Achieving Cybersecurity Maturity Model Certification

Saviynt's **Enterprise Identity Cloud** Platform Helps Customers Gain and Maintain Compliance with the DoD's CMMC Program.

Contents

Introduction

The Cybersecurity Maturity Model Certification (CMMC) is a United States Department of Defense (DoD) security framework designed to prevent the exfiltration of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) from contractors and subcontractors within the Defense Industrial Base (DIB). This paper details how Saviynt's Identity Governance and Administration (IGA) platform helps customers gain and maintain compliance with the CMMC.

Cybersecurity is a top priority for the Department of Defense because its contractors and subcontractors in the DIB are increasingly targets of frequent and complex cyberattacks. The DoD developed **CMMC 2.0** as a dynamic certification program to enhance DIB cybersecurity posture — the program protects sensitive unclassified information shared by the Department with its contractors and subcontractors. By incorporating a set of cybersecurity requirements into acquisition programs, the CMMC program provides the DoD with increased assurance that contractors and subcontractors meet these requirements.

The CMMC Program Requirements for Contractors

The CMMC operates in a tiered model that requires DIB companies to meet different levels of compliance based on the type and sensitivity of the information they possess on their unclassified networks. In November 2021, the DoD announced its latest iteration, CMMC 2.0, which collapsed the previous five-level model down to three. CMMC 1.0 required government-approved third-party assessor certifications for all levels; CMMC 2.0 allows Level 1 and some Level 2 companies to demonstrate compliance through annual self-assessments. Level 2 and Level 3 DIB companies handling sensitive CUI data will require third-party assessments every three years.

CMMC consists of 17 security domains with focus areas such as:

Access Control

Audit and Accountability

Identification and Authentication

Risk Management

Within each domain are practices or controls derived from NIST 800-171 for Levels 1 and 2 and NIST 800-172 for Level 3. As of December 2021, the DoD has yet to publish how the previous CMMC 1.0 practices realign to the 2.0 three-level model or the new NIST 800-172 practices. CMMC 2.0 will not be a contractual requirement until the DoD completes its rulemaking process, estimated to take 9-24 months.

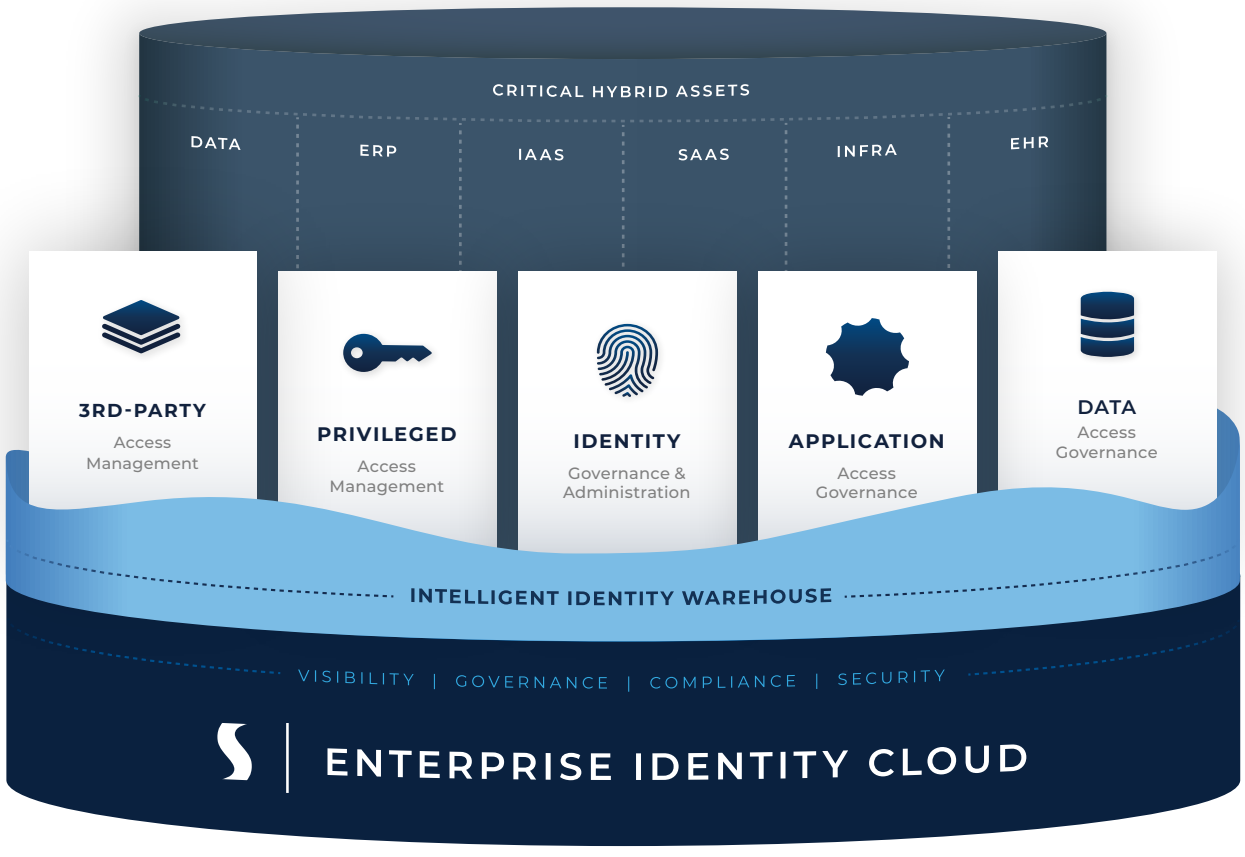
The CMMC practice levels are all NIST 800-171 controls previously outlined in CMMC 1.0. All NIST 800-171 controls are expected to be retained with CMMC 2.0, but the DoD has not specified how they will realign to the three-level model or the new NIST 800-172 based practices.

The principles of Identity Governance and Administration (IGA) occupy a significant portion of the practice requirements within the CMMC framework. IGA enables a zero-trust model of Identity Governance, ensuring users only have access to what they need, for the time they need it, and nothing more. This zero-trust model includes access to IaaS, SaaS, PaaS, and traditional on-premises resources for human and non-human entities such as bots, Internet of Things (IOT), and Robotic Process Automation (RPA).

Saviynt Enterprise Identity Cloud: An Integrated Platform for Achieving CMMC Compliance

Saviynt Enterprise Identity Cloud (EIC) is built in the cloud, for the cloud, and is the only FedRAMP authorized SaaS solution for Identity Governance and Administration (IGA) and Cloud Privileged Access Management (CPAM). The fundamentals of IGA align closely to the requirements outlined in **Federal Identity Credential and Access Management (FICAM).**

Saviynt EIC is a modular, converged cloud platform developed entirely in-house using a single code base without bolted-on solutions from third-party acquisitions to complicate the implementation process. Each solution can operate independently, allowing customers to select the product that suits them – and integrate EIC with existing solutions.



Saviynt EIC includes the following solutions:

Identity Governance and Administration (IGA)

Ensures that users have seamless access and your organization is in continuous compliance. Increases organizational efficiency and agility through automation and intuitive identity workflows. Powered by a comprehensive identity warehouse and user experience to drive frictionless access, Saviynt IGA enables Zero Trust in your hybrid and multi-cloud environment.

Cloud Privileged Access Management (CPAM)

Provides complete privileged access protection to support ongoing business transformation and scale as your business needs evolve. Gain visibility and governance for every identity across your entire environment to improve your security posture and maintain compliance. It's fast to deploy and easy to manage, so you realize value on day one. CPAM can limit users' actions in the end systems, and session recording provides an auditable record of the activities executed.

Application Access Governance (AAG)

Protects sensitive application access and satisfies governance, risk, compliance (GRC) requirements. Get comprehensive capabilities in Separation of Duty (SoD) analysis, emergency access management, role engineering and management, compliant provisioning, and access certification.

Third-Party Access Governance (TPAG)

Securely manages third parties throughout the engagement lifecycle. Internal and external sponsors shepherd the account from inception, through access management, periodic reviews, and eventual decommissioning.

Data Access Governance (DAG)

Discovers, analyzes, and protects sensitive structured and unstructured data – regardless of whether your IT ecosystem is on-premises, hybrid, or cloud-based.

The following sections detail how Saviynt enables customers to get and stay compliant within the various CMMC domains and practice levels.

Software Integrations Improve Speed and Accuracy

Saviynt has many built-in integrations for the rapid onboarding of users and applications in IaaS, SaaS, PaaS, and on-prem environments. As accounts get onboarded from various applications and endpoints, Saviynt's reconciliation rules match up the accounts and entitlements with the user identities gathered from the authoritative sources such as HRM / ERM applications like Workday, SAP, Oracle, Peoplesoft, Active Directory, and others.

Saviynt's identity warehouse becomes a single source of truth (SSOT) that identifies all the access entitlements at the user level. Being the central repository for all identity and access-related information enables Saviynt to enforce complex Governance, Risk, and Compliance (GRC) verifications. Peer group analyses compare individual entitlements to other members within the organization that possess the same roles or attributes to identify outlier access that doesn't adhere to typical requirements for that user type. Separation of Duties (SoD) analysis identifies risky combinations of access (e.g., creating a contractor organization and paying them). These capabilities apply to new access requests as well. As new access is requested, Saviynt identifies outlier entitlements and SoD violations and displays them to the approver so they can make informed decisions in their approval process.

Access certification campaigns provide a continuous process that establishes owners of users or applications responsible for recertifying access that has been granted. These campaigns can be scheduled at user-defined intervals or automatically generated based on changes in the environment (e.g., user role changes or location changes).

Governance Across the Entire Identity Lifecycle

Saviynt's IGA solution establishes a Zero Trust, least privilege, identity model by ensuring that all users go through a documented approval process — which identifies inappropriate privileges and risks associated with new and existing access through peer group analysis and SoD verifications.

One of the most critical aspects of the Saviynt IGA solution is establishing ownership of users and applications. Saviynt provides highly customizable, multi-level approval workflows that correlate user manager and system owner access to various end systems. This includes access to third-party and non-human identities such as bots, IOTs, and RPAs. Ongoing scheduled and automated access recertification campaigns continually verify that granted access is appropriate.

Highly privileged access has its own approval process and has additional keylogging and session recording capabilities for enhanced oversight of actions performed to organizational systems.

Privileged Access Only Where and When It’s Needed

For users that require privileged administrative access, Saviynt's Cloud Privileged Access Management (CPAM) solution provides time-bound credentialed and credential-less access with granular controls on the actions users can perform. CPAM prevents users from performing non-approved actions with screen notifications advising of the prohibited action. User connections can be automatically terminated when these prohibited actions are attempted. Keylogging and screen recording provides an auditable record of all actions performed.These capabilities all translate into the zero-trust principles of enforcing least privilege access and ensuring no standing privileges for critical IT resources.

The Saviynt CPAM solution stores privileged account credentials within a built-in HashiCorp vault and is unavailable to the end-user. Users must be approved for privileged access to specific endpoints and authenticate the PAM system to check the credentials and connect to the end system. The passwords are immediately reset upon the session's completion.

Saviynt CPAM ensures no standing access to system management functionality. It terminates connections to endpoints after specified timeframes, periods of inactivity, or when users attempt prohibited actions. All actions are logged and recorded, including permitted and prohibited actions that may have been attempted to establish an auditable record of all actions performed by a particular user in the end system.

Securing and Governing Data Access

Saviynt's Data Access Governance discovers, analyzes, and protects sensitive data by tying identity to authorized access in file sharing solutions such as Box, SharePoint, Oracle, and others. Built-in and configurable regular expression-based scanning rules provide the capability to identify documents with sensitive information and pair user identity to the authorization to view such files.

Saviynt has a customizable approval process for granting access to different systems within an organization, including having multiple levels of approval for sensitive systems. Saviynt's Data Access Governance further ties user identity to authorized access to Federal Contract Information systems.

Conclusion

The growth of cloud computing and the recent shift to blended work environments have been a boon to cyberattackers. CMMC standards are vital for the future of data security in the public sector and for contractors that work for the public sector. Getting ahead of the shift and finding ways to meet the requirements will be critical for contractors hoping to continue working in the federal sphere. Saviynt Enterprise Identity Cloud has many essential features to help contractors achieve and maintain compliance with the DoD's CMMC program.

About Saviynt

Saviynt's Enterprise Identity Cloud helps modern enterprises scale cloud initiatives and solve the toughest security and compliance challenges in record time. The company brings together identity governance (IGA), granular application access, cloud security, and privileged access management (PAM) to secure the entire business ecosystem and provide a frictionless user experience. For more information, please visit **www.saviynt.com.**

Sources

https://techcommunity.microsoft.com/t5/public-sector-blog/accelerating-cmmc-compliance-for-microsoft-cloud-in-depth-review/ba-p/1825671
https://techcommunity.microsoft.com/t5/public-sector-blog/microsoft-cmmc-acceleration-program-update-january-2021/ba-p/2033499
https://www.acq.osd.mil/cmmc/
https://www.acq.osd.mil/cmmc/faq.html