ITGlue

Checklist: Steps to Ensure Successful CMMC Compliance

The Cybersecurity Maturity Model Certification (CMMS) was introduced by the Department of Defense (DoD) to provide the necessary frameworks against the rising cyberthreats across the globe. Any company that does business with the Defense Industrial Base (DIB) must fully comply with the CMMC and obtain the required certification. MSPs catering to these companies must prepare their clients to be compliant with these regulations.

This checklist outlines the steps you must take to ensure successful CMMC compliance.

Assess Your Controlled Unclassified Information (CUI)

- [ ] The first step towards achieving CMMC compliance is to determine what part of your data is subject to CMMC. You need to identify where your data is:
  - [ ] Stored
  - [ ] Processed
  - [ ] Transmitted

Identify Applicable NIST Controls

- [ ] After assessing your CUI environment, you need to identify which of them fall within the scope of NIST 800-171. Based on whether they store, process or transmit CUI, this includes:
  - [ ] Systems
  - [ ] Services
  - [ ] Processes
- [ ] Segmented CUI environments will only have controls applicable to sub-networks whereas simple networks can have controls applied universally across the entire organization.

Determine the Required CMMC Maturity Level

- [ ] There are five levels of CMMC, with each level building upon the last. For instance, Level 2 requirements include all requirements for Level 1. Companies can check out the DoD Requests for Information (RFIs) to know the level of CMMC compliance required for a bid.
- [ ] Since the requirement for CMMC maturity differs from contract to contract, companies must strive to reach the highest level of CMMC certification possible for them.

Identify Internal Stakeholders

- [ ] This includes executive sponsors, IT and Information Security Department.
- [ ] If your team is light on internal resources, it may be beneficial early in the process to identify a registered provider organization (RPO).

Create Policies, Standards and Procedures

- [ ] Policy prescriptions are likely to change based on the level of risk. You must prepare by determining the different compliances applicable to your organization. This includes:
  - [ ] Domestic and international cybersecurity and privacy laws
  - [ ] Industry-specific regulations
  - [ ] Legally binding contracts
- [ ] Documentation is critical when it comes to maintaining compliance. You must clearly write out a hierarchical structure that includes various:
  - [ ] Policies
  - [ ] Standards
  - [ ] Controls
  - [ ] Procedures

Leverage Existing Frameworks

- [ ] The lower levels of CMMC compliance often overlap with many existing standards and regulations.
- [ ] For instance, if a company is compliant with NIST Special Publication 800-171, it is already compliant with CMMC levels 1 and 2.
- [ ] Your existing compliance framework could be a great starting point for your CMMC.

Document the CUI Environment

- [ ] Note the CUI environment's controls and known deficiencies by building out two primary documents:
  - [ ] System Security Plan (SSP) – This provides answers for all the relevant details including who, what, when, why and where. It will include information on the various people, technology solutions and processes contained within the CUI environment.
  - [ ] Risk Register or Plan of Action & Milestones (POA&M) – This highlights all of the control deficiencies for the NIST 800-171.

Remediate Any Gaps

- [ ] After identifying your target CMMC level and your existing controls from other frameworks, you can then fill the gaps between existing measures and remaining CMMC controls.

Obtain CMMC Certification

- [ ] The CMMC Accreditation Body handles the certification process in direct coordination with DoD. You can obtain your certification from independent CMMC third-party assessment organizations that are accredited by both these agencies.

How IT Glue Supports your Compliance Efforts

IT Glue is a cloud based, SOC 2 (Type II) compliant documentation platform that enables your business to securely store and document your compliance policies, processes, controls and evidence, linked together with relationship mapping and an immutable audit trail.

One of IT Glue's core values is trust. IT Glue champions complete vigilance for the privacy and security of information. We take our internal processes and compliance with industry-level security standards seriously. Through our platform, IT Glue offers you a way to effortlessly maintain the integrity and safety of your data and documents. By embedding security features into our software and maintaining rigorous adherence to our third-party audits, we continue to provide you with the documentation services your business requires on a daily basis.

Request a Demo

itglue.com