EXECUTIVE SECURITY ANALYSIS REPORT CARD

A 30-day engagement that replaces assumed readiness with validated reality

Your IT team says "A-." The evidence may say "C+."

We show leadership the difference, why it exists, and what to do next.

The executive problem

Security programs are often reported through tools deployed, policies written, and projects completed. CMMC readiness is different: controls must operate consistently across the defined environment, be documented, and be supported by evidence. This focused engagement gives leadership an independent, decision-ready baseline without beginning with a long, disruptive assessment.

How the 30 days work

1 PERCEPTION	2 VALIDATION	3 SCORING	4 EXECUTIVE READOUT
Days 1–3	**Days 4–15**	**Days 16–23**	**Days 24–30**
Quick interviews capture where leadership and IT believe the company stands.	Targeted review tests controls, evidence, configurations, and operating practices.	Findings are scored by requirement and rolled into domain readiness.	Report card, SPRS output, roadmap, and leadership briefing are delivered.

What leadership receives

- Initial perception report card across all 14 CMMC Level 2 domains.
- Validated executive report card comparing claimed readiness with evidence-based results.
- Reusable work-papers workbook covering all 14 domains, 110 requirements, and their assessment objectives, with status, evidence, gaps, owners, target dates, and management notes.
- Automated domain rollups and NIST SP 800-171 / SPRS status and score output for management review and authorized submission.
- Blank SSP templates and structured starting documents.
- Prioritized remediation roadmap and executive briefing focused on decisions, accountability, sequencing, and budget implications.

What the report answers

Where are we really? Validated readiness by domain and requirement.	**Why is the score lower?** Clear gaps in implementation, consistency, scope, documentation, and evidence.	**What must happen first?** Critical-path dependencies separated from quick wins.
What will it take? Owners, sequence, effort, and budget bands.	**What can we reuse?** Scoring work-papers, automated score model, and blank SSP templates.	**What should leadership decide?** A sequenced first remediation wave with accountable sponsorship.

FAST	INDEPENDENT	ACTIONABLE
Defined 30-day engagement	Evidence over opinion	Owners, priorities, and next steps

The goal is not to "grade" IT. It is to give leadership a credible baseline before contracts, customers, or assessors expose the gap.

Readiness and management-planning engagement only. It does not guarantee certification or replace an authorized CMMC assessment.

ILLUSTRATIVE CMMC LEVEL 2 EXECUTIVE REPORT CARD

Perceived readiness compared with evidence-based validated readiness

PERCEIVED READINESS	VALIDATED READINESS	READINESS GAP	ASSESSMENT READY
87%	54%	-33 pts	0 of 14
Leadership / IT view	Evidence-based result	Perception variance	Domains fully ready

Illustrative interview-to-evidence example

Interview prompt	Leadership / IT response	Validation focus	Illustrative finding
How are privileged and service accounts reviewed?	"MFA is enabled and administrators review access."	Sample privileged accounts, service accounts, approval records, review cadence, and CUI-flow authorizations.	MFA was present, but recurring privileged-access reviews, service-account ownership, and retained approvals were incomplete.

Complete domain comparison

Domain	Perceived	Validated	Gap	Readiness	Priority	Immediate management action
Access Control	92%	54%	-38	In Progress	Critical Path	Validate CUI flows, privileged access, service accounts, and recurring access reviews.
Awareness & Training	88%	71%	-17	Nearly Ready	Quick Win	Add CUI-specific and role-based training with retained completion evidence.
Audit & Accountability	90%	31%	-59	Major Gap	Major Remediation	Centralize priority logs; define retention, alerting, time sync, and review evidence.
Security Assessment	91%	38%	-53	Major Gap	High Priority	Modernize the SSP; validate evidence and establish formal POA&M governance.
Configuration Mgmt.	86%	42%	-44	In Progress	Foundational	Create secure baselines and documented change approval, testing, and rollback.
Identification & Auth.	90%	63%	-27	Nearly Ready	High Priority	Complete MFA coverage and service-account, password, and identity lifecycle evidence.
Incident Response	88%	67%	-21	Nearly Ready	Quick Win	Run a tabletop exercise and retain escalation, response, and after-action records.
Maintenance	82%	56%	-26	In Progress	Standard	Document approved tools, remote sessions, personnel, and maintenance records.
Media Protection	84%	45%	-39	In Progress	Standard	Standardize removable-media approval, encryption, transport, and sanitization.
Personnel Security	90%	78%	-12	Nearly Ready	Quick Win	Formalize screening, transfer, termination, and access-removal evidence.
Physical Protection	92%	82%	-10	Nearly Ready	Maintain	Close visitor-log and periodic access-review evidence gaps.
Risk Assessment	80%	52%	-28	In Progress	Foundational	Formalize risk ranking, remediation SLAs, acceptance, and executive reporting.
System & Comm. Protection	76%	29%	-47	Major Gap	Critical Path	Validate boundary, segmentation, encryption, remote access, and external connections.
System & Info. Integrity	87%	49%	-38	In Progress	High Priority	Define patch and vulnerability SLAs; strengthen monitoring and evidence retention.

All figures and findings are illustrative; actual results require requirement-level evidence validation.

EXECUTIVE OBSERVATIONS

Largest gaps: logging, security assessment, configuration management, and media protection. The issue is incomplete coverage, inconsistent operation, and insufficient evidence.

DAY 30 MANAGEMENT DECISION

Approve the first remediation wave: CUI scope, access governance, secure baselines, priority logging, and SSP modernization. Assign sponsors and accountable owners.