PEREGRINE SOLUTIONS GROUP

CMMC Level 2 Readiness Assessment

Vantage Aerospace Components LLC (SYNTHETIC SAMPLE)

NIST SP 800-171 Rev 2 · 110 Security Requirements

Readiness Score: **76.9%**
GAPS REQUIRE REMEDIATION

Preliminary SPRS Score: **0** / 110 (Basic self-assessment methodology)

Prepared by Peregrine Solutions Group LLC · peregrinesolutionsgroup.com
Assessment date: July 03, 2026

SAMPLE — SYNTHETIC DATA

Executive Summary

This report presents the CMMC Level 2 readiness of **Vantage Aerospace Components LLC (SYNTHETIC SAMPLE)** against all 110 NIST SP 800-171 Rev 2 security requirements. The current readiness score is **76.9%** (**GAPS REQUIRE REMEDIATION**). Of 110 controls assessed, **37** require remediation, including **30** high-severity gaps that must be closed before scheduling a C3PAO assessment. Remediation is sequenced into three phases below; POA&M items must be closed within 180 days of submission to remain eligible.

The preliminary SPRS score is **0** on the −203-to-110 DoD scale. This is a Basic (self-assessment, low confidence) calculation under the DoD Assessment Methodology v1.2.1 — not a submitted SPRS score. A defensible score requires objective-level assessment against NIST SP 800-171A.

Readiness Score	76.9%
Preliminary SPRS Score (Basic)	0 / 110 (floor −203)
Controls Assessed	110
Gaps Identified	37
High-Severity Gaps	30
Phase 1 (30–60 days)	30

Control Family Breakdown

Family	Implemented	Score	Status
AC — Access Control	14/22	64%	ACTION NEEDED
AT — Awareness & Training	3/3	100%	COMPLETE
AU — Audit & Accountability	6/9	67%	ACTION NEEDED
CA — Security Assessment	3/4	75%	GAPS
CM — Configuration Management	4/9	44%	ACTION NEEDED
IA — Identification & Authentication	8/11	73%	GAPS
IR — Incident Response	1/3	33%	ACTION NEEDED
MA — Maintenance	3/6	50%	ACTION NEEDED
MP — Media Protection	7/9	78%	GAPS
PE — Physical Protection	1/6	17%	ACTION NEEDED
PS — Personnel Security	1/2	50%	ACTION NEEDED
RA — Risk Assessment	3/3	100%	COMPLETE
SC — System & Communications Protection	9/16	56%	ACTION NEEDED
SI — System & Information Integrity	5/7	71%	GAPS

SAMPLE DATA

Priority Gaps & Remediation

High-severity gaps first. Remediation guidance is control-specific and platform-aware.

Control	Sev	Remediation
3.1.7 AC	HIGH	Implement 3.1.7 (Prevent non-privileged users from executing privileged functions and capture the execution). Azure / M365: Azure RBAC denying privileged operations to non-admin roles. Azure AD audit logs capturing all role activations. Azure Monitor alerts on privilege escalation attempts. Defender for Identity detecting lateral movement. Evidence to collect: RBAC deny policies, Azure AD audit logs showing role activations,…
3.1.10 AC	HIGH	Implement 3.1.10 (Use session lock with pattern-hiding displays to prevent access and viewing of data after). Azure / M365: Microsoft Intune device compliance policy enforcing screen lock (15 minutes max). Azure AD Conditional Access session timeout (max idle: 15 min for CUI apps). Windows GPO configuring screensaver with password protection. Evidence to collect: Intune compliance policy export, GPO screensaver settings,…
3.1.13 AC	HIGH	Implement 3.1.13 (Employ cryptographic mechanisms to protect the confidentiality of remote access sessions). Azure / M365: TLS 1.2+ enforced on all Azure services. Azure VPN Gateway with IPsec/IKEv2. Azure Bastion using TLS-encrypted browser sessions. HTTPS enforcement on all web applications via App Gateway/Front Door. Evidence to collect: TLS policy configurations, VPN encryption settings, Certificate configurations. Avoid…
3.1.15 AC	HIGH	Implement 3.1.15 (Authorize remote execution of privileged commands and remote access to security-relevant i). Azure / M365: Azure PIM requiring approval for remote privileged operations. Azure Bastion with JIT VM access. Conditional Access policies requiring elevated authentication strength for admin portals. Evidence to collect: PIM approval workflow logs, JIT VM access configurations, Session Manager command logs. Avoid…
3.1.16 AC	HIGH	Implement 3.1.16 (Authorize wireless access prior to allowing such connections). Azure / M365: Azure AD certificate-based authentication for wireless (802.1X). Intune Wi-Fi profiles restricting connections to authorized networks. Conditional Access evaluating network location. Evidence to collect: 802.1X/RADIUS configuration, Wi-Fi profile policies from Intune, Wireless access point configurations. Avoid common failures:…
3.1.19 AC	HIGH	Implement 3.1.19 (Encrypt CUI on mobile devices and mobile computing platforms). Azure / M365: Intune device encryption compliance (BitLocker on Windows, FileVault on Mac). iOS/Android device encryption requirement. Azure Information Protection encrypting CUI documents at rest on any device. Evidence to collect: Intune encryption compliance policy, BitLocker/FileVault status reports, Device compliance report showing…
3.1.20 AC	HIGH	Implement 3.1.20 (Verify and control/limit connections to and use of external systems). Azure / M365: Azure AD B2B with Conditional Access for external collaboration. Cross-tenant access policies controlling which external orgs can connect. Azure Firewall application rules limiting outbound connections. Evidence to collect: Cross-tenant access policy configurations, B2B access settings, Approved external systems list. Avoid…
3.3.2 AU	HIGH	Implement 3.3.2 (Ensure that the actions of individual system users can be uniquely traced to those users s). Azure / M365: Azure AD enforcing unique user accounts (no shared accounts). Azure AD audit logs correlating actions to UPN. Sentinel entity mapping linking activities to specific users. Service principal audit trails for automated actions. Evidence to collect: Shared account prohibition policy, Azure AD user account…
3.3.5 AU	HIGH	Implement 3.3.5 (Correlate audit record review, analysis, and reporting processes to support organizational). Azure / M365: Microsoft Sentinel correlation rules linking multiple log sources. Sentinel incidents aggregating related alerts. Automated investigation playbooks (SOAR). Workbooks providing analytical dashboards. Evidence to collect: Sentinel analytics rule library, Correlation rule documentation, Investigation…
3.3.8 AU	HIGH	Implement 3.3.8 (Protect audit information and audit logging tools from unauthorized access, modification,). Azure / M365: Log Analytics workspace with RBAC restricting write/delete to security team only. Immutable blob storage for archived logs. Azure Policy preventing diagnostic setting removal. Resource locks on log storage accounts. Evidence to collect: Log storage RBAC assignments, Immutable storage configuration,…

Control	Sev	Remediation
3.4.1 CM	HIGH	Implement 3.4.1 (Establish and maintain baseline configurations and inventories of organizational systems (). Azure / M365: Azure Resource Graph for real-time infrastructure inventory. Microsoft Intune device inventory for endpoints. Azure Policy enforcing baseline configurations. Desired State Configuration (DSC) for server baselines. Azure DevOps for IaC baseline management (Terraform/Bicep). Evidence to collect: IaC…
3.4.2 CM	HIGH	Implement 3.4.2 (Establish and enforce security configuration settings for information technology products). Azure / M365: Azure Policy enforcing CIS benchmarks. Intune security baselines for Windows/macOS. Defender for Cloud secure score recommendations. Azure AD security defaults or Conditional Access baselines. Evidence to collect: CIS benchmark policy assignments, Security baseline compliance reports, Secure…

+ 25 additional gaps detailed in the accompanying Gap Report and POA&M.

Remediation Roadmap

Phase 1 (30–60 days) — 30 items
Phase 2 (60–90 days) — 4 items
Phase 3 (90–120 days) — 3 items

C3PAO Readiness Gate

[ ] All 110 controls Implemented or covered by an approved POA&M
[ ] SSP complete and current
[ ] POA&M items have owners and target dates
[ ] Evidence collected and indexed for each control
[ ] SPRS score submitted
[ ] High-severity gaps remediated

Next step: Peregrine Solutions Group will support Phase 1 remediation and, once the readiness gate is satisfied, assist in selecting and scheduling an authorized C3PAO assessor.

SAMPLE — SYNTHETIC DATA