ILLINOIS TECH

Illinois Tech CMMC Audit

April 16th 2025

Ankita Varma

ITMS 578-02

Agenda

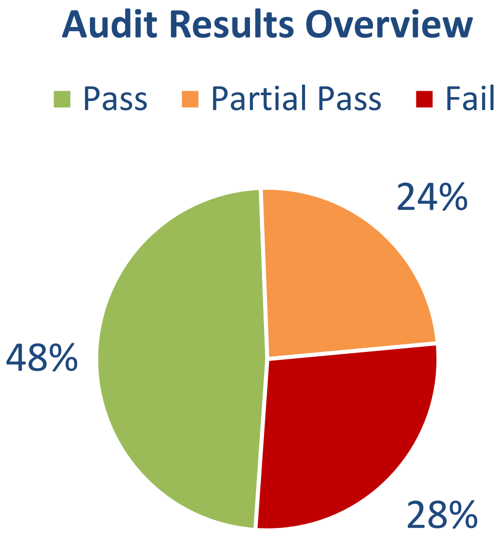
- Executive Summary
- Audit Scope
- Findings of Fact
- Recommendations

Executive Summary

- Illinois Tech commissioned a cybersecurity audit to assess compliance and identify gaps in order to achieve Cybersecurity Maturity Model Certification (CMMC)
- The scope of audit covered these documents:

IIT policy documents	Applicable CMMC domains
Authentication Policy	Access control, Identification and Authentication
Incident Response Policy	Incident Response
Risk Management Policy	Risk Assessment
Vulnerability Management Policy	Risk Assessment

- Compliance status:
  - 48% successfully met requirements (pass)
  - 24% partially met requirements (partial pass)
  - 28% did not meet requirements (fail)
- Lack of definition or availability of the definition were the most common cause of gaps
- Recommendations are made to make these definitions available or define them where they do not already exist



Audit Scope

Documents selected for auditing:

- Authentication Policy
- Incident Response Policy
- Risk Management Policy
- Vulnerability Management Policy

Above documents were applicable to the following CMMC domains:

- Access control
- Identification and Authentication
- Incident Response
- Risk Assessment

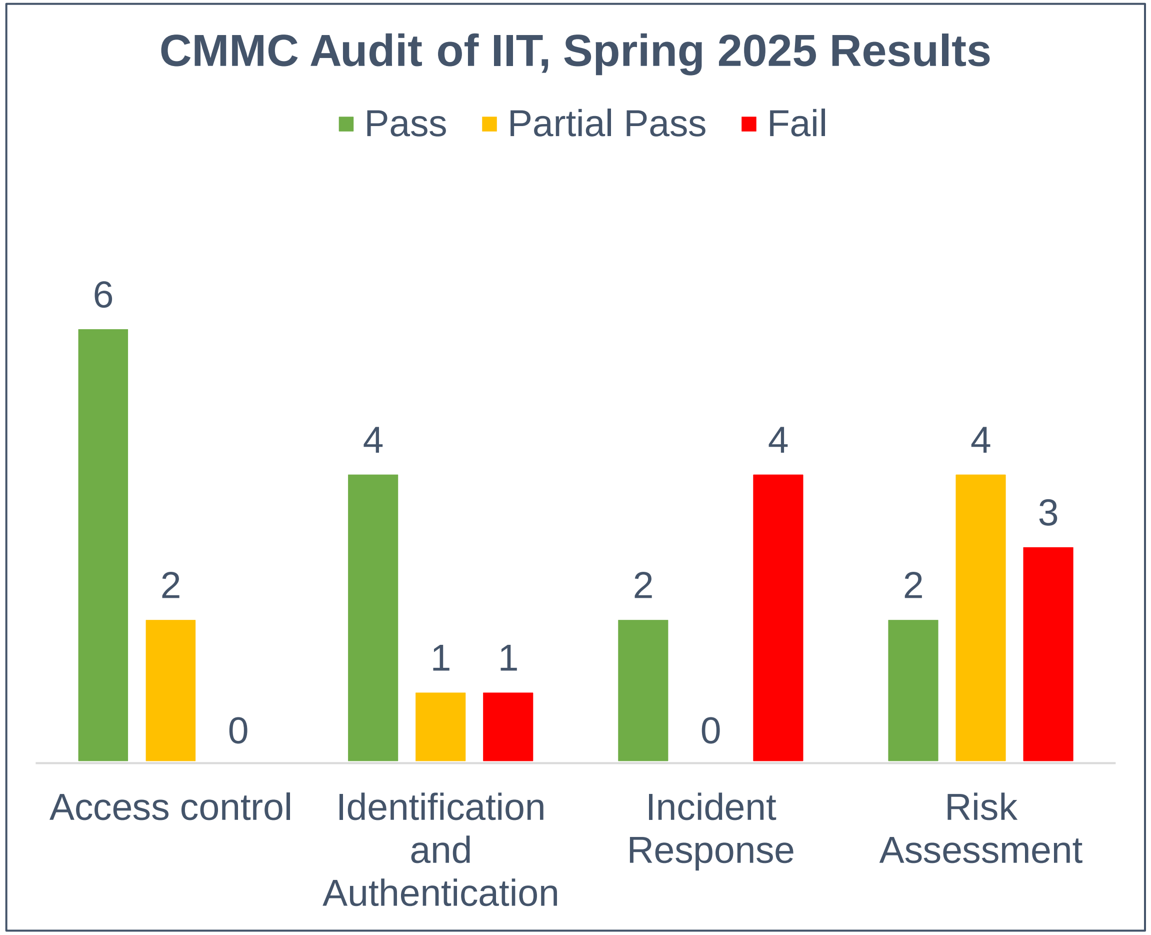
Findings of Fact Summary

Compliance status by domain:

- Access control: 6 out of 8 requirements met
- Identification and Authentication: 4 out of 6 requirements met
- Incident Response: 2 out of 6 requirements met
- Risk Assessment: 2 out of 9 requirements met

Gap analysis:

- Seven requirements are partially met and can be easily brought to complaint status
- Eight requirements were not met at all

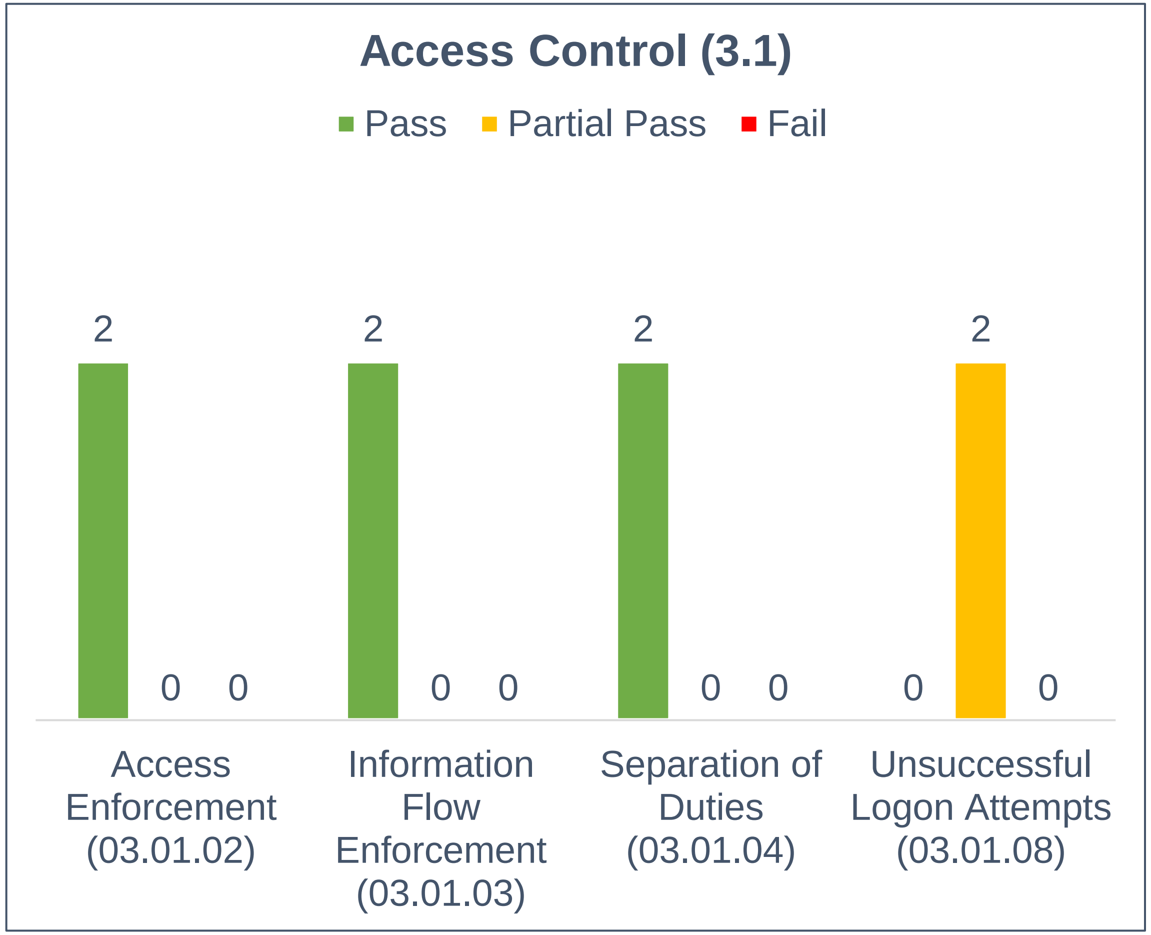


Access Control (3.1)

Applicable document: Authentication Policy

This domain checked for 4 categories:

- Access Enforcement – CMMC Lvl 1
  - 2 out of 2 requirements met
- Information Flow Enforcement – CMMC Lvl 2
  - 2 out of 2 requirements met
- Separation of Duties – CMMC Lvl 2
  - 2 out of 2 requirements met
- Unsuccessful Logon Attempts – CMMC Lvl 2
  - 0 out of 2 requirements met
  - Number of invalid login attempts, lock out time and other parameters were not defined

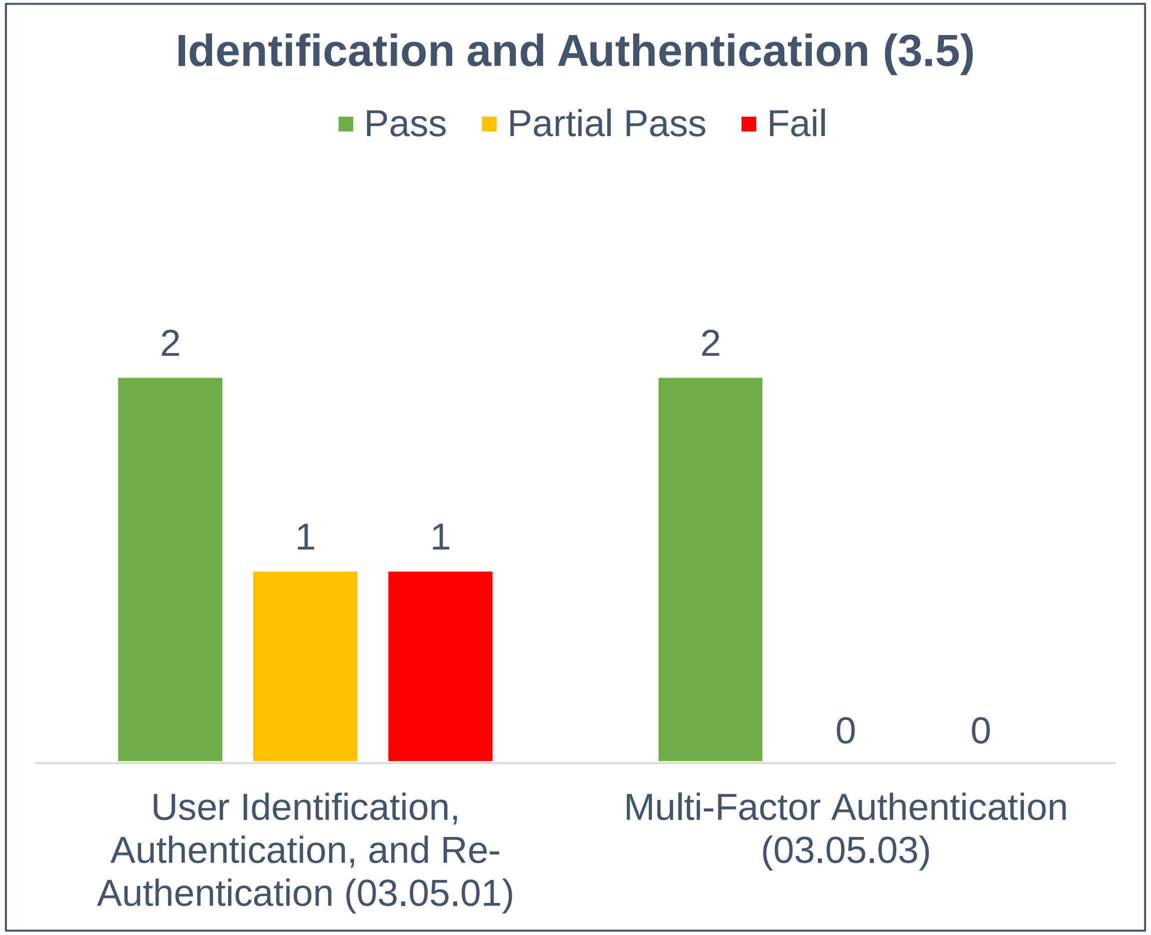


Identification and Authentication (3.5)

Applicable document: Authentication Policy

This domain checked for 2 categories:

- User Identification, Authentication, and Re-Authentication – CMMC Lvl 1
  - 2 out of 4 requirements met
  - Processes were not linked to uniquely identified and authenticated users
  - Definition of re-authentication circumstances is not provided
- Multi-Factor Authentication – CMMC Lvl 2
  - 2 out of 2 requirements met

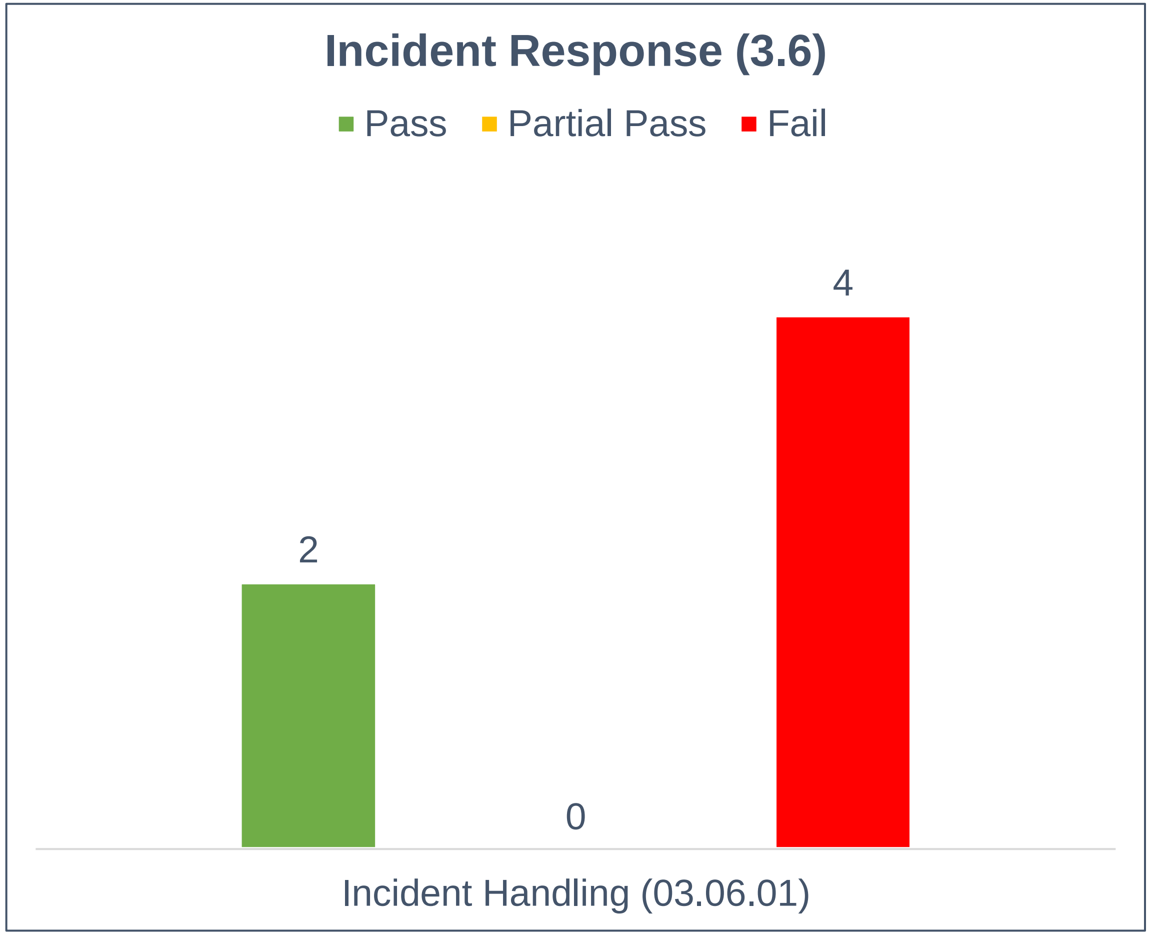


Incident Response (3.6)

Applicable document: Incident Response Policy

This domain checked for 1 category:

- Incident Handling – CMMC Lvl 2
  - 2 out of 6 requirements met
  - Incident-handling capability, including preparation, containment, and recovery, are not defined
  - Incident response plan is not available

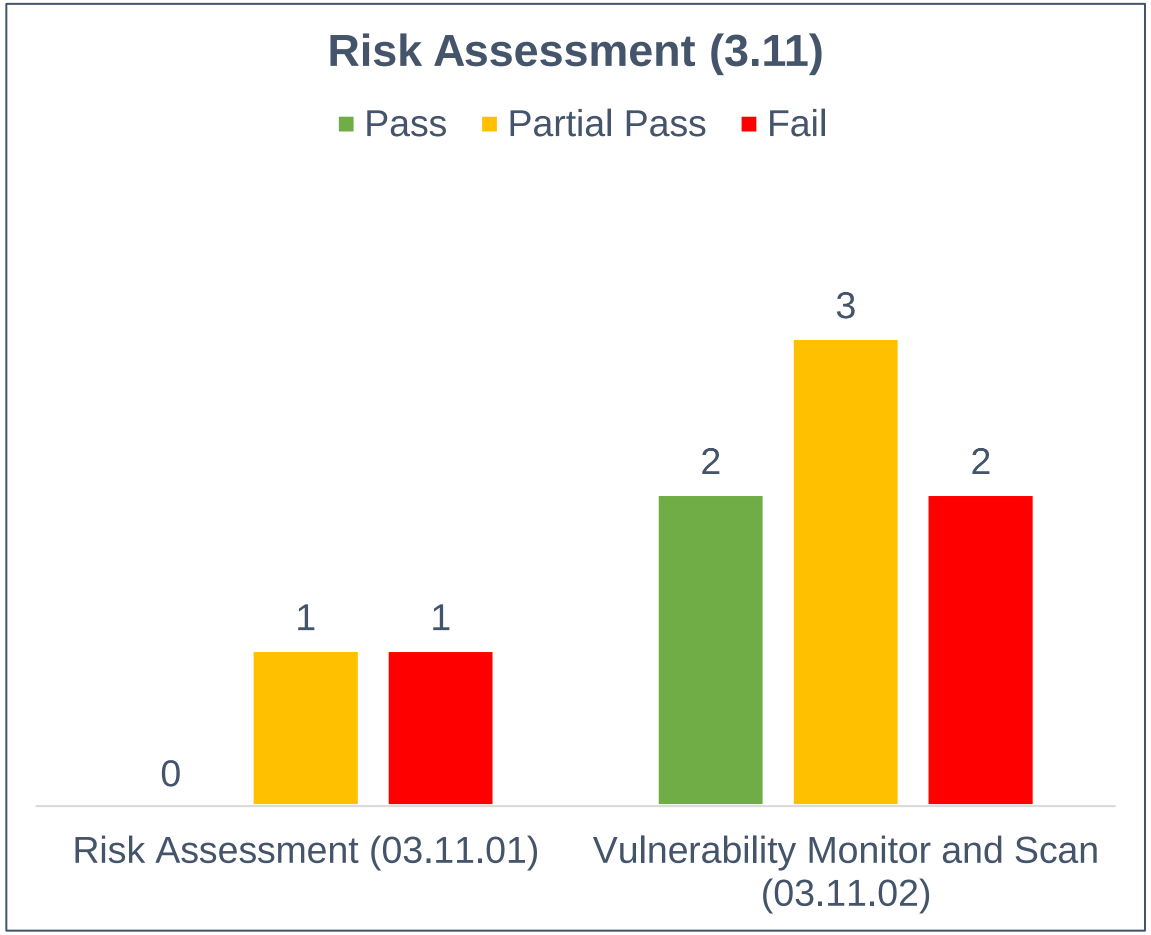


Risk Assessment (3.11)

Applicable documents: Risk Management Policy, Vulnerability Management Policy

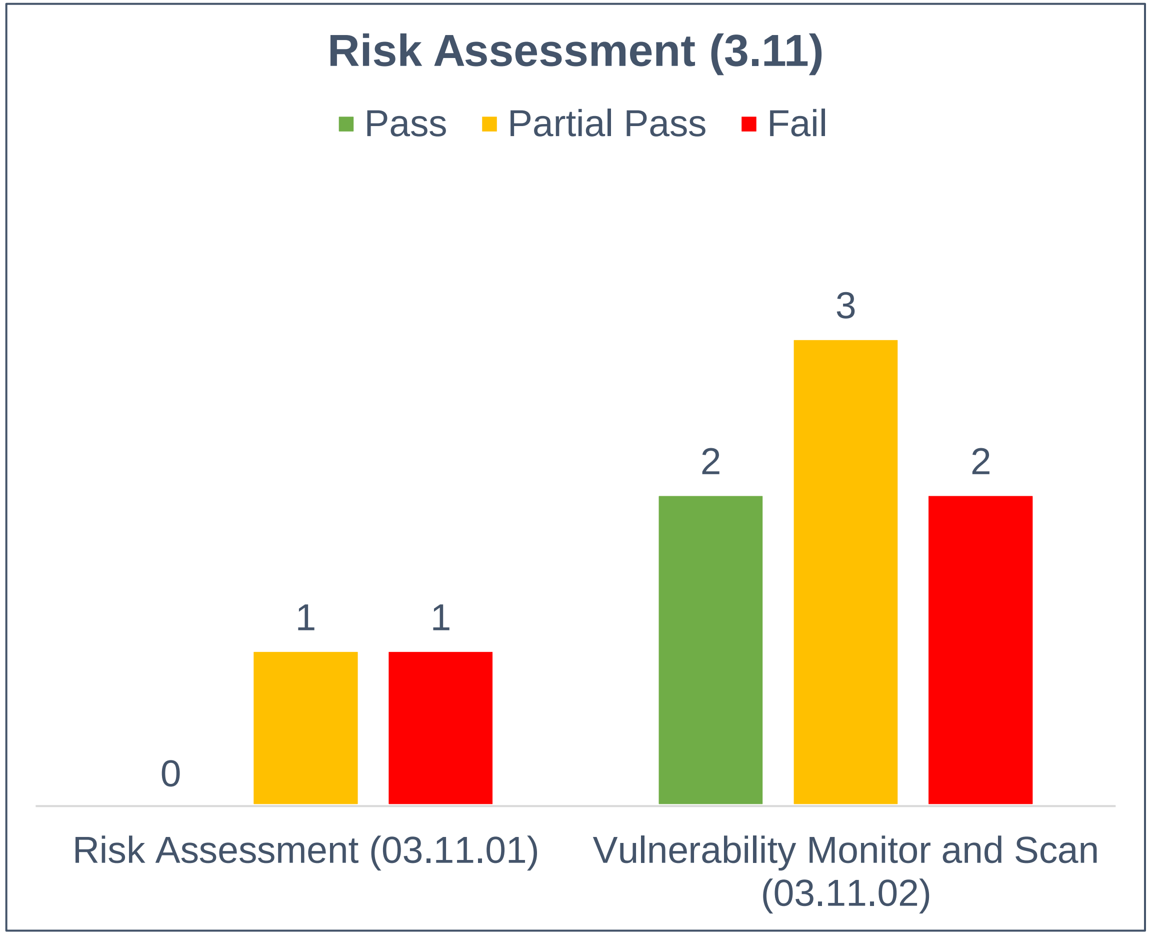
This domain checked for 2 categories:

- Risk Assessment – CMMC Lvl 2
  - 0 out of 2 requirements met
  - Risk assessment of unauthorized disclosure is not defined
  - Risk assessment does not define update frequency



Risk Assessment (3.11)

- Vulnerability Monitor and Scan – CMMC Lvl 2
  - 2 out of 7 requirements met
  - Frequency of scanning and monitoring of vulnerabilities is not defined
  - Response time of remediating vulnerabilities is not defined
  - System vulnerabilities to be scanned are not updated regularly or when new vulnerabilities are identified



Recommendations

Recommend to prioritize addressing gaps related to CMMC level 1.

Access Control Assessment (3.1)	Identification and Authentication Assessment (3.5)	Incident Response Assessment (3.6)	Risk Assessment (3.11)
Define number of invalid login attempts, lock out time and other parameters (03.01.08.a and 03.01.08.b)	Processes should be linked to uniquely identified and authenticated system users (03.05.01.a[03])	Make an Incident Response Plan available (03.06.01[01])	Define risk assessment of unauthorized disclosure is not defined and risk assessment update frequency (03.11.01.a, 03.11.01.b)
	Define circumstances requiring re-authentication (03.05.01.b)	Define Incident-handling capability, including implementation consistent with the incident response plan, preparation, containment, and recovery (03.06.01[02], 03.06.01[04], 03.06.01[06])	Define a clear frequency for scanning and monitoring vulnerabilities, establish specific response times for remediation, and implement a regular update process for scanning system vulnerabilities, including newly identified ones (03.11.02.a[01], 03.11.02.a[02], 03.11.02.b, 03.11.02.c[01], 03.11.02.c[02])