CMMC Backstop Readiness Self-Assessment

Nine questions to help you identify potential gaps before beginning the CMMC assessment process.

CMMC compliance involves detailed cybersecurity requirements, documented policies, and evidence that your organization consistently follows its established processes.

This quick readiness assessment is designed to help you identify areas that may require attention. Answer each question based on what your organization can verify today, not what you believe is probably happening.

Select Yes, No, or Unsure for each question.

1. MFA (Multi-Factor Authentication)

Does your organization require multi-factor authentication to access email, remote systems, and critical business applications, not just as an option, but enforced for all users?

☐ **Yes** ☐ **No** ☐ **Unsure**

2. Backups & Ransomware Survivability

Are your backups stored in a location separate from your primary systems, and have you tested a full restore within the past 12 months?

☐ **Yes** ☐ **No** ☐ **Unsure**

3. Endpoint Detection

Does your organization actively use managed endpoint protection that detects behavioral threats, not just traditional antivirus, across all workstations and servers?

☐ **Yes** ☐ **No** ☐ **Unsure**

4. Incident Response Readiness

Does your organization have a written, tested incident response plan with defined roles for who does what in the first hours of a cyberattack or breach?

☐ **Yes** ☐ **No** ☐ **Unsure**

5. Patch Management

Are security patches applied to all systems within a defined, tracked timeframe, and is someone provided with reporting to confirm compliance?

☐ **Yes** ☐ **No** ☐ **Unsure**

6. Access Control & Offboarding

When an employee is terminated or resigns, are all system and application access revoked on the same day, and can you confirm this is consistently followed?

☐ **Yes** ☐ **No** ☐ **Unsure**

7. Security Awareness Training

Do all employees receive cybersecurity awareness training at least annually, including simulated phishing tests with follow-up for those who fail?

☐ **Yes** ☐ **No** ☐ **Unsure**

8. Email Security

Does your organization have effective controls in place to filter spam, suspicious emails, malicious links, impersonation attempts, and messages designed to trick employees into sharing sensitive information?

☐ **Yes** ☐ **No** ☐ **Unsure**

9. Executive Visibility & IT Program Efficacy

Does your leadership team receive regular, meaningful reporting on the status of open security risks, remediation progress, and the overall effectiveness of your IT program, not just when something goes wrong?

☐ **Yes** ☐ **No** ☐ **Unsure**

How Did Your Business Do?

If you answered No or Unsure to any question, your organization may have security, documentation, or oversight gaps that could affect its CMMC readiness.

intelliSystems can help you determine what is missing, establish the appropriate safeguards and documentation, and prepare your organization for CMMC Level 1 or Level 2 self-assessment requirements.

TALK WITH A CMMC READINESS PROFESSIONAL

Contact intelliSystems at **(706) 722-2024** or visit **intelliSystems.com/CMMC-Compliance** to discuss your next steps.

This readiness questionnaire is an educational resource and is not an official CMMC assessment, certification, or guarantee of compliance. CMMC requirements vary based on the information an organization handles and its contractual obligations.

Learn more: Review the official CMMC assessment requirements in 32 CFR Part 170.