ILLINOIS TECH

Illinois Tech

Illinois Institute of Technology CMMC Audit

ITMS 578-02

Ankita Varma

4-16-2025

Contents

Executive Summary....3
Purpose....3
Scope....3
Key Findings & Recommendations....4
Methodology....5
CMMC Compliance Status....6
Findings of Fact....7
Access Control....8
Identification and Authentication....10
Incident Response....12
Risk Assessment....14
Recommendations....16
Appendices....19
Appendix A....19
Appendix B....19
Appendix C....19
Appendix D....20

Figures

Figure 1 CMMC audit result overview 4
Figure 2 CMMC Model Levels Overview (Source: CMMC Model Overview, Sept 2024) 6
Figure 3 CMMC audit result summary 7
Figure 4 Access Control compliance overview 8
Figure 5 Identification and Authentication compliance overview 10
Figure 6 Incident Response compliance overview 12
Figure 7 Risk Assessment compliance overview 14

Tables

Table 1 IIT Policy mapping to CMMC domains 3
Table 2 Recommendations per domain 18

Executive Summary

Purpose

Illinois Tech (IIT) is seeking to qualify for contracts and grants from the U.S. Department of Defense (DoD) by developing a strong cybersecurity infrastructure and obtaining the Cybersecurity Maturity Model Certification (CMMC) based on the NIST Special Publication 800-171 compliance. Therefore, the institute has commissioned a cybersecurity audit to assess their level of compliance and identify gaps.

Scope

This audit covered the documents and mapping to the applicable CMMC domains as per Table 1 below.

Table 1 IIT Policy mapping to CMMC domains

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

The CMMC offers multiple levels of certification encompassing varying sets of requirements from NIST SP 800-171. We converted the relevant CMMC domain requirements to NIST SP 800-171 requirements and performed an audit using NIST SP 800-171A. This will enable IIT to prioritize and address the gaps needed for CMMC compliance at each level.

Key Findings & Recommendations

The audit found that these IIT policies are not fully complaint with NIST SP 800-171 standards and therefore will not be eligible for any level of CMMC. The audit found that 48% of requirements were being met with the current policies (pass), 24% fell short of compliance (partial pass) and 28% were not addressed at all (fail), illustrated by Figure 1.

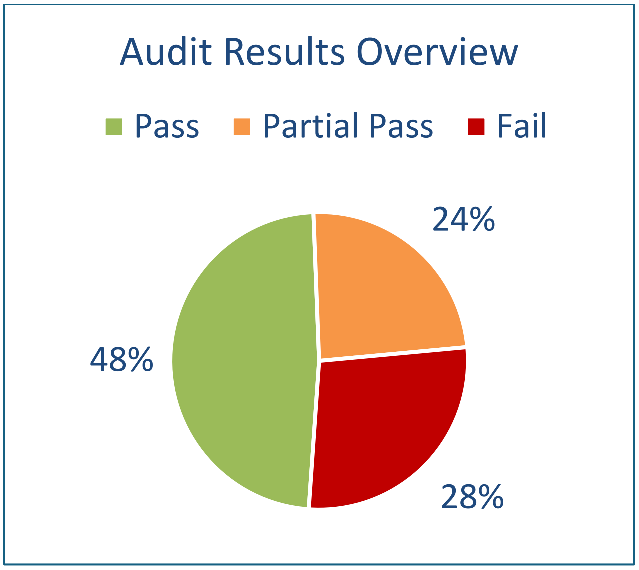


Figure 1 CMMC audit result overview

We identified three major categories causing gaps:

1. Lack of key parameter definitions
2. Policies did not meet the required standards
3. Policy documents were unavailable

We recommend prioritizing the resolution of gaps in CMMC Level 1 requirements.

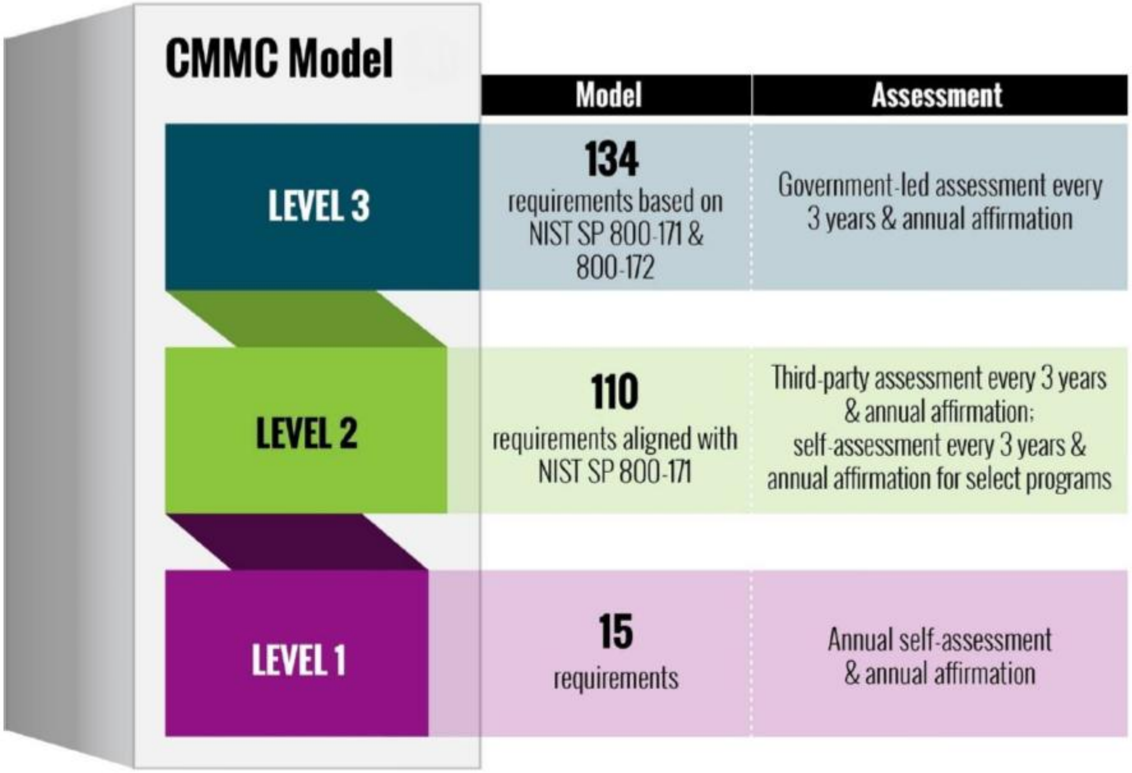
Methodology

Each policy document has been mapped to a NIST SP 800-171 procedure. We used the following strategy to complete the compliance audit:

1. Understand key requirements of CMMC
    a. Reference Cybersecurity Maturity Model Certification (CMMC) Model Overview to determine requirements for Level 1-3 CMMC
2. Determine audit scope, read relevant IIT policy documents, and map to applicable CMMC domains
    a. Authentication Policy
        i. Mapped to (1) Access Control and (2) Identification and Authentication
    b. Incident Response Policy
        i. Mapped to Incident Response
    c. Risk Management Policy
        i. Mapped to Risk Assessment
    d. Vulnerability Management Policy
        i. Mapped to Risk Assessment
3. Convert relevant CMMC domain requirements to NIST SP 800-171 requirements
    a. Access control - NIST SP 800-171 § 3.1
    b. Identification and Authentication - NIST SP 800-171 § 3.5
    c. Incident Response - NIST SP 800-171 § 3.6
    d. Risk Assessment - NIST SP 800-171 § 3.11
4. Perform audit using NIST SP 800-171A and analysis based on selected domain requirements
    a. Findings of Fact and perform gap analysis
    b. Create recommendations and next steps

CMMC Compliance Status

The CMMC Model has cumulative requirements across its levels, as seen in Figure 2. This assessment only assessed 2 out of 15 requirements for CMMC Level 1. The audit scope and lack of documents both contributed to the limited assessment of level 1 compliance. We recommend to increase the audit scope and make documents available for a full assessment of CMMC Level 1 compliance. Similarly, Level 2 was assessed for 7 out of 110 requirements. We recommend the same for a more complete Level 2 compliance assessment.



CMMC Model

CMMC Model	Model	Assessment
LEVEL 3	134 requirements based on NIST SP 800-171 & 800-172	Government-led assessment every 3 years & annual affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171	Third-party assessment every 3 years & annual affirmation; self-assessment every 3 years & annual affirmation for select programs
LEVEL 1	15 requirements	Annual self-assessment & annual affirmation

Figure 2 CMMC Model Levels Overview (Source: CMMC Model Overview, Sept 2024)

Findings of Fact

The compliance status, by domain, for in-scope requirements in Access Control was 6 out of 8 requirements were met; in Identification and Authentication, 4 out of 6 requirements were met; in Incident Response, 2 out of 6 requirements were met; and in Risk Assessment, 2 out of 9 requirements were met. In the gap analysis, it was determined that seven requirements are partially met and can be easily brought to compliance status, while eight requirements did not meet the necessary standards. The following section will deep dive into each domain's compliance status.

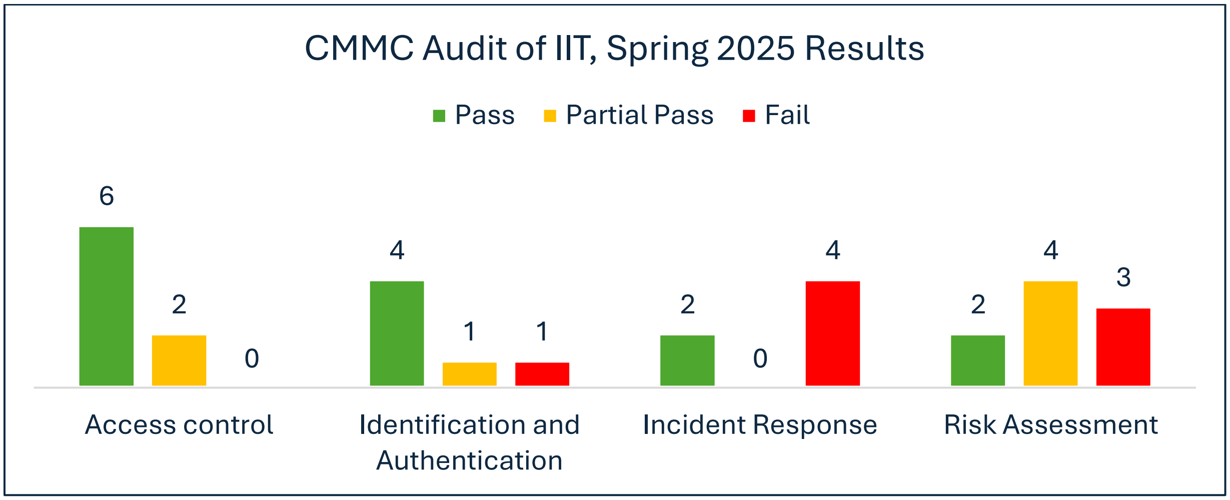


Figure 3 CMMC audit result summary

Access Control

Access control domain requirements are on track to being complaint for CMMC with 6 out of 8 requirements met, illustrated by Figure 4. The first requirement is for CMMC Level 1 while the rest are for CMMC Level 2. The policy document used for this analysis was Authentication Policy. The non-complaint category was:

- Unsuccessful Logon Attempts (03.01.08) – CMMC Lvl 2
    - Number of invalid login attempts, lock out time and other parameters were not defined (partial pass)

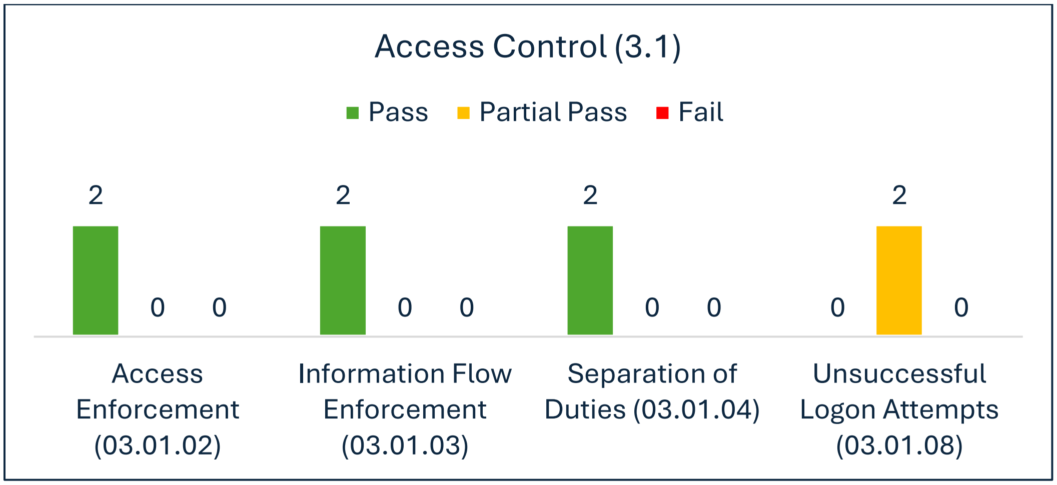
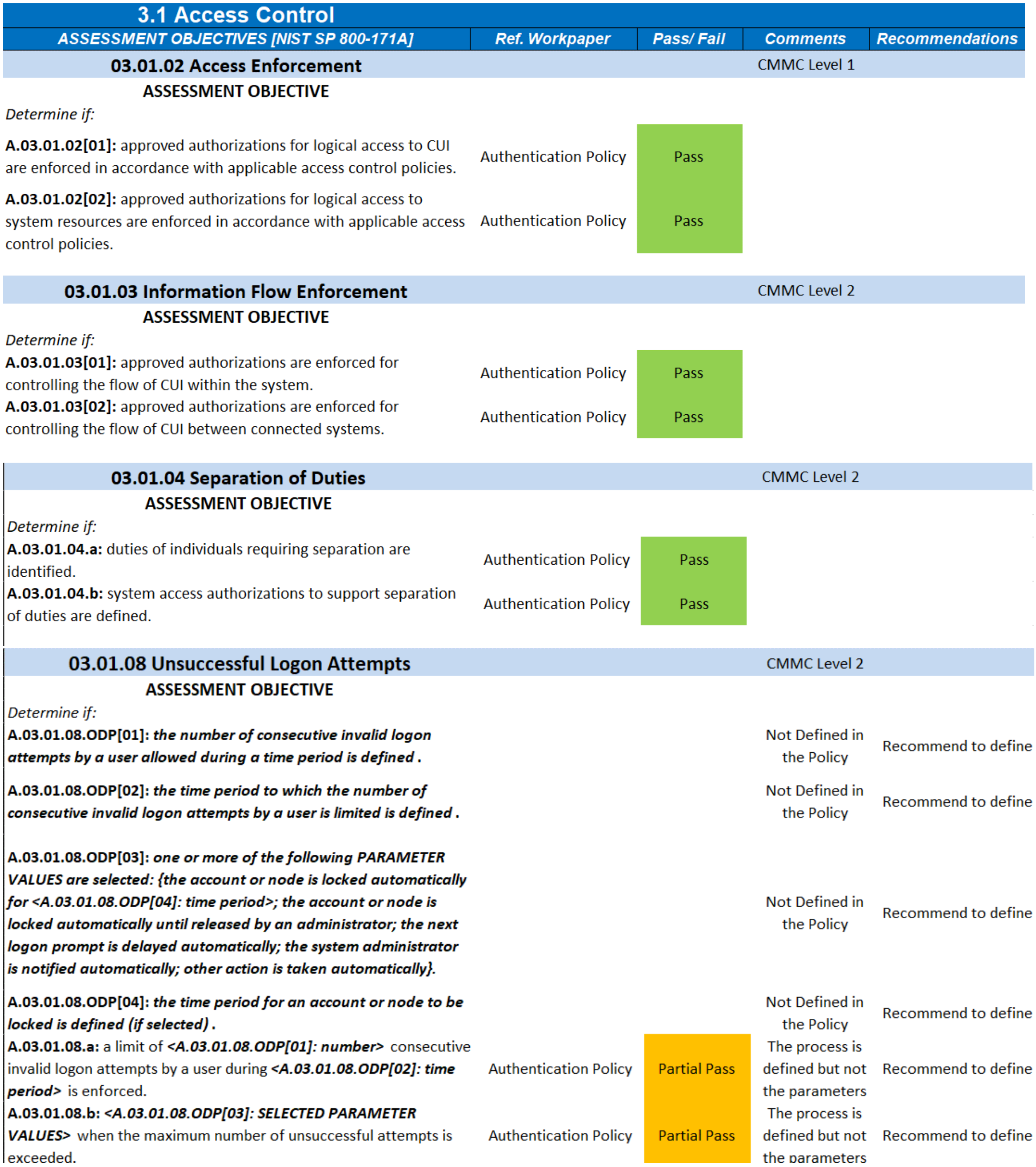


Figure 4 Access Control compliance overview

Detailed audit results:



3.1 Access Control				
ASSESSMENT OBJECTIVES [NIST SP 800-171A]	***Ref. Workpaper***	***Pass/ Fail***	***Comments***	***Recommendations***
03.01.02 Access Enforcement			CMMC Level 1	
ASSESSMENT OBJECTIVE				
Determine if:				
A.03.01.02[01]: approved authorizations for logical access to CUI are enforced in accordance with applicable access control policies.	Authentication Policy	Pass		
A.03.01.02[02]: approved authorizations for logical access to system resources are enforced in accordance with applicable access control policies.	Authentication Policy	Pass		
03.01.03 Information Flow Enforcement			CMMC Level 2	
ASSESSMENT OBJECTIVE				
Determine if:				
A.03.01.03[01]: approved authorizations are enforced for controlling the flow of CUI within the system.	Authentication Policy	Pass		
A.03.01.03[02]: approved authorizations are enforced for controlling the flow of CUI between connected systems.	Authentication Policy	Pass		
03.01.04 Separation of Duties			CMMC Level 2	
ASSESSMENT OBJECTIVE				
Determine if:				
A.03.01.04.a: duties of individuals requiring separation are identified.	Authentication Policy	Pass		
A.03.01.04.b: system access authorizations to support separation of duties are defined.	Authentication Policy	Pass		
03.01.08 Unsuccessful Logon Attempts			CMMC Level 2	
ASSESSMENT OBJECTIVE				
Determine if:				
A.03.01.08.ODP[01]: ***the number of consecutive invalid logon attempts by a user allowed during a time period is defined .***			Not Defined in the Policy	Recommend to define
A.03.01.08.ODP[02]: ***the time period to which the number of consecutive invalid logon attempts by a user is limited is defined .***			Not Defined in the Policy	Recommend to define
A.03.01.08.ODP[03]: ***one or more of the following PARAMETER VALUES are selected: {the account or node is locked automatically for <A.03.01.08.ODP[04]: time period>; the account or node is locked automatically until released by an administrator; the next logon prompt is delayed automatically; the system administrator is notified automatically; other action is taken automatically}.***			Not Defined in the Policy	Recommend to define
A.03.01.08.ODP[04]: ***the time period for an account or node to be locked is defined (if selected) .***			Not Defined in the Policy	Recommend to define
A.03.01.08.a: a limit of ***<A.03.01.08.ODP[01]: number>*** consecutive invalid logon attempts by a user during ***<A.03.01.08.ODP[02]: time period>*** is enforced.	Authentication Policy	Partial Pass	The process is defined but not the parameters	Recommend to define
A.03.01.08.b: ***<A.03.01.08.ODP[03]: SELECTED PARAMETER VALUES>*** when the maximum number of unsuccessful attempts is exceeded.	Authentication Policy	Partial Pass	The process is defined but not the parameters	Recommend to define

Identification and Authentication

Identification and authentication domain met 4 out of 6 requirements, illustrated by Figure 5. The first requirement is for CMMC Level 1, while the second requirement is for CMMC Level 2. The policy document used for this analysis was Authentication Policy. The non-compliant category was:

- User Identification, Authentication, and Re-Authentication (03.05.01) – CMMC Lvl 1
    - Processes were not linked to uniquely identified and authenticated users (fail)
    - Definition of circumstances requiring re-authentication is not provided (partial pass)

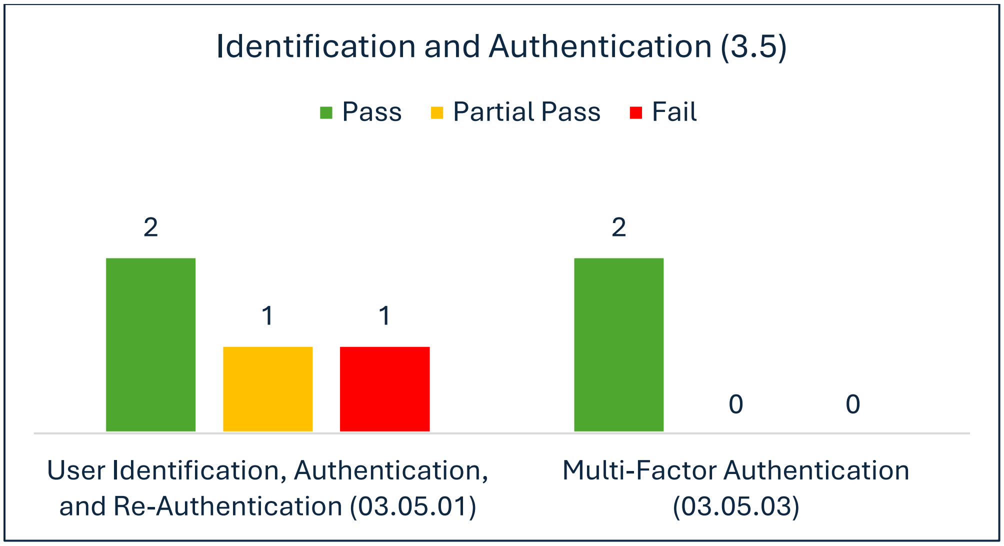
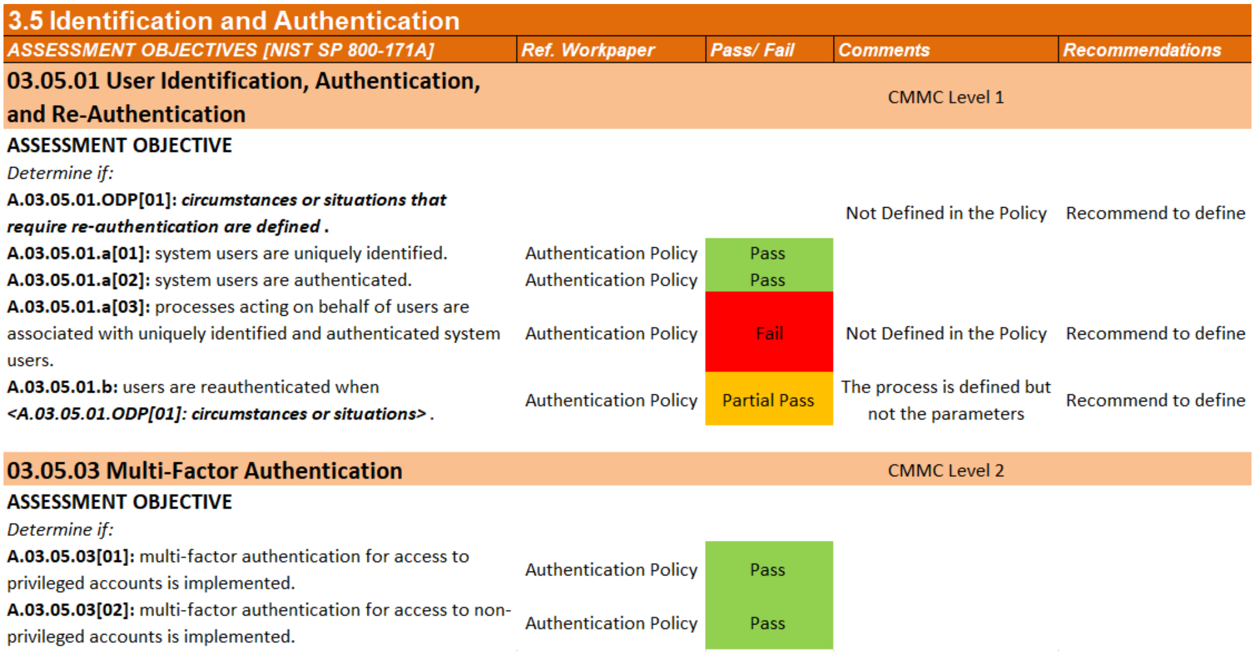


Figure 5 Identification and Authentication compliance overview

Detailed audit results:



3.5 Identification and Authentication

ASSESSMENT OBJECTIVES [NIST SP 800-171A]	*Ref. Workpaper*	*Pass/ Fail*	*Comments*	*Recommendations*
03.05.01 User Identification, Authentication, and Re-Authentication			CMMC Level 1	
ASSESSMENT OBJECTIVE				
Determine if:				
A.03.05.01.ODP[01]: ***circumstances or situations that require re-authentication are defined .***			Not Defined in the Policy	Recommend to define
A.03.05.01.a[01]: system users are uniquely identified.	Authentication Policy	🟩 Pass		
A.03.05.01.a[02]: system users are authenticated.	Authentication Policy	🟩 Pass		
A.03.05.01.a[03]: processes acting on behalf of users are associated with uniquely identified and authenticated system users.	Authentication Policy	🟥 Fail	Not Defined in the Policy	Recommend to define
A.03.05.01.b: users are reauthenticated when ***<A.03.05.01.ODP[01]: circumstances or situations>*** .	Authentication Policy	🟨 Partial Pass	The process is defined but not the parameters	Recommend to define
03.05.03 Multi-Factor Authentication			CMMC Level 2	
ASSESSMENT OBJECTIVE				
Determine if:				
A.03.05.03[01]: multi-factor authentication for access to privileged accounts is implemented.	Authentication Policy	🟩 Pass		
A.03.05.03[02]: multi-factor authentication for access to non-privileged accounts is implemented.	Authentication Policy	🟩 Pass		

Incident Response

Incident Handling domain met 2 out of 6 requirements, illustrated by Figure 6. This domain is only for CMMC Level 2. The policy document used for this analysis was Incident Response Policy. The non-compliant category was:

- Incident Handling (03.06.01) – CMMC Lvl 2
  - Incident-handling capability, including preparation, containment, and recovery, are not defined (fail)
  - Incident response plan is not available (fail)

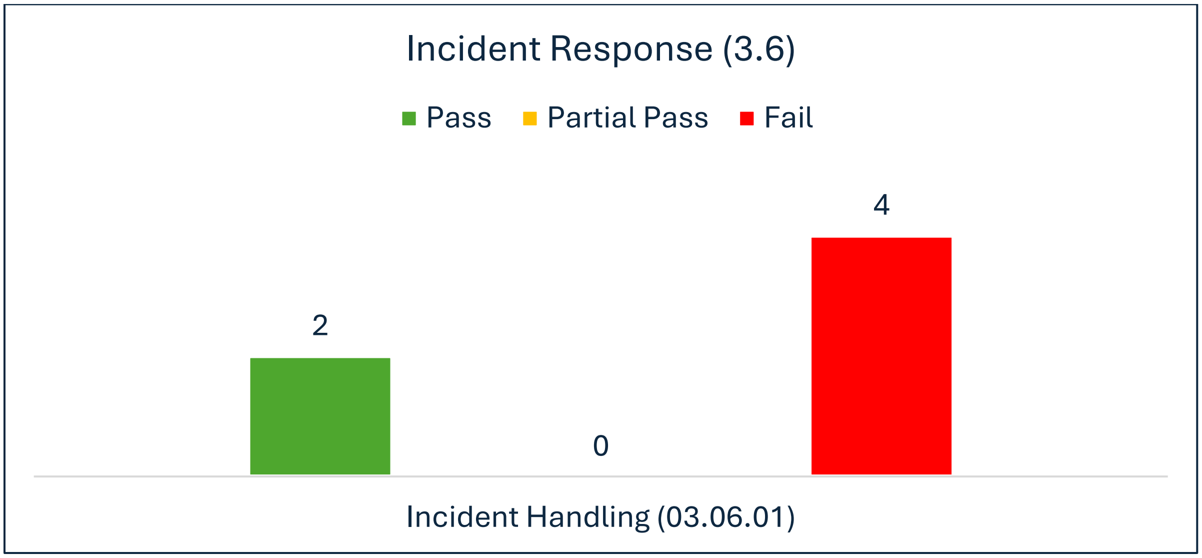
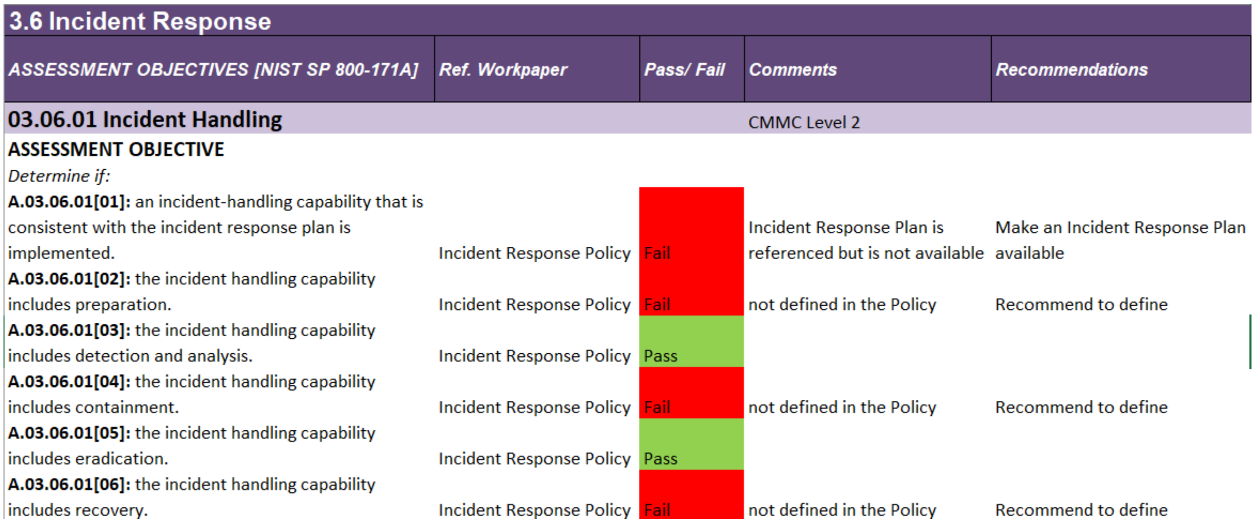


Figure 6 Incident Response compliance overview

Detailed audit results:



3.6 Incident Response				
ASSESSMENT OBJECTIVES [NIST SP 800-171A]	*Ref. Workpaper*	*Pass/ Fail*	*Comments*	*Recommendations*
03.06.01 Incident Handling			CMMC Level 2	
ASSESSMENT OBJECTIVE *Determine if:*				
A.03.06.01[01]: an incident-handling capability that is consistent with the incident response plan is implemented.	Incident Response Policy	Fail	Incident Response Plan is referenced but is not available	Make an Incident Response Plan available
A.03.06.01[02]: the incident handling capability includes preparation.	Incident Response Policy	Fail	not defined in the Policy	Recommend to define
A.03.06.01[03]: the incident handling capability includes detection and analysis.	Incident Response Policy	Pass		
A.03.06.01[04]: the incident handling capability includes containment.	Incident Response Policy	Fail	not defined in the Policy	Recommend to define
A.03.06.01[05]: the incident handling capability includes eradication.	Incident Response Policy	Pass		
A.03.06.01[06]: the incident handling capability includes recovery.	Incident Response Policy	Fail	not defined in the Policy	Recommend to define

Risk Assessment

Risk assessment domain met 2 out of 9 requirements, illustrated by Figure 7. These domains are only for CMMC Level 2. The policy documents used for this analysis were Risk Management Policy and Vulnerability Management Policy. The non-compliant categories were:

- Risk Assessment (03.11.01) – CMMC Lvl 2
  - Risk assessment of unauthorized disclosure is not defined (fail)
  - Risk assessment does not define update frequency (partial pass)
- Vulnerability Monitor and Scan (03.11.02) – CMMC Lvl 2
  - Frequency of scanning and monitoring of vulnerabilities is not defined (partial pass)
  - Response time of remediating vulnerabilities is not defined (partial pass)
  - System vulnerabilities to be scanned are not updated regularly or when new vulnerabilities are identified (fail)

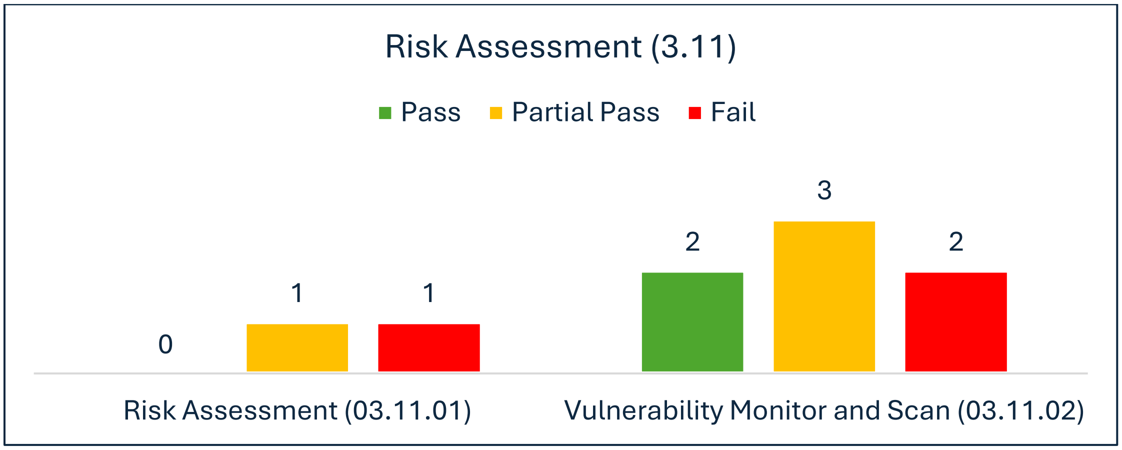
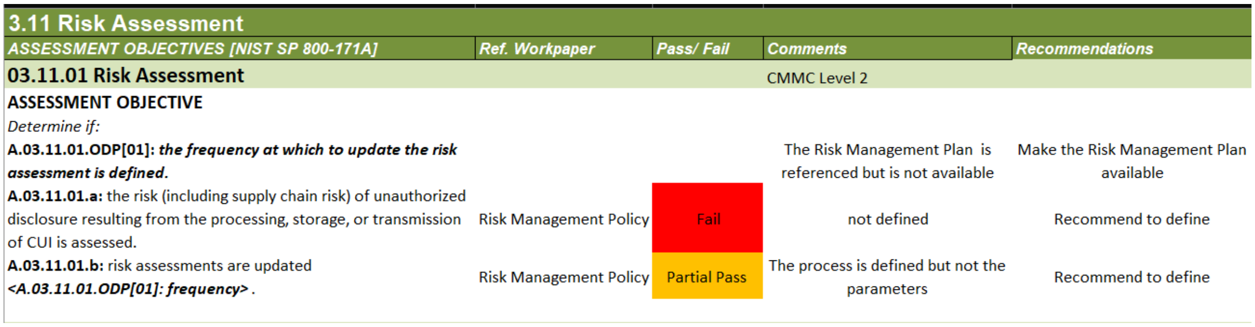
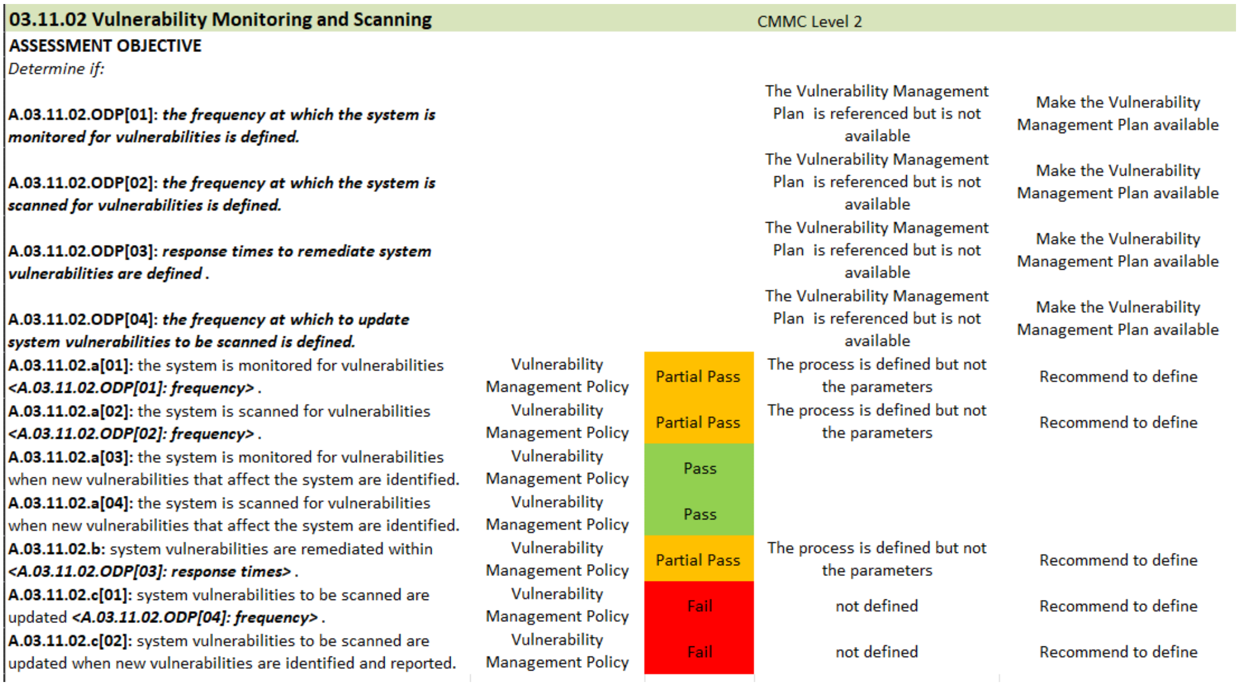


Figure 7 Risk Assessment compliance overview

Detailed audit results:



3.11 Risk Assessment				
ASSESSMENT OBJECTIVES [NIST SP 800-171A]	*Ref. Workpaper*	*Pass/ Fail*	*Comments*	*Recommendations*
03.11.01 Risk Assessment			CMMC Level 2	
ASSESSMENT OBJECTIVE				
Determine if:				
A.03.11.01.ODP[01]: ***the frequency at which to update the risk assessment is defined.***			The Risk Management Plan is referenced but is not available	Make the Risk Management Plan available
A.03.11.01.a: the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	Risk Management Policy	Fail	not defined	Recommend to define
A.03.11.01.b: risk assessments are updated ***<A.03.11.01.ODP[01]: frequency>*** .	Risk Management Policy	Partial Pass	The process is defined but not the parameters	Recommend to define



03.11.02 Vulnerability Monitoring and Scanning			CMMC Level 2	
ASSESSMENT OBJECTIVE				
Determine if:				
A.03.11.02.ODP[01]: ***the frequency at which the system is monitored for vulnerabilities is defined.***			The Vulnerability Management Plan is referenced but is not available	Make the Vulnerability Management Plan available
A.03.11.02.ODP[02]: ***the frequency at which the system is scanned for vulnerabilities is defined.***			The Vulnerability Management Plan is referenced but is not available	Make the Vulnerability Management Plan available
A.03.11.02.ODP[03]: ***response times to remediate system vulnerabilities are defined .***			The Vulnerability Management Plan is referenced but is not available	Make the Vulnerability Management Plan available
A.03.11.02.ODP[04]: ***the frequency at which to update system vulnerabilities to be scanned is defined.***			The Vulnerability Management Plan is referenced but is not available	Make the Vulnerability Management Plan available
A.03.11.02.a[01]: the system is monitored for vulnerabilities ***<A.03.11.02.ODP[01]: frequency>*** .	Vulnerability Management Policy	Partial Pass	The process is defined but not the parameters	Recommend to define
A.03.11.02.a[02]: the system is scanned for vulnerabilities ***<A.03.11.02.ODP[02]: frequency>*** .	Vulnerability Management Policy	Partial Pass	The process is defined but not the parameters	Recommend to define
A.03.11.02.a[03]: the system is monitored for vulnerabilities when new vulnerabilities that affect the system are identified.	Vulnerability Management Policy	Pass		
A.03.11.02.a[04]: the system is scanned for vulnerabilities when new vulnerabilities that affect the system are identified.	Vulnerability Management Policy	Pass		
A.03.11.02.b: system vulnerabilities are remediated within ***<A.03.11.02.ODP[03]: response times>*** .	Vulnerability Management Policy	Partial Pass	The process is defined but not the parameters	Recommend to define
A.03.11.02.c[01]: system vulnerabilities to be scanned are updated ***<A.03.11.02.ODP[04]: frequency>*** .	Vulnerability Management Policy	Fail	not defined	Recommend to define
A.03.11.02.c[02]: system vulnerabilities to be scanned are updated when new vulnerabilities are identified and reported.	Vulnerability Management Policy	Fail	not defined	Recommend to define

Recommendations

While the policy documents audited are relevant to both CMMC Level 1 and Level 2, we recommend to pursue CMMC Level 1 first and prioritize addressing relevant gaps. Recommendations are provided per domain in

Table 2 below.

We recommend to prioritize addressing requirement 03.05.01 User Identification, Authentication, and Re-Authentication in the Identification and Authentication domain as it is required for attaining CMMC Level 1 (highlighted gray below).Details about the exact requirement gaps should be obtained from the appropriate domain section in Findings of Fact or Appendix A

CMMC Cybersecurity Audit spreadsheet. We also recommend making the documents listed in Appendix D available for a full assessment of CMMC Levels 1-3 compliance.

Table 2 Recommendations per domain

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 as stated in 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])

Appendices

Appendix A

CMMC Cybersecurity Audit spreadsheet

CMMC Cybersecurity
Audit spreadsheet.xls

Appendix B

IIT CMMC Audit Presentation

CMMC Audit of
Illinois Institute of Tec

Appendix C

Cybersecurity Maturity Model Certification (CMMC) Model Overview

ModelOverview.pdf

Appendix D

Documents descoped from audit due to unavailability

Standards:

Data Standard

Encryption Standard

Incident Response Standard

Multi-Factor Authentication Standard

Vulnerability Management Standard

Plans:

Access Control Plan

Audit Plan

Data Plan

Disaster Recovery Plan

Incident Response Plan

Risk Management Plan

System and Communications Protection Plan

System and Data Integrity Plan

System, Services, and Asset Lifecycle Management Plan

Vulnerability Management Plan