

Client Review Summary



Synthetic example — fictional client and commentary

Prepared by Meridian Assurance Partners · assurance@meridian.example

Northwind Avionics

Scan of **2026-10-04** · Includes reviewer commentary

Reviewer assessment

Reviewed by: J. Mensah, Principal Consultant (illustrative sample)

Conclusion

Illustrative sample text. Nobody has assessed these findings.

The supplied inventory lists log4j-core 2.17.2 where the baseline listed 2.14.0, and CVE-2021-44228 — the only finding in this project listed in CISA's Known Exploited Vulnerabilities catalog — is no longer detected in this comparison. That is what the two inventories say; it is not confirmation that anything was deployed or verified. Four findings in total are no longer detected. Nothing in the current inventory is URGENT.

Seven findings remain across five components: commons-text at HIGH, postgresql at MED, and commons-lang3, log4j-api and log4j-core at LOW. Each is tracked below with an owner and a target date. One component, the telemetry agent, is unpinned in the manifest and was therefore not checked at all. That is a gap in the inventory rather than a clean result.

Next steps

Pin the telemetry agent so the next review can check it.

Agree a revised target date for the overdue postgresql item.

Obtain written confirmation of the proposed November migration window.

Review the three log4j-core findings still detected at 2.17.2 and decide whether they are accepted or scheduled.

Written by the named reviewer: the conclusion and next steps above, and any explanations recorded against unresolved items below. Generated from stored data: the scan facts, the comparison, and the list of items flagged for review.

Findings in this scan

Priority	Components with findings	Findings (CVEs)
URGENT	0	0
HIGH	1	1
MED	1	1
LOW	3	5
Total	5	7

Counted two ways. A **component with findings** is one package at one version that has at least one CVE against it; a **finding** is one CVE, so a single component may account for several. 0 finding(s) appear in the CISA Known Exploited Vulnerabilities catalog. 8 of 9 components were checked against the vulnerability databases; 1 could not be checked. Describes the dependency file named below, not a running system.

- 1 unpinned component(s) were not scanned for vulnerabilities. Pin to exact versions (e.g., pkg==1.2.3) to enable scanning.

Changes against baseline

Compared against baseline scan **3d678b76 · 2026-10-04 06:43:19 · northwind_baseline.cdx.json**.

No longer detected	Newly detected	Still detected
4	0	7

“No longer detected” means exactly that: the finding appeared in the baseline scan and does not appear in this one. It does not establish that the issue was fixed, that any deployed system was patched, or that a person verified it. A finding can also disappear because the component left the inventory, or because the vulnerability databases changed.

Outstanding follow-up

Current POA&M tracking state as at 2026-10-04, not a snapshot of the scan above. Tracked items are live project records and may cover findings from other scans. **7 of 7** tracked item(s) are open; **7** of those are detected in this scan. The rest are not necessarily resolved — see the column below for what this scan can and cannot tell you about each.

Recorded priority comes from the most recent scan in this project that reported the finding — it is not a reading of the scan above, and the tracked record is never reprioritised. **In this scan** says what this scan can tell you, which is a four-way question:

- **Detected** — this scan reports the finding.
- **Not detected** — the component is in this inventory, the lookup completed, and this finding was not among the results.
- **Not checked** — the component is in this inventory but was not looked up (unpinned, an unsupported ecosystem, or an incomplete vulnerability lookup). No conclusion can be drawn either way.
- **Not in inventory** — the component does not appear in this scan at all. Tracked items belong to the project and may come from other scans, so this says nothing about whether the issue was addressed.

Only **Not detected** means the scan looked and did not find it, and even then it does not establish that anything was fixed. An item stays open until a person closes it.

ID	Component	CVE	Recorded priority	In this scan	Status	Owner	Target
POAM-001	commons-text (Maven)	CVE-2022-42889	HIGH	Detected	open	A. Mensah	2026-11-30
POAM-002	postgresql (Maven)	CVE-2026-42198	MED	Detected	open	D. Okoro	2026-09-15
POAM-003	commons-lang3 (Maven)	CVE-2025-48924	LOW	Detected	open	D. Okoro	2027-01-31

Showing 3 of 7 tracked items, ordered: detected in this scan first, then items this scan cannot speak to (not checked, or not in this inventory), then items the scan looked for and did not find, then closed. The full list is in the POA&M report.

Unresolved review items

2 item(s) were flagged for review: **1** with a current explanation, **1** with no explanation, and **0** with an outdated explanation — text written when the item looked different, kept here but no longer describing it.

An explanation records why something is still outstanding. It does not resolve it, close any POA&M entry, establish compliance, or constitute approval — and an item with no explanation has not been approved either, only left unaddressed here.

Item flagged for review	Affected entries	Reviewer's explanation
1 outstanding tracked item is past its target date.	POAM-002 · postgresql (Maven) <i>Detected in this scan</i>	A migration to a newer branch is proposed for November, which would also move this component. The window is not confirmed and no acceptance has been recorded, so the item stays open and the date below needs renegotiating.
7 open tracked items are still detected in this scan.	—	<i>No explanation recorded.</i>

Provenance and scan details

Client / project	Northwind Avionics
Scan reviewed	6b05228f · 2026-10-04 06:43:22 UTC
Input file	northwind_current.cdx.json
Input SHA-256	35f0ae8147b1bbef5eed39e56f8c40a047509c303ed3dad4ebe26a207119fad6
Baseline compared	3d678b76 · 2026-10-04 06:43:19 · northwind_baseline.cdx.json
Versions	scanned with RiskSnap v0.8.0; summary generated 2026-10-04 06:43:29 UTC by v0.8.0