

GOVERNANCE DOCS

CMMC Level 2

Gap Assessment Report

CMMC 2.0 Level 2 / NIST SP 800-171 Rev 2

Keystone Precision Machining (sample)

The CUI enclave used for defence drawings and purchase orders, and the machine shop network that connects to it.

ASSESSED	25 September 2026
EDITION	32 CFR Part 170, assessed against NIST SP 800-171 Rev 2
IN SCOPE	123 requirements, 121 applicable
PROFILE	Manufacturing and industrial · 10 to 49 people · US Department of Defense
PREPARED BY	Governance Docs

CONTENTS

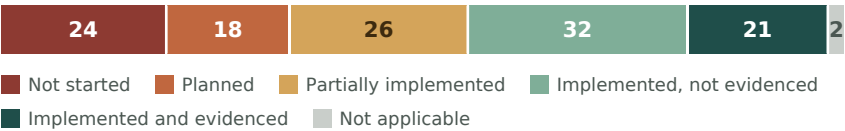
- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Keystone Precision Machining (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Keystone Precision Machining (sample) stands against CMMC 2.0



STATUS OF EVERY REQUIREMENT



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 51.7% against CMMC 2.0 across 121 applicable controls. 21 of them are implemented and evidenced.
- Most open gaps: AC - Access Control, with 21 at 39%. Strongest area: AT - Awareness and Training at 83%.
- 32 controls are operating but not evidenced. Collecting their records alone lifts the score to 58.3% (+6.6 points), the cheapest gain available.
- 42 gaps are high priority (not started or only planned); 11 of them are in AC - Access Control.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 11 high-priority gaps in AC - Access Control	IT Manager	Least Privilege Implementation Procedure
2	MEDIUM	Adopt and tailor the Encryption Standard (Data at Rest and in Transit), which closes 7 open gaps	To assign	Encryption Standard (Data at Rest and in Transit)
3	LOW	Evidence the 32 controls that already operate (+6.6 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

At 51.7% readiness, you must establish baseline documentation and evidence existing practices to build momentum.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our self-assessment shows a score of 51.7% at the Developing level, with 100 open gaps across 121 applicable requirements. Our main exposure comes from 42 high priority gaps and 32 controls that operate without formal evidence, which does not meet the expectations of the US Department of Defense. Leadership support is needed to mandate control ownership across the team, approve system security policies, and ensure technical staff have dedicated time to produce required operational records.

WHERE YOU STAND

You currently stand at a Developing readiness level with an overall score of 51.7%. Out of 121 applicable requirements, you have 100 open gaps, including 42 high priority gaps. While 21 controls are implemented and evidenced, 32 requirements are implemented without evidence and 26 are partially implemented. Scope and programme sits at 37.5%, while Access Control is at 38.6%. Only 42 gaps have an assigned owner and 18 have target completion dates, showing that foundational governance is not yet complete.

WHAT IT MEANS FOR THE ORGANIZATION

The assessment shows that your operational practices run ahead of your formal documentation. Having 32 controls implemented without evidence means an external assessment team cannot verify your current cybersecurity posture. Low scores in core areas like Access Control and Configuration Management create operational friction. As a supplier in manufacturing and industrial contracting with the US Department of Defense, unverified practices fall short of expectations. Closing documentation gaps will rapidly improve your standing and reduce delivery risks across defense supply contracts.

WHERE TO FOCUS FIRST

Focus first on establishing your baseline documentation and scoping controls. Evidencing what already runs will immediately lift your score from 51.7% to 58.3%. You should formalize system boundaries using the System Security Plan and address the 24 controls that have not started. Next, complete partially implemented controls to reach 69% and assign owners to all remaining unassigned gaps. Establishing standard policies for encryption, remote access, and least functionality will address the greatest number of outstanding high priority gaps.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN	
1	Establish system boundaries and system security plan SP.1 CUI identification · SP.3 System security plan	Without defined boundaries and a system security plan, the organization cannot validate which systems handle sensitive defense data. This prevents successful external evaluation.	Draft the System Security Plan using the standard template to document current system boundaries.	System Security Plan (SSP) Template Comprehensive CMMC Documentation Toolkit – 107 Compliance Templates	30 DAYS
2	Implement standardized data encryption standards SC.L2-3.13.16 Confidentiality of CUI at rest · SC.L2-3.13.8 Transmission confidentiality	Unprotected transmission and storage of sensitive data directly breaches baseline security expectations. Addressing encryption resolves seven related compliance gaps across your environment.	Review current storage and transmission channels against the encryption standard.	Encryption Standard (Data at Rest and in Transit) Comprehensive CMMC Documentation Toolkit – 107 Compliance Templates	30 DAYS
3	Enforce least privilege and secure remote access AC.L2-3.1.7 Preventing privileged function execution · AC.L2-3.1.13 Remote access confidentiality	Unrestricted privileged execution and unsecured remote connections leave administrative systems vulnerable to unauthorized compromise. Securing remote access resolves five gaps.	Audit all active remote access pathways against the remote access procedure.	Remote Access Management Procedure Comprehensive CMMC Documentation Toolkit – 107 Compliance Templates	60 DAYS
4	Restrict nonessential functions and configure least functionality CM.L2-3.4.6 Least functionality · CM.L2-3.4.7 Restricting nonessential functions	Permitting unnecessary services expands the attack surface across your network. Restricting software and ports closes five gaps across configuration management.	Generate an inventory of nonessential software and services running on production endpoints.	Least Functionality and Software Restriction Standard Comprehensive CMMC Documentation Toolkit – 107 Compliance Templates	60 DAYS
5	Assign governance owners and formalize incident tracking SP.6 Governance and ownership · IR.L2-3.6.2 Incident tracking and reporting	58 open gaps lack an assigned owner, leaving remediation uncoordinated. Establishing incident tracking ensures security events are properly recorded and reported.	Assign designated owners and completion dates to all 42 high priority gaps.	Incident Register Comprehensive CMMC Documentation Toolkit – 107 Compliance Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Adopt the System Security Plan template and define initial system boundaries.
- Collect and file audit evidence for the 32 implemented but unevidenced controls.
- Implement the encryption standard across data storage and transmission points.

DAYS 31 TO 60

- Roll out the remote access management procedure and review remote user accounts.
- Apply the least functionality standard to eliminate nonessential software and system ports.
- Assign formal owners and target dates to all remaining unassigned open gaps.

DAYS 61 TO 90

- Operationalize the incident register and verify incident reporting workflows.
- Complete partially implemented controls to advance the overall score toward 69%.
- Initiate remediation for remaining controls that have not started across access control.

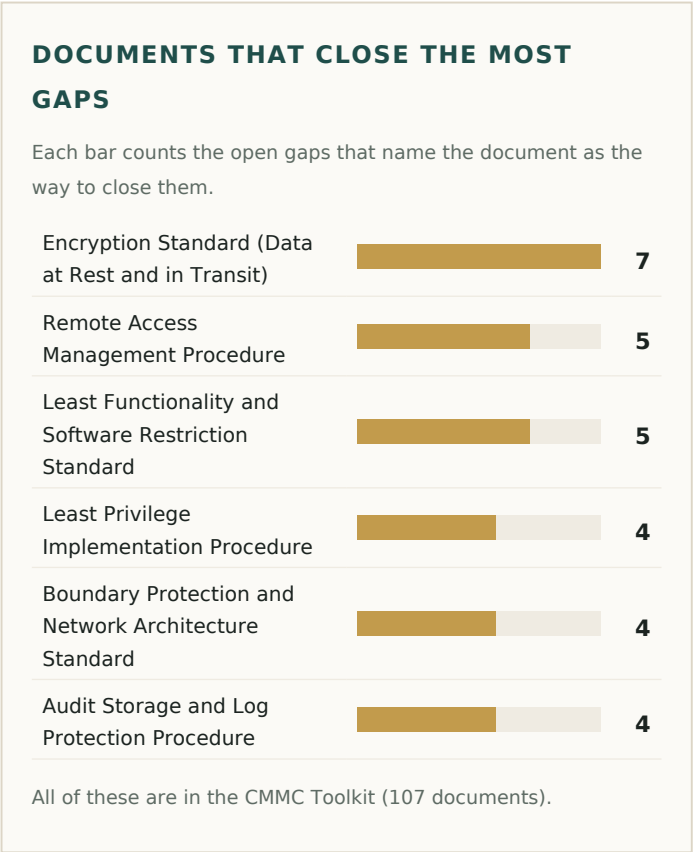
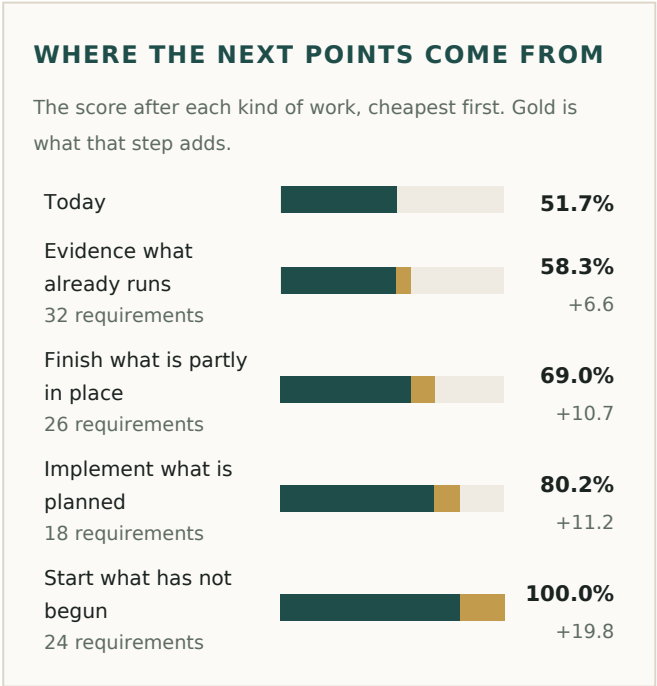
Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope and programme	3 3	38%	3 0 3
AC - Access Control	8 3 3 7	39%	11 3 7
AT - Awareness and Training	1 2	83%	0 1 0
AU - Audit and Accountability	2 2 3 1 1	59%	2 2 3
CM - Configuration Management	3 2 1 2 1	39%	5 1 2
IA - Identification and Authentication	3 4	65%	2 3 1
IR - Incident Response	1 2	58%	1 0 2
MA - Maintenance	2 1 1 2	63%	2 1 1
MP - Media Protection	3 2 1 3	53%	3 2 1
PS - Personnel Security	1 1	50%	1 0 0
PE - Physical Protection	2 1 3	79%	0 2 1
RA - Risk Assessment	1 1 1	75%	0 1 1
CA - Security Assessment	2 2	63%	0 2 2
SC - System and Communications Protection	3 4 5 4	41%	7 5 4
SI - System and Information Integrity	2 1 2 2	39%	3 2 2
Assessment readiness and SPRS	2 1 2 2	64%	2 1 2

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced
Not applicable

Where the next points come from



Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 24

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
SP.1	CUI identification	Scope and programme	To assign	CUI Asset Inventory and Data Flow Diagram Guide · CUI Scoping and Boundary Definition Guide
SP.3	System security plan	Scope and programme	IT Manager 24 Dec 2026	System Security Plan (SSP) Template
SP.6	Governance and ownership	Scope and programme	To assign	CMMC Governance and Oversight Framework
AC.L2-3.1.7	Preventing privileged function execution	AC	IT Manager 12 Nov 2026	Least Privilege Implementation Procedure · Audit Logging Configuration Standard
AC.L2-3.1.9	Privacy and security notices	AC	IT Manager 7 Jan 2027	Access Control Policy
AC.L2-3.1.10	Session lock	AC	To assign	Session Termination and Management Standard
AC.L2-3.1.11	Session termination	AC	To assign	Session Termination and Management Standard
AC.L2-3.1.13	Remote access confidentiality	AC	Compliance Lead	Remote Access Management Procedure · Encryption Standard (Data at Rest and in Transit)
AC.L2-3.1.17	Wireless protection	AC	Compliance Lead	Wireless Access Control Procedure
AC.L2-3.1.18	Mobile device connection control	AC	Risk Manager	Mobile Device Management Procedure
AC.L2-3.1.22	Publicly accessible content	AC	Risk Manager 26 Nov 2026	Public-Access System Separation Procedure
CM.L2-3.4.3	Change tracking and approval	CM	Operations Manager 7 Jan 2027	Configuration Change Control Procedure
CM.L2-3.4.6	Least functionality	CM	Compliance Lead 7 Jan 2027	Least Functionality and Software Restriction Standard
CM.L2-3.4.7	Restricting nonessential functions	CM	HR Manager	Least Functionality and Software Restriction Standard

IA.L2-3.5.11	Obscured authentication feedback	IA	Risk Manager	Identification and Authentication Policy
MP.L2-3.8.2	Access to CUI on media	MP	HR Manager	Media Storage and Access Control Procedure
MP.L2-3.8.4	Media marking	MP	Risk Manager	CUI Media Marking Procedure
MP.L2-3.8.7	Removable media control	MP	HR Manager	Media Protection Policy · Media Storage and Access Control Procedure
PS.L2-3.9.1	Personnel screening	PS	To assign	Personnel Security Policy · Personnel Screening Procedure
SC.L2-3.13.5	Public-access system separation	SC	To assign	Public-Access System Separation Procedure
SC.L2-3.13.12	Collaborative computing devices	SC	Operations Manager 21 Jan 2027	Collaborative Computing and VoIP Security Procedure
SC.L2-3.13.16	Confidentiality of CUI at rest	SC	To assign	Encryption Standard (Data at Rest and in Transit)
SI.L2-3.14.1	Flaw remediation	SI	HR Manager 26 Nov 2026	Flaw Remediation and Patch Management Procedure
SI.L2-3.14.6	Monitoring for attacks	SI	HR Manager 24 Dec 2026	System Monitoring and Intrusion Detection Procedure · Inbound/Outbound Communications Analysis Procedure

HIGH Planned · 18

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
AC.L2-3.1.3	Control CUI flow	AC	To assign	Access Enforcement and Information Flow Procedure · Network Segmentation and CUI Enclave Procedure
AC.L2-3.1.4	Separation of duties	AC	To assign	Separation of Duties Matrix
AC.L2-3.1.8	Unsuccessful logon attempts	AC	IT Manager	Password Policy and Complexity Standard · Account Management Procedure
AU.L2-3.3.8	Audit information protection	AU	To assign	Audit Storage and Log Protection Procedure

AU.L2-3.3.9	Audit management restriction	AU	To assign	Audit Storage and Log Protection Procedure · Separation of Duties Matrix
CM.L2-3.4.4	Security impact analysis	CM	Risk Manager 24 Dec 2026	Security Impact Analysis Procedure
CM.L2-3.4.8	Application allowlisting	CM	To assign	Least Functionality and Software Restriction Standard
IA.L2-3.5.10	Cryptographically protected passwords	IA	IT Manager	Cryptographic Authentication Standard · Encryption Standard (Data at Rest and in Transit)
IR.L2-3.6.2	Incident tracking and reporting	IR	Operations Manager 4 Feb 2027	Incident Register · DoD Cyber Incident Reporting Procedure (72-Hour Notification)
MA.L2-3.7.2	Maintenance tools control	MA	IT Manager 10 Dec 2026	Maintenance Tools Control Procedure
MA.L2-3.7.3	Sanitising equipment for off-site maintenance	MA	Compliance Lead	Media Sanitization and Disposal Procedure · Controlled Maintenance Procedure
SC.L2-3.13.7	Split tunnelling prevention	SC	HR Manager	Remote Access Management Procedure
SC.L2-3.13.8	Transmission confidentiality	SC	To assign	Encryption Standard (Data at Rest and in Transit)
SC.L2-3.13.10	Cryptographic key management	SC	Risk Manager	Cryptographic Key Management Procedure
SC.L2-3.13.14	Voice over IP	SC	Risk Manager 7 Jan 2027	Collaborative Computing and VoIP Security Procedure
SI.L2-3.14.2	Malicious code protection	SI	To assign	Malicious Code Protection Procedure
RD.2	Score meets the conditional threshold	Assessment readiness and SPRS	HR Manager	SPRS Score Calculation Workbook Guide · CMMC Gap Analysis Workbook Template
RD.3	POA&M eligibility understood	Assessment readiness and SPRS	To assign	Plan of Action and Milestones (POA&M) Procedure · CMMC Assessment Readiness Checklist

MEDIUM Partially implemented · 26

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
-----	-------------	------	----------------	-----------

AC.L2-3.1.5	Least privilege	AC	To assign	Least Privilege Implementation Procedure
AC.L2-3.1.12	Remote access monitoring and control	AC	Risk Manager	Remote Access Management Procedure
AC.L2-3.1.15	Privileged remote access	AC	HR Manager 4 Feb 2027	Remote Access Management Procedure · Least Privilege Implementation Procedure
AT.L2-3.2.3	Insider threat awareness	AT	HR Manager 7 Jan 2027	Insider Threat Awareness Program
AU.L2-3.3.2	Traceability to individuals	AU	Operations Manager	Audit Record Content and Format Standard · Identifier Management Procedure
AU.L2-3.3.4	Audit logging process failure	AU	Risk Manager	Audit Storage and Log Protection Procedure
CM.L2-3.4.1	Baseline configurations and inventories	CM	Operations Manager	Baseline Configuration Standard · System Component Inventory Register
IA.L2-3.5.2	Authentication	IA	To assign	Identification and Authentication Policy · Authenticator Management Procedure
IA.L2-3.5.7	Password complexity	IA	Compliance Lead	Password Policy and Complexity Standard
IA.L2-3.5.9	Temporary passwords	IA	To assign	Authenticator Management Procedure
MA.L2-3.7.1	System maintenance	MA	Operations Manager 21 Jan 2027	System Maintenance Policy · Controlled Maintenance Procedure
MP.L2-3.8.1	Media protection	MP	To assign	Media Protection Policy · Media Storage and Access Control Procedure
MP.L2-3.8.3	Media sanitisation before disposal	MP	IT Manager 12 Nov 2026	Media Sanitization and Disposal Procedure
PE.L2-3.10.3	Escorting visitors	PE	HR Manager	Visitor Management Procedure
PE.L2-3.10.4	Physical access audit logs	PE	To assign	Physical Access Log Template
RA.L2-3.11.1	Risk assessments	RA	To assign	Risk Assessment Policy · Risk Assessment Procedure +1 more
CA.L2-3.12.2	Plans of action	CA	Risk Manager	Plan of Action and Milestones (POA&M) Procedure · POA&M Register Template

CA.L2-3.12.4	System security plan	CA	To assign	System Security Plan (SSP) Template
SC.L2-3.13.1	Boundary protection	SC	To assign	Boundary Protection and Network Architecture Standard
SC.L2-3.13.2	Security engineering	SC	To assign	System and Communications Protection Policy · Boundary Protection and Network Architecture Standard
SC.L2-3.13.6	Deny by default network traffic	SC	To assign	Boundary Protection and Network Architecture Standard
SC.L2-3.13.11	FIPS-validated cryptography	SC	Compliance Lead	Encryption Standard (Data at Rest and in Transit)
SC.L2-3.13.13	Mobile code	SC	Risk Manager	Least Functionality and Software Restriction Standard
SI.L2-3.14.3	Security alerts and advisories	SI	To assign	Security Alert and Advisory Monitoring Procedure
SI.L2-3.14.7	Identifying unauthorised use	SI	IT Manager	System Monitoring and Intrusion Detection Procedure · Software and Information Integrity Verification Procedure
RD.7	Programme status tracked	Assessment readiness and SPRS	Operations Manager 4 Feb 2027	CMMC Continual Improvement and Reassessment Procedure

LOW Implemented, not evidenced · 32

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
SP.2	Assessment scope	Scope and programme	To assign	CMMC Assessment Scope Determination Procedure · CUI Scoping and Boundary Definition Guide
SP.4	Cloud service providers	Scope and programme	To assign	Cloud Service Provider (CSP) Security Requirements Guide
SP.5	Subcontractor flow-down	Scope and programme	To assign	Subcontractor Flow-Down Requirements Procedure

AC.L2-3.1.1	Authorised access control	AC	To assign	Access Control Policy · Account Management Procedure
AC.L2-3.1.2	Transaction and function control	AC	To assign	Access Enforcement and Information Flow Procedure
AC.L2-3.1.6	Non-privileged accounts	AC	To assign	Least Privilege Implementation Procedure · Account Management Procedure
AC.L2-3.1.14	Managed access control points	AC	To assign	Remote Access Management Procedure · Boundary Protection and Network Architecture Standard
AC.L2-3.1.19	CUI encryption on mobile	AC	To assign	Mobile Device Management Procedure · Encryption Standard (Data at Rest and in Transit)
AC.L2-3.1.20	External system connections	AC	To assign	External System Connection Procedure · System Connection Authorization Procedure
AC.L2-3.1.21	Portable storage on external systems	AC	To assign	Media Transport Protection Procedure · External System Connection Procedure
AU.L2-3.3.1	Audit record creation and retention	AU	To assign	Audit Logging Configuration Standard · Audit Storage and Log Protection Procedure
AU.L2-3.3.3	Review of logged events	AU	To assign	Audit Log Review and Analysis Procedure
AU.L2-3.3.6	Audit reduction and reporting	AU	To assign	Audit Reduction and Report Generation Procedure
CM.L2-3.4.2	Security configuration enforcement	CM	To assign	Baseline Configuration Standard · Configuration Management Policy

CM.L2-3.4.9	User-installed software	CM	To assign	Configuration Management Policy · Least Functionality and Software Restriction Standard
IA.L2-3.5.4	Replay-resistant authentication	IA	To assign	Cryptographic Authentication Standard
IR.L2-3.6.1	Incident handling capability	IR	To assign	Incident Response Policy · Incident Response Plan +1 more
IR.L2-3.6.3	Incident response testing	IR	To assign	Incident Response Testing and Exercise Procedure · Post-Incident Review and Lessons Learned Template
MA.L2-3.7.6	Maintenance personnel supervision	MA	To assign	Maintenance Personnel Oversight Procedure
MP.L2-3.8.9	Backup CUI confidentiality	MP	To assign	Media Storage and Access Control Procedure · Encryption Standard (Data at Rest and in Transit)
PE.L2-3.10.2	Protecting the physical facility	PE	To assign	Facility Physical Access Monitoring Procedure
RA.L2-3.11.3	Vulnerability remediation	RA	To assign	Vulnerability Remediation Procedure · Risk Register
CA.L2-3.12.1	Periodic control assessment	CA	To assign	Security Assessment Policy · Security Assessment Procedure
CA.L2-3.12.3	Continuous monitoring	CA	To assign	Continuous Monitoring Strategy and Plan
SC.L2-3.13.3	Separating user and management functionality	SC	To assign	Network Segmentation and CUI Enclave Procedure
SC.L2-3.13.4	Preventing shared resource information transfer	SC	To assign	System and Communications Protection Policy
SC.L2-3.13.9	Terminating network connections	SC	To assign	Session Termination and Management Standard
SC.L2-3.13.15	Communications session authenticity	SC	To assign	DNS and Communications Integrity Standard
SI.L2-3.14.4	Updating malicious code protection	SI	To assign	Malicious Code Protection Procedure

SI.L2-3.14.5	System and file scanning	SI	To assign	Malicious Code Protection Procedure
RD.5	Evidence assembled	Assessment readiness and SPRS	To assign	CMMC Assessment Readiness Checklist · CMMC Gap Analysis Workbook Template
RD.6	Affirmation	Assessment readiness and SPRS	To assign	CMMC Governance and Oversight Framework

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com