alyne

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

CMMC

CYBERSECURITY MATURITY MODEL CERTIFICATION

Prepare for **CMMC** leveraging Alyne's Control Sets and Cybersecurity Frameworks.

ABOUT THE PAPER

The Cybersecurity Maturity Model Certification (CMMC) combines several best practices defined in many leading security frameworks, including NIST 800-171, ISO 270001 and others. The license equires all defense contractors to undergo a CMMC Audit in order to be CMMC Certified. In this paper you will learn more about the requirements and how you can leverage Alyne's predefined Control Sets and built-in capability to attain CMMC Level 3 with ease.

alyne

CMMC WITH ALYNE

WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

The Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity standard which was first publicly released on 31 January 2020 by the Department of Defense (DoD).

This framework was designed to ensure that organisations in the defense industrial base (DIB) supply chain are undertaking appropriate cybersecurity measures to maintain confidentiality and security of sensitive defense information. These data include Federal Contract Information and Controlled Unclassified Information (CUI).

WHY IS IT IMPORTANT?

Before CMMC was implemented, defense contractors were responsible for monitoring and certifying the security of their own IT systems, and any DoD data stored or transmitted by them.

However, without proper infrastructure and defined processes in place to ensure compliance, critical cybersecurity requirements were mostly based on contractors' self-attestation, which creates grounds for grey areas and gaps for ambiguity.

To offer clarity in this area, CMMC was introduced to enhance the security of information systems when managing confidential information from the DoD. The license requires all defense contractors to undergo CMMC Audit in order to be CMMC Certified, which certification will be valid for a period of 3 years.

The whole process will be assessed by CMMC Third Party Assessment Organisations (C3PAOs) which are licensed by CMMC Accreditation Body.

C3PAOs ensure that defense contractors receive the appropriate guidance in the implementation and execution of critical cybersecurity requirements. More specifically, C3PAOs offer clear directions and guidelines for defense contractors to adhere to with reference to certain mandatory practices, procedures and capabilities. Simply put, this process aims to assist contractors and organisations in adapting to ever-changing and evolving cyber threats.

alyne

CMMC WITH ALYNE

WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

TIMELINE

31 JAN 2020

V1.0 of CMMC publicly released.

18 MAR 2020

V1.02 of CMMC publicly released.

JUNE 2020

CMMC requirements present in RFI Process.

SEPT 2020

CMMC requirements present in RFP Process.

OCT 2020

DoD Contractors required to be certified by an Assessor/C3PAO.

alyne

CMMC WITH ALYNE

WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

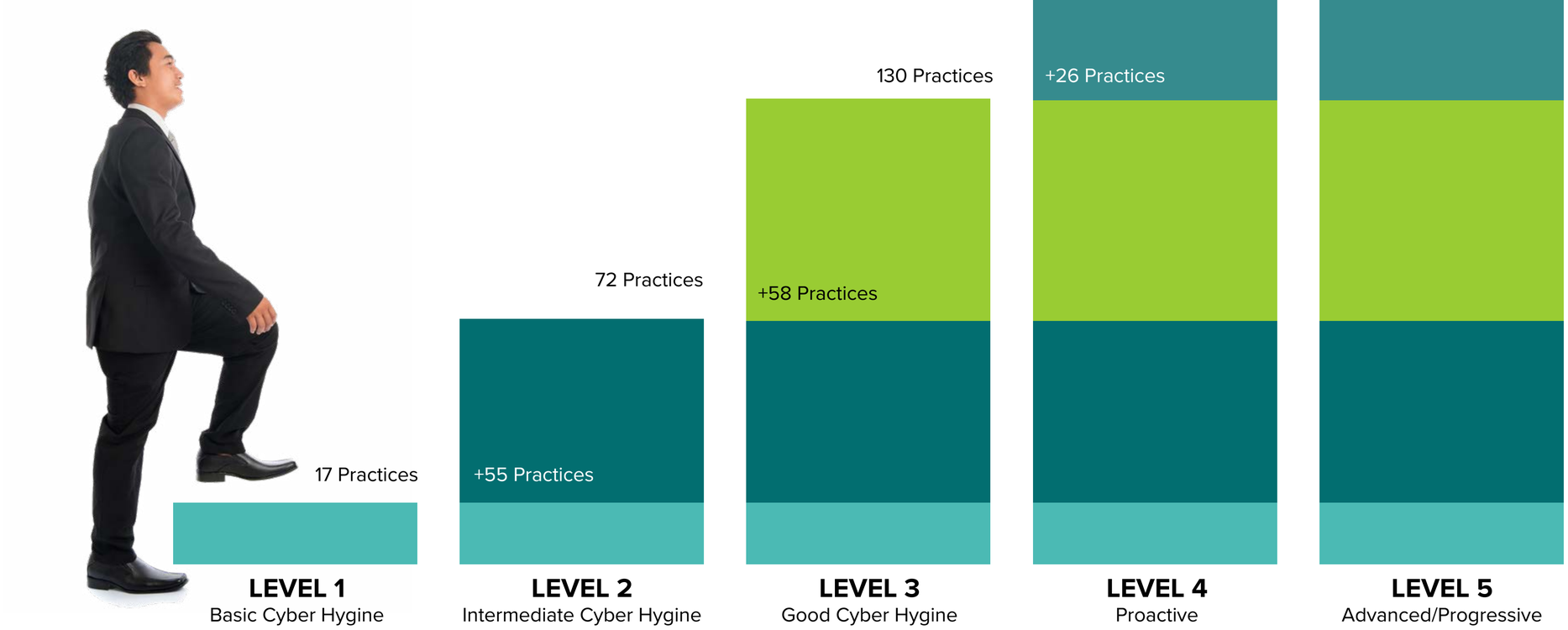
ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

CMMC FRAMEWORK AND ANALYSIS

The CMMC establishes 5 certification levels, 17 Domains, 43 Capabilities, 171 Practices, all of which aim to effectively reflect the maturity of an organisation's cybersecurity infrastructure in safeguarding sensitive government information on contractors' information systems.



alyne

CMMC WITH ALYNE

WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

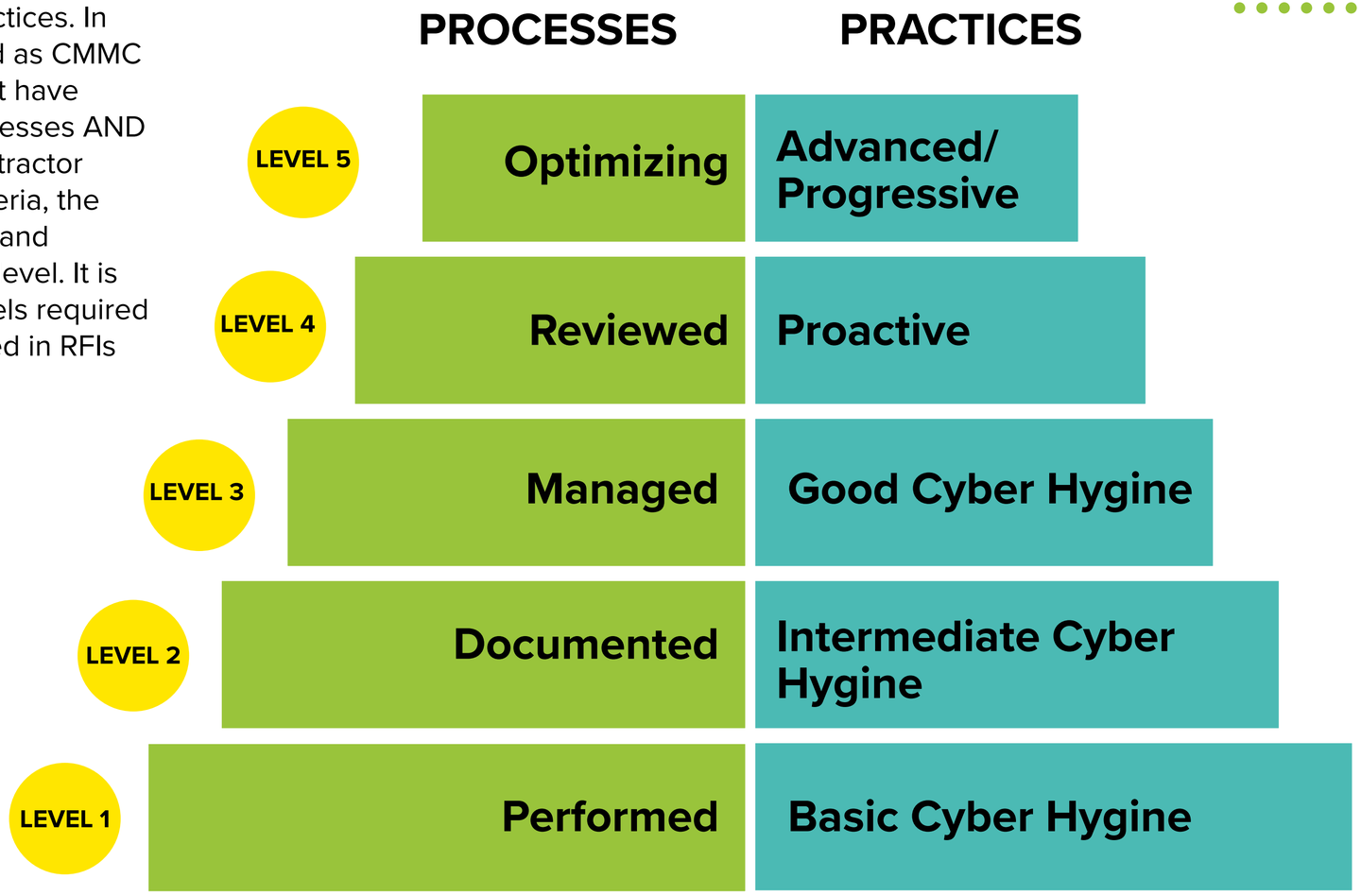
HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

The 5 levels are tiered and cumulative, meaning that in order to achieve a maturity at a certain level, organisations are required to build upon the previous lower-level processes, and can only be certified so long that it meets both the process and the required practices. In other words, to be recognised as CMMC Level 2, DoD contractors must have achieved Level 2 in both processes AND practices. However, if the contractor has only met either of the criteria, the contractor will be recognised and certified for the lower CMMC level. It is important to note that the levels required for contractors will be specified in RFIs and RFPs.



WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

LEVEL 1 Safeguarding Federal Contract Information (FCI)

At this level, the company must be performing “basic cyber hygiene” practices. In this case, some practices may include the use of antivirus software or ensuring members within the organisation regularly review and change their passwords to protect confidential information that is not intended for public release, also known as the Federal Contract Information.

At this level, some process maturity is required of the contractor. In order to pass an audit for this level, 17 controls of NIST 800-1171 r1 will need to be implemented by the DoD contractor.

LEVEL 2 Brings focus to Controlled Unclassified Information (CUI)

At this level, the company must demonstrate “intermediate cyber hygiene” practices to protect any Controlled Unclassified Information (CUI).

To demonstrate process maturity at this level, the company should be incorporating Standard Operating Procedures with policies established for all practices. This can be achieved through implementation of another 46 controls of NIST 800-1171 r1.

LEVEL 3 Increased focus on CUI

At this level, the company must have increased their focus on protecting CUI by having an institutionalised management plan to implement “good cyber hygiene” practices. This includes compliance with all the NIST 800-171 r1 security requirements as well as additional standards.

Contractors at this level are expected to demonstrate management of practice implementation and to review adherence to relevant policies and procedures.

The organisation is also required to ensure that it is adequately resourced, which for example might include an established budget; people resources; access to all tools required to perform domain activities; relevant stakeholders are involved in the process.

WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

LEVEL 4 Aims to be minimum level for prime contractors working with CUI

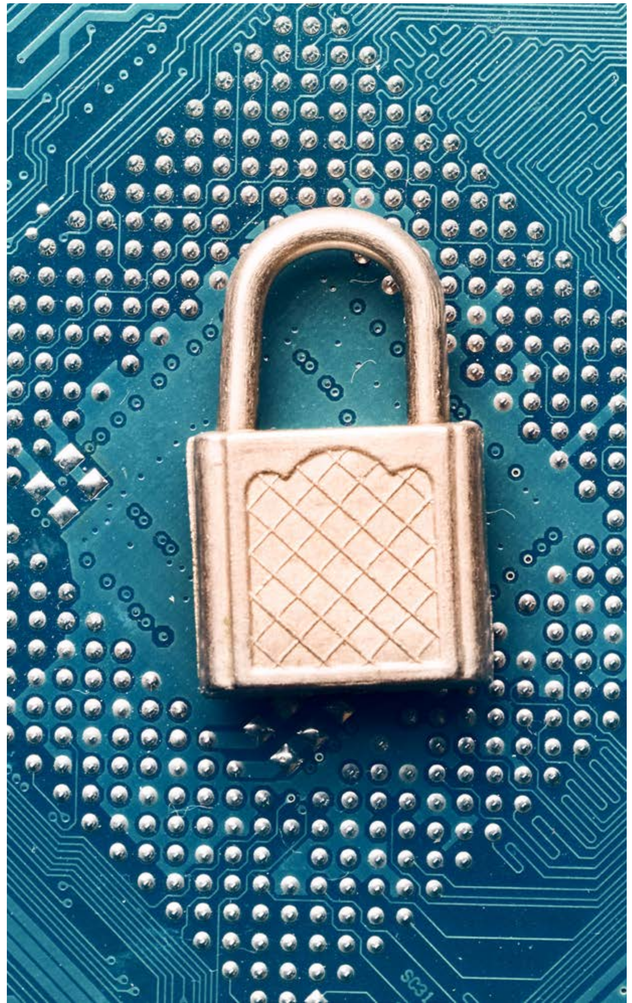
At this level, the company must have implemented processes for reviewing and measuring the effectiveness of practices to demonstrate substantial and proactive cybersecurity programs. These processes should also include detection and response to changes of Advanced Persistent Threats (APTs).

To demonstrate process maturity at this level, the company has to review the effectiveness of its activities and raise issues to the management, if any. In the case of issues identified, mitigative actions should be developed to resolve them, which should be monitored through a regular review process.

LEVEL 5 Protect CUI and reduce risk of APTs

At this level, the company must have standardised and optimised processes implemented and executed across the organisation. These processes should also include additional enhanced practices that provide more sophisticated capabilities to detect and respond to APTs.

To demonstrate process maturity at this level, the company has to standardise all activities across the responsible organisational units and highlight the improvements necessary.



WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

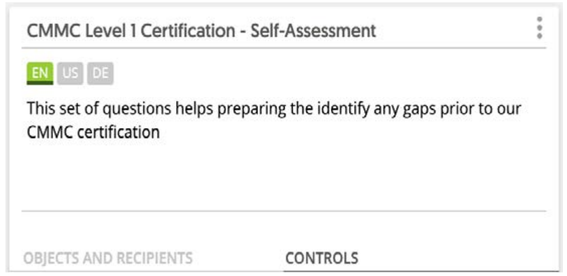
CMMC LEVEL 3 PREPARATION WITH ALYNE

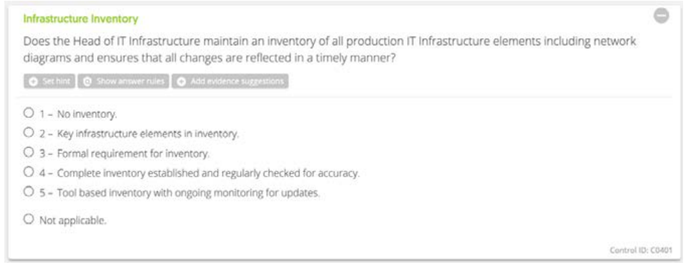
CMMC Maturity Process Progression

Organisation leaders can easily obtain an in-depth overview of their Process Maturity leveraging the Control Sets that are based on the different levels of CMMC, containing 130 Controls.

CMMC Practice Progression

Organisation leaders can also carry out Assessments to quantify and measure Controls maturity based on the CMMI Model with Alyne's Assessment. This allows organisations to obtain a quick overview of their current maturity level to allow efficient allocation of resources and to better plan their preparation for the certification.





WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

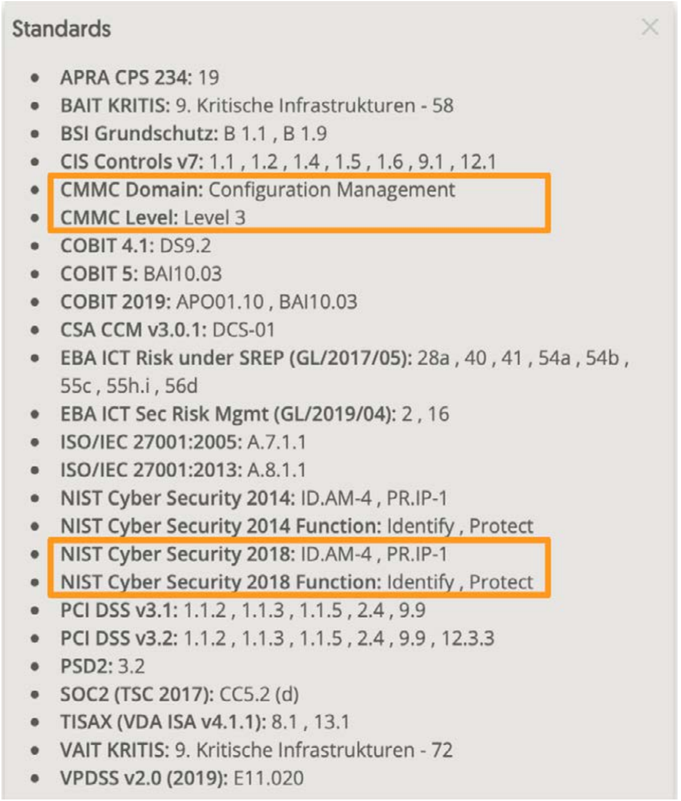
ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

While CMMC does go further to ensure data is protected, achieving one of the higher maturity levels will require an organisation to have many of the security controls outlined by NIST 800-171 in place.

ISO 27001, if already implemented as your ISMS, has built a great foundation for identifying your information assets with appropriate safeguards. With ISO 27001, your controls are selected based on your identified risks for your specific environment. With CMMC however, the level you need to achieve and the corresponding controls required are specified in your contract. In some cases, there might be an overlap of controls and processes already in motion.



WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

ALYNE ACTION PLAN

How DoD contractors can prepare for CMMC

Although the detailed procedures have yet to be released, the Alyne team has identified actionable steps for organisations to prepare ahead for a more efficient assessment and audit.

1

Prepare your document practices and procedures that are already in compliance with CMMC practices or processes

By preparing your documents in advance according to NIST 800-171, it gives your organisation a head start as it offers clarity as to the degree of preparedness and the procedures and practices that are required to be complied with. Performing a Self-Assessment and GAP analysis here will help to determine your current maturity and level of compliance.

2

Plan ahead to implement procedures and practices to obtain the target certification level

Depending on the organisation's structure and requirement, prime contractors can now design an action plan on how to work with other contractors throughout the supply chain to ensure that compliance takes place as soon as possible.

At Alyne, we recommend contractors aim for the highest certification level that is most applicable based on their organisational structure. It is important for DoD contractors to prepare ahead as the regulation would soon be the minimum requirement for them to be eligible for future contracts, potentially affecting their engagements in future.

WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

ALYNE ACTION PLAN

How DoD contractors can prepare for CMMC

Although the detailed procedures have yet to be released, the Alyne team has identified actionable steps for organisations to prepare ahead for a more efficient assessment and audit.

3

Actively engage with agencies

Be proactive when reviewing RFIs and RFPs that include minimum certification requirements. This ensures that the entire supply chain is aware of the minimum required certification level.

4

Regularly review cyber compliance by building a culture of cyber resilience

Moving forward, after the contracts have been recognised for the respective CMMC certification which is valid for a period of three years, contractors should not be complacent in maintaining cyber compliance within the organisation. Instead, contractors should aim to instill a culture of cyber resilience within the organisation in response to the evolving cyber threats. This not only maintains the cybersecurity strength of the organisation during the three year period of validation, but also adds to good preparation for the next CMMC Audit.

CMMC WITH ALYNE

WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

TIMELINE

CMMC FRAMEWORK AND ANALYSIS

RELEVANT PROCESSES AND PRACTICES OF EACH LEVEL

CMMC LEVEL 3 PREPARATION WITH ALYNE

HOW DO OTHER LEADING CYBERSECURITY STANDARDS OVERLAP WITH CMMC REQUIREMENTS?

ALYNE ACTION PLAN

WHERE DOES ALYNE COME INTO PLAY?

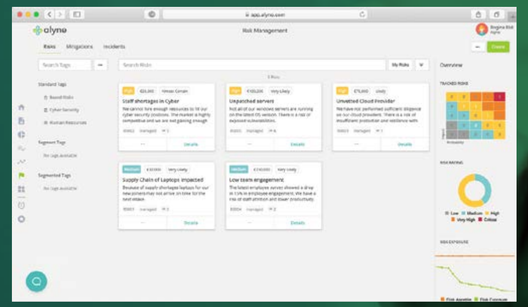
WHERE DOES ALYNE COME INTO PLAY?

Alyne experts have designed a Library of Controls which assists organisations to comply with various international standards and regulations in a seamless manner, including the capability to prepare for a CMMC Level 3 certification.

The Alyne Content Library contains NIST CSF which is extensively mapped to a large portion of the NIST 800- 171 standard. This is a cybersecurity framework which organisations are required to comply with in order to achieve at least CMMC Level 3, consisting of 130 Controls.

With Alyne, business leaders can utilise Alyne's predefined Control Sets to easily perform an internal self-assessment in order to understand organisational maturity level. A Risk Report can then be generated, providing further analysis into gaps and clarity on current cybersecurity posture. This deep insight allows for internal alignment and strengthening of processes before the organisation undergoes a formal CMMC audit.

Alyne can assist organisations in achieving CMMC Level 3 efficiently and easily, allowing organisation leaders to focus their attention on more sophisticated capabilities for detection and response to Advanced Persistent Threats (APTs) and other areas which require more attention and resources required in the further 2 levels of CMMC certification.



Get in touch with us to learn more about Alyne's nextgeneration risk management solution can assist with your organisation's CMMC

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

SPEAK TO AN EXPERT

CONTACT HAPPIEST MINDS

alyne

Founded in 2015 with the vision to build technology that is easy to use and that simplifies risk management for all organisations, Alyne now operates globally to provide extensive capabilities in managing Cyber Security, Governance, Risk Management and Compliance processes through a Software as a Service platform. Alyne's technology is powered by industry experts and enables risk and assurance professionals to easily understand complex data and gain actionable insights, through it's powerful Content Library, Assessments and Risk Reporting features - mapped to relevant standards, laws and regulations. Keep your organisation at the forefront of Cyber Security, Risk Management and Compliance with Alyne as your Mission Control.

Alyne USA Inc.
43 West 23rd Street, NY 10010, New York

Alyne GmbH
Ganghoferstr. 70a 80339 Munich, Germany

Alyne UK Ltd.
41 Luke St, Shoreditch, London EC2A 4DP, UK

Alyne Australia Pty Ltd.
312 Centre Road, Bentleigh VIC, Australia 3204

For more information, visit **www.alyne.com**