Compliance NIST (National Institute of Standards and Technology Framework)

CMMC certification-preparation process, and once certified, helps you document your ongoing compliance to the standard. CMMC stands for “Cybersecurity Maturity Model Certification”. There are 5 levels of certification under this standard, with the vast majority of contracts to require Levels 1-3.

CMMC Module is purpose-built and addresses Levels 1-3 assessments as well as the DoD NIST 800-171 Self-Assessment. This module also generates detailed compliance reporting that document the CMMC controls that have been implemented in preparation of certification by a Certified Third-Party Assessment Organization.

CMMC Manager provides the scans and documentation you need:

Interim Rule Primary Documents

NIST 800-171 Scoring Supplement Worksheet

This is a temporary worksheet that “bridges the gap” of 800-171 controls that are not already covered by the CMMC Level 2 certification requirements. First complete the Level 2 CMMC assessment built into Compliance Manager, and then complete this supplemental scoring worksheet. The documents will be automatically combined, analysed and used to create the final self-assessment scorecard.

Plan of Action & Milestones (POA&M)

The POA&M is a requirement of the Interim Rule and includes information about security control implementation weaknesses and gaps found during the assessment, lists the any mitigating steps the contractor intends to make in order to fully implement, along with a specific deadline for completion. This document is provided in Excel format, and follows the DoD’s best practices template.

System Security Plan (SSP)

The System Security Plan (SSP) is the most important document in the event of an audit. IT sums up the system description, system boundary, architecture, and security controls in one document. The SSP document generated by Compliance Manager follows the exact format as prescribed in best practice templates supplied by the DoD.

NIST 800-171 DoD Assessment Score Report

This report is a line-item scorecard showing the results of the implementation review of each of the 110 controls included in NIST (SP) 800-171, and the total score based on the Department of Defense’s official scoring rubri, with a starting maximum score of 110, and specified deductions made for non-implementation of a given control. A summary score is provided for each of the 14 main control families, and then for each individual control, it lists in tabular fashion: The NIST control ID number, security requirement description, control implementation status, amount deducted (if not implemented), and comments (if applicable).

Primary Reports Documents

CMMC Level 3 Policy and Procedures

The CMMC Level 3 requires the client to generate and maintain a comprehensive written IT Security Compliance Policies and Procedures manual. I must list all of the IT Security policies that the company has in place to protect its network environment and data, along with specific descriptions of how each policy is implemented and measured. For organizations that don't have a set of data protection policies – or at least one that conforms to CMMC requirements, this report provides an "out of the box" version of policies and procedures that they can use or start with.

CMMC Evidence of Compliance Compiles compliance information from automated scans, augmented data, and questionnaires. Gathers evidence into one document to back up the CMMC Assessor Checklist with real data.

CMMC Risk Analysis

CMMC Risk Analysis is the foundation for the entire CMMC compliance and IT security program. The CMMC Risk Analysis identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of sensitive data at rest and/or during its transmission.

CMMC Risk Treatment Plan

Based on the findings in the CMMC Compliance Assessment, the organization must create a Risk Treatment Plan with tasks required to minimize, avoid, or respond to risks. Beyond gathering information, CMMC Manager provides a risk scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources and ensure that issues identified are issues solved. The Risk Treatment plan defines the strategies and tactics the organization will use to address its risks.

CMMC Assessor Checklist

The CMMC Assessor Checklist gives you a high-level overview of how well the organization complies with the CMMC (Cybersecurity Maturity Model Certification) requirements. The checklist details specific compliance items, their status, and helpful references. Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Supporting Documents

External Vulnerability Scan Detail by Issue

Detailed report showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

CMMC Windows Patch Assurance Report

The CMMC Windows Patch Assurance Report helps verify the effectiveness of the client's patch management program. The report uses scan data to detail which patches are missing on the network.

CMMC Login History Report

This report presents user login history by computer to enable workforce members responsible for IT Security to audit access to computers connected to a company's network. Quite useful, in particular, for looking at a commonly accessed machines (file server, domain controller, etc.) – or a particularly sensitive "CUI" computers that are used to collect, process, transmit, or store CUI for failed login attempts.

CMMC Full Detail Excel Export

The CMMC Full Detail Excel Export includes every detail uncovered during the CMMC assessment's network and computer endpoint scanning process. Details are presented in line-item fashion in an editable Excel workbook document. The report is organized by titled worksheets to help you locate the specific findings of interest, and problem areas are conveniently highlighted in red, making it easy to spot individual problems to be rectified.

CMMC Risk Update Assessment Reports

External Vulnerability Scan Detail

Detailed report showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

CMMC Risk Treatment Plan Update

Based on the findings in the CMMC Risk Update Assessment, the organization must create a CMMC Risk Treatment Plan with tasks required to minimize, avoid, or respond to identified risks to IT security.

The CMMC Risk Treatment Plan Update contains a list of tasks that can be executed to mitigate identified IT Security risks.

CMMC Change Summary Report

Every time you use Compliance Manager for CMMC to run a CMMC Risk Update Assessment on a given network, Compliance Manager for CMMC generates the CMMC Change Summary report.

This report compares the results the last Full CMMC Assessment with the Risk Update Assessment's network scan, local computer scan(s), and external vulnerability scan results performed during the Risk Update Assessment process.

This report details changes in the network's User Accounts, Local Computer Accounts, Active Directory (A/D) Computers, Non-A/D Computers, Non-A/D Devices, External Vulnerabilities, along with a Windows computer Patch Summary.

CMMC Risk Analysis Update

The CMMC Risk Analysis Update report lists IT Security risks identified during a Risk Update Assessment that impact the state of IT network security. The CMMC Risk Analysis Update identifies what protections are in place and where there is a need for more.

The CMMC Risk Analysis Update report presents results in a list of items that must be remediated to ensure the security and confidentiality of sensitive or confidential information at rest and/or during its transmission

Worksheet Documents

Documents generated at the end of a CMMC Assessment vary based on the Level of CMMC Controls assessed based on CMMC Level 3 Assessments

CMMC Antivirus Verification Worksheet

Compliance Manager will automatically detect any anti-virus software installed on PCs on the target network. The Anti-virus Verification Worksheet details whether each endpoint on the network has anti-virus software installed. It also displays the type of anti-virus software.

CMMC Application Inventory Worksheet

This worksheet is used to document the “necessity” of the applications identified as being installed on the computer endpoints operating within the network.

CMMC User Access Review Worksheet

The User Access Worksheet is used to augment the user data that was collected during the internal network scan. Complete the worksheet to provide the additional information requested.

CMMC Asset Inventory Worksheet

The Asset Inventory Worksheet is used to augment the asset data that was collected during the internal network scan. Details include the asset owner, acceptable use, environment, backup agent status, as well as device and asset criticality classification. The asset criticality classification is used to determine the risk to the organization in the event of a security incident where the asset’s access or availability is compromised.

CMMC External Information System Worksheet

This worksheet is used to document external information systems used by your organization. Add entries for each external information system along with a description, purpose for using the system, name of the business owner of the system, along with its criticality. Examples of external information systems include Salesforce, QuickBooks Online, and Office 365.

CMMC External Port Use Worksheet

This worksheet allows you to document business justifications for all of the allowed external ports, the protocol configured to use a specific port, and the documentation of any insecure configurations implemented and in use for a given protocol.

CMMC Access Control Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Access Control” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Identification and Authentication Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Identification and Authentication” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Media Protection Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Media Protection” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Physical Protection Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Physical Protection” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC System and Communications Protection Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “System and Communications Protection” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC System and Information Integrity Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “System and Information Integrity” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Awareness and Training Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Awareness and Training” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Audit and Accountability Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Audit and Accountability” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Configuration Management Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Configuration Management” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Incident Response Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Incident Response” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Maintenance Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Maintenance” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Personnel Security Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Personnel Security” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Recovery Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “recovery” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Risk Management Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Risk Management” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Security Assessment Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Security Assessment” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Asset Management Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Asset Management” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Situational Awareness Worksheet

This worksheet is used to collect information required to demonstrate compliance with the CMMC “Situational Awareness” control domain requirements that cannot be discovered and assessed through automated scans.

CMMC Level 3 Policy and Procedures

The CMMC Level 3 requires the client to generate and maintain a comprehensive written IT Security Compliance Policies and Procedures manual. I must list all of the IT Security policies that the company has in place to protect its network environment and data, along with specific descriptions of how each policy is implemented and measured. For organizations that don’t have a set of data protection policies – or at least one that conforms to

CMMC requirements, this report provides an “out of the box” version of policies and procedures that they can use or start with.