CONFIDENTIAL

AIRA

AI RISK & GOVERNANCE PLATFORM

AI Governance Compliance Report

A comprehensive assessment of organizational AI governance posture, risk exposure, framework compliance, and remediation status across all registered AI systems.

ORGANIZATION	REPORT DATE	AUDIENCE	AI SYSTEMS
CMMC Audit Package	May 6, 2026	Board / C-Suite	11 Registered

TOC Table of Contents

Report Generated: May 6, 2026
Organization: CMMC Audit Package
Audience: Board / C-Suite
Frameworks: 23 selected

01 Executive Summary

As of May 6, 2026, CMMC Audit Package's AI governance program is **operating at an acceptable level** based on a composite governance score of **93%**. This score reflects the organization's ability to demonstrate compliance across 1 regulatory and industry framework through 110 mapped controls covering 11 registered AI systems.

The organization's current risk exposure includes **8 open findings**. All findings with assigned due dates are within their remediation timelines. The mean time to remediate resolved findings is **not yet measurable**.

Framework compliance stands at 93% across assessed frameworks. The organization is positioned to pass a formal audit against its primary frameworks with continued diligence.

93%
Governance Score
102/110 controls compliant

0
Critical Findings
None overdue

8
Unresolved Risks
1 open, 0 in progress

0
Overdue Items
Past remediation deadline

102
Compliant Controls
1 gap identified

11
AI Systems
Under governance oversight

RISK SEVERITY DISTRIBUTION · 8 UNRESOLVED

0 Critical 1 High 7 Medium 0 Low

02 Scope & Methodology

Scope: This report assesses CMMC Audit Package's AI governance posture across 23 compliance frameworks: NIST AI RMF, OWASP LLM, OWASP Agentic, EU AI Act, ISO 42001, NIST CSF 2.0, SOC 2 TSC, ISO 27001, NIST 800-53, CMMC, CIS Controls, PCI DSS v4.0, HITRUST CSF, FedRAMP, StateRAMP, ISO 27701, GLBA, CCPA, GDPR, FCRA, NYDFS, SHIELD Act, Colorado Privacy Act. The assessment covers 11 registered AI systems and 110 governance controls.

Methodology:

METRIC	CALCULATION METHOD
Governance Score	Percentage of controls in "compliant" status out of total controls mapped to selected frameworks. A control is marked compliant when evidence has been uploaded and attested, or when an authorized user has verified implementation.
Risk Severity	Findings are classified using a 4-tier model (Critical, High, Medium, Low) based on assessed likelihood and business impact using a 5×5 risk matrix.
Framework Compliance	Per-framework scores represent the ratio of compliant controls to total controls mapped to that specific framework.
MTTR	Mean Time to Remediate — average calendar days from finding identification date to resolution date, calculated from resolved findings with documented identification dates.

Limitations

This report is based on self-reported control status and evidence. Independent verification of control effectiveness is outside the scope of this automated assessment. Compliance percentages reflect control mapping completeness — frameworks with fewer mapped controls may show artificially high or low scores. All data reflects the state of the AIRA platform at the time of generation (May 6, 2026) and may not capture changes made after this date.

Report ID: AIRA-CR-20260506-0002

Prepared By: System

Classification: CONFIDENTIAL

Data Currency: May 6, 2026

03 Framework Compliance

CMMC Audit Package's AI governance program is assessed against 1 industry-recognized framework. The following analysis provides compliance percentages calculated from the ratio of compliant controls to total controls mapped to each framework. The organization demonstrates strongest alignment with **CMMC** (93%).

CMMC

102 of 110 controls compliant

93%

04 Risk Register Detail

The following section provides a detailed view of all 8 findings currently tracked in the risk register, organized by severity. Each finding includes ownership information, current remediation status, risk assessment parameters, and any documented description or remediation plans. All findings with assigned due dates are within their remediation timelines.

HIGH 1 finding

High

IA.L2-3.5.11 — Not Met: Authentication Feedback Obscuring

CMMC · IA.L2-3.5.11

OWNER	STATUS	DUE DATE
Unassigned	Open	May 23, 2026
LIKELIHOOD	**IMPACT**	**RISK RESPONSE**
High	High	Mitigate

DESCRIPTION

CMMC L2 assessment finding against practice IA.L2-3.5.11. Current state: not implemented — compensating controls under evaluation. Practice objective: Obscure feedback of authentication information.

REMEDIATION PLAN

POA&M: Implement per NIST SP 800-171 guidance. 30-day mitigation window. Compensating controls documented in SSP Appendix.

MEDIUM 7 findings

Medium

CM.L2-3.4.7 — Partially Met: Nonessential Service Restriction

CMMC · CM.L2-3.4.7

OWNER	STATUS	DUE DATE
Unassigned	In Review	July 22, 2026
LIKELIHOOD	**IMPACT**	**RISK RESPONSE**
Medium	Medium	Mitigate

DESCRIPTION

CMMC L2 assessment finding against practice CM.L2-3.4.7. Current state: partially implemented; enforcement and/or documentation gaps identified. Practice objective: Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

REMEDIATION PLAN

POA&M: Close enforcement and documentation gaps; 90-day target. Evidence refresh on closure.

Medium

SI.L2-3.14.2 — Partially Met: Malicious Code Protection

CMMC · SI.L2-3.14.2

OWNER	STATUS	DUE DATE
Unassigned	In Review	July 22, 2026

LIKELIHOOD	IMPACT	RISK RESPONSE
Medium	Medium	Mitigate

DESCRIPTION

CMMC L2 assessment finding against practice SI.L2-3.14.2. Current state: partially implemented; enforcement and/or documentation gaps identified. Practice objective: Provide protection from malicious code at appropriate locations within organizational information systems.

REMEDIATION PLAN

POA&M: Close enforcement and documentation gaps; 90-day target. Evidence refresh on closure.

Medium

SC.L2-3.13.9 — Partially Met: Network Session Termination

CMMC · SC.L2-3.13.9

OWNER	STATUS	DUE DATE
Unassigned	In Review	July 22, 2026

LIKELIHOOD	IMPACT	RISK RESPONSE
Medium	Medium	Mitigate

DESCRIPTION

CMMC L2 assessment finding against practice SC.L2-3.13.9. Current state: partially implemented; enforcement and/or documentation gaps identified. Practice objective: Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

REMEDIATION PLAN

POA&M: Close enforcement and documentation gaps; 90-day target. Evidence refresh on closure.

Medium

MA.L2-3.7.3 — Partially Met: Off-Site Maintenance Sanitization

CMMC · MA.L2-3.7.3

OWNER	STATUS	DUE DATE
Unassigned	In Review	July 22, 2026

LIKELIHOOD	IMPACT	RISK RESPONSE
Medium	Medium	Mitigate

DESCRIPTION

CMMC L2 assessment finding against practice MA.L2-3.7.3. Current state: partially implemented; enforcement and/or documentation gaps identified. Practice objective: Ensure equipment removed for off-site maintenance is sanitized of any CUI.

REMEDIATION PLAN

POA&M: Close enforcement and documentation gaps; 90-day target. Evidence refresh on closure.

Medium

AC.L2-3.1.8 — Partially Met: Unsuccessful Logon Attempt Limits

CMMC · AC.L2-3.1.8

OWNER	STATUS	DUE DATE
Unassigned	In Review	July 22, 2026

LIKELIHOOD	IMPACT	RISK RESPONSE
Medium	Medium	Mitigate

DESCRIPTION

CMMC L2 assessment finding against practice AC.L2-3.1.8. Current state: partially implemented; enforcement and/or documentation gaps identified. Practice objective: Limit unsuccessful logon attempts.

REMEDIATION PLAN

POA&M: Close enforcement and documentation gaps; 90-day target. Evidence refresh on closure.

Medium

MP.L2-3.8.6 — Partially Met: Digital Media Transport Encryption

CMMC · MP.L2-3.8.6

OWNER	STATUS	DUE DATE
Unassigned	In Review	July 22, 2026

LIKELIHOOD	IMPACT	RISK RESPONSE
Medium	Medium	Mitigate

DESCRIPTION

CMMC L2 assessment finding against practice MP.L2-3.8.6. Current state: partially implemented; enforcement and/or documentation gaps identified. Practice objective: Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

REMEDIATION PLAN

POA&M: Close enforcement and documentation gaps; 90-day target. Evidence refresh on closure.

Medium

AU.L2-3.3.2 — Partially Met: User Accountability & Traceability

CMMC · AU.L2-3.3.2

OWNER	STATUS	DUE DATE
Unassigned	In Review	July 22, 2026

LIKELIHOOD	IMPACT	RISK RESPONSE
Medium	Medium	Mitigate

DESCRIPTION

CMMC L2 assessment finding against practice AU.L2-3.3.2. Current state: partially implemented; enforcement and/or documentation gaps identified. Practice objective: Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

REMEDIATION PLAN

POA&M: Close enforcement and documentation gaps; 90-day target. Evidence refresh on closure.

05 AI System Inventory

CMMC Audit Package currently maintains 11 registered AI systems under governance oversight. The inventory below details each system's classification, operational environment, assessed risk level, and current compliance posture. Systems with compliance scores below 50% should be prioritized for assessment and control implementation.

SYSTEM	TYPE	RISK LEVEL	ENVIRONMENT	COMPLIANCE
Export Control (EAR/ITAR) Classifier	ML Model	Critical	production	94%
Contract Proposal Assistant (GCC-High)	LLM Application	High	production	88%
Firmware Vulnerability Scanner	ML Model	High	production	81%
Supply Chain Risk Monitor	ML Model	High	production	77%
Insider Threat Risk Scoring	ML Model	High	production	79%
Engineering Drawing Search (RAG)	LLM Application	High	production	85%
CUI Document Classification Model	ML Model	High	production	92%
Org Baseline Unassigned	Environment	Medium	production	0%
Facility Badge Anomaly Detector	ML Model	Medium	production	90%
Phishing Triage Agent	Agentic AI	Medium	production	82%
Help Desk Assistant (CUI-aware)	LLM Application	Medium	production	86%

06 Control Status

This section provides a comprehensive view of all 110 controls tracked across the organization's AI governance program. Controls are organized by framework and include current implementation status and evidence attestation state. 1 control remains in gap status, requiring implementation or evidence upload to achieve compliance.

102	1	0	0
Compliant	Gap	In Progress	N/A

CMMC · 110 CONTROLS

CONTROL	REFERENCE	STATUS	ATTESTATION
Remote Access Monitoring & Control	AC.L2-3.1.12	Compliant	Completed
Remote Access Routing	AC.L2-3.1.14	Compliant	Completed
Remote Privileged Command Authorization	AC.L2-3.1.15	Compliant	Completed
Wireless Access Authorization	AC.L2-3.1.16	Compliant	Completed
Wireless Access Protection	AC.L2-3.1.17	Compliant	Completed
Mobile Device CUI Encryption	AC.L2-3.1.19	Compliant	In Progress
External System Connection Control	AC.L2-3.1.20	Compliant	Completed
Portable Storage on External Systems	AC.L2-3.1.21	Compliant	Completed
Publicly Accessible CUI Control	AC.L2-3.1.22	Compliant	Completed
Security Risk Awareness	AT.L2-3.2.1	Compliant	Completed
Insider Threat Awareness	AT.L2-3.2.3	Compliant	Completed
Audit Log Creation & Retention	AU.L2-3.3.1	Compliant	Completed
Audit Record Correlation	AU.L2-3.3.5	Compliant	Completed
Audit Reduction & Reporting	AU.L2-3.3.6	Compliant	In Progress
Time Source Synchronization	AU.L2-3.3.7	Compliant	Completed
Audit Information Protection	AU.L2-3.3.8	Compliant	Completed
Unsuccessful Logon Attempt Limits	AC.L2-3.1.8	Partial	In Progress
User Accountability & Traceability	AU.L2-3.3.2	Partial	In Progress

CONTROL	REFERENCE	STATUS	ATTESTATION
Audit Logging Failure Alerting	AU.L2-3.3.4	Compliant	Completed
Nonessential Service Restriction	CM.L2-3.4.7	Partial	In Progress
Off-Site Maintenance Sanitization	MA.L2-3.7.3	Partial	In Progress
Digital Media Transport Encryption	MP.L2-3.8.6	Partial	In Progress
Network Session Termination	SC.L2-3.13.9	Partial	In Progress
Malicious Code Protection	SI.L2-3.14.2	Partial	In Progress
Malware Protection Updates	SI.L2-3.14.4	Compliant	Completed
CUI At-Rest Confidentiality	SC.L2-3.13.16	Compliant	Completed
Flaw Identification & Remediation	SI.L2-3.14.1	Compliant	Completed
Authentication Feedback Obscuring	IA.L2-3.5.11	Gap	Not Started
Periodic & Real-Time Malware Scanning	SI.L2-3.14.5	Compliant	Completed
Attack & Intrusion Monitoring	SI.L2-3.14.6	Compliant	Completed
Unauthorized Use Identification	SI.L2-3.14.7	Compliant	Completed
Non-Privileged Account Use	AC.L2-3.1.6	Compliant	Completed
Remote Access Encryption	AC.L2-3.1.13	Compliant	Completed
Mobile Device Control	AC.L2-3.1.18	Compliant	Completed
Role-Based Security Training	AT.L2-3.2.2	Compliant	Completed
Audit Event Review & Update	AU.L2-3.3.3	Compliant	In Progress
Change Tracking & Approval	CM.L2-3.4.3	Compliant	Completed
User-Installed Software Control	CM.L2-3.4.9	Compliant	Completed
Replay-Resistant Authentication	IA.L2-3.5.4	Compliant	Completed
Temporary Password Management	IA.L2-3.5.9	Compliant	Completed
Incident Response Testing	IR.L2-3.6.3	Compliant	Completed
Media Sanitization & Destruction	MP.L2-3.8.3	Compliant	Completed
Backup CUI Confidentiality	MP.L2-3.8.9	Compliant	Completed

CONTROL	REFERENCE	STATUS	ATTESTATION
Visitor Escort & Monitoring	PE.L2-3.10.3	Compliant	Completed
Security Architecture & Engineering	SC.L2-3.13.2	Compliant	Completed
Split Tunneling Prevention	SC.L2-3.13.7	Compliant	Completed
Collaborative Device Control	SC.L2-3.13.12	Compliant	Completed
Security Alert & Advisory Response	SI.L2-3.14.3	Compliant	Completed
Authorized User Access Control	AC.L2-3.1.1	Compliant	In Progress
Transaction & Function Access Control	AC.L2-3.1.2	Compliant	Completed
CUI Information Flow Enforcement	AC.L2-3.1.3	Compliant	Completed
Separation of Duties	AC.L2-3.1.4	Compliant	Completed
Least Privilege	AC.L2-3.1.5	Compliant	Completed
Privileged Function Restrictions	AC.L2-3.1.7	Compliant	Completed
System Use Notification	AC.L2-3.1.9	Compliant	Completed
Session Lock	AC.L2-3.1.10	Compliant	Completed
Session Termination	AC.L2-3.1.11	Compliant	In Progress
Audit Management Restriction	AU.L2-3.3.9	Compliant	Completed
Baseline Configuration & Inventory	CM.L2-3.4.1	Compliant	Completed
Security Configuration Enforcement	CM.L2-3.4.2	Compliant	Completed
Security Impact Analysis	CM.L2-3.4.4	Compliant	Completed
Change Access Restrictions	CM.L2-3.4.5	Compliant	In Progress
Least Functionality	CM.L2-3.4.6	Compliant	In Progress
Software Execution Policy	CM.L2-3.4.8	Compliant	Completed
User, Process & Device Identification	IA.L2-3.5.1	Compliant	In Progress
Identity Authentication	IA.L2-3.5.2	Compliant	In Progress
Multifactor Authentication	IA.L2-3.5.3	Compliant	Completed
Identifier Reuse Prevention	IA.L2-3.5.5	Compliant	Completed

CONTROL	REFERENCE	STATUS	ATTESTATION
Inactive Identifier Disabling	IA.L2-3.5.6	Compliant	Completed
Password Complexity	IA.L2-3.5.7	Compliant	In Progress
Password Reuse Prevention	IA.L2-3.5.8	Compliant	Completed
Cryptographic Password Protection	IA.L2-3.5.10	Compliant	Completed
Incident Handling Capability	IR.L2-3.6.1	Compliant	Completed
Incident Tracking & Reporting	IR.L2-3.6.2	Compliant	Completed
System Maintenance Performance	MA.L2-3.7.1	Compliant	In Progress
Maintenance Tool & Personnel Control	MA.L2-3.7.2	Compliant	Completed
Maintenance Media Malware Check	MA.L2-3.7.4	Compliant	Completed
Nonlocal Maintenance Authentication	MA.L2-3.7.5	Compliant	Completed
Maintenance Personnel Supervision	MA.L2-3.7.6	Compliant	Completed
CUI Media Physical Protection	MP.L2-3.8.1	Compliant	Completed
CUI Media Access Restriction	MP.L2-3.8.2	Compliant	Completed
CUI Media Marking	MP.L2-3.8.4	Compliant	In Progress
CUI Media Transport Accountability	MP.L2-3.8.5	Compliant	Completed
Removable Media Control	MP.L2-3.8.7	Compliant	Completed
Unowned Portable Storage Prohibition	MP.L2-3.8.8	Compliant	Completed
Personnel Screening	PS.L2-3.9.1	Compliant	Completed
Personnel Action CUI Protection	PS.L2-3.9.2	Compliant	Completed
Physical Access Limitation	PE.L2-3.10.1	Compliant	Completed
Facility Protection & Monitoring	PE.L2-3.10.2	Compliant	Completed
Physical Access Audit Logs	PE.L2-3.10.4	Compliant	Completed
Physical Access Device Management	PE.L2-3.10.5	Compliant	Completed
Alternate Work Site Safeguards	PE.L2-3.10.6	Compliant	Completed
Periodic Risk Assessment	RA.L2-3.11.1	Compliant	Completed

CONTROL	REFERENCE	STATUS	ATTESTATION
Vulnerability Scanning	RA.L2-3.11.2	Compliant	Completed
Risk-Based Vulnerability Remediation	RA.L2-3.11.3	Compliant	In Progress
Security Control Assessment	CA.L2-3.12.1	Compliant	Completed
Plans of Action & Milestones	CA.L2-3.12.2	Compliant	Completed
Continuous Security Monitoring	CA.L2-3.12.3	Compliant	Completed
System Security Plan	CA.L2-3.12.4	Compliant	In Progress
Boundary Communications Protection	SC.L2-3.13.1	Compliant	Completed
User-Management Function Separation	SC.L2-3.13.3	Compliant	Completed
Shared Resource Information Transfer Prevention	SC.L2-3.13.4	Compliant	Completed
Public-Facing Network Separation	SC.L2-3.13.5	Compliant	Completed
Default-Deny Network Traffic	SC.L2-3.13.6	Compliant	Completed
CUI Transmission Encryption	SC.L2-3.13.8	Compliant	Completed
Cryptographic Key Management	SC.L2-3.13.10	Compliant	Completed
FIPS-Validated Cryptography	SC.L2-3.13.11	Compliant	Completed
Mobile Code Control	SC.L2-3.13.13	Compliant	Completed
VoIP Control & Monitoring	SC.L2-3.13.14	Compliant	Completed
Session Authenticity Protection	SC.L2-3.13.15	Compliant	In Progress

07 Gap Analysis

1 control is currently identified as compliance gaps across 1 framework. Each gap represents a control requirement that has not yet been satisfied through implementation or evidence documentation. Closing these gaps should be prioritized based on the associated framework requirements and the organization's risk appetite.

Compliance Gaps Requiring Attention

1 control requires evidence upload or implementation to achieve compliance: **Authentication Feedback Obscuring**.

CONTROL	FRAMEWORK	REFERENCE	ATTESTATION
Authentication Feedback Obscuring	CMMC	IA.L2-3.5.11	Not Started

08 Recommendations

Based on the findings and compliance analysis presented in this report, the following 3 recommendations are provided to strengthen CMMC Audit Package's AI governance posture. Recommendations are data-driven and prioritized by urgency.

1. Close Control Gaps with Evidence

1 control is in gap status. Prioritize evidence collection for frameworks with the lowest compliance scores. Focus on: **CMMC** (93%).

Priority: High **Timeline:** 30 days **Owner:** Control Owners / Compliance

2. Complete Governance Maturity Assessment

No maturity assessment has been completed. A baseline maturity assessment establishes governance capability across 5 dimensions and identifies priority improvement areas.

Priority: Medium **Timeline:** 60 days **Owner:** CISO / GRC Lead

3. Maintain Governance Review Cadence

Schedule quarterly governance review meetings. Review risk register aging, control attestation freshness, assessment completion rates, and framework coverage. Ensure new AI systems are registered and assessed before production deployment.

Priority: Ongoing **Timeline:** Continuous **Owner:** CISO / Governance Board

NO.	ACTION ITEM	PRIORITY	TIMELINE	OWNER
1	Close Control Gaps with Evidence	High	30 days	Control Owners / Compliance
2	Complete Governance Maturity Assessment	Medium	60 days	CISO / GRC Lead
3	Maintain Governance Review Cadence	Ongoing	Continuous	CISO / Governance Board

09 Governance Maturity

No maturity assessment has been completed yet. It is recommended that CMMC Audit Package conduct a governance maturity assessment to establish a baseline understanding of organizational AI governance capability across key dimensions.

Assessment Not Yet Completed

Navigate to AI Governance → Maturity in AIRA to complete the initial maturity assessment. This evaluates the organization across 5 dimensions: Policy & Standards, Oversight & Accountability, Risk Integration, Monitoring & Measurement, and Culture & Training.

10 Policy Compliance

No AI governance policies have been created yet. Establishing formal policies is a foundational step in building a mature AI governance program. It is recommended that CMMC Audit Package develop policies covering AI ethics, data governance, model risk management, and regulatory compliance.

No Policies Established

Navigate to AI Governance → Policies in AIRA to create your first governance policy. Policies define the organizational rules and expectations for responsible AI use.

REF Glossary of Terms

TERM	DEFINITION
Governance Score	Percentage of controls in compliant status out of total mapped controls. Reflects overall compliance posture.
Control	A specific requirement or safeguard derived from a compliance framework, mapped to the organization's AI systems.
Finding	An identified risk, vulnerability, or non-compliance issue requiring remediation and tracked in the risk register.
Gap	A control that has not yet been implemented or evidenced. Gaps reduce the governance score and indicate audit exposure.
Attestation	Formal acknowledgment by a control owner that a control is implemented and operating as intended.
Evidence	Documentation (files, screenshots, policies, configurations) uploaded to demonstrate control implementation.
Framework	A compliance or governance standard (e.g., NIST AI RMF, EU AI Act, SOC 2) containing control requirements.
Severity	Risk classification of a finding: Critical (immediate action), High (escalation needed), Medium (planned remediation), Low (acceptable risk).
Remediation	The process of addressing and resolving an identified finding, tracked through status transitions.
MTTR	Mean Time to Remediate — average calendar days from finding identification to resolution.
Risk Response	Strategy for addressing a finding: Mitigate, Accept, Transfer, or Avoid.

Prepared By: System (saas_owner)

Report ID: AIRA-CR-20260506-0002

Generated: May 6, 2026

Classification: CONFIDENTIAL — Internal Use Only

APPROVED BY (SIGNATURE)

DATE