IronOrbit
The Cloud Made Simple.

UNDERSTANDING NIST 800-171 AND CMMC LEVEL 2 COMPLIANCE

A Guide to Certification

As cybersecurity threats continue to grow, the U.S. Department of Defense (DoD) has begun to implement stricter compliance requirements to protect Controlled Unclassified Information (CUI).

Two key frameworks that businesses handling DoD contracts must understand are NIST 800-171r2 and CMMC 2.0. In this document, we will break down these compliance standards, explore the certification process, and discuss the role of authorized third-party vendors.

What is NIST 800-171?

The National Institute of Standards and Technology (NIST) Special Publication 800-171r2 establishes security requirements for protecting CUI in non-federal systems and organizations. It includes 14 control families covering areas such as access control, incident response, and system integrity.

Organizations handling CUI must comply with NIST 800-171r2 to meet federal cybersecurity standards. While self-assessment was previously acceptable, the Cybersecurity Maturity Model Certification (CMMC) 2.0 introduces a more stringent verification process.

Call us at: **714-777-3222** or send us an email at: **info@ironorbit.com**

Follow for More!

WHAT IS CMMC 2.0?

CMMC, or the Cybersecurity Maturity Model Certification, is a DoD program designed to enhance cybersecurity across the defense industrial base (DIB). CMMC 2.0 streamlines requirements into three levels (Level 1, Level 2 (low & high, Level 3. CMMC 2 Level 2 aligns closely with NIST 800-171r2 and is the most common requirement for organizations handling CUI.

Whereas in the past (and with L2 low) a self-assessment was required for registration, contracts now specifying CMMC Level 2 High in the organizational handling of CUI, require third-party assessments. This ensures that companies have effectively implemented the 110 security controls specified in NIST 800-171r2.

THE PROCESS TO BECOME CMMC LEVEL 2 CERTIFIED

Achieving CMMC Level 2 certification is a multi-step process that requires significant preparation.

Below is a breakdown of the key steps:

1. **Conduct a Preliminary Discovery and Gap Readiness Assessment**

   Before undergoing a formal audit, organizations should perform discovery in the form of an internal gap assessment against NIST 800-171r2 requirements.

   This helps identify gaps in security practices and build a remediation plan to address missing controls and vulnerabilities.

2. **Close the GAP**

   Build the system, policies, and procedures and deploy solutions and remediate to build a framework to meet controls that when nearing compliance can be built into a SSP.

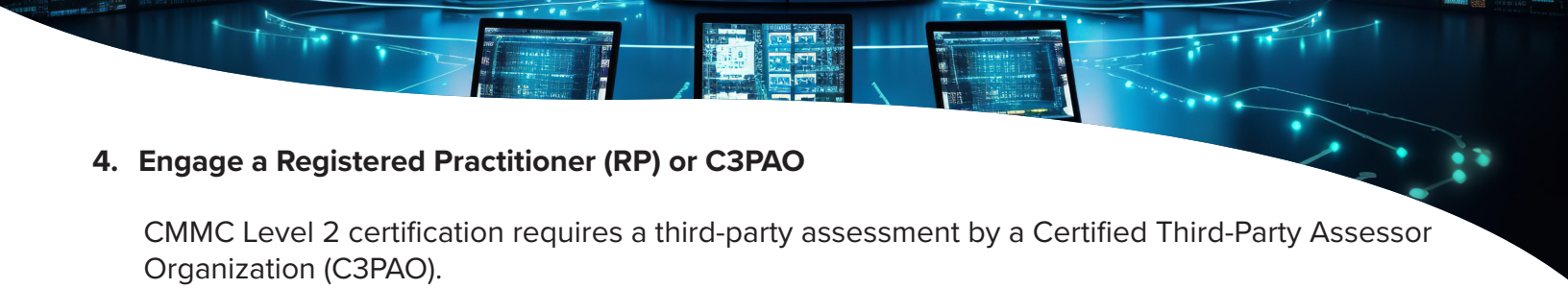
3. **Develop a System Security Plan (SSP) and POA&M**

   A critical component of compliance is the System Security Plan (SSP), which documents how an organization implements security controls.

   If any gaps exist, a Plan of Action and Milestones (POA&M) outlines the steps to remediate deficiencies.

Call us at: **714-777-3222** or send us an email at: **info@ironorbit.com**

Follow for More!



4. **Engage a Registered Practitioner (RP) or C3PAO**

   CMMC Level 2 certification requires a third-party assessment by a Certified Third-Party Assessor Organization (C3PAO).

   With the gap mitigated and a SSP developed, organizations can work with a Registered Practitioner (RP) to review readiness prior to engaging a C3PAO.

   Recently, for those with higher confidence, there is an option to have an engaged C3PAO perform a pre-audit to ensure they meet all requirements before the official audit.

5. **Undergo a Third-Party Assessment**

   A C3PAO conducts an in-depth evaluation to verify compliance with all 110 NIST 800-171r2 controls.

   The assessment typically includes:

   • Interviews with personnel
   • Review of security documentation
   • Technical testing of security controls

   If the organization passes, it receives CMMC Level 2 certification, allowing it to handle DoD contracts requiring CUI protection.

   If there are gaps (to non-major controls), a POA&M for each item must be developed, and the certification becomes pending completion of those action plans.

6. **Maintain Compliance and Continuous Monitoring**

   Certification is not a one-time process; organizations must continuously monitor and improve their security posture.
   Regular self-assessments, employee training, and updates to security policies are essential to maintaining compliance.

How Many Vendors Can Perform CMMC Level 2 Certification?

Only authorized C3PAOs can conduct CMMC Level 2 assessments. The Cyber AB (formerly the CMMC Accreditation Body) maintains a list of approved C3PAOs.

As of now, the number of accredited C3PAOs remains limited, creating high demand for their services.

Organizations should begin the certification process early to secure an assessment slot, as the demand for C3PAO services is expected to increase as CMMC enforcement expands.

Key Takeaways

- NIST 800-171r2 defines 110 security controls to protect CUI.
- CMMC 2.0 aligns with NIST 800-171r2 and the most common Level 2 high requires third-party assessments.
- Preparation requires in depth internal discovery and gap analysis to substantially prepare technical solutions, remediations, policy, procedure and training.
- The certification process includes readiness assessments, SSP documentation, third-party audits, and continuous monitoring.
- Only accredited C3PAOs can conduct CMMC Level 2 assessments, and availability is limited.

Final Thoughts

CMMC 2.0 Level 2 certification is essential for businesses that handle CUI and seek to secure DoD contracts. Understanding the requirements, preparing in advance, and engaging with a qualified C3PAO can streamline the certification process. As the DoD strengthens cybersecurity compliance enforcement, organizations must proactively ensure their security frameworks align with NIST 800-171r2 and CMMC 2.0 Level 2 requirements.

IronOrbit is CMMC 2.0 L2 ready, delivering secure, compliant cloud solutions that help businesses confidently meet stringent requirements. Our Virtual Chief Information Security Officer (vCISO) program enables companies to proactively prepare for, remediate, and achieve compliance.

IronOrbit
The Cloud Made Simple.

IronOrbit is Recognized in the 2023 and 2024 Gartner Magic Quadrant for DaaS (Desktop as a Service) and is included in the 2021 & 2023 Gartner Market Guide for DaaS.

Call us at: **714-777-3222** or send us an email at: **info@ironorbit.com**

Follow for More!