



Sample deliverable

Sample: CMMC Level 2 Readiness Assessment

Sample document. All findings, scores, account identifiers, and company details are fictional demonstration data created to show report format and depth. This is not a real client engagement.

CLIENT

Northbridge Defense Systems (sample)

EMPLOYEES

240

ASSESSED

Mar 2026

SPRS SCORE

41 of 110

Executive summary

Northbridge's CUI environment spans a GovCloud (US) enclave for engineering data and a commercial AWS account for corporate IT. Of the 110 NIST SP 800-171 requirements, **58 are met**, **29 are partially met**, and **23 are not met**, producing a current SPRS score of **41**.

The dominant gaps are documentation rather than technology: the GovCloud enclave already provides FIPS-validated cryptography, audit logging, and access control, but the System Security Plan does not describe them, and no POA&M has been maintained since the 2024 self-assessment. Closing the 23 unmet requirements is estimated at 14 to 18 weeks of effort, most of it in policy, procedure, and evidence collection.

Scoping note. Reducing the CUI boundary to the GovCloud enclave plus four engineering workstations removes 26 corporate systems from assessment scope. This single decision is the largest available cost reduction and is reflected in the scoring below.

Domain scoring

DOMAIN	REQS	MET	PARTIAL	NOT MET	COVERAGE
Access Control (3.1)	22	12	6	4	
Awareness and Training (3.2)	3	1	1	1	
Audit and Accountability (3.3)	9	6	2	1	
Configuration Management (3.4)	9	4	3	2	
Identification and Authentication (3.5)	11	8	2	1	
Incident Response (3.6)	3	1	1	1	
Maintenance (3.7)	6	4	1	1	
Media Protection (3.8)	9	4	2	3	
Personnel Security (3.9)	2	2	0	0	
Physical Protection (3.10)	6	5	1	0	
Risk Assessment (3.11)	3	1	1	1	
Security Assessment (3.12)	4	1	2	1	
System and Communications (3.13)	16	6	5	5	
System and Information Integrity (3.14)	7	3	2	2	

Gap analysis excerpt

Six of 110 rows shown. The delivered analysis covers every requirement with evidence notes.

REQ	REQUIREMENT	STATUS	EVIDENCE REVIEWED	GAP
3.1.1	Limit system access to authorized users	Met	IAM Identity Center with Okta federation; quarterly access review records	None
3.1.12	Monitor and control remote access sessions	Partial	Session Manager logging enabled in GovCloud; no equivalent control on corporate VPN	Remote access to corporate systems holding CUI is not session-logged
3.3.3	Review and update logged events	Not met	CloudTrail enabled; no documented review cadence or evidence of reviews	No procedure defines who reviews audit events, how often, or what triggers escalation
3.4.2	Establish and enforce security configuration settings	Partial	AWS Config conformance pack for GovCloud; engineering workstations manually configured	Workstation baselines are undocumented and unenforced
3.6.1	Establish operational incident-handling capability	Not met	Informal escalation to the IT manager; no written plan	No incident response plan, defined roles, or tested procedure
3.13.11	Employ FIPS-validated cryptography to protect CUI	Met	AWS KMS FIPS 140-2 endpoints in GovCloud; TLS 1.2 enforced	None

POA&M excerpt

ID	WEAKNESS	REQS	OWNER	MILESTONE	TARGET
P-01	No documented audit review procedure	3.3.3, 3.3.5	Security Lead	Draft procedure, assign reviewers, run first review	30 Apr 2026
P-02	No incident response plan	3.6.1, 3.6.2, 3.6.3	Security Lead	Author plan, define roles, run tabletop exercise	31 May 2026
P-03	Workstation baselines undocumented	3.4.1, 3.4.2	IT Manager	Define baseline, deploy via MDM, capture evidence	15 Jun 2026
P-04	Remote access sessions not logged for corporate CUI access	3.1.12	Network Lead	Route CUI access through the GovCloud enclave bastion	30 Jun 2026
P-05	Media sanitization procedure absent	3.8.3	IT Manager	Author procedure, procure sanitization tooling, train staff	31 Jul 2026

Path to assessment readiness

PHASE	FOCUS	SCORE IMPACT	DURATION
Phase 1	Documentation: SSP completion, audit review, incident response, media protection procedures	41 → 72	6 weeks
Phase 2	Technical: workstation baselines, remote access rerouting, vulnerability management cadence	72 → 95	6 weeks
Phase 3	Evidence maturity: run the procedures, collect artifacts, complete internal validation	95 → 110	4 weeks

Readiness, not certification. This assessment prepares Northbridge for a C3PAO assessment; certification itself must be performed by an authorized C3PAO. Scores reflect the environment and documentation observed during the engagement

window.