Partners
Audits Without Anxiety®

CMMC Audit Checklist

STEP 1: Identify the type of information that needs to be protected.

Identify the FCI, CUI, and CDI that will need to be handled as part of the DoD contract. In addition to the information itself, you will also need to determine how the information would be processed, stored, and transmitted since the CMMC auditor will evaluate this information closely.

The information that needs to be protected will be defined in the contract information of the DoD project. If you are unsure whether the data you handled qualifies as CUI or CDI, you can get information from the contracting official for DoD (or the prime contractor if you are a subcontractor).

STEP 2: Identify the controls to be implemented.

Since CMMC is related to controls specified in DFARS and NIST SP 800-171, you will need to identify the systems, processes, and services that are in the scope of these frameworks.

For these systems, processes, and services, you will need to identify the controls that are applicable. The controls to be applied will also depend on the type of data being handled and the target CMMC level.

STEP 3: Identify the regulatory requirements to address CMMC compliance.

You will need to identify the domestic and international laws and regulations applicable to your organization in the context of the DoD contract. This includes cybersecurity regulations, industry-specific regulations, data privacy and protection laws, etc.

STEP 4: Create relevant documentation.

Documentation is important from the perspective of a CMMC audit. The controls being implemented, policies, and procedures need to be adequately documented. Documentation will not only help in providing the necessary information to the CMMC auditor but will also be useful in making organizational decisions about managing risks.

STEP 5: Implement the cybersecurity controls.

Implementing cybersecurity controls applicable to the organization will require aligning people, processes, policies, etc. It will be a step to improve the cybersecurity maturity and be ready for the CMMC audit.

To implement appropriate NIST SP 800-171 and CMMC controls effectively, identify the right people in charge of each environment in scope and define roles and responsibilities related to implementing controls and measuring their effectiveness.

STEP 6: Create POA&M and SSP.

Sometimes, it might not be possible to implement all applicable NIST SP 800-171 and CMMC controls. In this case, the control deficiencies need to be documented in a POA&M (Plan of Action and Milestones). The POA&M is a time-bound document and will have an action plan to address the control deficiencies within 180 days of the assessment.

Similarly, you will also need to create a System Security Plan (SSP) which will detail how each control will be useful fo improving the cybersecurity posture. Both POA&M and SSP are important documents that a CMMC auditor will check.

STEP 7: Evaluate the effectiveness of the implemented controls.

You can choose an appropriate risk management methodology to get a better view of security risks and evaluate how the implemented controls would reduce or remove the identified risks. Any third-party risks also need to be taken into account and the effectiveness of the controls needs to be determined.

STEP 8: Monitor and improve controls.

Tracking key metrics is an effective way to monitor CMMC controls. Metrics can also help understand long-term trends that can help in identifying areas of improvement. You will need to identify Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) relevant to your organization and the controls being implemented. The KPIs and KRIs