

SPECIMEN DELIVERABLE · EXECUTIVE SUMMARY

Information Security Program Assessment

Prepared for Northstar Fabrication Co. — a fictitious defense-industrial-base manufacturer

Assessment period: representative six-week engagement · Report date: specimen edition, August 2026

ILLUSTRATIVE SPECIMEN — READ FIRST. This document is a composite constructed by Apogee Defense to show the structure, depth, and voice of a real program-assessment executive summary. Northstar Fabrication Co. does not exist. Every finding, rating, and figure is invented for illustration; no client engagement is described or implied, and no real environment was assessed to produce it. A real report is written against your environment, your contracts, and your obligations — and is delivered to you alone.

ENGAGEMENT TYPE	Cybersecurity current-state assessment — information security program review
FRAMEWORK BASIS	NIST Cybersecurity Framework; NIST SP 800-171 Rev 2 control families where CUI is in scope
DELIVERY	Leadership readout plus this written summary; full report contains per-domain detail and evidence
FULL REPORT CONTENTS	Executive summary · High-priority recommendations · Thirteen-domain program assessment · Priority-rating and maturity-model appendices
PREPARED BY	Apogee Defense LLC · 14425 Falcon Head Blvd, Suite E100, Austin, TX 78738 · apogeedefense.com

Engagement overview and statement of work

Apogee Defense was engaged to assess the current state of Northstar Fabrication's information security program. The statement of work covered a document review, structured interviews with engineering, IT, and operations leadership, and a configuration-level review of the systems that store, process, or transmit the company's most sensitive information — including contract-controlled technical data. The engagement ran six weeks and required roughly seven hours of Northstar staff time.

The objective was not a compliance score. It was an honest answer to three questions leadership had been unable to get from inside the organization: what is actually in place, what is documented but not practiced, and what is missing entirely — with each answer supported by evidence rather than assurance.

Assessment results summary

The program shows the profile common to organizations that grew security controls organically alongside the business: capable individual practices in the areas daily operations depend on, thin formalization everywhere an auditor, assessor, or incident would look first. Of the thirteen domains assessed, none rated *Not Implemented*, five rated *Partial*, six rated *Risk-Informed*, and two rated *Repeatable*. No domain reached *Adaptive* — typical for a first formal assessment and not, by itself, a finding.

The strongest domains are those closest to production: network security and access control both benefit from disciplined, if undocumented, administration. The largest gaps are procedural: incident response exists as individual knowledge rather than a rehearsed process; logging exists without monitoring; and data classification — the decision every other control depends on — has never been formally made.

What the ratings mean for the business

Nine recommendations carry a High priority. None require major capital spending; all require ownership and calendar time. Sequenced as proposed in Section 2, the program can reach a defensible *Repeatable* posture across the domains that matter most within two quarters — a position from which a customer questionnaire, a DFARS self-assessment, or an insurance renewal stops being an emergency.

Program maturity by domain

DOMAIN	RATING	ASSESSMENT NOTE
Program management & governance	PARTIAL	No named owner; decisions made ad hoc
Data management	PARTIAL	No classification scheme; handling varies by team
Inventory management	RISK-INFORMED	Asset list exists; coverage of OT devices unverified
System configuration & hardening	PARTIAL	No baseline; images differ by installer
System testing & vulnerability management	RISK-INFORMED	Scanning runs; remediation untracked
Network security	REPEATABLE	Segmented, documented, reviewed after changes
Access control	REPEATABLE	MFA enforced; reviews informal but performed
Monitoring & detection	PARTIAL	Logs collected; nobody watches them
Application security	RISK-INFORMED	Vendor updates applied; no review of custom tooling
Vendor management	RISK-INFORMED	Contracts reviewed at signing, never after
Incident response	PARTIAL	Depends on two individuals; never exercised
Education & awareness	RISK-INFORMED	Annual training; no role-specific content
Physical security	RISK-INFORMED	Controlled entry; visitor logging inconsistent

NOT IMPLEMENTED

PARTIAL

RISK-INFORMED

REPEATABLE

ADAPTIVE

Tier definitions in Appendix C. Ratings are evidence-based: a control counts only when it can be shown operating.

Nine actions, sequenced — first five

Formalize emergency response processes

INCIDENT RESPONSE • PRIORITY HIGH • 30-DAY HORIZON

Response knowledge lives in two people. Write the plan they already carry in their heads — roles, first hour, isolation-before-wipe evidence handling, who calls the customer and the insurer — then run one tabletop against it. A plan that has never been exercised is a document, not a capability.

Formalize logging, monitoring, and alerting

MONITORING & DETECTION • PRIORITY HIGH • 30-60 DAYS

Logs are collected and nobody reads them; an intrusion today would be discovered by a customer or by luck. Define the dozen events that matter, route them to alerts with a named owner, and review the quiet weeks — a log first opened during an incident is always missing something.

Perform access reviews

ACCESS CONTROL • PRIORITY HIGH • 30 DAYS, THEN QUARTERLY

Access is well-controlled at grant and never reviewed afterward. Two departed contractors retain VPN entries today. A quarterly review — every account, every entitlement, a named certifier — converts good instincts into a control an assessor can accept.

Establish change control processes

CONFIGURATION • PRIORITY HIGH • 60 DAYS

Production changes are competent and invisible: no record of what changed, when, or why. A lightweight ticket-and-approval flow — sized to a team this small, not to an enterprise — creates the audit trail that every framework in scope asks for first.

Define system hardening processes

CONFIGURATION • PRIORITY HIGH • 60-90 DAYS

Each machine reflects its installer. Adopt one benchmark, build one golden image per platform, and record deviations with reasons. Hardening by standard replaces hardening by memory.

Remaining four

Establish audit calendar

GOVERNANCE • PRIORITY HIGH • 90 DAYS

Reviews happen when someone remembers. A single calendar — access reviews, log reviews, vendor reviews, policy refresh, tabletop — with owners and dates turns the program from episodic to periodic, which is the difference between *Risk-Informed* and *Repeatable* in nearly every domain above.

Enhance policy library

GOVERNANCE • PRIORITY HIGH • 90 DAYS

Policies exist where a customer once demanded one, and nowhere else. Close the gaps against the control set actually in scope — not a 40-document template pack; the eight policies this business needs, written to match what it really does, so practice and paper stop diverging.

Enhance data awareness

DATA MANAGEMENT • PRIORITY HIGH • 90 DAYS

Staff handle contract-controlled technical data without consistently knowing which files qualify. Short, role-specific guidance — what CUI looks like here, where it may live, how it moves — does more for real protection than a second hour of generic annual training.

Define data classification

DATA MANAGEMENT • PRIORITY HIGH • 90–120 DAYS

Every other control inherits this decision. Three tiers are enough: controlled (CUI/contract data), business confidential, and general. Mark the systems, not just the documents — the boundary decisions that follow (enclave scope, backup handling, sharing rules) all key off this one definition.

Medium- and low-priority recommendations, per-domain detail, and the evidence supporting each rating appear in the full report (Section 3), which runs to roughly forty pages for an environment of this size.

How priorities are assigned

- **High** — a gap an attacker, assessor, or obligation would find first; close before or alongside everything else.
- **Medium** — materially improves the program once High items are underway; sequence within two quarters.
- **Low** — worth doing when the calendar allows; deferring it does not change the risk picture this year.

Priorities weigh exploitability and blast radius against the obligations the business actually carries — not against a generic threat model.

Five tiers, aligned to the NIST CSF

NOT IMPLEMENTED The capability does not exist in any form. No practice, no document, no owner.	REPEATABLE The practice is documented, assigned, performed on a calendar, and produces evidence. It survives the departure of any one person.
PARTIAL Practices exist but are ad hoc and person-dependent. Outcomes vary with who performs the work; little is written down.	ADAPTIVE The practice improves itself: lessons from incidents, metrics, and change feed back into the control. Rare, and only worth pursuing where the risk justifies it.
RISK-INFORMED Management has approved the practice and risk informs decisions, but execution is not consistent organization-wide and reviews are irregular.	

A rating is earned by evidence: a control that cannot be shown operating is rated as though it does not operate. That standard is what makes the score honest — and what makes improvement measurable.

Questions about what a real assessment of your environment would cover: info@apogeedefense.com · 512-994-4441 · apogeedefense.com/current-state-assessment