

Plan of Action & Milestones (POA&M)



Software Supply Chain Risk Evidence for CMMC Level 2

Synthetic example — fictional client and commentary

Prepared by Meridian Assurance Partners · assurance@meridian.example

Generated: 2026-10-04T06:43:29+00:00

Project Metadata

Project	Northwind Avionics
Project ID	northwind_avionics
POA&M items	7
Open items	7
In progress	0
Mitigated	0
Closed items	0
Items past due	1
Due within 30 days	0
Report generated	2026-10-04T06:43:29+00:00

■ Action Required
1 POA&M item is past their target completion date.

POA&M Summary

POAM ID	Status	Severity	Target Date	Days Until/Past	Component
POAM-002	open	MED	2026-09-15	19 days past due	postgresql (Maven)
POAM-001	open	HIGH	2026-11-30	57 days	commons-text (Maven)
POAM-003	open	LOW	2027-01-31	119 days	commons-lang3 (Maven)
POAM-004	open	LOW	2027-02-28	147 days	log4j-api (Maven)
POAM-005	open	LOW	2027-03-31	178 days	log4j-core (Maven)
POAM-006	open	LOW	2027-04-30	208 days	log4j-core (Maven)
POAM-007	open	LOW	2027-05-31	239 days	log4j-core (Maven)

POA&M Detail Sections

Control Reference

Applies to: RA.L2-3.11.2 (Scan for vulnerabilities), RA.L2-3.11.3 (Remediate vulnerabilities), CM.L2-3.4.1 (Establish baseline configuration)

Weakness

Component	postgresql (Maven)
CVE	CVE-2026-42198
Risk Level	MED
First Found	2026-10-04

Remediation Plan

Illustrative. Past its original date. A driver upgrade is expected to be carried by the proposed November migration, which is not yet confirmed. Until that window is agreed, treat the date as lapsed rather than extended, and re-establish it with the client.

Responsible Party

D. Okoro

Resources Required

(not specified)

Schedule

Target Date	2026-09-15
Status	OPEN
Days Remaining	19 days past due

Milestones

(no milestones defined)

Closure

(item is open)

Control Reference

Applies to: RA.L2-3.11.2 (Scan for vulnerabilities), RA.L2-3.11.3 (Remediate vulnerabilities), CM.L2-3.4.1 (Establish baseline configuration)

Weakness

Component	commons-text (Maven)
CVE	CVE-2022-42889
Risk Level	HIGH
First Found	2026-10-04

Remediation Plan

Illustrative. Highest-priority item. Identify the first release that does not report CVE-2022-42889 and confirm it against the vendor advisory before scheduling; no target version has been verified yet. Usage review pending to establish whether the affected interpolation path is reachable from this application.

Responsible Party

A. Mensah

Resources Required

(not specified)

Schedule

Target Date	2026-11-30
Status	OPEN
Days Remaining	57 days

Milestones

(no milestones defined)

Closure

(item is open)

Control Reference

Applies to: RA.L2-3.11.2 (Scan for vulnerabilities), RA.L2-3.11.3 (Remediate vulnerabilities), CM.L2-3.4.1 (Establish baseline configuration)

Weakness

Component	commons-lang3 (Maven)
CVE	CVE-2025-48924
Risk Level	LOW
First Found	2026-10-04

Remediation Plan

(not yet documented)

Responsible Party

D. Okoro

Resources Required

(not specified)

Schedule

Target Date	2027-01-31
Status	OPEN
Days Remaining	119 days

Milestones

(no milestones defined)

Closure

(item is open)

Control Reference

Applies to: RA.L2-3.11.2 (Scan for vulnerabilities), RA.L2-3.11.3 (Remediate vulnerabilities), CM.L2-3.4.1 (Establish baseline configuration)

Weakness

Component	log4j-api (Maven)
CVE	CVE-2026-49844
Risk Level	LOW
First Found	2026-10-04

Remediation Plan

(not yet documented)

Responsible Party

B. Lindqvist

Resources Required

(not specified)

Schedule

Target Date	2027-02-28
Status	OPEN
Days Remaining	147 days

Milestones

(no milestones defined)

Closure

(item is open)

Control Reference

Applies to: RA.L2-3.11.2 (Scan for vulnerabilities), RA.L2-3.11.3 (Remediate vulnerabilities), CM.L2-3.4.1 (Establish baseline configuration)

Weakness

Component	log4j-core (Maven)
CVE	CVE-2025-68161
Risk Level	LOW
First Found	2026-10-04

Remediation Plan

(not yet documented)

Responsible Party

A. Mensah

Resources Required

(not specified)

Schedule

Target Date	2027-03-31
Status	OPEN
Days Remaining	178 days

Milestones

(no milestones defined)

Closure

(item is open)

Control Reference

Applies to: RA.L2-3.11.2 (Scan for vulnerabilities), RA.L2-3.11.3 (Remediate vulnerabilities), CM.L2-3.4.1 (Establish baseline configuration)

Weakness

Component	log4j-core (Maven)
CVE	CVE-2026-34477
Risk Level	LOW
First Found	2026-10-04

Remediation Plan

(not yet documented)

Responsible Party

B. Lindqvist

Resources Required

(not specified)

Schedule

Target Date	2027-04-30
Status	OPEN
Days Remaining	208 days

Milestones

(no milestones defined)

Closure

(item is open)

Control Reference

Applies to: RA.L2-3.11.2 (Scan for vulnerabilities), RA.L2-3.11.3 (Remediate vulnerabilities), CM.L2-3.4.1 (Establish baseline configuration)

Weakness

Component	log4j-core (Maven)
CVE	CVE-2026-34480
Risk Level	LOW
First Found	2026-10-04

Remediation Plan

(not yet documented)

Responsible Party

D. Okoro

Resources Required

(not specified)

Schedule

Target Date	2027-05-31
Status	OPEN
Days Remaining	239 days

Milestones

(no milestones defined)

Closure

(item is open)

Disclaimer

This evidence pack documents software dependency vulnerability analysis suitable for supporting CMMC Level 2 controls related to vulnerability scanning (RA.L2-3.11.2), vulnerability remediation (RA.L2-3.11.3), system flaw identification (SI.L2-3.14.1), and software component inventory (CM.L2-3.4.1). This documentation contributes to the body of evidence required for these controls but does not by itself satisfy any single control. Final determination of compliance is the responsibility of the assessing organization.

RiskSnap is an automated analysis tool. Results are based on public vulnerability databases (OSV, CISA KEV). This report does not guarantee full compliance, does not cover all vulnerability types, and is not a substitute for professional security review or formal CMMC assessment. Users are responsible for final validation. Generated by Meridian Assurance Partners.

No uploads stored. Generated in-session.