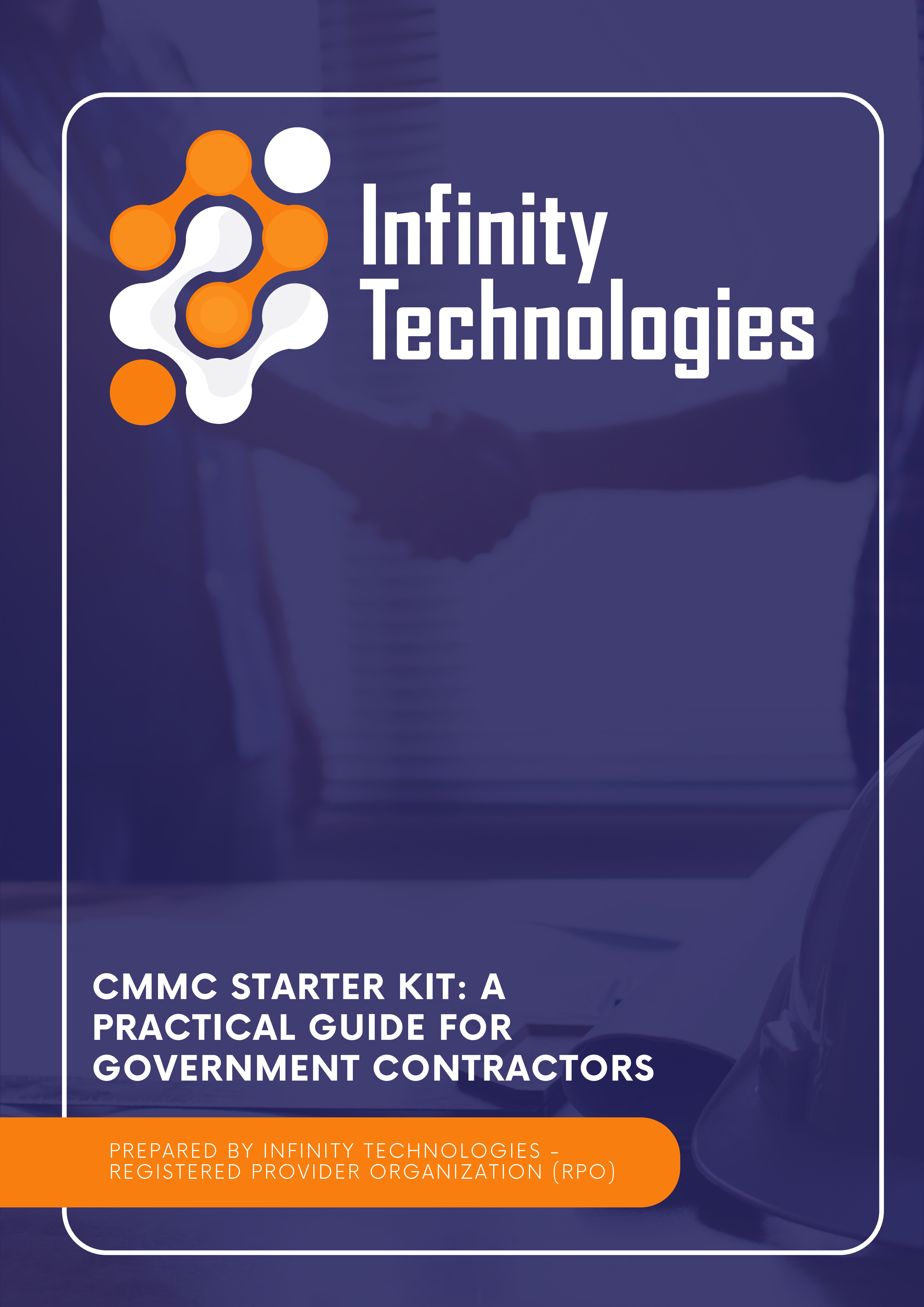

Infinity Technologies

CMMC STARTER KIT: A PRACTICAL GUIDE FOR GOVERNMENT CONTRACTORS

PREPARED BY INFINITY TECHNOLOGIES - REGISTERED PROVIDER ORGANIZATION (RPO)

IN THIS GUIDE

Infinity Technologies

GETTING STARTED WITH CMMC 2.0

The Cybersecurity Maturity Model Certification (CMMC) 2.0 program officially went into effect on December 16, 2024. For small and medium businesses in the defense industrial base, understanding CMMC requirements and taking the first steps toward compliance can feel overwhelming.

This starter kit provides the essential tools you need to begin your CMMC journey with confidence.

ICYMI: Key Facts About CMMC 2.0

Three Levels: CMMC has three certification levels (Level 1, 2, and 3)

Most Common: Level 2 applies to contractors handling Controlled Unclassified Information (CUI)

Based on NIST: Level 2 requirements are built on NIST SP 800-171 Rev. 2 (110 controls)

Phased Implementation: CMMC requirements will be phased into DoD contracts over time

Assessment Required: Most contractors need third-party assessment by a Certified Third-Party Assessment Organization (C3PAO)

Why Start Now?

If you haven't started yet, it's not too late to pursue CMMC compliance. The sooner you start, the sooner you'll get to reap the rewards.

·Prime contractors are already requiring CMMC compliance from subcontractors

·Assessment preparation typically takes 6-12 months for most organizations

·Early compliance provides a competitive advantage in contract opportunities

·Delays increase costs and limit future contract eligibility

Infinity Technologies

CMMC SCOPING CHECKLIST

Proper scoping is the foundation of an efficient and cost-effective CMMC compliance program. Use this checklist to get a better idea of what systems and data are in scope for your CMMC assessment.

Data Identification

Federal Contract Information (FCI) - Level 1

☐ Identify all systems that process, store, or transmit FCI

☐ Document where FCI enters your organization

☐ Map FCI flow through your systems and processes

☐ Identify where FCI is stored (cloud, on-premises, mobile devices)

Controlled Unclassified Information (CUI) - Level 2

☐ Identify all systems that process, store, or transmit CUI

☐ Document CUI marking and handling procedures

☐ Map CUI data flows from receipt to disposal

☐ Identify who has access to CUI and why

System Inventory

In-Scope Systems Assessment

☐ List all computers that process, store, or transmit FCI/CUI

☐ Identify network infrastructure supporting FCI/CUI systems

☐ Document cloud services used for FCI/CUI

☐ Map mobile devices accessing FCI/CUI

☐ Identify backup and recovery systems for FCI/CUI

Network Boundaries

□ Define your CMMC Assessment Scope Boundary

□ Identify systems outside the boundary

□ Document network connections between in-scope and out-of-scope systems

□ Plan network segmentation if needed

Access Control Review

User Access

□ List all users with access to FCI/CUI systems

□ Document user roles and responsibilities

□ Identify privileged users and administrators

□ Review contractor and vendor access requirements

Physical Access

□ Identify physical locations where FCI/CUI is processed

□ Document who has physical access to these areas

□ Review physical security controls (locks, cameras, etc.)

Documentation Requirements

Current State

□ Inventory existing security policies and procedures

□ Document current technical controls (firewalls, antivirus, etc.)

□ Review current training programs

□ Assess current incident response capabilities

Infinity Technologies

CMMC TIMELINE PLANNER

Every business's CMMC compliance timeline is going to look different. This timeline aims to give you a general idea of how long you can expect each stage of the journey to last. Adjust timeframes based on your organization's size and complexity.

Months 1-2: Assessment and Planning

Week 1-2: Initial Scoping

- Complete scoping checklist
- Engage a CMMC consultant/RPO
- Define assessment scope boundary

Week 3-4: Gap Assessment

- Conduct a formal gap assessment against NIST SP 800-171
- Identify priority remediation areas
- Estimate implementation costs and timeline

Week 5-8: Planning and Budgeting

- Develop a detailed implementation plan
- Secure budget approval
- Select vendors and tools
- Create project timeline

Months 3-6: Implementation Phase 1

Technical Controls Implementation

- Deploy essential security tools (MFA, endpoint protection, etc.)
- Implement network segmentation if required
- Configure backup and recovery systems
- Deploy logging and monitoring tools

Policy Development

- Develop required security policies
- Create incident response procedures
- Document system security plan (SSP)
- Establish training programs

Months 7-9: Implementation Phase 2

Advanced Controls

- Complete remaining technical implementations
- Conduct security awareness training
- Implement access control procedures
- Test incident response processes

Documentation and Evidence

- Complete all required documentation
- Collect implementation evidence
- Conduct internal readiness review
- Address any remaining gaps

Months 10-12: Assessment Preparation

Pre-Assessment Activities

- Engage C3PAO for assessment
- Complete practice assessment/readiness review
- Address any final gaps and update the SSP
- Prepare assessment artifacts

Official Assessment

- Undergo C3PAO assessment
- Address any findings
- Receive CMMC certification
- Plan for ongoing compliance

Ongoing: Maintenance

Continuous Compliance

- Maintain security controls
- Conduct regular training
- Monitor for changes requiring reassessment
- Plan for 3-year recertification

Infinity Technologies

ESSENTIAL CMMC GLOSSARY

Assessment Terms

C3PAO (Certified Third-Party Assessment Organization): Organizations authorized to conduct CMMC Level 2 and Level 3 assessments.

CMMC Assessment Scope: The boundaries of the assessment, including all systems that process, store, or transmit FCI or CUI.

POA&M (Plan of Action and Milestones): Documentation of planned actions to correct deficiencies and reduce or eliminate vulnerabilities.

RPO (Registered Provider Organization): Organizations registered to help contractors prepare for CMMC assessments and maintain compliance.

Data Classifications

CUI (Controlled Unclassified Information): Information that requires safeguarding or dissemination controls but is not classified.

FCI (Federal Contract Information): Information provided by or generated for the government that is not intended for public release.

SPRS (Supplier Performance Risk System): DoD system where contractors report their cyber security implementation status.

Technical Terms

Enclave: An isolated network environment designed to protect sensitive information.

MFA (Multi-Factor Authentication): Authentication method requiring two or more verification factors.

Network Segmentation: Dividing a network into smaller segments to limit access and contain potential breaches.

SIEM (Security Information and Event Management): Technology that provides real-time analysis of security alerts.

Compliance Framework Terms

DFARS 252.204-7012: The Defense Federal Acquisition Regulation Supplement clause requiring implementation of NIST SP 800-171.

NIST SP 800-171: National Institute of Standards and Technology publication defining security requirements for protecting CUI.

System Security Plan (SSP): Document describing security controls implemented or planned for an information system.

YOUR NEXT STEPS

Congratulations on taking the first step toward CMMC compliance! Here's how to move forward:

Immediate Actions (This Week)

- Complete the Scoping Checklist - Use the checklist in this guide to understand your current environment
- Assess Your Timeline - Determine when you need to be CMMC compliant based on your contracts
- Engage Expert Help - Partner with a Registered Provider Organization (RPO) for guidance

Short-Term Actions (Next Month)

- Conduct Gap Assessment - Get a professional evaluation of your current compliance posture
- Develop Implementation Plan - Create a detailed roadmap for achieving compliance
- Secure Resources - Ensure you have the budget and personnel needed for success

Infinity Technologies

Why Choose Infinity Technologies as Your RPO?

As a Registered Provider Organization, Infinity Technologies specializes in helping small and medium government contractors achieve CMMC compliance efficiently and cost-effectively. Our team understands the difficulties government contractors in the defense industrial base are facing when it comes to navigating ever-growing compliance demands – and we're here to lighten the load.

Our Services Include:

- Comprehensive gap assessments
- CMMC scoping and implementation planning
- Technical control implementation
- Policy development and documentation
- Assessment preparation and support
- Ongoing compliance maintenance

Why Government Contractors Choose Us:

- Specialized expertise in CMMC for smaller contractors
- Focus on right-sizing solutions to your actual needs
- Cost-effective approaches that don't break your budget
- Local presence serving Virginia's defense industrial base
- Proven track record with successful CMMC implementations

Ready to Get Started?

Don't let CMMC compliance overwhelm your business. Our expert team is ready to guide you through every step of the process, from initial scoping to successful certification and beyond.

Free Consultation Available - Schedule a no-obligation consultation to discuss your specific CMMC needs and learn how we can help accelerate your compliance journey.

This guide provides general information about CMMC requirements. For specific compliance guidance tailored to your organization, consult with qualified CMMC professionals.