GRAENNLAB Strategic Implementation Lab

CASE STUDY

Readiness Assessment

Policy, procedure, and control-gap assessment for federal cybersecurity readiness.

CMMC	NIST 800-171	COMPLIANCE READINESS

POSITIONING LINE

Graennlab helped translate federal cybersecurity requirements into a practical readiness view by reviewing existing documentation, assessing gaps, and preparing findings for remediation planning.

Work Type	Cybersecurity compliance support and readiness assessment
Client Need	Review existing SOPs and policies against CMMC / NIST 800-171 requirements
Graennlab Role	Third-party compliance support, gap analysis, control review, policy coordination
Core Deliverables	Gap assessment, control review support, artifact preparation, findings support

Client Challenge

The client needed a practical review of existing standard operating procedures and policies against CMMC and NIST 800-171 expectations. The engagement was scoped as a gap assessment to determine the level of effort required to move toward the required cybersecurity compliance standard.

Graennlab Approach

Graennlab supported our client through a third-party compliance readiness engagement. The team reviewed 28 SOPs or policy documents, assessed gaps against NIST 800-171, participated in control review activity, coordinated policy/procedure work, and contributed to artifact generation and findings preparation.

Work Performed

- Reviewed 28 SOPs and policy documents against NIST 800-171 expectations.
- Conducted gap analysis to identify missing or deficient compliance coverage.

- Participated in control review sessions under the client's CMMC NIST 800-171 project.
- Supported procedure work, policy coordination, policy review sessions, and artifact generation.
- Prepared findings in a spreadsheet or mutually agreed delivery format for client use.
- Coordinated project activity under the broader client delivery structure.
- Provided a client-facing compliance narrative suitable for broader Graennlab cybersecurity specialty positioning.

Outcome

The engagement produced a structured understanding of policy and procedure gaps against federal cybersecurity requirements. The work demonstrated Graennlab's capacity to combine compliance analysis, project coordination, documentation review, and evidence-oriented execution for organizations facing CMMC and NIST 800-171 alignment needs.

WHY IT MATTERS

This engagement demonstrates Graennlab's ability to move beyond advice and provide embedded execution, governance, and operational momentum inside client environments.