CMMC Level 1 Do-It-Yourself (DIY) Product Description

Do-It-Yourself Kit

CMMC Level 1

Update after all Testing complete

KAMIND IT, Inc.
5200 Meadows Rd, STE. 150
Lake Oswego, OR 97035

Contents

Document Change and Review History

Version Number	Summary of Changes	Changes Made/ Reviewed By	Date
Ver. 1	Document created	Krystal Williamson	January 24th, 2023

History

Brief overview of CMMC

There are currently thousands of organizations that provide services and products to the government through the form of government contracts. These organizations/contracts are collectively known as the Defense Industrial Base (DIB). The governing agency overseeing these contracts is the Department of Defense (DoD).

In order to assist the DIB with protecting this sensitive contract and service information, the National Institute of Standards and Technology (NIST) published a list of 110 controls (NIST SP 800-171) in 2015. In 2016, the DoD passed the DFARS clause 252.204-7012 to provide additional safeguards including mandatory reporting requirements and providing the DoD investigative access to facilitate damage control in the event of a breach. Neither of these documents required the use of a third party assessment before the contractor could begin performing work.

The DoD realized that in order to verify contract information was being properly safeguarded, an additional framework utilizing a third-party assessment was needed. This is where the CMMC (Cybersecurity Maturity Model Certification) was developed to verify organizations had mature and sufficient processes and environments to protect contract information. In 2020, the first rule was announced and a 2025 deadline set for achieving certification.

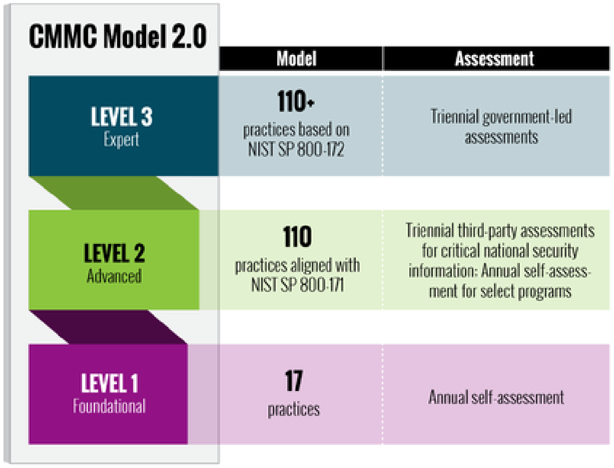
FCI vs. CUI

Not all contract information is treated with the same sensitivity. It became necessary to define differing levels of classification in order to later identify the safeguards needed to protect this information.

The Federal Register defines Federal Contract Information (FCI) as “information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.” For example, the Government posting a requisition seeking an organization to provide engine parts would not be FCI as it has been announced to the public. However, once the Government has found a vendor (let’s name this vendor EngineB) and signed a contract but *has not released that information publicly*, EngineB would be privy to FCI as no other organization is aware they have obtained a federal contract and what the details of that contract includes. (Federal Register :: Federal Acquisition Regulation; Basic Safeguarding of Contractor Information Systems)

NIST has defined Controlled Unclassified Information (CUI) as “Information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.” To elaborate on our example from the previous paragraph, whatever specifications, product descriptions, and materials EngineB creates as a result of their contract would be considered CUI. *CUI is considered more sensitive than FCI* and thus should be treated with a higher level of care. (controlled unclassified information (CUI) - Glossary | CSRC (nist.gov))

CMMC Levels



CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

In implementing CMMC, the DoD realized differing levels of controls were needed depending on the sensitivity of information the contractor was privy to.

CMMC Level 1 is focused on safeguarding FCI. Level 1 is comprised of 6 domains (also referred to as "families") with 17 practices (also referred to as "controls"). Each practice may contain qualifying requirements (known as "objectives"), each of which must be met in order for the control to be passed. Organizations must perform and report yearly self-assessments proving alignment with the framework.

CMMC Level 2 is focused on safeguarding CUI and is thus more comprehensive in scope. Level 2 is comprised of 14 domains with 110 practices. These 110 practices contain over 300 objectives. Additionally, organizations must be assessed by a CMMC Third-Party Assessment Organization (C3PAO) to achieve the initial certification and every third year after to maintain certification. In the years between third party assessments, organizations are required to perform and report self-assessments.

CMMC Level 3 will be an additional certification for organizations handling CUI, but details have not yet been released on further requirements.

Purpose

The purpose of this product is to provide assistance and framework for Organizations Seeking Certification (OSCs) needing CMMC Level 1. This product is a Do-It-Yourself (DIY) Kit for preparing an organization for readiness and provides futher explanation on the requirements, examples of templated policies that can be modified to match the client's environment, and work instructions on how to gather evidence.

Target Audience

The target audience for this product is an operational IT manager at a small business (20-100 users) needing to become CMMC L1 compliant. The organization is relatively small and needing certification, however they don't have a large compliance budget. They are looking for help in knowing what to do and are conscientious of time/money it takes to implement. They may either be underwater and looking for help or have a drive for knowledge and want ownership in the process.

Assessment Ready Clarification

This product approaches certification readiness with a strategy of policy documentation as well as providing evidence of practices.

The client should be aware when performing assessments that CMMC considers both "accuracy" and "sufficiency" when proving evidence of meeting the control. "Accuracy" refers to whether the policy/evidence appropriately addresses the intent of the control. For example, a Paid Time Off policy uploaded as proof of meeting the "Physical Protection" domain would not be considered accurate. Uploading a copy of the organization's policy of badge access with evidence showing records of badge access logs would be accurate. "Sufficiency" refers to whether the policies and evidence are comprehensive enough to satisfy the intent of the objective. Uploading a screenshot of one organizational unit entitled "HR Employees" as the only evidence for the "Identification and Authentication" control requiring identification of system users would not be sufficient (assuming the organization has more than just HR employees). Uploading a copy of the organization's policy regarding employee identification and authentication methods, while also uploading several screenshots of employee lists from both current HR records and the system's Active Directory (AD) showing synchronicity between systems would be sufficient.

Scope

What is Included

The DIY Kit includes:

- A copy of the CMMC Level 1 Self-Assessment Guide
- A copy of the CMMC Self-Assessment Scope
- 10 hours of consulting time
- An instructional playbook
- A proposed timeline for implementation (to be confirmed with client)
- A CMMC DIY Compliance Checklist
- An Assessment Information Collection Document to be completed by client and provided to assigned KAMIND compliance analyst
- 6 templated policies for each of the domains
- FutureFeed Level 1 subscription for 12 months
- List of other resources available for helping with Level 1 readiness

Consulting

The 10 hours of consultation are broken down into the following functions

- 1 hour is dedicated to an initial assessment of the organization's policies, procedures, and initial evidence
- 2 hours are dedicated to reviewing updated client documentation

- 6 hours are dedicated to client check-ins, including providing feedback on updated documentation, answering questions, and providing instruction for the next domain.
- There is 1 hour remaining that the client can utilize to their discretion. Examples of what you may want to use that hour for include adding another hour for discussing a challenging domain, performing a final assessment of materials, assisting with the self-reporting process, etc.

What is not included

KAMIND IT makes no claims or assertions that an organization will achieve certification after using this product. To do so would be a breach of the CMMC Code of Professional Conduct. The purpose of this product and any other consultation service is to prepare the organization for readiness, but no organization (including KAMIND IT) should be guaranteeing clients will achieve certification as a result of using those services.

This product does not include document writing or revision. It is the client's responsibility to prepare any documentation and evidence. The consultant assigned will review and provide feedback on any resources provided, but will not be responsible for contributing to the actual production of documents.

This service does not include the assigned consultant gathering evidence. For Microsoft environments, the consultant may provide advice and/or limited work instructions on where to go in the system to gather evidence, however the consultant will not be the one to gather evidence directly.

It needs to be overstated there are certain domains the client will ultimately always be responsible for, despite Microsoft or Azure licensing. This includes owning documentation and ensuring they have appropriate documentation management. This also includes some domains that cover physical protection, networking, physical media protection, and publishing of information to the public.

This service also does not include support for on-premise infrastructure. We can provide consulting and research potentially if the client has questions about their on-premise infrastructure, but as KAMIND deals primarily in cloud products, it needs to be overstated we are simply providing for CMMC requirements and make no claims or assertions that their on-premise/physical infrastructure meets the requirements.

Requirements

In order to best guide the client, KAMIND IT requires the client have an MS 365 E5 licensing subscription as well as an MS Azure subscription. It is assumed the client is working with a Windows 10 or 11 operating system.

Pricing

CMMC Level 1 DIY Kit

This kit costs $5~~3~~500

Packaging

2 options available: Digital or Sent via mail

Primary focus will be digital delivery via FutureFeed.

Are there additional options available?

Additional items would be turned into a 1) project and/or 2) subscription covered in an SOW. The scope would have to be very defined and controlled with either assigned hours and/or charging per hour. Options include:

1. Gap analysis for CMMC Level 1
    a. Primary focus would be on verifying controls set up with Azure/Microsoft cloud products
    b. Items included:
        i. Initial SPRS score
        ii. Report detailing findings and recommendations
        iii. Access to FutureFeed
        iv. Plan of Action and Milestone (POA&M) for unmet controls and assistance with organization into projects
    c. Risk: it would need to be overcommunicated that KAMIND specializes in AZ/MS cloud products. We can perform a basic gap analysis on all of the controls but are very dependent on the client providing sufficient evidence for physical, on-premise infrastructure, and any external connections that KAMIND does not support. Additionally, KAMIND makes no claims for depth of knowledge with on-premise equipment and recommendations.
2. Gap analysis for CMMC Level 2
    a. Primary focus would be on verifying controls set up with Azure/Microsoft cloud products
    b. Items included:
        i. Initial SPRS score
        ii. Report detailing findings and recommendations
        iii. Access to FutureFeed
        iv. Plan of Action and Milestone (POA&M) for unmet controls and assistance with organization into projects
    c. Risk: it would need to be overcommunicated that KAMIND specializes in AZ/MS cloud products. We can perform a basic gap analysis on all of the controls but are very dependent on the client providing sufficient evidence for physical, on-premise infrastructure, and any external connections that KAMIND does not support. Additionally, KAMIND makes no claims for depth of knowledge with on-premise equipment and recommendations.
3. Guard deployment for technical implementation of 9 out of 17* (see list below) controls
    a. Additional benefits include that this is a CMMC 1+ implementation and KAMIND will help with alerting and incidence response.
4. Guard deployment with CMMC Level 1 readiness assessment consulting
    a. It is recommended client transition to a fully cloud-environment utilizing Microsoft and Azure products.
    b. Included in Guard deployment with impact on CMMC L1
        i. Determining if each implementation/current service is configured based on Microsoft documentation – this leads to inherited compliance from Microsoft and Azure
        ii. Security alerting by KAMIND
        iii. Access to FutureFeed
        iv. Also included is determining POA&Ms and helping organizing into projects
5. Fortress-G technical implementation for ___ out of 110 controls* (see list below) (KAMIND is still determining Shared Responsibility Matrix)
6. Fortress-G deployment with CMMC Level 2 readiness assessment consulting
    a. ONLY for cloud products. We would recommend transitioning client to fully cloud-environment utilizing Microsoft and Azure products with a Guard deployment

Formatted: Highlight

i. Determining if each implementation/current service is configured based on Microsoft documentation – this leads to inherited compliance from Microsoft and Azure
ii. Security alerting by KAMIND
iii. Access to FutureFeed
iv. Also included is determining POA&Ms and helping organizing into projects

Controls KAMIND can provide support for in Level 1 with a Guard Implementation

- Access Control
  - AC.L1-3.1.1 – Authorized Access Control
  - AC.L1-3.1.2 – Transaction & Function Control
- Identification and Authentication
  - IA.L1-3.5.1 – Identification
  - IA.L1-3.5.2 – Authentication
- System and Communications Protection (with Azure Firewall or Fortinet firewall only)
  - SC.L1-3.13.1 – Boundary Protection
- System and Information Integrity
  - SI.L1-3.14.1 – Flaw Remediation
  - SI.L1-3.14.2 – Malicious Code Protection
  - SI.L1-3.14.4 – Update Malicious Code Protection
  - SI.L1-3.14.5 – System & File Scanning

Not included are AC.L1-3.1.20 – External Connections, AC.L1-3.1.22 – Control Public Information, Media Protection control, Physical Protection controls, and SC.L1-3.13.5 – Public-Access System Separation. These controls are not included because they cover access to resources/applications or physical resources client is responsible for managing. This includes any networking beyond what we agree to with firewall agreements.

Controls KAMIND can provide support for in Level 2 with a Fortress-G Implementation – TBD

Related Resources

Document ID & Title	Purpose of relation

References

Keywords

- SOP
- Template