CMMC 2.0 Automated Mapping Summary

Accurately automate the assessment of CMMC 2.0 network requirements

CMMC 2.0 Mapping Document

Nipper automatically analyse CMMC non-compliances they identify, to reveal the risk to the network if the misconfiguration is exploited, providing an easy way to categorize risks and helping to inform remediation workflows.

Domain	Level	Requirement #	Nipper	See page
Identification and Authentication (IA)	1	IA.L1-b.1.vi Authentication [FCI Data]	✓	3
System and Communications Protection (SC)	1	SC.L1-b.1.x Boundary Protection [FCI Data]	✓	3
Access Control (AC)	2	AC.L2-3.1.1 Authorized Access Control [CUI Data]	✓	4
		AC.L2-3.1.8 Unsuccessful Logon Attempts	✓	
		AC.L2-3.1.9 Privacy & Security Notices	✓	
		AC.L2-3.1.10 Session Lock	✓	
		AC.L2-3.1.12 Control Remote Access	✓	
		AC.L2-3.1.13 Remote Access Confidentiality	✓	
		AC.L2-3.1.17 Wireless Access Protection	✓	
Audit and Accountability (AU)	2	AU.L2-3.3.1 System Auditing	✓	5
		AU.L2-3.3.2 User Accountability	✓	
		AU.L2-3.3.7 Authoritative Time Source	✓	
Configuration Management (CM)	2	CM.L2-3.4.3 System Change Management	✓	5
		CM.L2-3.4.7 Nonessential Functionality	✓	
Identification and Authentication (IA)	2	IA.L2-3.5.7 Password Complexity	✓	6
		IA.L2-3.5.8 Password Reuse	✓	
		IA.L2-3.5.9 Temporary Passwords	✓	
		IA.L2-3.5.10 Cryptographically-Protected	✓	
System and Communications Protection (SC)	2	SC.L2-3.13.6 Network Communication by Exception	✓	6
		SC.L2-3.13.11 CUI Encryption	✓	

Security Domain:
Identification and Authentication (IA)

Security Domain	Level	Requirement #	Requirement Statement	Assessment Objective	Autom ated Check
Identification and Authentication (IA)	1	IA.L1-b.1.vi Authentication [FCI Data]	Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances]	[a] Determine if the identity of each user is authenticated or verified as a prerequisite to system\access	✓

Security Domain:
System and Communications Protection (SC)

Security Domain	Level	Requirement #	Requirement Statement	Assessment Objective	Autom ated Check
Identification and Authentication (IA)	1	SC.L1-b.1.x Boundary Protection [FCI Data]	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems)	[c,d] Determine if communications are monitored at the external system boundary, and communications are monitored at key internal boundaries	✓
				[e,f] Determine if the identity of each user is authenticated or verified as a prerequisite to system\access	✓

Security Domain: Access Control (AC)

Security Domain	Level	Requirement #	Requirement Statement	Assessment Objective	Automated Check
Access Control (AC)	2	AC.L2-3.1.1 Authorized Access Control [CUI Data]	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	[d] Determine if system access is limited to authorized users	✓
		AC.L2-3.1.8 Unsuccessful Logon Attempts	Limit unsuccessful logon attempts.	[b] Determine if the defined means of limiting unsuccessful logon attempts is implemented	✓
		AC.L2-3.1.9 Privacy & Security Notices	Provide privacy and security notices consistent with applicable CUI rules.	[b] Determine if privacy and security notices are displayed	✓
		AC.L2-3.1.10 Session Lock	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	[b] Determine if access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity	✓
		AC.L2-3.1.12 Control Remote Access	Monitor and control remote access sessions.	[c] Determine if remote access sessions are controlled	✓
		AC.L2-3.1.13 Remote Access Confidentiality	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	[b]Determine if cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented	✓
		AC.L2-3.1.17 Wireless Access Protection	Protect wireless access using authentication and encryption	[a] Determine if wireless access to the system is protected using authentication	✓

Security Domain:
Audit and Accountability (AU)

Security Domain	Level	Requirement #	Requirement Statement	Assessment Objective	Autom ated Check
Audit and Accountability (AU)	2	AU.L2-3.3.1 System Auditing	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity	[c] Determine if audit records are created (generated)	✓
		AU.L2-3.3.2 User Accountability	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	[a,b] Determine if the content of the audit records needed to support the ability to uniquely trace users to their actions is defined; and audit records, once created, contain the defined content	✓
		AU.L2-3.3.7 Authoritative Time Source	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	[a] Determine if internal system clocks are used to generate time stamps for audit records	✓
				[c] Determine if internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source	✓

Security Domain:
Configuration Management (CM)

Security Domain	Level	Requirement #	Requirement Statement	Assessment Objective	Autom ated Check
Configuration Management (CM)	2	CM.L2-3.4.3 System Change Management	Track, review, approve or disapprove, and log changes to organizational systems.	[d] Determine if changes to the system are logged	✓
		CM.L2-3.4.7 Nonessential Functionality	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	[o] Determine if the use of nonessential services is restricted, disabled, or prevented as defined	✓

Security Domain:
Identification and Authentication (IA)

Security Domain	Level	Requirement #	Requirement Statement	Assessment Objective	Automated Check
Identification and Authentication (IA)	2	IA.L2-3.5.7 Password Complexity	Enforce a minimum password complexity and change of characters when new passwords are created.	[c] Determine if minimum password complexity requirements as defined are enforced when new passwords are created [d] Determine if minimum password change of character requirements as defined are enforced when new passwords are created	✓
		IA.L2-3.5.8 Password Reuse	Prohibit password reuse for a specified number of generations.	[b] Determine if reuse of passwords is prohibited during the specified number of generations	✓
		IA.L2-3.5.9 Temporary Passwords	Allow temporary password use for system logons with an immediate change to a permanent password.	[a] Determine if an immediate change to a permanent password is required when a temporary password is used for system logon	✓
		IA.L2-3.5.10 Cryptographically-Protected	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	[a] Determine if passwords are cryptographically protected in storage	✓

Security Domain:
System and Communications Protection (SC)

Security Domain	Level	Requirement #	Requirement Statement	Assessment Objective	Automated Check
Identification and Authentication (IA)	1	SC.L2-3.13.6 Network Communication by exception	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	[a] Determine if network communications traffic is denied by default	✓
		SC.L2-3.13.11 CUI Encryption	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	[a] Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI	✓

Why Titania

For more than a decade, elite cyber teams have relied on Titania's accurate network configuration assessment software, Nipper, to determine whether their routers, switches and firewalls leave their networks open to attack due to misconfigurations and exploitable vulnerabilities. Nipper helps organizations close these security gaps by automatically prioritizing risks by criticality, allowing users to view vulnerabilities through their chosen compliance and security policy lenses, and providing insights and advice that are proven to accelerate the mean time to remediate. Nipper's pass/fail compliance evidence also accelerates vulnerability assessment reporting, making it the tool of choice for many assessors.

Get in touch

Get in touch to arrange a demonstration of how to automate the process of assessing network infrastructure and prioritizing remediation based on CMMC risk.

titania.com/try/demo

USA
Suite 6500,
2451 Crystal Dr, 6th Floor,
Arlington, VA 22202

UK
167-169 Great Portland Street,
London, England,
W1W 5PF

TITANIA
www.titania.com