	PASS
T07-02 Backup retention and deletion	Backup lifecycle evidence unavailable.	PENDING
T07-03 Third-party data destinations	Subprocessor inventory awaiting review.	PENDING
T07-04 Canary removed from application cache	Canary absent after the deletion window.	PASS
T07-05 Application log redaction	Sensitive canary fields are masked.	PASS
T07-06 Disconnect approved AWS account	New collection requests cease.	PASS
T07-07 Expired saved report link	Expired report cannot be downloaded.	PASS
T07-08 Viewer accesses restricted data settings	Access limited to authorized role.	PASS
T07-09 Replica deletion propagation	Replica lifecycle evidence unavailable.	PENDING
T07-10 Third-party retention configuration	Provider retention evidence unavailable.	PENDING
T08-01 Inspect finding evidence references	Account, resource, rule and time retained.	PASS

Subtotal: 12 cases, 7 pass, 0 fail, 5 pending.

11 / CASE LEDGER / 7 OF 7

Cases 73-81

Each case supplies one verdict to the executive scorecard. Finding IDs connect failed cases to the remediation register.

Case / input	Output or observation	Verdict
T08-02 Inspect role-change event history	Actor, action and timestamp recorded.	PASS
T08-03 Export one findings report	Evidence and run references preserved.	PASS
T08-04 Reproduce scan from run metadata	Build and configuration are identifiable.	PASS
T08-05 Check finding rule version	Rule version is retained.	PASS
T08-06 Inspect a finding status change	Actor, time and new status are recorded.	PASS
T08-07 Inspect an accepted-risk entry	Reason and responsible owner retained.	PASS
T08-08 Compare baseline with retest result	Original evidence remains available.	PASS
T08-09 Export excludes another tenant	Export scope and tenant are recorded.	PASS
T08-10 Resolve a finding evidence reference	Evidence reference maps to correct run.	PASS

Subtotal: 9 cases, 9 pass, 0 fail, 0 pending.

12 / REMEDIATION AND RETEST

Close issues against measurable targets

Targets below are proposed for agreement before live testing. Owners and dates would be assigned with Quantinev.

Work item	Baseline	Proposed closure target
F-02 / Tenant access	8 / 10 cases pass	10 / 10 pass; 0 cross-tenant records returned. Repeat through every in-scope access path.
F-01 / Scan completeness	6 / 10 cases pass	10 / 10 pass; 0 clear/complete summaries on the four failed collection paths.
F-03 / Detection	5 / 8 violations found	8 / 8 seeded violations found; 0 / 4 false alarms on compliant controls. Add held-out configurations.
Billing evidence	7 / 9 cases covered	9 / 9 covered. Agree a cost basis and tolerance before comparing totals.
Data handling	6 / 10 cases covered	10 / 10 supported by observed behavior or reviewed evidence, with retention exceptions documented.
Full rerun	66 / 75 scored cases pass	81 / 81 cases have a disposition; all required cases pass; unresolved findings and accepted risks remain explicit.

What the final handoff contains

A signed-off scope, executive scorecard, findings register, case results, redacted evidence pack, and a baseline-to-retest comparison. Every metric carries its denominator, run date, build identifier, and coverage limits.

Required assessment inputs

Quantinev would provide an approved environment and build, two synthetic tenants, role and trust policies, supported check definitions, sample exports and billing references, data-handling documentation, and written test boundaries.

References and report record

AWS third-party role access guidance - test design for role and external-ID checks.

Rubrex assessment methodology - evidence labels, findings, scope, and retest structure.

RUB-ARGUS-01 | v1.3 | Prepared by Rubrex
Report date 6 November 2026 | Contact evals@rubrex.ai