WASHINGTON PROCESS GROUP

CMMC Level 1 & Level 2 DIY Readiness Kit

Sample Preview

A structured DIY toolkit for DoD contractors and subcontractors preparing for CMMC Level 1 or Level 2 readiness requirements.

SAMPLE PREVIEW — LIMITED CONTENT

This is a limited sample preview. The full kit includes complete templates, trackers, and implementation support materials.

FULL KIT CONTENTS

What's Included in the Full Kit

The CMMC Level 1 & Level 2 DIY Kit includes structured tools and support materials organized around the full CMMC readiness process — from initial gap assessment through evidence organization and assessment preparation. The following is a high-level overview of what the full kit contains.

CMMC Level 1 & Level 2 Readiness Support	Structured tools covering both Level 1 (17 practices) and Level 2 (110 NIST SP 800-171 practices) requirements.
CMMC Readiness Checklist	A structured checklist covering Level 1 and Level 2 practice areas — organized so your team can track readiness status across each domain.
NIST SP 800-171 Alignment Support	Materials organized around the 14 NIST SP 800-171 practice families to support Level 2 gap assessment and documentation work.
System Security Plan (SSP) Template	SSP template structured for assessor review and aligned to NIST SP 800-171 requirements. Customized by your team to describe your environment.
Plan of Action & Milestones (POA&M) Tracker	Documents gaps identified in the assessment with milestones, responsible owners, and target dates.
Evidence Tracker	Organizes evidence artifacts by practice area — helping your team track what has been collected, where it lives, and who owns it.
Policy and Procedure Templates	Core cybersecurity policies and procedures aligned to CMMC practice families — ready to customize for your organization.
Implementation Roadmap	A phase-by-phase roadmap aligned to Level 1 and Level 2 requirements — giving your team a logical sequence for working through readiness activities.
Internal Review Support Tools	Tools to help your team self-assess readiness before engaging an assessor or submitting an SPRS score.

Note: This sample preview shows the format and structure of selected kit components only. Full templates, complete trackers, and all support materials are included in the purchased kit.

SAMPLE — READINESS CHECKLIST

Sample Readiness Checklist

The full kit includes a structured readiness checklist covering all applicable Level 1 and Level 2 practice areas. The sample below shows the format and column structure only — it does not represent the complete checklist.

CMMC Area	Sample Requirement	Example Evidence	Status	Notes
Access Control	Limit system access to authorized users	User access list, account policy documentation	In Progress	
Access Control	Control CUI access based on least privilege	Role-based access control documentation	Not Started	
Incident Response	Establish an incident response capability	Incident response plan document	Complete	
Configuration Mgmt	Establish baseline configurations	System configuration documentation	In Progress	
Identification & Auth	Enforce password complexity requirements	Password policy, authentication settings	Complete	
Media Protection	Protect system media containing CUI	Media handling policy and procedures	Not Started	
System & Comm. Prot.	Monitor and control comms at boundaries	Network diagram, firewall rules	In Progress	

SAMPLE ONLY — The full kit checklist covers all 17 Level 1 practices and all 110 NIST SP 800-171 Level 2 practices across all 14 domain families.

SAMPLE — EVIDENCE TRACKER

Sample Evidence Tracker

The full kit includes a structured evidence tracker to help your team identify, organize, and locate evidence artifacts for each practice area. The sample below shows the format only.

Requirement Area	Evidence Needed	Evidence Location	Owner	Status	Notes
Access Control	User access list and account review records	IT / SharePoint	IT Manager	In Progress	
Audit & Accountability	Audit log retention policy and sample logs	SIEM / Log system	Security Lead	Not Started	
Config. Management	System baseline documentation	IT Documentation folder	IT Manager	Complete	
Incident Response	Incident response plan and test records	Policy library	Compliance Lead	In Progress	
Media Protection	Removable media policy and inventory	HR / Policy folder	HR / IT	Not Started	
Personnel Security	Background check process documentation	HR records	HR Manager	Complete	
System & Comm. Prot.	Network boundary documentation and firewall rules	IT / Network docs	IT Manager	In Progress	

SAMPLE ONLY — The full evidence tracker covers all applicable practice areas across Level 1 and Level 2. This preview shows format and column structure only.

SAMPLE — POA&M TRACKER

Sample Plan of Action & Milestones (POA&M)

The full kit includes a POA&M tracker to document identified gaps, assign corrective actions, track owners, and manage target completion dates. The sample below shows the format only.

Gap / Finding	Risk Level	Corrective Action	Owner	Target Date	Status
Multi-factor authentication not implemented for remote access	High	Deploy MFA for all remote access connections	IT Manager	2026-03-31	In Progress
No formal incident response plan documented	High	Develop and approve incident response plan; conduct tabletop exercise	Compliance Lead	2026-02-28	Not Started
Audit log retention policy not formally documented	Medium	Document log retention requirements; configure SIEM settings	IT Manager	2026-03-15	In Progress
Removable media policy not in place	Medium	Draft and approve media protection policy; communicate to staff	HR / IT	2026-04-15	Not Started
System baseline configuration not documented	Medium	Document baseline configs for all in-scope systems	IT Manager	2026-03-31	In Progress

SAMPLE ONLY — The full POA&M tracker covers all identified gaps across the complete gap assessment. This preview shows format, column structure, and example entries only.

SAMPLE — POLICY TEMPLATE

Sample Template Preview: Access Control Policy

SAMPLE PREVIEW

The following is a partial excerpt from the Access Control Policy template included in the full kit. Actual template language must be customized to reflect your organization's specific environment, systems, and controls.

ACCESS CONTROL POLICY — SAMPLE PREVIEW ONLY

1. Purpose

This policy establishes requirements for controlling access to [Organization Name] information systems and the Controlled Unclassified Information (CUI) processed, stored, or transmitted on those systems. The purpose of this policy is to ensure that access to organizational systems and CUI is limited to authorized users, processes acting on behalf of authorized users, and authorized devices.

2. Scope

This policy applies to all [Organization Name] employees, contractors, and third-party users who access organizational information systems. It applies to all systems that process, store, or transmit Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).

3. Responsibilities

System Administrator: Responsible for implementing technical access controls, managing user accounts, and enforcing least-privilege access configurations.

Manager / Supervisor: Responsible for initiating access requests for direct reports and notifying IT of personnel changes requiring access modification or removal.

All Users: Responsible for protecting assigned credentials and reporting suspected unauthorized access.

4. Sample Policy Statements

4.1 Access to [Organization Name] information systems shall be granted on a least-privilege basis. Users shall be provided only the access required to perform their assigned job functions.

4.2 All user accounts shall be uniquely identified. Shared or generic accounts are prohibited except where technically required and explicitly approved by [designated authority].

4.3 Multi-factor authentication (MFA) shall be required for all remote access connections to organizational systems that process or store CUI.

[Additional policy sections, enforcement provisions, exception process, review schedule, and approval signatures are included in the full template.]

SAMPLE ONLY — This is a partial excerpt for preview purposes. The full Access Control Policy template and all other policy templates are included in the purchased kit.

INTENDED AUDIENCE

Who This Kit Is For

The CMMC Level 1 & Level 2 DIY Kit is designed for organizations that need a structured, practical path to CMMC readiness and want to manage the work internally using templates, trackers, and implementation tools.

- Small businesses in the DoD supply chain preparing for Level 1 or Level 2 requirements
- Government contractors handling Federal Contract Information (FCI) or Controlled Unclassified Information (CUI)
- Subcontractors with CMMC flow-down requirements from prime contractors
- Organizations preparing for CMMC Level 1 self-assessment and SPRS score submission
- Organizations working toward a Level 2 C3PAO assessment and needing structured pre-assessment documentation
- Teams that need templates, trackers, and a structured roadmap before or instead of working with a full-service consultant
- Organizations that want to own their compliance program internally and understand their own documentation

LIMITATIONS

What This Kit Does Not Replace

This kit is a structured DIY readiness and documentation support resource. It is important to understand what it is not intended to provide.

- Does not guarantee CMMC certification or assessment success
- Does not replace a C3PAO assessment for Level 2 requirements
- Does not replace legal, technical, or cybersecurity advisory services
- Does not constitute compliance consulting or managed implementation
- Does not write your SSP, POAM, or policies — your team customizes and completes the templates
- Does not engage assessors or coordinate with government bodies on your behalf

GET THE FULL KIT

Purchase the Complete CMMC Level 1 & Level 2 DIY Kit

CMMC Level 1 & Level 2 DIY Readiness Kit

Washington Process Group

Full Kit Price

$1,697

One-time purchase · Instant digital download · Self-paced

The full kit includes the complete CMMC readiness checklist, gap assessment tool mapped to all 110 NIST SP 800-171 practices, System Security Plan template, POA&M tracker, evidence tracker, cybersecurity policy and procedure templates, implementation roadmap, and internal review support tools.

Visit washingtonprocessgroup.com/cmmc to purchase the full CMMC Level 1 & Level 2 DIY Kit.

washingtonprocessgroup.com

Full Kit Includes — Complete Components

CMMC Readiness Checklist	All Level 1 and Level 2 practice areas — complete
Gap Assessment Tool	Mapped to all 110 NIST SP 800-171 practices across 14 domains
System Security Plan Template	Structured for assessor review — customized by your team
POA&M Tracker	Full tracker with all gap, owner, date, and status fields
Evidence Tracker	Complete evidence tracking across all practice areas
Policy & Procedure Templates	Core cybersecurity policies aligned to CMMC practice families
Implementation Roadmap	Phase-by-phase from gap assessment to assessment readiness
Internal Review Support Tools	Self-assessment support before engaging a C3PAO or submitting SPRS

Washington Process Group | washingtonprocessgroup.com | yolanda@washingtonprocessgroup.com