ACME Manufacturing

CMMC Level 2 Rapid Mock Assessment

Cohort 1 and Cohort 2

December 1, 2025

GaMEP
Georgia Manufacturing Extension Partnership

Table of Contents

SECTION I – ASSESSMENT INFORMATION

1. Dates of Assessment....3
2. Purpose....3
3. Assessment Scope and Boundaries....3
4. Assessment Participants....3
5. Company Background....4
6. Preliminary SPRS Score....4
7. Executive Summary of Findings....4

APPENDIX A - CMMC Control Assessment Scoring Spreadsheet....6

APPENDIX B - CMMC Rapid Assessment Scoring Spreadsheet....8

APPENDIX C – Findings....9

SECTION I – ASSESSMENT INFORMATION

1. Dates of Assessment

November 17, 2025

2. Purpose

The purpose of this assessment is to:

1. Evaluate [redacted]'s progress towards CMMC Level 2 compliance
2. Identify and document gaps
3. Calculate a moderate confidence SPRS score
4. Recommend a roadmap leading to compliance

3. Assessment Scope and Boundaries

The scope of this assessment is [redacted].

4. Assessment Participants

[redacted]	President of Operations, [redacted]
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
[redacted]	Assessor
Camilo Castrillon	Lead Assessor

[redacted] Overseer

5. Company Background

ACME Manufacturing is a machine shop in Georgia servicing the DoD under contracts concerning both FCI and CUI.

6. Preliminary SPRS Score

A scoring sheet (Appendix B) was used to determine compliance with the applicable 5 CMMC Level 2 controls and 1 CMMC Level 1 control listed in Appendix A, based on the 24 relevant control objectives. Each of the 6 controls is scored with either 5 or 1 point. A control with all its associated objectives scored as MET receives all the points related to that control.

7. Executive Summary of Findings

A total of six controls were assessed during the interview with the representative from AMCE. The scoring and findings assessed in Appendices B and C provide more detailed information regarding specific qualifications that are required to meet each control. Based on our assessment, ACME is compliant with the scope of our assessment (outside of the assessment they are known to already be CMMC Level 2 Compliant). The scoring in Appendix B, along with the findings in Appendix C, details gaps identified during the assessment.

Findings

The assessment confirmed that ACME Manufacturing has effectively implemented the NIST SP 800-171 controls that the interview was based on. The controls spanned areas such as training, access management, authentication, physical security, and continuous security oversight. The company has all employees undergo multiple levels of training, including role-based risk awareness, MSP-updated cybersecurity lessons, and simulated phishing attacks. ACME also deploys strong access restriction measures through services like GCC High and Azure, which allows the company to enforce time-bound elevated privileges, monthly identity reviews of employees in their database, and formalized change-control policies. Employees' company identities, devices, and processes are also protected by authentication controls. These controls include Multifactor Authentication, on-site device encryption using Bit-Locker, strict off-site device restrictions (only two encrypted, MFA-protected devices are allowed to be used by the owners offsite), and prohibited use of unmanaged device policy.

On top of deploying these resources to meet the controls, ACME also ensures that continuous monitoring is conducted through a 24/7 Security Operations Center (SOC), that is reinforced through quarterly vulnerability and compliance reviews with the MSP. The companies documented procedures governing control assessments, monitoring, privilege escalation, and employee training demonstrate a mature, repeatable security governance program that maintains ACME's compliance posture.

SECTION II – APPENDICES

APPENDIX A - CMMC Control Assessment Scoring Spreadsheet

CMMC Level 1 Controls (1 total) are highlighted in blue.

CMMC Level 2 Controls includes 5 specific controls listed below.

At a minimum, an OSC cannot be assessed unless all five (5) point controls are scored as MET. All 5-point controls are highlighted in **gray blue**

NIST 800-171 Control Number	Control Family	Control Text	Compliance Status	SPRS Base Score	Calculated SPRS Score
3.2.1	Awareness and Training	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	**YES**	5	5
3.4.5	Configuration Management	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	**YES**	5	5
3.5.2	Identification and Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	**YES**	5	5
3.10.6	Physical Protection	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	**YES**	1	1

NIST 800-171 Control Number	Control Family	Control Text	Compliance Status	SPRS Base Score	Calculated SPRS Score
3.12.1	Security Assessment	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	**YES**	5	5
3.12.3	Security Assessment	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	**YES**	5	5

APPENDIX B - CMMC Rapid Assessment Scoring Spreadsheet

CMMC Level 2 Controls include all 110 controls listed below.

Awareness and Training		***Yes***	***No***
AT.L2-3.2.1 Role-Based Risk Awareness			
	Security awareness and training policy; procedures addressing security awareness training implementation; relevant codes of federal regulations; security awareness training curriculum; security awareness training materials; training records; other relevant documents or records		
71	Security risks associated with organizational activities involving CUI are identified.	☒	☐
72	Policies, standards, and procedures related to the security of the system are identified.	☒	☐
73	Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.	☒	☐
74	Managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.	☒	☐
Configuration Management		***Yes***	***No***
CM.L2-3.4.5 Access Restrictions for Change			
	Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; logical access approvals; physical access approvals; access credentials; change control records; system audit logs and records; other relevant documents or records		
122	Physical access restrictions associated with changes to the system are defined	☒	☐
123	Physical access restrictions associated with changes to the system are documented	☒	☐
124	Physical access restrictions associated with changes to the system are approved.	☒	☐
125	Physical access restrictions associated with changes to the system are enforced.	☒	☐
126	Logical access restrictions associated with changes to the system are defined.	☒	☐
127	Logical access restrictions associated with changes to the system are documented.	☒	☐
128	Logical access restrictions associated with changes to the system are approved.	☒	☐
129	Logical access restrictions associated with changes to the system are enforced.	☒	☐
Identification and Authentication		***Yes***	***No***
IA.L2-3.5.2 Authentication			
	Identification and authentication policy; procedures addressing authenticator management; procedures addressing user identification and authentication; system design documentation; list of system authenticator types; system configuration settings and associated documentation; change control records associated with managing system authenticators; system audit logs and records; other relevant documents or records		

156	The identity of each user is authenticated or verified as a prerequisite to system access.	☒	☐
157	The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.	☒	☐
158	The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.	☒	☐
Personnel Protection		***Yes***	***No***
PE.L2-3.10.6 Alternative Work Sites			
	Physical and environmental protection policy; procedures addressing alternate work sites for personnel; list of safeguards required for alternate work sites; assessments of safeguards at alternate work sites.		
234	Safeguarding measures for CUI are defined for alternate work sites.	☒	☐
235	Safeguarding measures for CUI are enforced for alternate work sites.	☒	☐
System Assessment		***Yes***	***No***
CA.L2-3.12.1 Security Control Assessment			
	Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan.		
245	The frequency of security control assessments is defined.	☒	☐
246	Security controls are assessed with the defined frequency to determine if the controls are effective in their application	☒	☐
CA.L2-3.12.3 Security Control Monitoring			
	Security planning policy; organizational procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; records of system security plan reviews and updates.		
250	Determine if security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.	☒	☐

APPENDIX C – Findings

Specific Findings

AT.L2-3.2.1 Role-Based Risk Awareness
Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

Assessment Results: MET

Information Provided by Assessor:

- Employees of this organization are required to take an onboarding cybersecurity assessment using the Know4 online application
- The employer integrates pre-generated cybersecurity training assessments into the training modules
- Internal users must complete DoD mandatory training within the DoD CUI registry training
- Training is updated to reflect emerging threats and is reviewed quarterly via a Managed Service Provider (MSP)

Findings:
This company has implemented sufficient employee training modules, policies, and procedures to inform its employees of the risks associated with their roles. Additionally, the training modules are properly updated through an MSP, which provides the company with up-to-date emerging threats and strategies to integrate these threats into the training modules to increase awareness. Finally, the company also deploys phishing tests via email as a method of training and increasing awareness. and trains its employees on the applicability of their roles.

CM.L2-3.4.5 Access Restrictions for Change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

Assessment Results: MET

Information Provided by Assessor:

- This organization uses Privileged Identity Management within GCC High and Azure.
- The organization has a feature to request temporary elevated access if someone needs to patch something or approve something to install. This temporary access would stop automatically within 2 hours, and only certain people would have access.

- In Azure Identity Management, the organization has a list of identities that are all in the system that they go through monthly to see which ones they still need.
- The organization has formalized policies and documents with all of the above privilege and access related material.

Findings:
This company has clearly implemented and enforced both logical and procedural access restrictions for system changes. Their use of Privileged Identity Management in GCC High and Azure ensures that only authorized personnel can elevate access, and even then, only for a limited, pre-approved timeframe (automatic expiration after 2 hours). This directly supports controlled, auditable changes to systems. The requirement is further satisfied by the company's monthly review of identities within Azure Identity Management to validate which accounts remain necessary, ensuring that only appropriate users retain access to change-related roles. In addition, the existence of formalized policies and documented procedures for privilege management, access approvals, and change control demonstrates that their processes are not only practiced but formally established and maintained.

IA.L2-3.5.2 Authentication

Authenticate the identities of users, processes, or devices before allowing them access to organizational systems.

Assessment Result: MET

Information Provided by Assessor:
- Users and devices are authenticated every time they log in through Azure, GCC High, Intune MDM, and AWS IAM.
- All users have unique accounts and work only on secured, BitLocker encrypted PC workstations.
- Only two (owners') managed mobile devices are allowed, both controlled through Intune MDM with MFA and remote wipe.
- No unmanaged or take home devices are permitted, and all access requires identity verification.
- Privileged access is controlled through Azure Privileged Identity Management with JIT access and monthly reviews.

Findings:
The organization successfully meets the authentication requirements by enforcing user, device, and process identity verification prior to system access. All users have unique accounts; MFA is applied where applicable, and each login triggers identity checks on the backend. Failed login attempts are monitored, and lockout rules are in place.

Device authentication is strongly controlled. Only authorized devices are permitted, with no company devices allowed off site. PC workstations are encrypted with BitLocker and meet FIPS 140 2 standards. The only permitted mobile devices are managed through Intune MDM, include MFA, and can be remotely wiped if needed.

The company also verifies identities associated with processes and privileged actions. Azure Privileged Identity Management, AWS IAM, and GCC High provide structured identity governance, including temporary elevation, backend verification, and monthly identity reviews. These controls ensure that all users, devices, and processes are authenticated before accessing systems.

3.10.6 - Alternative Work Sites
Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Assessment Result: MET

Information Provided by Assessor:

- No devices are allowed outside the facilities, and workers are not allowed to work from home.
- Only two mobile devices that contain CUI information leave the building: the owners' phones.
    - MFA.
    - Device encryption.
    - Remote deletion procedures are in place even if phones are stolen.
- Workstation devices are protected with BitLocker and encryption.
    - Devices are locked behind keycard doors and require a valid, unique username to access.
- The company has CMMC facility inspections twice a year and contracts an additional service for threat analysis on workstation devices.

Findings:
The company has no alternative worksites and does not allow employees to work outside the facility. By default, this makes reaching PE.L2-3.10.6 more straightforward. The company has a series of controls to ensure the devices are never taken outside the facility, such as security doors and reception staff, to ensure that no devices are even taken outside the building.

The only two devices that leave the building that contain CUI information are mobile phones, which belong to the owners. These phones have MFA, encryption, and a remote-deletion procedure in case the phone is ever stolen. These controls are sufficient safeguards to protect CUI information. Although there was no mention of defined worksite procedures, they are not applicable, as the devices are at the owners' discretion only.

For additional security, mobile phone users could be assigned additional cybersecurity training. However, the defined controls are sufficient to meet compliance approval for PE.L2-3.10.6.

3.12.1 – Security Control Assessment
Organizations must regularly assess the security controls in place to ensure they remain effective and aligned with policy and regulatory changes.

Assessment Result: MET

Information Provided by Assessor:
During the assessment discussion, this company demonstrated a defined and documented process for the periodic assessment of implemented security controls.

- A Security Operations Center (SOC) that tracks security performance and control behavior over time.
- Quarterly review meetings with MPS, during which dashboards of vulnerabilities, system issues, and relevant NIST updates are reviewed.
- Meeting records showing documented logs and recordings, demonstrating consistent oversight and traceability.
- A decision-making process that evaluates how updated requirements or risks align with existing practices.

Findings:
This company has demonstrated both automated continuous monitoring through its Security Operations Center (SOC) and structured quarterly vulnerability reviews with MPS. In addition to these activities, the organization maintains a documented and standardized procedure that outlines how periodic assessments are conducted, which controls are evaluated, how assessment results are escalated, and how these results integrate into broader risk-management decisions. These processes show that the company performs regular oversight of its implemented controls and ensures that updates, vulnerabilities, and regulatory changes are evaluated in a consistent manner.

3.12.3 Security Control Monitoring:
Organizations must continuously monitor security controls to determine ongoing effectiveness, identify new vulnerabilities, and support risk-based decisions.

Assessment Result: MET

Information Provided by Assessor:

- The Security Operations Center (SOC) provides 24/7 real-time monitoring across systems and security controls.
- Quarterly meetings with MPS are held to review a dashboard of current vulnerabilities, alerts, and any updates issued by NIST.
- Decision-making includes evaluating how new or changed requirements align with existing practices.
- Meetings and review sessions are logged and recorded, providing an audit trail.

Findings:
This company has performed both automated continuous monitoring (via the SOC) and quarterly vulnerability reviews with MPS. The organization has a documented, standardized procedure describing how continuous monitoring is performed, which controls are monitored, how monitoring results are escalated, and how these results integrate with risk management.

Disclaimer Statement

The content and information contained in this Cybersecurity Assessment is provided as is and based on reasonable research efforts. Georgia Institute of Technology ("Georgia Tech") makes no representations or warranties of any kind, express or implied, regarding, but not limited to, the accuracy, completeness, timeliness, utility, suitability, reliability or availability with respect to such content, information or services provided in connection therewith. Your use of or reliance on this Cybersecurity Assessment or the content or information contained herein or services provided in connection therewith are strictly at your own risk.

Georgia Tech shall not be liable under any circumstances, directly or indirectly, for any damage or loss of any kind, regardless of whether they have been advised of the possibility of such loss or damages, including but not limited to, direct, indirect, special, incidental or consequential loss or damage, arising from, caused or alleged to be caused by or in connection with any use of or reliance on this Cybersecurity Assessment or the content or information contained herein or services provided in connection therewith.

ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESSED, IMPLIED OR STATUTORY, REGARDING THIS CYBERSECURITY ASSESSMENT AND THE CONTENT OR INFORMAITON CONTAINED HEREIN OR SERVICES PROVIDED IN CONNECTION THEREWITH ARE EXPRESSLY DISCLAIMED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF PERFORMANCE, MERCHANTIABILITY, FITNESS FOR A PARTICULAR USE OR PURPOSE, NONINFRINGEMENT OR WARRANTY THAT THE ASSESSMENT, CONTENT, INFORMATION OR SERVICES PROVIDED ARE ERROR FREE.

For avoidance of doubt, Georgia Tech includes its Enterprise Innovation Institute ("EI^2") and Georgia Manufacturing Extension Partnership ("GaMEP") as well as The Board of Regents of the University System of Georgia ("BOR") and our respective affiliated organizations and individual members, officers, trustees, directors, employees, agents and representatives.