Authlogics

CMMC Framework

Achieving Cybersecurity Maturity Model Compliance with Authlogics

White Paper

Call us on: +44 1344 568 900 (UK/EMEA)
+1 408 706 2866 (US)

Email us: sales@authlogics.com

Table of Contents

Introduction

The Cybersecurity Maturity Model Certification (CMMC) is a certification and compliance process developed by the Department of Defense (DoD). Released in January 2020, CMMC brings together a collection of compliance processes namely NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, and AIA NAS9933 to certify that contractors have the controls in place to protect sensitive data.

CMMC requires DoD contractors to have their systems audited by a 3rd-party now. The contractor remains responsible for the implementation, monitoring, and certification of the appropriate cybersecurity controls whereas previously, these controls were not independently verified via a 3rd-party audit. CMMC addresses this to ensure mandatory practices, procedures, and capabilities are adhered to counter the evolving cyber threats from adversaries.

The following shows the key dates for the implementation of CMMC:

Jan 2020	Full version release of CMMC
Jun 2020	CMMC requirements becoming visible in RFP process
Sep 2020	CMMC more visible in RFP process
Oct 2020 +	DoD contractors need to be officially certified by C3PAO/ Assessor

CMMC Framework

CMMC has 5 certification levels which reflect the maturity and reliability of a company's cybersecurity to protect sensitive government data on the organization's I.T. systems.

The 5 levels are as follows:

Level 1: Basic Cyber Hygiene

A company must perform "basic cyber hygiene" practices, such as using antivirus software and password complexity requirements required to protect the Federal Contract Information (information that is not intended for public release or certain transactional information).

Level 2: Intermediate Cyber Hygiene

A company must document certain "intermediate cyber hygiene" practices to begin to protect any Controlled Unclassified Information (CUI) through the implementation of some of the US Department of Commerce National Institute of Standards and Technology's (NIST's) Special Publication 800-171 Revision 2 (NIST 800-171 r2) security requirements. CUI is "any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls," but does not include certain classified information.

Level 3: Good Cyber Hygiene

A company must have an institutionalized management plan to implement "good cyber hygiene" practices to safeguard CUI, including all the NIST 800-171 r2 security requirements as well as additional standards.

Level 4: Enhanced Cyber Hygiene

A company must have implemented procedures for defining and measuring the efficiency of implemented controls as well as establishing enhanced practices to detect and respond to changing tactics, techniques and procedures of advanced persistent threats (APTs). An APT is defined as an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors.

Level 5: Advanced Cyber Hygiene

A company must have standardized and optimized processes in place across the organization with enhanced controls which provide more sophisticated capabilities to detect and respond to Advanced Persistent Threats.

Compliance using Authlogics

Authlogics provides multiple complementary solutions to assist companies in achieving Cybersecurity Maturity Model Compliance for **all** 5 levels of certification. CMMC is an amalgamation of numerous compliance publications that cater to all aspects of cybersecurity. Organizations are required to adhere to best-practice standards and additional supplementary compliance requirements that are outlined in these publications, with an ongoing commitment.

Authlogics solutions have been designed to comply with best practices with a key focus on adhering to NIST compliance for password security and user authentication. Authlogics has numerous tools and solutions to assist the organization to achieve CMMC and ensure on-going compliance with the framework. This is achieved with our Password Compliance and Multi-Factor Authentication solutions, both of which are prescribed requirements for secure and compliant environments.

Password Authentication Requirements

NIST Special Publication 800-53 specifies authentication requirements and in particular, highlights the following password-based authentication specifications:

a) **Maintain a list of commonly used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;**
b) **Verify, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly used, expected, or compromised passwords;**
c) Transmit only cryptographically protected passwords;
d) Store passwords using an approved hash algorithm and salt, preferably using a keyed hash;
e) Require immediate selection of a new password upon account recovery;
f) **Allow user selection of long passwords and passphrases, including spaces and all printable characters;**
g) **Employ automated tools to assist the user in selecting strong password authenticators;**
h) **Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].**

NIST Special Publication 800-63 (not specifically listed within CMMC directly, it is referenced in SP 800-171 with detailing best-practices for password security) goes into more detail and provides additional granularity regarding acceptable passwords. The high-level requirements specified within this SP state that passwords cannot be:

a) **Passwords obtained from previous breach corpora;**
b) **Dictionary words;**
c) **Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd');**
d) **Context-specific words, such as the name of the service, the username, and derivatives thereof.**

Authlogics Password Security Management (PSM) solution assists organizations complying with the above requirements and includes comprehensive tamper-proof logging for audit and accountability with the use of the Authlogics Password Breach Database.

Compromised passwords are detected through the Authlogics Password Breach Database which is compiled of over 2 billion credentials that have been breached, including over 520 million unique clear text passwords. If a user selects a password that exists in the Password Breach Database, PSM will identify this as being compromised and flag it accordingly. Without access to a Password Breach Database, an organization will not be able to determine whether a password has been previously breached or not.

Furthermore, organizations can create their custom defined list of commonly used, expected, or compromised passwords which PSM will validate.

PSM includes detailed administrative defined complexity checks allowing organizations to enforce composition and complexity checks and deny usage of passwords that fail the prescribed password checks. These checks include specifying minimum and maximum lengths, usage of month and day names, usernames or partial username, and a whole host of additional rules ensuring sufficient password strength.

Furthermore, Authlogics PSM ensures that passwords used internally are unique and not shared between multiple user accounts. Although not directly specified as a CMMC requirement, this functionality is core to maintain a high level of password security and accountability.

All Authlogics solutions include the self-service portal which provides the necessary tools to assist users with selecting strong passwords that comply with the complex requirements.

Authlogics Password Auditing

Authlogics Active Directory Password Audit service is designed for an organization's internal audit group and assessors to reliably determine the vulnerability of a network to password-based attacks and provide a detailed report outlining the risks and issues. The Audit tool is designed to be a non-intrusive process that checks for previously breached and shared passwords and highlights compliance issues against the NIST password policy standards.

Running the AD Audit tool regularly ensures on-going compliance as per CMMC requirements.

Multi-Factor Authentication

CMMC requires organizations to ensure that authentication are not solely limited to strong and secure passwords but also additional secure authentication factors. Multi-factor Authentication (MFA) solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card.

In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security.

CMMC breaks down MFA requirements for privileged accounts and non-privileged accounts. However, irrespective of the account and access type, both privileged and non-privileged accounts **must** authenticate using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Furthermore, NIST SP 800-53 states that: Adversaries may compromise individual authentication mechanisms employed by organizations and subsequently attempt to impersonate legitimate users. To address this threat, organizations may employ specific techniques or mechanisms and establish protocols to assess suspicious behavior. Suspicious behavior may include accessing information that individuals do not typically access as part of their duties, roles, or responsibilities; accessing greater quantities of information than

individuals would routinely access; or attempting to access information from suspicious network addresses. When pre-established conditions or triggers occur, organizations can require individuals to provide additional authentication information.

Authentication MFA provides a complete cost-effective multi-factor authentication, password replacement, and single sign-on authentication solution for traditional desktops, over the phone, in the browser, or from any device.

Authlogics provides many options to choose from, including alternative “knowledge-based” factors to passwords paving the way for their replacement. Our pioneering deviceless (1.5-Factor) opens new use case scenarios by providing the benefits of a traditional Once Time Code logon but without the overhead of managing physical devices. MFA tokens are delivered via the Authlogics Authenticator soft token, delivered via SMS & email tokens (pre or post-send), and on-premise YubiKey hardware tokens. Furthermore, the award-winning PINgrid and PINpass technologies include transaction signing functionality (3 Factor) to deliver the most secure solution available in the industry without requiring dedicated hardware.

Authlogics provides organizations with numerous MFA options and the ability to satisfy CMMC MFA requirements, deliver secure risk-appropriate authentication for both end-point devices such as VPNs and Server, and integrate Authlogics with applications.

Executive Summary

The compliance concept can be daunting but cannot be avoided. Major regulatory acts such as the CMMC have been introduced to ensure that DoD contractors are employing the best practices and standards to ensure the maturity of cybersecurity. With the abundance and sophistication of cyber threats, more legislation is being introduced to ensure contractors conform to the required standards and highest level requirements for Password.

Authlogics solutions can assist you to achieve your required CMMC level and provide continuous protection and security.

About Authlogics

Award-winning authentication experts Authlogics are committed to assisting IT managers to improve security while making it easier for users to access their information. Authlogics focuses on helping your business transition from password-driven environments while increasing your security posture and compliance to policy.

To find out more about Authlogics and our products and technologies, please visit our website at https://authlogics.com or contact us on info@authlogics.com. Our technical team are only a call away and are happy to discuss your needs and requirements (US: +1 408 706 2866 | UK/MEA: +44 1344 568900).