ServiceNow Continuous Authorization and Monitoring for CMMC

The NIST Risk Management Framework and Cybersecurity Maturity Model Certification

The NIST Risk Management Framework (RMF) is a highly mature set of processes that provides a "common information security framework" for the federal government and its contractors. The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense's (DoD) newest verification system designed to ensure the protection of Controlled Unclassified Information (CUI) that resides on the Defense Industrial Base (DIB) systems and networks. The DIB includes over 300,000 defense contractors in the supply chain. In 2021, DoD contracts will be specifying CMMC maturity level requirements.

Ensuring you are adhering to requirements in NIST 800-171 r2 and 48 CFR 52.24-21 is the best first step to becoming CMMC compliant, as they are focused on protecting CUI. CMMC is made up of 5 levels, which range from basic cyber hygiene to implementing a robust cybersecurity program. As the maturity level increases the cybersecurity program begins to look very much like what you would create for NIST RMF, with potentially hundreds of controls that must be applied and continuously monitored.

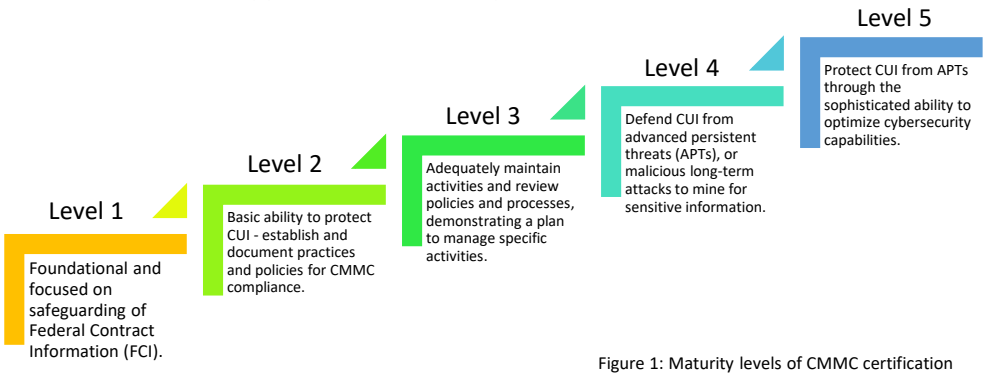


Figure 1: Maturity levels of CMMC certification

When scaled, this results in thousands of controls and tasks that must be managed across multiple departments and roles. You will find NIST 800-171 and NIST RMF 800-53 have many controls in common. Automating RMF or 800-171 with ServiceNow Continuous Authorization and Monitoring allows you to automate more of the overall process and its associated tasks and reduce risk and costs while decreasing time and effort.

The Continuous Authorization and Monitoring (CAM) application applies ServiceNow Integrated Risk Management to RMF, CMMC and other high assurance frameworks. CAM makes it easy to automate more of the work in the platform, manage the levels of CMMC, and prove compliance faster and easier.

Built on ServiceNow Integrated Risk Management

ServiceNow Integrated Risk Management (IRM) works with the Now Platform® to provide a framework for managing policies, controls, and risks. It includes the ability to easily create controls, continuously monitor for compliance, identify risks, obtain approvals or exceptions, and track responses throughout your enterprise. The ServiceNow cloud-based platform consolidates the data into a single platform with flexible workflows, context for prioritization, and automation and orchestration capabilities. ServiceNow IRM includes Policy and Compliance, Risk, Operational/Advanced Risk, Vendor Risk, and Business Continuity Management. It helps organizations manage everything from OMB A-123, Enterprise Risk, Operational Risk, CMMC, and now high maturity cyber risk frameworks such as RMF on a single platform.

"… An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. Such risks include, but are not limited to, strategic, market, cyber, legal, reputational, political, and a broad range of operational risks such as information security, human capital, business continuity, and related risks…"

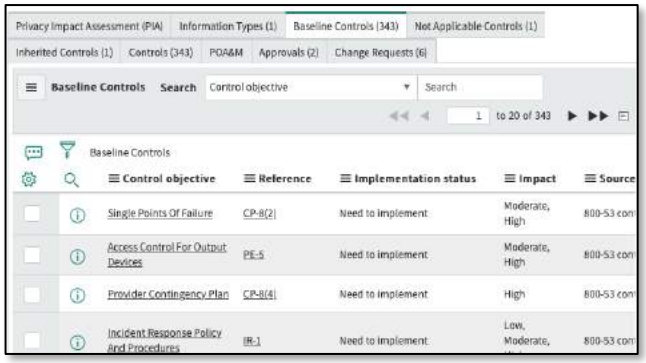
OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [OMB M-17-25]

Prepare

Contractors should be aware of the systems and services they use that are part of the certification process. CAM works with the CMDB to create entity filters to identify assets, as well as manually add or remove individual assets. You can also attach diagrams and documents, determine impact thresholds and perform impact analyses as well as manage roles and responsibilities.

Categorize

Contractor requirements are driven by the processes determined by the governmental agencies they support. Ensure the appropriate settings are replicated in CAM. With CAM you can manage and tailor NIST 800-60 information types, their impacts, and the overall system impact, with justifications for any overrides. System categorization approvals are automatically performed in the platform.



Select

Easily select security controls commensurate with contract requirements. CAM will automatically assign baseline controls based on categorization, let you manage control overlays, tailor individual and designate non-applicable controls. Controls can be inherited with visibility into the common control, and common control providers can easily select controls they wish to provide to others. Control selection can be overridden to align with contract requirements.

Implement

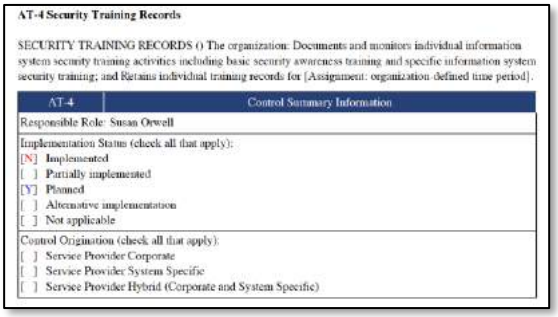
CAM automatically assigns controls to the system owners, or they can be created manually. You can trigger attestations to the System Owners to ensure controls are implemented for the respective information assets and ask for evidence. In case of non-compliance, IRM automatically generates an issue to ensure remediation is done quickly and controls are implemented.

Assess

Even though federal agencies will be the authority to assess, contractors should engage in self-assessment. The self-assessment procedures in CAM use built-in Audit management to automatically create an Audit Engagement. Audit Tasks are automatically created and assigned, allowing individuals to manage, perform, and report on control design and operational effectiveness tests within the platform. Ineffective controls automatically generate an Issue, which are tracked as a Plan of Action & Milestones (POA&M) along with their associated remediation tasks.

Authorize

Although CAM allows you to easily review evidence and documentation, control status, POA&Ms and other data to generate a System Security Plan, this is an activity you will not need to perform for CMMC certification. It is reserved for federal entities that must authorize and approve systems.



Monitor

Easily monitor your systems with data from the CMDB, ITSM, ITOM and Security Operations. View all vulnerabilities, POA&Ms, configuration compliance failures, security incidents and more for each boundary in a single place. CAM ships with dashboards built specifically for various roles that you can customize and build upon - or build your own.

Communicate through Third Party Risk Management

ServiceNow Vendor Risk Management can help federal departments and agencies manage the process of auditing contractors, It consolidates communication and collaboration when defining requirements and collecting implementation artifacts and attestations. An audit trail of interactions is kept for all contractors and every level.

Built on ServiceNow

Leverage ServiceNow's broad enterprise service management, workflow, and automation capabilities to transform and automate work processes, gain visibility into the network, and monitor key metrics.

www.servicenow.com/risk

SN-Solution-Brief-cam-cmmc-081323