KAMIND®

Cloud Solutions Advisors

The Cybersecurity Maturity Model Certification (CMMC) 2.0

Written By: KAMIND IT Inc.

The CMMC 2.0

Introduction

The original goals and objectives of the CMMC have fallen behind schedule, and there is still a great deal of confusion as to what needs to get done and how to go about. Also, many of the participants that are required to become CMMC Certified are complaining about its lengthy process, and the sheer amount of expense that is occurring to become certified. At the same time, the DOD has not changed the timeline for contractor compliance.

Because of this, the Federal Government and the Department of Defense have come up with a newer version of it, which is known as the "CMMC 2.0". This is a huge effort that is currently being undertaken in order to streamline the entire process, and of course, make it financially more affordable for small businesses.

The goal of this whitepaper is to provide more detail about the CMMC 2.0, but before that is done, it is first important to give a solid background into the first version of the CMMC, which can be termed as the "CMMC 1.0".

An Overview Into The CMMC 1.0

Background

According to a recent study that was conducted by Juniper Research, the overall amount of financial cybersecurity losses that the United States will experience by the year of 2024 is expected to far exceed an overwhelming $5 trillion (SOURCE: 1). This represents a Year Over Year (YoY) growth rate of nearly 11% until we hit that mark.

It is expected that this statistic is only going to proliferate further down the road. But one of the largest Cyber victims in all of this is what is known as the "Defense Industrial Base", also referred to as the "DIB" for short. The grouping of companies that is involved in this network is very large.

For example, it represents more than 220,000 businesses across Corporate America, and even any subsidiaries or branch offices that have locations on a worldwide basis. But this number grows even more when you include the nonprofit organizations and academic institutions that are tasked to do the following for our nations' military system:

- Research and engineering;
- The development of new system designs;
- The acquirement and procurement of the needed raw materials;
- The final production and delivery of newer products and services.

Introduction To The CUI

If any of the above have been compromised in any way, shape or form, this would of course have huge and devastating consequences for the United States armed forces on a gl obal level. This is especially true when it comes to the loss of both Intellectual Property (IP) and Controlled Unclassified Information (CUI). The latter can be defined specifically as follows:

"CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.

CUI is not classified information. It is not corporate intellectual property unless created for or included in requirements related to a government contract."

(SOURCE: 2).

In other words, CUI is information that can be accessed to varying degrees by external third parties, but it is not designed to be released to the public at large, because of some of the sensitivity that is involved with the datasets. As a result, there are fewer controls that are associated with the CUI, and because of that, this presents a prime opportunity for the Cyberattacker to gain access to the classified information, in a covert fashion. According to the DOD, there are 80,000 companies that will be impacted with CUI safeguarding under CMMC Level 3.

The Catalysts of The CMMC 1.0

In order to provide specific safeguards and controls to help further protect the CUI, the "Cybersecurity Maturity Model Certification", or the "CMMC" has been established.

This framework was actually launched by the Office of the Under Secretary of Defense for Acquisition and Sustainment, also known specifically as the "OUSD(AS)" for short. Although one of the primary objectives of the CMMC is to provide protection for the CUI, one of the other main themes of it is to limit access to the external contractors that can gain access to it. Although these parties primarily reside in the United States, they could very well also have connections to associates in overseas offices, where the CUI could be released intentionally or non-intentionally to potential, malicious third parties.

These contractors form what is known as the "Supply Chain" for the Department of Defense (DoD). Along with the other entities described earlier in this whitepaper, this category also includes many small to medium sized businesses. These organizations are the most prone to Cyberattacks, and according to the Verizon 2019 Data Breach Investigations Report, it is those entities that have up to 250 contractors (or more) that are at most risk for exposing CUI via Email, or any other electronic means. (SOURCE: 3).

One of the driving forces behind the CMMC are the list of best practices and standards that have been set forth by the National Institute of Standards and Technology, also known as "NIST". Before the adoption of the NIST framework, the guiding principles for implementing some of sort of controls for the CUI came from the "NIST SP 800-171", and the "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations".

In order to prove their level of trustworthiness when it comes to accessing the CUI, these external contractors in the DoD Supply Chain will have to be certified through the CMMC framework primarily via through CMMC based Third Party Organizations also known as "C3PAOs" for short. This is a requirement before any bidding on DoD contracts can take place, and direct proof of certification must be stipulated in any Request For Proposals (RFPs) that will be submitted.

It is important to keep in mind that simply achieving CMMC certification does not guarantee that the third-party contractors will gain immediate and automatic access to the CUI datasets. Rather, the DoD will have final oversight as to the types of CUI that will be disseminated. T

The Structure Of The CMMC Model

The CMMC is composed of 17 specific domains, which are as follows:

- Access Control (AC);
- Asset Management (AM);
- Audit and Accountability (AU);
- Awareness and Training (AT);
- Configuration Management (CM);
- Identification and Authentication (IA);
- Incident Response (IR);
- Maintenance (MA);
- Media Protection (MP);
- Personnel Security (PS);
- Physical Protection (PE);
- Recovery (RE);
- Risk Management (RM);
- Security Assessment (CA);
- Situational Awareness (SA);
- System and Communication Protection (SC);
- System and Information Integrity (SI).

These are illustrated in the diagram below:

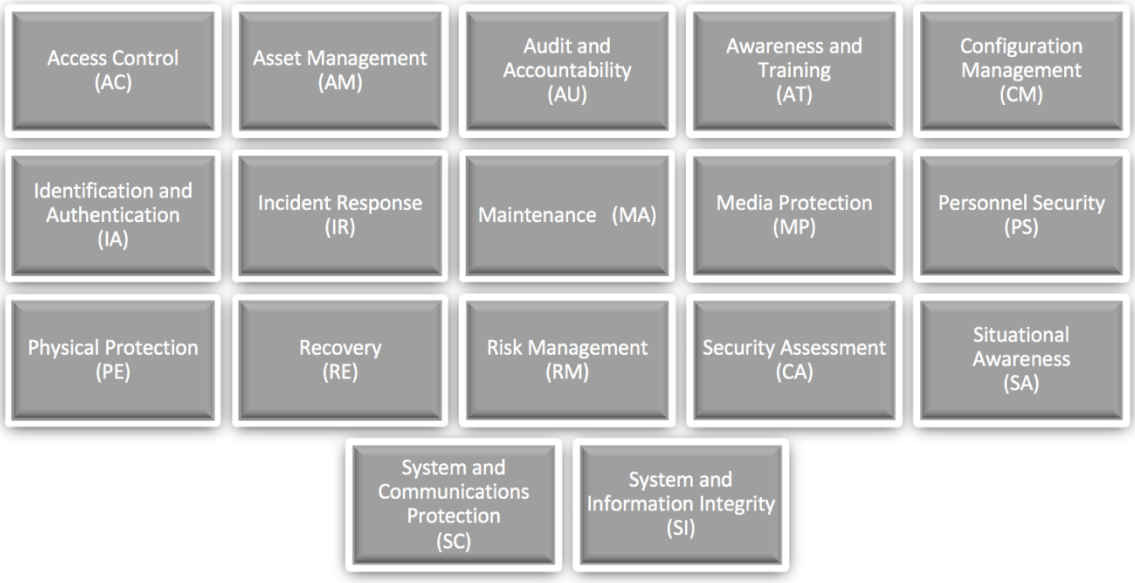


Figure 1. CMMC Domains.

(SOURCE: 4).

Each of these domains actually have five levels of certification (designated as L1, L2, L3, L4, L5). Before any external, third-party contractor can gain access to any type of CUI, they must have achieved at least the L3 level of certification. These domains have actually have their originations from the following sets of publications:

- The Federal Information Processing Standards (FIPS) Publication 200;
- The NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
- CMMC 1.0 is a combination of NIST 800-171, Delta 20 (Enhancements to 20 technical areas not in the current CMMC 2.0 standard) and NIST 800-172 (for CMMC level 4 and 5 of CMMC 1.0).

Also, these 17 domains cover a grand total of over 171 technical areas.

An Overview Into the CMMC 2.0

As mentioned earlier in this whitepaper, there were many complaints that the CMMC 1.0 was a painstaking process to accomplish with the requirement for formal accreditation at Level 1, and also an expensive proposition for the Defense Industrial Base (DIB) to incur. In fact, there were over 850 negative public comments that the Department of Defense about the CMMC 1.0. As a result, the CMMC 2.0 was born, in November 2021.

It is very important to note here that the exact timeline for the full implementation of the CMMC 2.0 is still in the air, and in fact, there is wide speculation that it could even up to two years. But, the DoD has marked this first announcement of it as a major milestone in the new step taking forward.

What Is New In The CMMC 2.0?

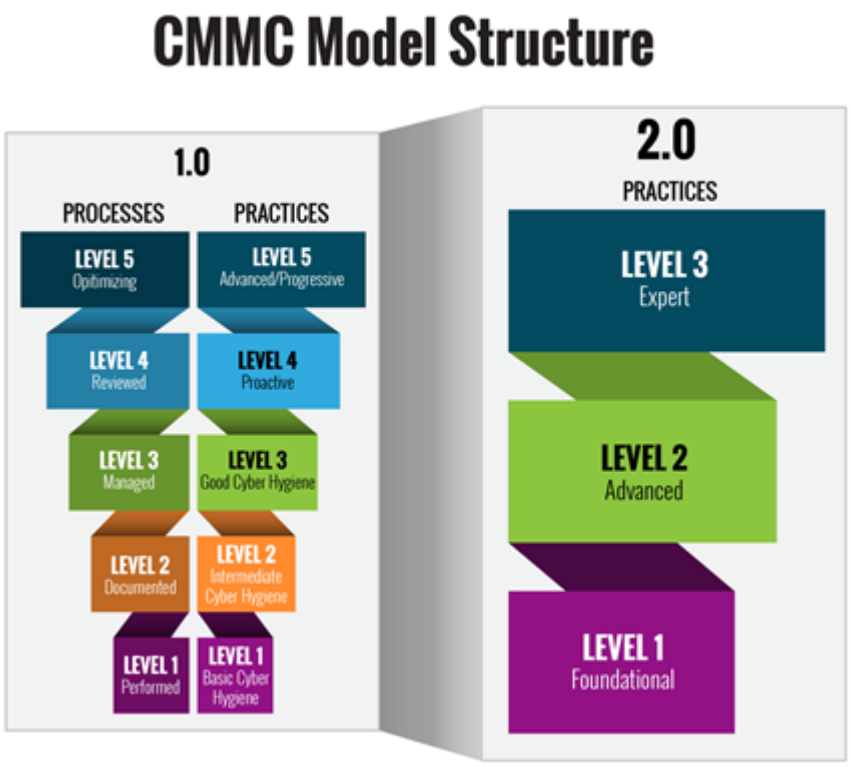
Self-Assessments of Controls

With the CMMC 1.0, defense contractors and their subcontractors could not fill out self-assessment questionnaires on their own, rather these had to be filled out by an independent CMMC Third-Party Assessor Organization, also known as a “C3PAO”.

But now, with the CMMC 2.0, these parties can self-assess their own controls that have been put into place to protect both the CUI and FCI datasets. However, this is subject to random audit by the DoD in order to make sure is all up to par, and that the self-assessment is accurate to the degree when it was first submitted. In this regard, the CMMC 1.0 was deemed to be rigid, but this new flexibility that has been offered by the CMMC 2.0 has received a warmer reception. Along with other CMMC 2.0 changes, the technical areas (called Delta 20 and required in CMMC 1.0) were removed from CMMC 2.0.

Maturity Levels

Another key difference here is in the number of Maturity Levels. With the CMMC 1.0, there were five of them, but with the CMMC 2.0, there are now only three of them, which makes obtaining certification a quicker process in order to bid on a contract. This is illustrated in the diagram below:



(SOURCE: 5).

More detail on these Maturity Levels (1-3) are as follows:

1) Maturity Level 1:

   This signifies the basic “Cyber Hygiene” and represents only those minimal controls that are needed for the protection of the CUI, as it is stipulated in the document "Basic Safeguarding of Covered Contractor Information Systems", also known as the “48 CFR 52.204-21”. At this level, the business has to implement and enforce these minimal controls.

2) Maturity Level 2:

   This level is the steppingstone for achieving a baseline of Cybersecurity for the CUI, as it is stipulated in NIST SP 800-171. At this point, the business is required to actually document on how they will establish the needed policies and procedures for a particular domain, as illustrated previously.

3) Maturity Level 3:

   This level emphasizes the full protection of the CUI, as also spelled out in NIST SP 800-171. In this stage, the business is required to create, deploy, and maintain specific plans of action for managing their activities in a particular domain.

An Increase In the Total Number of Controls

In addition to the 17 controls outlined earlier in this whitepaper, under the CMMC 2.0, there will be three new ones added, which are as follows:

- The Penetration Resistant Architecture;
- The Damage Limiting Operations;
- The Cyber Resiliency Survivability.

These can be seen in the illustration below:

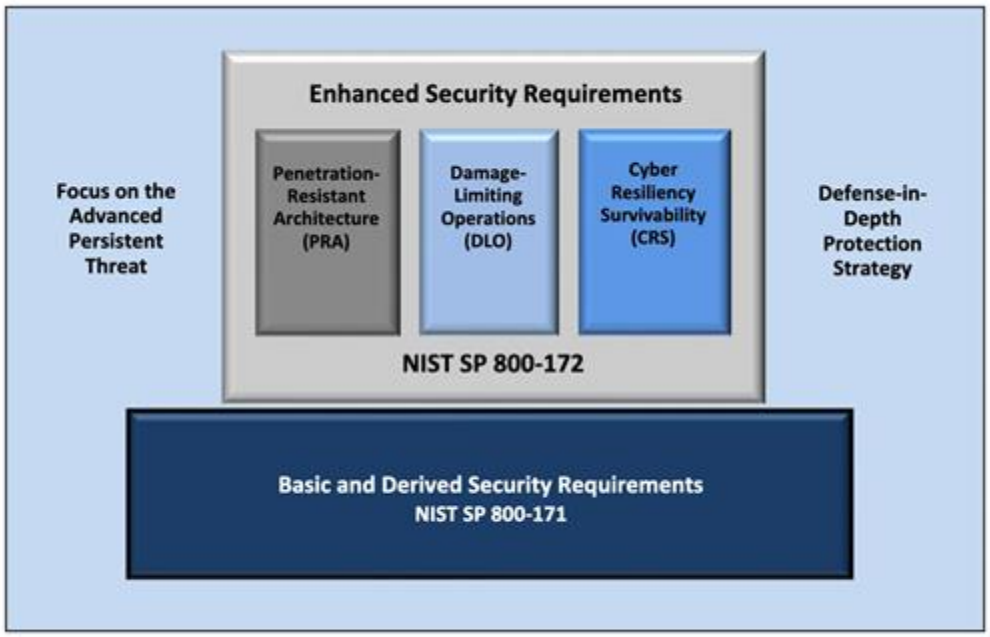


FIGURE 1: MULTIDIMENSIONAL (DEFENSE-IN-DEPTH) PROTECTION STRATEGY

(SOURCE: 5).

Choices In the Types of Assessments

With the CMMC 1.0, the rules for the assessments of controls were very strict. But with the CMMC 2.0, these have become much more relaxed. DOD has estimated that 220,000 DIBs will need CMMC certification. Here is some more detail into this:

1) At Maturity Level 1:

   Defense contractors and their respective sub-contractors can now conduct assessments on their own. The results of this must be certified by the C-Suite, and the questionnaires or checklists utilized must strictly follow the stipulations as set forth in FAR 52.204-21. DOD estimates that 140,000 DIBs will need to go through the self-attestation program.

2) At Maturity Level 2:

Self-assessments will also be allowed at this level, but for those defense contractors and subcontractors that will handle the CUI datasets, they must be fully assessed by the C3PAOs. DOD estimates that 80,000 DIBs will need to go through a C3PAO accreditation process.

3) At Maturity Level 3:

At this level, all defense contractors and subcontractors must be certified at a minimum of every three years, by a DIBCAC (Defense Industrial Base Cybersecurity Assessment Center). It is estimated that about 800 companies will need to achieve both Level 2 and level 3 certification by a C3PAO (level 2) and DIBCAC (level 3).

This is summarized in the matrix below:

Maturity Level	*Type of Assessment*
Level 1- Foundational	Annual self-assessment
Level 2 – Advanced	C3PAO or government assessments; Other programs annual self-assessment
Level 3- Expert	A government-level assessment will be required, by the Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) and CPAOs

The Use Of Waivers & POA&Ms

Another primary tool that defense contractors and their subcontractors can use is what is known as the "Plan of Actions and Milestones, or the "POA&M" for short. This is another way to conduct a self-assessment of the controls that are already in place, but the caveat here is that this plan also has to have an actionable set of items that show how any gaps or vulnerabilities will be remediated.

The POA&M was not allowed under the CMMC 1.0, but with the CMMC 2.0, it is now allowed for self-attestation and SPRS (Supplier Performance Risk System) registration, but not formal accreditation. In fact, defense contractors and subcontractors can also use this as a path to achieve CMMC certification for their particular level that they are trying to achieve. But, along with the plan of action as just described, there must also be concrete deadlines set in place as well.

Although the DoD has not exactly specified exactly what kinds of controls can be used in the POA&M, they do highly recommend that the defense contractors and the subcontractors follow closely the

guidelines that are outlined by the NIST Special Publication 800-171. Also, certain high value activities surrounding the protection of the CUI datasets cannot be included in the POA&M.

These include the following:

- Any type of Identity & Authentication Management processes or processes;
- Any Security Awareness Training programs for your employees or subcontractors;
- Any control-based audits, reviews, analyses, reporting processes, and record archiving;
- Any kind of portable storage destruction techniques;
- Any Risk Assessments, such as conducting Vulnerability, Penetration Testing, or Threat Hunting exercises.

How To Prepare For the CMMC 2.0

Now that some of the key differences between the CMMC 1.0 and the CMMC 2.0 have been detailed, the next question to be asked is how to prepare for the latter. Here are some recommendations provided by the DoD and the C3PAOs so far:

1) Make use of technology:

   Don't just rely upon the traditional paper and pen methods to keep track of all of your CMMC certification activities and milestones. Instead, centralize all of this into one electronic based recording tool so it can be accessed from one central location. Remember, the CMMC compliance process is simply not a start and stop process, rather, it is an ongoing one in which you must take action very proactively. With this in mind, it is highly recommended that you make use of tools such as the following:

   - The Microsoft Compliance Manager;
   - The use of premade templates that are available in the Compliance Manager;
   - Test your CMMC level of cloud compliance with the Microsoft Defender for Cloud Apps.

2) Avoid CUI data sprawl:

   Whenever a defense contractor or subcontractor has to deal with large CUI datasets, they tend to be stored and accessed across a wide myriad of storage devices, which include both databases and portable devices. The main security risk here is that it greatly increases the attack surface for the Cyberattacker to penetrate. You need to understand why these CUI datasets actually exist, how to label and categorize them, how to protect them, and most importantly how to avoid any sort of data leakages or exfiltration. Thus, one of the best ways to do this, is to centralize all of your CUI datasets that you are responsible for into one place. Thus, a highly recommended tool to use in this regard is the Microsoft Information Protection. Equally important in this regard is getting help and advice on the types of controls that should be put into place to protect these CUI datasets. Another tool that can be used here is the Azure Security Benchmark.

3) Further centralize your datasets:

Many contractors and subcontractors are afraid to intermingle their ERP systems with the CUI datasets they are responsible for. But, it is important to note here that such technology is another way to further centralize those pieces of data. But the right controls have to be put onto the ERP system as well. In order to do this, it is highly recommended that you make use of a tool such as the Continuous Threat Monitoring program for ERPs from Microsoft.

4) Break up the tasks:

There is no doubt that achieving the CMMC Certification at Levels 1, 2, or 3 can be a very daunting task, especially when the information on how to proceed can be confusing. Many C3PAOs have recommended that you break down the big tasks into much smaller ones, so that not only will it become much more manageable, but this will also further enhance your CMMC compliance credibility. Although in theory any project management software package can do this for you, you need one that is designed specifically for the CMMC. One of these is the Azure Landing Zone package from Microsoft.

5) Improve data analysis and correlation:

The world today, especially our own Federal Government, is driven by data, and lots of it. It is almost impossible for a human being or any team to comb through all of these datasets, especially when it comes to the CUI to find any trends, especially those that are hidden. Of course, you can always make the use of Artificial Intelligence (AI) and Machine Learning (ML) tools to do this for you, but keep in mind that these have to be CMMC compliant. If they are not, you could quite easily lose your certification by the DoD. Therefore, you want to make use of something that is already CMMC approved, such as the Central Logging & Monitoring tools that are currently available from Microsoft. Also, more than likely, your subcontractors will be involved in these kinds of processes, so the chances of any Insider Attacks from happening are even greater. To help avoid this kind of risk, it is recommended that you make use of the Microsoft Insider Risk Management Solution.

6) Show that you can handle a security breach:

Even despite all of the best efforts taken to protect the CUI datasets, any contractor or subcontractor can still become a victim of a Cyberattack. In order to lessen the statistical odds of this happening, you need to be able to respond quickly and be able to conduct a detailed analysis of what happened after the fact. Therefore, you want to use some of the advanced tools that are out there, especially when it comes to Incident Response and Forensics Investigations. Some highly recommended tools to use in this regard is the Advanced Audit from Microsoft. Although the CMMC mandates that you show your steps to compliance, it is always an added benefit to show to the DoD that you are thinking of all scenarios, including even being breached. This will show to any auditor that your organization is being extremely proactive in safeguarding the CUI datasets. Equally important here is to also prove that you are taking a huge step forward when it comes to implementing Security Awareness Training programs. Microsoft has a huge plethora of e-learning training tools that are highly regarded, with one of them being the Microsoft Learn platform.

Conclusions - The Implications Of the CMMC 2.0

As mentioned earlier in this whitepaper, the DoD has not set forth any specific timetable for the CMMC 2.0 to completely roll out, but it is highly anticipated that it will take at least two years to accomplish this goal. Although the tendency now will be for defense contractors and their sub subcontractors to take a wait and see attitude, this is actually the wrong one to take. In fact, the DoD is highly recommending that all current efforts you are now undertaking should not only be continued, but you should also try to ramp up those efforts. A cautionary note: ***Until the DOD formally changes the 2025 timeline, do not assume the timeline will change***.

Here are some key reasons why you want to take this kind of approach:

- Once the CMMC 2.0 is finally approved there will be a huge influx of defense contractors and subcontractors to get certified, and in fact, it could be as many 40,000 of them that have waited until literally the last minute. This will of course not only cause a huge backlog, but even further exacerbate the time it will take to get CMMC certified. By taking active steps now, more than likely you will achieve certification much sooner.

- By taking the certification actions that are recommended by the DoD, you will be at the front lines to be on all sorts of lucrative contracts, and those that have waited will not be able to take advantage of this. In the latest DOD town hall, DOD has stated the CMMC Level 2 will required a C3PAO for accreditation, and self-attestation will not be accepted.

- Although not publicly stated yet, there is high speculation that the DoD will even offer special incentives for those defense contractors and sub-contractors that have achieved CMMC certification earlier.

- At the recent 2022 town hall, the DOD stated that the Delta 20 (part of CMMC Release 1.0), will be integrated into future NIST 800-171 releases. The take away here is that CMMC specifications are based on the NIST 800-171 framework and will be continuously enhanced to meet current and future cyber threats.

Also, if your entire IT and Network Infrastructure is 100% deployed in Microsoft Azure, one of the best tools (along with the others mentioned in this whitepaper) you can use is the Microsoft Product Placemat for CMMC 2.0. This will allow you to view your progress towards CMMC compliance through one easy to understand dashboard.

Finally, at KAMIND IT, we have a dedicated staff that wants to help you through every step of the way to get your CMMC certification. Contact us today to see how we can work with you in this regard.

Sources

1) https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches
2) https://www.dcsa.mil/mc/ctp/cui/
3) https://enterprise.verizon.com/en-gb/resources/reports/dbir/

4) https://insights.sei.cmu.edu/sei_blog/2020/03/an-introduction-to-the-cybersecurity-maturity-model-certification-cmmc.html
5) https://techcommunity.microsoft.com/t5/public-sector-blog/the-basics-of-cmmc-2-0-and-preparation-recommendations/ba-p/3057526
6) https://techcommunity.microsoft.com/t5/public-sector-blog/evaluate-cmmc-posture-with-compliance-manager-in-gcc-gcc-high/ba-p/2179714
7) https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-list?view=o365-worldwide
8) https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps
9) https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide
10) https://docs.microsoft.com/en-us/security/benchmark/azure/overview
11) https://docs.microsoft.com/en-us/azure/sentinel/sap-deploy-solution
12) https://techcommunity.microsoft.com/t5/public-sector-blog/aligning-cmmc-controls-with-your-azure-landing-zone/ba-p/2736511
13) https://techcommunity.microsoft.com/t5/public-sector-blog/the-basics-of-cmmc-2-0-and-preparation-recommendations/ba-p/3057526
14) https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/announcing-the-microsoft-sentinel-microsoft-insider-risk/ba-p/2955786
15) https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide
16) https://docs.microsoft.com/en-us/learn/
17) https://www.microsoft.com/en-us/download/details.aspx?id=102536