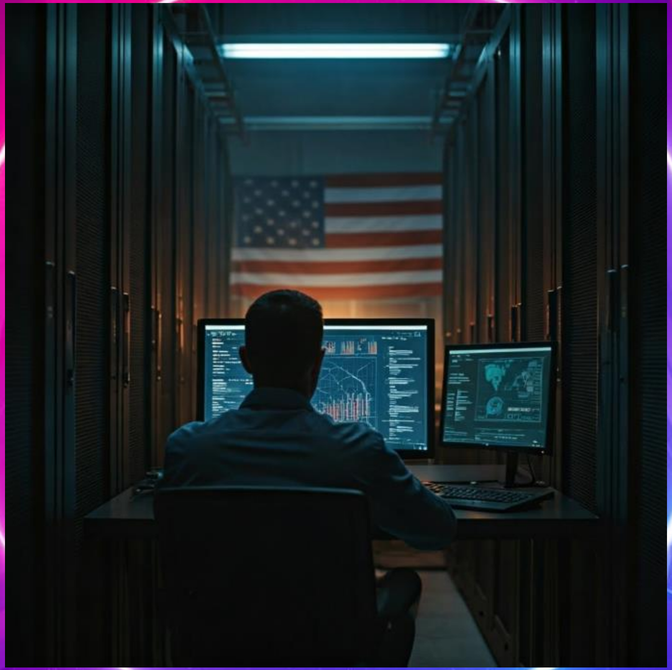


The Compliance Officer's Essential Corporate Environment DOD-Compliant Cybersecurity Checklist

DFARS, NIST SP 800-171, & CMMC COMPLIANCE MASTERY SIMPLIFIED

INTRODUCTION

Navigating the complexities of DFARS, NIST SP 800-171, and CMMC 2.0, alongside SOC 2 and ISO 27001, can be a daunting task for compliance officers in small defense contractors and regulated industries.

This checklist is designed to simplify your journey, providing a practical, step-by-step guide to achieving and maintaining compliance in your corporate environment.

At SecRed Knowledge Inc., we understand these challenges firsthand. We are actively working towards becoming a C3PAO, having achieved self-assessed CMMC Level 1 status, and are committed to sharing our insights and expertise to help you succeed.

This checklist is specifically tailored for organizations like yours, focusing on the core requirements for protecting sensitive information within your corporate IT infrastructure.

1. UNDERSTANDING THE REGULATORY LANDSCAPE

□ Review and comprehend the full text of DFARS 252.204-7012, NIST SP 800-171, and CMMC 2.0 requirements.

Resource: [Links to official NIST, DoD, and CMMC resources] LEAD MAGNET LANDING PAGE

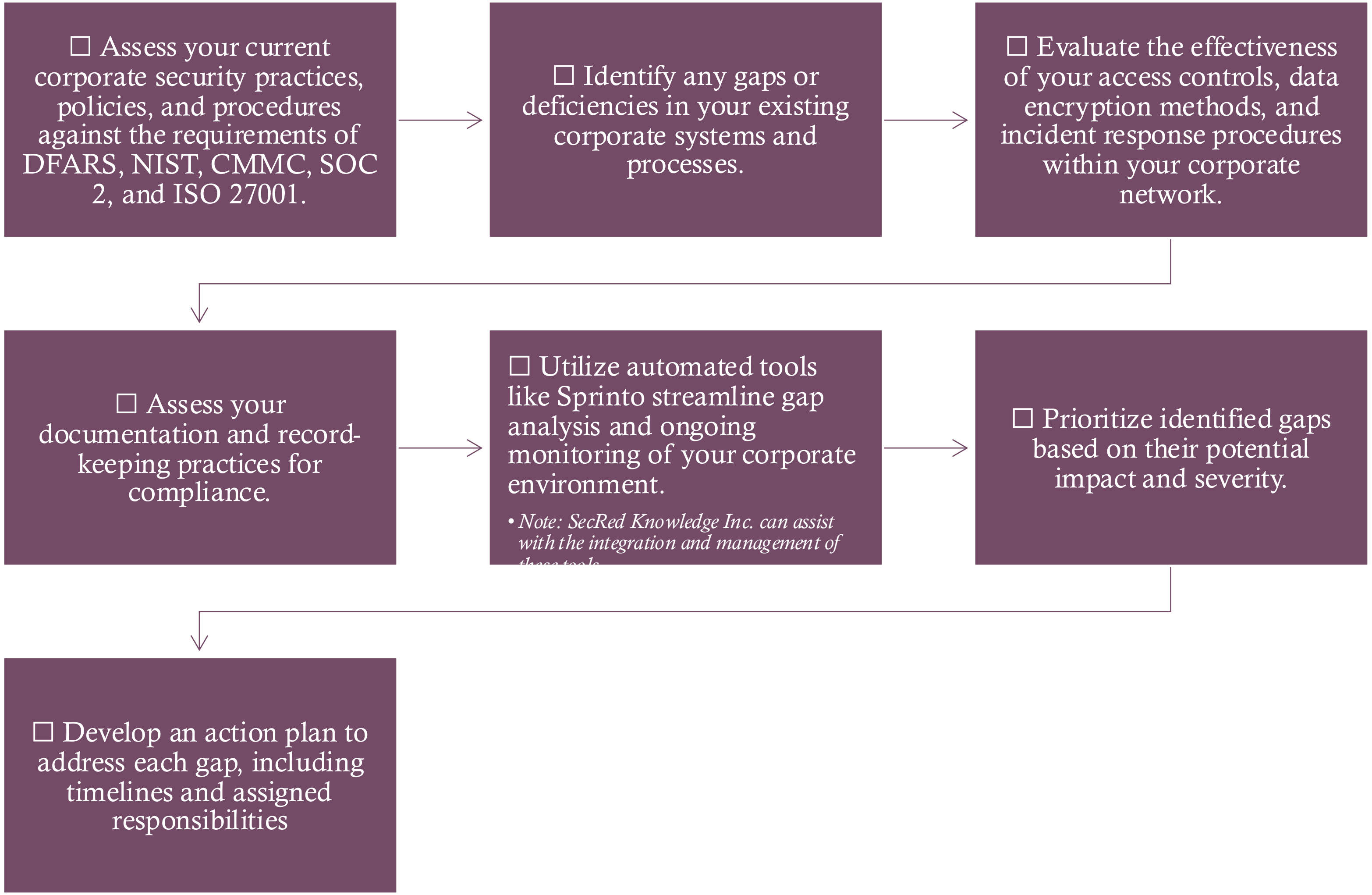
□ Determine the applicability of these regulations to your organization and specific contracts, focusing on how they affect your corporate network, systems, and data.

□ Identify the specific controls and safeguards outlined in NIST SP 800-171 and CMMC 2.0 that are relevant to your corporate environment (e.g., access control, data encryption, incident response).

□ Understand the requirements for SOC 2 and ISO 27001 and how they align and overlap with DFARS/NIST/CMMC in the context of corporate compliance.

□ Familiarize yourself with compliance deadlines and reporting requirements.

2. CONDUCTING A COMPREHENSIVE GAP ANALYSIS



☐ Assess your current corporate security practices, policies, and procedures against the requirements of DFARS, NIST, CMMC, SOC 2, and ISO 27001.

☐ Identify any gaps or deficiencies in your existing corporate systems and processes.

☐ Evaluate the effectiveness of your access controls, data encryption methods, and incident response procedures within your corporate network.

☐ Assess your documentation and record-keeping practices for compliance.

☐ Utilize automated tools like Sprinto streamline gap analysis and ongoing monitoring of your corporate environment.

- *Note: SecRed Knowledge Inc. can assist with the integration and management of these tools*

☐ Prioritize identified gaps based on their potential impact and severity.

☐ Develop an action plan to address each gap, including timelines and assigned responsibilities

3. DEVELOPING AND IMPLEMENTING A ROBUST SYSTEM SECURITY PLAN (SSP)

☐ Define the scope of your SSP based on the requirements of DFARS, NIST, and CMMC, specifically addressing your corporate IT infrastructure.

☐ Identify the categories of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) your organization handles within its corporate systems.

☐ Assess the risks associated with the storage, processing, and transmission of CUI/FCI within your corporate environment.

☐ Document the security controls required to protect CUI/FCI within your corporate network, including hardware, software, and data.

☐ Assign responsibility for the implementation and oversight of each security control.

☐ Establish corporate policies and procedures to ensure employees understand their roles and responsibilities in safeguarding CUI/FCI.

☐ Develop incident response procedures to address security breaches and data breaches within your corporate environment.

☐ Regularly review and update your SSP to reflect changes in technology, regulations, or organizational requirements.

4. IMPLEMENTING AND MAINTAINING EFFECTIVE SECURITY CONTROLS

□ Implement the specific security controls required by NIST SP 800-171 and CMMC 2.0 within your corporate environment.

□ Utilize robust Identity and Access Management & Privilege Access Management (IAM/PAM) solutions, such as *EVO Security*, to control access to corporate resources.

□ Implement AI-driven endpoint and network protection for all corporate devices using solutions like *Heimdal Security* and/or *HPE Inc* security products powered by hybrid cloud HPE GreenLake.

□ Secure corporate applications and APIs with WAF tools like *Indusface*.

□ Ensure secure remote access to the corporate network with solutions like *OpenVPN* and/or All-In-One Platform like *Heimdal Security*.

Note: SecRed Knowledge Inc. can help you integrate and manage these security tools as part of our CaaS formula.

□ Implement monitoring and auditing mechanisms to track user activities and detect suspicious behavior on the corporate network.

□ Regularly patch and update software, firmware, and operating systems on all corporate devices and servers.

5. TRAINING AND EDUCATING EMPLOYEES/C-SUITE

☐ Develop a comprehensive training program covering DFARS, NIST, CMMC, SOC 2, and ISO 27001 compliance, tailored to the responsibilities of employees within a corporate setting.

☐ Ensure all employees understand their roles and responsibilities in maintaining compliance within the corporate environment.

☐ Educate employees on the proper handling of CUI/FCI, including storage, transmission, and disposal, within corporate systems.

☐ Train employees on recognizing and reporting potential security incidents, such as phishing attempts or malware infections, targeting corporate assets.

☐ Provide regular updates and refresher training sessions.

☐ Establish clear guidelines on acceptable use of company devices and networks.

6. ESTABLISHING INCIDENT RESPONSE AND REPORTING PROCEDURES

- □ Create an incident response plan outlining the steps to be taken in the event of a security incident within your corporate environment.
- □ Establish a dedicated incident response team or designate responsible individuals.
- □ Clearly define roles and responsibilities within the incident response team.
- □ Implement mechanisms for monitoring and detecting security incidents within your corporate network and systems.
- □ Establish protocols for documenting and preserving evidence.
- □ Ensure incident response procedures align with regulatory requirements and industry best practices.

7. CONTINUOUS MONITORING AND UPDATES

- □ Establish a compliance monitoring program to regularly assess the effectiveness of your compliance efforts within your corporate environment.
- □ Conduct periodic compliance audits or assessments.
- □ Review and update policies, procedures, and documentation to reflect changes in regulations.
- □ Monitor changes in your organization's operations, systems, or processes that may impact compliance.
- □ Utilize automated compliance tools like Sprinto to streamline monitoring and reporting.
- □ Engage with compliance experts to stay informed about industry best practices.

8. COLLABORATING WITH COMPLIANCE EXPERTS

☐ Recognize the value of working with compliance experts to navigate the complexities of regulatory requirements.

☐ Consider SecRed Knowledge Inc. as a partner in your compliance journey, leveraging our CaaS formula and experience.

Note: As a soon-to-be Veteran-Owned Small Business (VOSB), we offer unique advantages for federal contractors.

☐ Collaborate with us to develop a tailored compliance strategy that integrates security and automation for your corporate environment.

SECRED KNOWLEDGE INC.'S CMMC 2.0 JOURNEY

- As we navigate the CMMC 2.0 process, we're gaining invaluable firsthand experience. We're committed to sharing our insights and helping other organizations achieve compliance. Our goal is to become a C3PAO, and this checklist reflects our dedication to providing practical guidance to organizations like yours.
- **What's Next ? Taking Action… Success Like Speed, Strategic & Tactical Speed!**
- Ready to simplify your compliance efforts for your corporate environment?
- Contact SecRed Knowledge Inc. today to learn how our CaaS formula can help you achieve and maintain compliance: https://www.secredknowledgeinc.tech/contact
- Book a Call with The Expert vCISO, Creator of CaaS Formula behind our Compliance Enablement Work: https://www.calendly.com/cybersouhimbou
- Resources on next page

RESOURCES LINKS

- **SecRed Knowledge Inc:** https://www.secredknowledgeinc.tech
- **DoD Resources:**
- **DoD CMMC Website:** https://dodcio.defense.gov/CMMC/
- **CMMC Resources & Documentation:** https://dodcio.defense.gov/cmmc/Resources-Documentation/
- **NIST Resources:**
- **NIST SP 800-171:** https://csrc.nist.gov/pubs/sp/800-171/r2/final
- **NIST Cybersecurity Program:** https://www.nist.gov/cyberframework
- **CMMC Resources:**
- **CMMC Accreditation Body:** https://cyberab.org/