ArmorPoint's Coverage of CMMC Requirements

Drive CMMC Compliance Outcomes with ArmorPoint

WHAT IS THIS GUIDE FOR?

The Department of Defense introduced the Cybersecurity Maturity Model Certification, or CMMC, to strengthen cyber resilience across the defense industrial base (DIB). This guide shows how ArmorPoint's Managed Security Services support your organization's journey to CMMC compliance by addressing key controls across multiple domains.

UNDERSTANDING CMMC CONTROLS

CMMC outlines three certification levels, each including a set of practices mapped to a number of capability domains depending on the level. For example, CMMC Level 2 details 110 practices divided amongst 14 capability domains and ArmorPoint can help organizations align with the following:

Access Control (AC)
16 OF 22 PRACTICES

Maintenance (MA)
3 OF 6 PRACTICES

Audit and Accountability (AU)
8 OF 9 PRACTICES

Physical Protection (PE)
1 OF 6 PRACTICES

Incident Response (IR)
3 OF 3 PRACTICES

Security Assessment (CA)
3 OF 4 PRACTICES

Personnel Security (PS)

System and Information Integrity (SI)
7 OF 7 PRACTICES

Risk Assessment (RA)
3 OF 3 PRACTICES

Awareness and Training (AT)
3 OF 3 PRACTICES

System and Communications Protection (SC)
9 OF 16 PRACTICES

Identification and Authentication (IA)
7 OF 11 PRACTICES

Media Protection (MP)
4 OF 9 PRACTICES

Configuration Management (CM)
5 OF 9 PRACTICES

THE CLOSE UP

ArmorPoint helps meet these controls:

Shared Responsibility: *ArmorPoint can collaborate with your organization to implement changes in order to meet the practice.*

Covered by ArmorPoint: *ArmorPoint offers services that meet the practice and can provide evidence for audit requirements.*

Capability Domain	Practice ID	Practice Title	Responsibility
Access Control	**AC.1.001**	Limit system access to authorized users, processes, and devices	Shared Responsibility
	AC.1.002	Limit system access to allowed functions/ transactions	Shared Responsibility
	AC.1.003	Control external system connections	Shared Responsibility
	AC.1.004	Control public system information	Shared Responsibility
	AC.2.006	Restrict system resources to authorized entities	Shared Responsibility
	AC.2.007	Enforce least privilege	Shared Responsibility
	AC.2.008	Use non-privileged accounts for nonsecurity functions	Shared Responsibility
	AC.2.009	Limit unsuccessful logon attempts	Shared Responsibility
	AC.2.012	Monitor and control remote access sessions	Shared Responsibility
	AC.2.013	Protect remote sessions using cryptographic mechanisms	Shared Responsibility
	AC.2.014	Route remote access through managed control points	Shared Responsibility
	AC.2.015	Authorize remote execution of privileged commands	Shared Responsibility
	AC.2.016	Authorize wireless access prior to connections	Shared Responsibility
	AC.3.018	Restrict non-privileged users from executing privileged functions	Shared Responsibility
	AC.3.020	Protect mobile devices accessing CUI	Shared Responsibility
	AC.3.021	Restrict portable storage on external systems	Shared Responsibility

Capability Domain	Practice ID	Practice Title	Responsibility
Awareness & Training	**AT.2.056**	Inform users/admins of security risks	Shared Responsibility
	AT.2.057	Train personnel on their security responsibilities	Shared Responsibility
	AT.3.058	Provide insider threat awareness training	Shared Responsibility
Audit & Accountability	**AU.2.041**	Trace user actions to individuals	Covered by ArmorPoint
	AU.2.042	Create and retain system audit logs	Covered by ArmorPoint
	AU.2.043	Support audit review and reporting	Covered by ArmorPoint
	AU.3.045	Log nonlocal maintenance/diagnostics	Shared Responsibility
	AU.3.046	Alert on audit logging failure	Covered by ArmorPoint
	AU.3.047	Synchronize audit records	Covered by ArmorPoint
	AU.3.048	Provide audit reduction/reporting	Covered by ArmorPoint
	AU.3.049	Ensure audit logs aren't altered in reporting	Covered by ArmorPoint
Configuration Management	**CM.2.063**	Monitor user-installed software	Shared Responsibility
	CM.2.064	Enforce security configuration settings	Shared Responsibility
	CM.3.067	Restrict unnecessary services/functions	Shared Responsibility
	CM.3.068	Apply blacklist/whitelist policies	Shared Responsibility
	CM.3.069	Control unauthorized software installation	Shared Responsibility
Identification & Authentication	**IA.1.076**	Identify users/processes/devices	Shared Responsibility
	IA.1.077	Authenticate identities before access	Shared Responsibility
	IA.2.078	Use MFA for privileged/non-privileged access	Shared Responsibility
	IA.2.079	Use replay-resistant authentication	Shared Responsibility
	IA.2.080	Protect passwords with cryptography	Shared Responsibility
	IA.3.083	Use replay-resistant authentication servers	Shared Responsibility
	IA.3.086	Disable inactive identifiers	Shared Responsibility
Incident Response	**IR.2.092**	Establish incident-handling capability	Shared Responsibility
	IR.2.093	Track, report, and document incidents	Shared Responsibility
	IR.2.094	Test incident response capabilities	Shared Responsibility

Capability Domain	Practice ID	Practice Title	Responsibility
Maintenance	**MA.2.112**	Control maintenance tools/personnel	Shared Responsibility
	MA.3.113	Require MFA for remote maintenance	Shared Responsibility
	MA.3.116	Scan diagnostic/test media for malware	Covered by ArmorPoint
Media Protection	**MP.3.121**	Control removable media usage	Shared Responsibility
	MP.3.122	Prohibit unidentifiable portable storage	Shared Responsibility
	MP.3.123	Restrict external system portable storage	Shared Responsibility
	MP.3.125	Prohibit use of unowned portable storage	Shared Responsibility
Physical Protection	**PE.3.136**	Protect CUI at alternate work sites	Shared Responsibility
Risk Assessment	**RA.3.137**	Perform periodic risk assessments	Shared Responsibility
	RA.3.138	Conduct vulnerability scans	Shared Responsibility
	RA.3.139	Perform penetration testing	Shared Responsibility
Security Assessment	**CA.2.158**	Assess security controls periodically	Shared Responsibility
	CA.2.159	Implement POA&Ms for deficiencies	Shared Responsibility
	CA.3.161	Continuously monitor security controls	Shared Responsibility
System & Communications Protection	**SC.1.175**	Monitor/control system communications	Shared Responsibility
	SC.2.179	Prevent unintended data transfer	Shared Responsibility
	SC.2.180	Default-deny network traffic policy	Shared Responsibility
	SC.2.181	Prevent split tunneling	Shared Responsibility
	SC.2.182	Protect CUI in transit with cryptography	Shared Responsibility
	SC.3.186	Protect authenticity of sessions	Shared Responsibility
	SC.3.188	Use DNS filtering services	Shared Responsibility
	SC.3.189	Ensure CUI integrity in transit	Shared Responsibility
	SC.3.190	Use secure software/architecture	Shared Responsibility

Capability Domain	Practice ID	Practice Title	Responsibility
System & Information Integrity	**SI.1.210**	Identify, report, correct flaws	Shared Responsibility
	SI.1.211	Protect against malicious code	Covered by ArmorPoint
	SI.1.212	Update malware protection tools	Covered by ArmorPoint
	SI.2.213	Monitor system alerts/advisories	Shared Responsibility
	SI.2.214	Respond to unauthorized software detection	Shared Responsibility
	SI.2.215	Monitor traffic for threats	Covered by ArmorPoint
	SI.3.216	Employ spam protection at entry	Shared Responsibility

Why Choose ArmorPoint?

If your goal is to work within the Defense Industrial Base, it's imperative to remain a step ahead in cybersecurity readiness. Choosing ArmorPoint demonstrates a proactive, robust approach to safeguarding your organization's sensitive information. Our team is not just an auxiliary tool but a long-term partner equipped with the knowledge and foresight to scale solutions as your organization grows.

Don't let CMMC non-compliance prevent you from bidding on, or winning, a DoD contract. Partner with ArmorPoint to ensure your organization meets and maintains the robust requirements of CMMC 2.0.

Contact us today to get started.

ArmorPoint.

(877) 942-2568

sales@armorpoint.com

Speak with a solutions expert →