7 Steps to Cybersecurity Maturity Model Certification (CMMC)

Step 1: Define CUI specific to the contract and identify where it is stored, processed and transmitted.

Your first step is to identify the "CUI Environment" which is where Controlled Unclassified Information (CUI) is stored, processed and transmitted. For your specific situation, CUI is defined by the US Government's contracting official for the prime contractor. Prime contractors are required to identify CUI in contracts to its sub-contractors. Everything starts with knowing what the CUI environment is - it defines the systems, services and processes that are in scope for NIST 800-171.

So what exactly is CUI? Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. CUI is a broad category that encompasses many different types of sensitive, but not classified information. For example, personally identifiable information such as health documents, proprietary material and information related to legal proceedings would all count as CUI.

If you don't know what your CUI is, ask your contracting officer or prime.

Step 2: Based on the CUI environment, identify applicable NIST 800-171 controls. By doing this you will now be able to identify what systems, services and processes are in scope for NIST 800-171, based on storing, processing or transmitting CUI.
Out of the 110 CUI and 62 Non-Federal Organization (NFO) controls, you now need to identify what controls are applicable to your CUI environment. For simple/flat networks, it is likely that all controls will be applicable across the entire organization. For segmented CUI environments, most controls should only be applicable to those sub-networks and not every system across the organization.

You can reference FirstTeamCyber's NIST 800-171 Compliance Scoping Guide for CUI for guidance on this process.

Step 3: Documentation is the foundation of any governance program and it requires written policies, standards, controls and procedures. Well-designed documentation is hierarchical and builds on supporting components to enable a strong governance structure that utilizes an integrated approach to managing requirements. Understanding the hierarchy of cybersecurity documentation can lead to well-informed risk decisions, which influence technology purchases, staffing resources, and management involvement.

7 Steps to Cybersecurity Maturity Model Certification (CMMC)

You will need to develop policies, standards and procedures to address cybersecurity compliance requirements while identifying all applicable laws, regulations and contracts that your organization is required to comply with. This includes both domestic and international cybersecurity and privacy laws, industry-specific regulations and legally-binding contract requirements from clients and partners (e.g., NIST 800-171 or CMMC). Ample due diligence is required to find what is right for your unique situation.

All too often, documentation is not scoped properly, and this leads to the governance function being viewed as more of an obstacle as compared to being an asset. Documentation should be concise, clearly-written and have direct mapping to all compliance requirements. A multiple-page "policy" document that blends high-level security concepts (e.g., policies), configuration requirements (e.g., standards), and work assignments (e.g., procedures) is an example of poor documentation that leads to confusion and inefficiencies across technology, cybersecurity, and privacy operations.

Step 4: In this step, responsible parties for specific CUI controls need to be identified and roles/responsibilities for those individuals/teams need to be defined, so that requirements do not "fall through gaps" or are improperly implemented due to misunderstandings of who is responsible for certain controls.

Operationalize the policies & standards to implement NIST 800-171/CMMC controls. Implementing NIST 800-171 controls is "where the rubber meets the road" from a compliance perspective - this is where the combination of people, processes and technology (P-P-T) come together to operationalize a cybersecurity and privacy program. Essentially, addressing NIST 800-171 controls bring your policies and standards to life by implementing the exact requirements necessary to comply.

Step 5: Document the CUI environment, its controls and any known deficiencies. This step is where the System Security Plan (SSP) and Plan of Action & Milestones (POA&M) are populated with details – both are "living documents" that continue to get updates as changes impact the CUI environment. These two documents are central to documenting a NIST 800-171 compliance program:

The SSP is meant to be a repository for the who, what, how, when, why & where information – it documents the people, processes and technologies (P-P-T) about the CUI environment. The POA&M is essentially a "risk register" for NIST 800-171 control deficiencies.

You can expect that both the SSP and POA&M's will be key artifacts that a CMMC auditor will ask for in order to understand your CUI environment. The SSP & POA&M's are requirements for

7 Steps to Cybersecurity Maturity Model Certification (CMMC)

NIST 800-171 compliance, so lacking these documents will be considered non-compliant that could have significant negative consequences (e.g., False Claims Act (FCA) violation).

Step 6: It is important to keep in mind that a "perfect" risk methodology does not exist to assess risk across technology and business processes. What matters is that the risk methodology chosen best supports how the organization actually functions. It is acceptable to have a different risk methodology used for tactical, operational and strategic risk decisions, since each methodology has its own strengths and weaknesses. The goal is to define and attain a level of optimal risk taking.

Leverage the controls to assess both risk and maturity across technology and business processes. There are numerous methodologies available for an organization to manage risk. These risk models range from NIST 800-37 to FAIR, ISO 31010, OCTAVE and others. What is similar between these risk methodologies is they all have to assess how well controls are implemented and the extent that risk is reduced from the control's existence and level of maturity.

Managing risk is a process that must exist across all phases of the Secure Development Lifecycle (SDLC), regardless if the solution being worked on is a system, application or service. The scope of assessing risk must consider not only the immediate assets in the scope of the SDLC, but those supporting systems, processes and possibly third-party service providers that impact confidentiality, integrity, availability and safety aspects.

Step 7: Utilize metrics from control execution to identify areas of improvement. The concept of "monitoring controls" is synonymous with gathering metrics. While metrics are a point-in-time snapshot into a control's performance, the broader view of metrics leads to longer-term trend analysis. It is through this trend analysis that your organization's leadership can identify areas of improvement. This can be done through defining Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to have insights into the controls that are particularly important to the organization. KPIs and KRIs will differ between organizations, due to varying priorities assigned to controls from variations in statutory, regulatory and contractual obligations that affect the relative importance of certain controls.

Step 7 is required to meet maturity levels 4 and 5. Call First Team Cyber today for your detailed cybersecurity compliance and risk management assessment.

Contact us today!

First Team Cyber, LLC | 877- 684-TEAM (8326) | info@FirstTeamCyber.com | www.FirstTeamCyber.com