Strike Graph

CMMC SSP Example

Large Business

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: Enterprise Systems and Networks (ESN)

1.1.1. System Categorization: FIPS 199 — Moderate for Confidentiality; Moderate for Integrity; Moderate for Availability

1.1.2. System Unique Identifier: ESN-TITAN-2025

1.2. Responsible Organization:

Name:	Titan Defense Systems
Address:	Titan Defense HQ, 4500 Defense Park Drive, Arlington, VA 22202
Phone:	000-000-0000

1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI**):**

Name:	John Miller
Title:	Contracting Officer's Representative (COR), PEO Missiles and Space, U.S. Army
Office Address:	5000 Army Pentagon, Washington, DC 20310
Work Phone:	000-000-0000
E-mail Address:	john.miller.civ@army.mil

1.2.1.1. System Owner (assignment of security responsibility)**:**

Name:	John Smith
Title:	Chief Information Security Officer (CISO)
Office Address:	Building 3, #203 Titan Defense HQ, 4500 Defense Park Drive, Arlington, VA 22202
Work Phone:	000-000-000
E-mail Address:	Jsmith02@titandef.com

1.2.1.2. System Security Officer:

Name:	Cora Williams
Title:	Enterprise ISSO, Corporate IT Security Team
Office Address:	Building 2, #355
Work Phone:	000-000-0000
E-mail Address:	cwilliams@titandef.com

1.3. General Description/Purpose of System: What is the function/purpose of the system?

Titan's Enterprise Systems and Networks support more than 500 end users across multiple facilities delivering defense programs. The environment includes on-premises Active Directory integrated with Azure AD, enterprise identity and access management, collaboration platforms, and program support applications. The corporate SOC provides 24×7 monitoring using Splunk SIEM. This system underpins day-to-day engineering, production, and supplier coordination and is operated to meet CMMC Level 2 expectations across the identified authorization boundary.

1.3.1. Number of end users and privileged users: [In the table below, provide the *approximate* number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users
End users: 500+	System admins: 25
	Database admins: 5
	Application admins: 10

1.4. **General Description of Information:** CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list.

Titan has CUI and FCI related to defense programs, including engineering designs, production schedules, supplier data, and contract documentation. Information resides in enterprise applications and repositories governed by access control, logging, and retention requirements; CUI handling and markings follow contract/CUI rules across the authorization boundary.

2. SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note**:** *this does not require depicting every workstation or desktop*, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.

SYSTEM BOUNDARIES: Titan operates multiple facilities linked via MPLS and site-to-site VPNs. Identity services use on-prem Active Directory with federation/sync to Azure AD; Conditional Access and MFA are enforced. Users connect from managed Windows workstations and hardened server hosts; remote access uses a corporate VPN with MFA and centralized logging. The corporate SOC ingests logs from AD, VPN gateways, EDR, and firewalls into Splunk SIEM for correlation and alerting. Manufacturing networks are segmented from corporate IT with tightly controlled inter-zone gateways.

SYSTEM INTERCONNECTIONS: The Enterprise Systems and Networks maintain several trusted interconnections for enterprise services. All are subject to risk review, documented agreements, and centralized monitoring. Vendor sessions are tightly controlled, require MFA, and expire automatically.

System Name	Type of Connection	Data/Services Exchanged	Security/ Encryption Method	Responsible Party
Azure AD + On-Prem AD	Federated Identity	Authentication, directory sync	Secure federation, TLS 1.2+, Conditional Access	Corporate IT
Splunk SIEM	Log Aggregation	Security events, audit logs, alerts	TLS ingestion, RBAC	SOC
ServiceNow	Ticketing/Workflow	Access requests, incident/change records	TLS 1.2+, SSO, RBAC	Corporate IT
Vendor VPN Connections	Remote Access (temporary)	Time-bound vendor maintenance sessions	IPsec/SSL VPN with MFA; ephemeral accounts	Corporate IT / Divisions

[Titan to insert a topology diagram showing facility LANs, data centers, AD/Azure AD, VPN concentrators, SOC/Splunk, and segmented manufacturing zones.]

2.1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

* **Windows Server domain controllers (multiple sites), virtualization hosts, file/application servers (Owner: Corporate IT)**
*** Cisco/Juniper routers, firewalls, and site-to-site VPN appliances (Owner: Network Engineering)**
*** Managed Windows 10/11 workstations and engineering workstations (Owner: Division IT)**

2.2. List all software components installed on the system.

* **Active Directory / Azure AD (federation and sync), Azure AD Conditional Access, MFA**
*** Splunk Enterprise/SIEM, EDR/antivirus agents, vulnerability scanner (e.g., Tenable.sc)**
*** ServiceNow (ITSM/IRM), enterprise collaboration suites, engineering/PLM tools**

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization?

Yes. Corporate IT manages core infrastructure, identity, network security, and endpoint standards. The SOC operates 24×7 monitoring, detection, and incident response. Division IT teams administer local applications under central policy. Changes to baselines and critical systems require CAB review and documented approvals.

3. REQUIREMENTS (For this example, we show a sample, not all)

(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

Family 3.1: Access Control (AC)

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

Status**: Implemented**

Access requests at Titan are initiated through ServiceNow and require dual approval from the user's manager and the IT security team. Accounts are provisioned in both Azure AD and on-prem Active Directory to maintain integration across enterprise applications. No generic or shared accounts are permitted, and privileged accounts are strictly separated from day-to-day user accounts.

Device compliance is also enforced before access is granted. All systems must be domain-joined, BitLocker encrypted, and registered in the endpoint management platform. Compliance checks are automated and logged, with non-compliant devices immediately blocked from accessing company systems.

Quarterly access reviews are conducted by division leads and summarized for the CISO. Evidence includes ServiceNow approval tickets, quarterly access attestation reports, and compliance dashboards showing device enrollment and encryption status.

3.1.8 Limit unsuccessful logon attempts.

Status: **Implemented**

Titan enforces account lockouts after five failed login attempts within 10 minutes across both Azure AD and on-prem AD. These events are forwarded to Splunk SIEM, where they

are correlated with other security events. Administrative accounts require MFA reauthentication after lockouts to ensure resilience against brute force attacks.

Family 3.3: Audit & Accountability (AU)

3.3.1 Create and retain system audit logs and records to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.

Status: **Implemented**

Titan uses Splunk SIEM to collect logs from Active Directory, VPN gateways, firewalls, and cloud applications. Logs are retained for a minimum of one year, with certain high-value systems retaining logs for up to three years.

SOC analysts review logs daily for anomalies such as privilege escalation, failed login attempts, and unusual data transfers. Automated alerts are configured for high-severity events. Monthly summary reports are provided to IT security leadership.

Evidence includes Splunk dashboards, log retention policies, and SOC monthly reporting records.

Family 3.4: Configuration Management (CM)

3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Status: **Implemented**

Baseline configurations for servers, workstations, and network devices are defined and stored in version-controlled repositories. These baselines include hardening settings aligned to CIS benchmarks and DISA STIGs. Configurations are deployed using automated tools to ensure consistency across environments.

Changes to baselines require approval by the Change Advisory Board (CAB) and are logged in ServiceNow. Deviations from baseline are detected by compliance scans and remediated as part of standard patch cycles.

Evidence includes baseline configuration documents in Git, ServiceNow CAB meeting notes, and compliance scan reports.

Family 3.5: Identification & Authentication (IA)

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Status: **Implemented**

Titan requires MFA for all accounts, both privileged and non-privileged. Azure AD Conditional Access integrates with on-prem AD federation to enforce MFA requirements enterprise-wide. MFA is mandatory for both remote and local access, including all privileged administrative accounts.

The SOC actively monitors MFA bypass attempts using Splunk queries, correlating anomalies with other login events. Regular reports are generated for IT security leadership, ensuring that compliance is consistently enforced.

Evidence includes MFA enrollment logs, Azure AD Conditional Access policies, and SOC monitoring reports highlighting MFA enforcement metrics.

Family 3.6: Incident Response (IR)

3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Status: **Implemented**

Titan operates a corporate SOC that provides continuous, 24/7 monitoring of all enterprise systems. Splunk SIEM ingests logs from Active Directory, VPN gateways, endpoint detection systems, and network firewalls. Correlation rules are used to identify incidents ranging from credential misuse to malware infections.

When an incident is confirmed, SOC analysts follow the IR playbook, escalating cases to divisional incident liaisons. Liaisons coordinate local containment actions, such as disabling user accounts or isolating affected systems, while the SOC manages

enterprise-wide response. Communication with external partners is coordinated through the CISO's office.

Evidence includes incident escalation records in Splunk, division-specific response plans, and after-action reports from prior incidents.

3.6.3 Test the organizational incident response capability.

Status: **Implemented**

Titan conducts quarterly tabletop exercises simulating scenarios such as insider threats, ransomware, and supply chain compromise. An annual red-team penetration test is also performed to validate detection and response capabilities. All divisions, contractors, and IT staff participate in these events to ensure full coverage.

After-action reports identify deficiencies and corrective action plans are documented in ServiceNow for tracking. The CISO reviews progress quarterly to ensure improvements are implemented across divisions.

Evidence includes red-team engagement reports, tabletop attendance records, and corrective action tracking logs in ServiceNow.

Family 3.8: Media Protection (MP)

3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

Status**: Implemented**

Titan follows NIST 800-88 standards for all media sanitization. Before disposal, drives are sanitized and logged by system administrators. Media requiring destruction is sent to certified vendors under contract.

Vendors provide certificates of destruction, which are uploaded to SharePoint for recordkeeping. The corporate compliance team performs annual audits of vendor processes, verifying chain-of-custody and destruction methods.

Evidence includes sanitization logs, vendor destruction certificates, and compliance audit reports.

Family 3.10: Physical Protection (PE)

3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

Status: **Implemented**

Titan facilities use electronic badge-based access for all staff. Sensitive areas, including data centers and secure labs, require dual authentication with badge and PIN. Facility Security Officers (FSOs) are responsible for managing and auditing access.

Visitor access is logged in ServiceNow, including escort assignments and duration of visit. FSOs review visitor logs monthly to ensure compliance with physical security policies.

Evidence includes badge access logs, ServiceNow visitor reports, and FSO quarterly review records.

Family 3.11: Risk Assessment (RA)

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Status: **Planned**

Titan conducts monthly vulnerability scans, quarterly tabletop exercises, and annual red-team engagements. However, the company has not yet produced a formal documented risk assessment mapping threats, vulnerabilities, likelihood, and impact. Corporate IT Security will establish a process aligned to NIST SP 800-30, complete the initial documented assessment by Q2 2025, and update it annually thereafter.

Evidence (planned): Signed risk assessment report, annual review meeting minutes, updated POA&M entries.

POA&M Reference: “Develop and publish enterprise risk assessment aligned with NIST SP 800-30. Owner: CISO. Target Completion: 30 Sept 2025.”

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Assessment Objectives:

[a] scans for vulnerabilities in organizational systems and applications periodically;
[b] scans for vulnerabilities in organizational systems and applications when new vulnerabilities are identified.

Status: **Implemented**

Titan conducts monthly enterprise-wide vulnerability scans using Tenable.sc. Coverage includes servers, workstations, network appliances, and cloud applications. The SOC triages results and assigns remediation tasks through ServiceNow.

System owners are responsible for patching and remediation, which are verified in the next scan cycle. The SOC generates trend reports showing vulnerability reduction over time, which are reviewed by the CISO.

Evidence includes Tenable scan results, ServiceNow remediation tickets, and SOC vulnerability trend reports.

Strike Graph

CMMC SSP Example

Small Business

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: Engineering Support Systems (ESS)

1.1.1. System Categorization: FIPS 199 – Moderate for Confidentiality, Low for Integrity and Availability

1.1.2. System Unique Identifier: ESS-ACME-2025

1.2. Responsible Organization:

Name:	Acme Engineering Headquarters
Address:	123 Main Street, Dayton, OH 45402
Phone:	000-000-0000

1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI)**:**

Name:	Jane Smith
Title:	Program Manager, Prime Contractor (Lockheed Martin)
Office Address:	1 Lockheed Way, Bethesda, MD 20817
Work Phone:	000-000-0000
E-mail Address:	Email: jane.smith@lmco.com

1.2.1.1. System Owner (assignment of security responsibility)**:**

Name:	Corinne Doe
Title:	Chief Financial Officer (CFO)
Office Address:	123 Main St., Dayton, OH 45402
Work Phone:	000-000-0000
E-mail Address:	cdoe@acme-eng.com

1.2.1.2. System Security Officer:

Name:	John Brown
Title:	Security Engineer, Managed Service Provider
Office Address:	200 MSP Drive, Columbus, OH 43085
Work Phone:	000-000-0000
E-mail Address:	jbrown@mspservices.com

1.3. General Description/Purpose of System: What is the function/purpose of the system?

The Engineering Support Systems support subcontracting work for prime DoD contractors. The system provides secure collaboration, file storage, and email through Microsoft 365 GCC High, with all access controlled through Intune-managed laptops encrypted with BitLocker. The system enables Acme's 15 employees to prepare proposals, share controlled specifications, and manage technical drawings.

1.3.1. Number of end users and privileged users:

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users
End Users (engineers, PMs): 15	System Administrator (MSP): 1

1.4. General Description of Information: CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list.

CUI and FCI related to defense subcontracting, including:

- Technical drawings (Defense Technical Information CUI)
- Contract deliverables (Procurement and Acquisition CUI)
- Controlled specifications (Defense CUI)

2. SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system

boundaries, system interconnections, and key devices. (Note**:** *this does not require depicting every workstation or desktop*, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.

System Boundaries: Acme Engineering operates from a single office in Dayton, OH. All staff use Intune-managed Windows 11 Enterprise laptops encrypted with BitLocker. Collaboration and storage are provided via Microsoft 365 GCC High (Exchange, SharePoint/OneDrive, Teams). Remote access requires VPN with MFA. The MSP provides administration, patching, monitoring, and a managed SOC for incident detection. The authorization boundary includes the laptops, VPN, and GCC High tenant.

System Interconnections:

System Name	Type of Connection	Data/Services Exchanged	Security / Encryption Method	Responsible Party
Microsoft 365 GCC High	Cloud SaaS	Email, file storage, collaboration (CUI/FCI)	TLS 1.2+, Azure AD Conditional Access, MFA	MSP / CFO
MSP Remote Management Platform	Secure Remote	Device inventory, patching, endpoint telemetry	TLS 1.2+, agent mutual auth, RBAC	MSP
Corporate VPN Gateway	Remote Access	Encrypted user sessions to GCC High and SaaS	IPsec/SSL VPN with MFA, split tunneling disabled	MSP
FedEx Shipping Portal	Third-party Logistics	Shipment tracking for secure laptop transport	TLS 1.2+, account-based access	CFO

2.1 Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

* User endpoints: 15 × HP ProBook laptops, Windows 11 Enterprise, Intune-managed,

BitLocker enabled
* Network infrastructure: Cisco ASA VPN gateway (managed by MSP), small business-class switches and Wi-Fi access points (WPA2-Enterprise/WPA3 configured)

2.2 List all software components installed on the system.

* Productivity and collaboration: Microsoft 365 GCC High (Exchange Online, SharePoint/OneDrive, Teams, Azure AD)
* Endpoint and device management: Microsoft Intune (MDM/MAM), Microsoft Defender for Endpoint, MSP remote management and patching agent
* Remote access: Corporate VPN client with Microsoft Authenticator MFA

2.3 Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization?

Hardware and software are maintained jointly by Acme's Managed Service Provider (MSP) and the Acme CFO, who serves as the system owner. The MSP is responsible for day-to-day administration, including patching, antivirus/EDR updates, Intune policy enforcement, VPN configuration, and endpoint monitoring. The MSP also manages warranty service and vendor support escalations. The CFO maintains ownership of the devices, software licenses, and cloud service subscriptions, reviews MSP activity reports, and approves configuration changes. This shared arrangement ensures technical maintenance is handled by specialists while compliance accountability remains with Acme.

3. REQUIREMENTS (THIS EXAMPLE PROVIDES ONLY A SAMPLE)

(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

Family 3.1: Access Control (AC)

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

Status: **Implemented**

All user accounts are provisioned in Microsoft 365 GCC High by Acme's managed service provider (MSP). Account requests must be submitted by department managers, and the MSP confirms the request with HR before creating the account. Each user is assigned a unique user ID, and accounts are added only to security groups required for their job role. No shared accounts are permitted.

Acme enforces device-level controls to further restrict access. Only company-issued laptops enrolled in Intune and encrypted with BitLocker are permitted to connect to Microsoft 365 services. Device compliance is verified automatically at login; non-compliant devices are denied access until corrected. This ensures that all systems accessing CUI are hardened and under company control.

Evidence maintained includes MSP provisioning tickets, HR approval emails, Intune compliance reports, and quarterly access review forms signed by the CFO. The CFO and MSP jointly conduct these reviews, comparing active user accounts against the HR roster and ensuring terminated users are promptly deprovisioned.

Family 3.3: Audit & Accountability (AU)

3.3.1 Create and retain system audit logs and records to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.

Status: **Implemented**

Microsoft 365 and Intune generate audit logs of user and administrator activity, including logon attempts, privilege changes, and policy updates. These logs are configured for retention in GCC High for one year. The MSP has read-only access to monitor logs for anomalies.

The MSP's SOC reviews audit logs daily, flagging anomalies such as repeated failed login attempts or unusual privilege escalations. Monthly reports are delivered to the CFO summarizing log review findings and any anomalies investigated.

Evidence includes Microsoft 365 audit exports, retention policy settings, and MSP monthly log review reports.

Family 3.4: Configuration Management (CM)

3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Status: **Implemented**

The MSP maintains standard baseline images for laptops, which include hardened security settings and required software. These baselines are enforced through Intune compliance profiles. All new devices are provisioned using these baseline images.

Changes to baseline configurations require review and approval through the MSP's change control process. Baselines are updated quarterly or when Microsoft issues critical security guidance. Deviations from baseline are logged and remediated during regular patching.

Evidence includes Intune compliance profiles, MSP baseline documentation, and change control tickets.

Family 3.5: Identification & Authentication (IA)

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Status: **Implemented**

Acme requires all employees, including privileged users, to enroll in Microsoft Authenticator for MFA. MFA is enforced for all network access, both on-site and remote,

and for local privileged account access. This ensures that both user and admin accounts have strong protections against unauthorized access.

Conditional Access policies prevent login from unmanaged or non-compliant devices and enforce re-prompting of MFA every twelve hours. The MSP monitors MFA enrollment and login events using Azure AD audit logs, verifying that all staff remain enrolled and no bypass attempts occur.

Evidence includes Azure AD Conditional Access policy exports, MFA enrollment records, and MSP monthly compliance reports provided to the CFO.

Family 3.6: Incident Response (IR)

3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Status: Implemented

Acme contracts with its MSP to provide incident detection and response through a managed SOC. The SOC monitors alerts from Microsoft 365, Intune, and endpoint protection platforms around the clock. Correlation rules are applied to identify suspicious activity, including unusual login behavior, malware detections, or policy violations.

When an incident is confirmed, the MSP escalates it to Acme's CFO within one hour. The CFO is responsible for coordinating containment measures with the MSP, communicating with affected employees, and notifying prime contractors as required. For example, when a phishing campaign targeted staff in early 2025, the MSP disabled compromised accounts and the CFO issued company-wide guidance.

Evidence includes the MSP's incident response policy, incident ticket records stored in the MSP portal, and escalation emails showing CFO involvement. The CFO maintains a compliance binder with incident summaries and corrective actions.

3.6.3 Test the organizational incident response capability.

Status: **Implemented**

Acme conducts annual tabletop exercises with its MSP to validate incident response readiness. Scenarios include phishing campaigns, malware infections, and lost laptops. Participants include the CFO, department managers, and MSP security analysts.

The exercises simulate end-to-end response, from detection and escalation to communication and recovery. Lessons learned are documented in after-action reports, and corrective actions are tracked to closure by the CFO. Training materials are updated annually to reflect these lessons.

Evidence includes tabletop agendas, attendance logs, after-action reports, and records of completed corrective actions.

Family 3.8: Media Protection (MP)

3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

Status: **Implemented**

All company laptops are securely wiped using BitLocker before they are retired. The MSP verifies that encryption keys are destroyed before devices are released. After sanitization, laptops are shipped to a certified destruction vendor using a bonded courier.

The vendor physically destroys drives and provides a certificate of destruction for each batch. These certificates are reviewed by the CFO and retained in Acme's compliance records. The MSP maintains logs confirming the wipe was performed before shipment.

Evidence includes MSP sanitization logs, vendor destruction certificates, and FedEx shipment tracking records.

Family 3.10: Physical Protection (PE)

3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

Status**: Implemented**

Acme's office uses electronic badge access to restrict entry. Access cards are issued only to employees with a need for physical access. Visitors must sign in on a paper log and be escorted at all times. Server equipment is located in a locked closet, with access limited to the CFO and MSP staff.

Badge access logs are reviewed quarterly by the CFO to ensure only active employees have access. The server closet key is controlled directly by the CFO and must be checked out for any MSP maintenance activity.

Evidence includes badge system reports, visitor logs, and server closet key control records.

Family 3.11: Risk Assessment (RA)

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Status: **Implemented**

The MSP performs quarterly vulnerability scans using Nessus. Scans include all company laptops, the Microsoft 365 tenant, and the VPN infrastructure. Findings are categorized by severity and remediation tickets are created in the MSP's tracking system.

The CFO reviews scan reports during quarterly IT review meetings with the MSP. Critical vulnerabilities are remediated immediately, while medium and low issues are tracked to resolution in subsequent patch cycles.

Evidence includes Nessus scan reports, remediation tickets, and CFO meeting minutes.

Family 3.13: System and Communications Protection (SC)

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Status: **Planned**

Implementation Description:
Acme Engineering currently relies on BitLocker (FIPS-validated) for endpoint encryption and Microsoft 365 GCC High (FIPS-validated) for storage and communications. However, the corporate VPN gateway and certain MSP remote management tools have not yet been verified against the NIST FIPS 140-2 validated module list. The MSP is scheduling a review in Q3 2025 to confirm FIPS validation status for all cryptographic modules. If any modules are not validated, they will be upgraded or replaced.

Evidence (planned):
Vendor FIPS validation certificates, VPN firmware upgrade records, MSP validation report.

POA&M Reference:
“Verify FIPS validation status for all encryption modules; upgrade or replace as required. Owner: CFO/MSP. Target Completion: 30 September 2025.”