WHITEPAPER

Redspin
A Division of Clearwater

10 Excellent Tips to Smooth Out Your CMMC Assessment

The Demonstration and Muscle Memory Edition

While a large part of the conversation about implementing Cybersecurity Maturity Model Certification (CMMC) requirements has been around the documentation components, the documentation is only half of the equation. The other half is demonstrating the technical configurations and providing this evidence to the assessors confidently. In doing so, the assessors can gain a sense of understanding that the organization properly knows how to address each objective in CMMC for Level 2.

Here are 10 ways organizations can ensure their assessment goes smoothly through demonstration and muscle memory:

1. **REHEARSE:**
   Assess yourself! Part of the requirements under Defense Federal Acquisition Regulation Supplement (DFARS) is to update your self-assessment score in Supplier Performance Risk System (SPRS) at least annually. Not only is this self-reporting required for DFARS, but it also satisfies one of the practice areas in CMMC at Level 2. Additionally, by rehearsing, organizations can better prepare themselves for how assessors may walk them through the assessment.

Redspin, an early adopter working with Cyber-AB to help define the program is the first Authorized CMMC C3PAO and is a RPO.

Understanding what is required for each method assessors are allowed to use, and having evidence prepared for each through the self-assessment, means that the hard work is done.

When doing the self-assessment, or rehearsal, be honest with yourself as an organization. Step through each practice and objective as if you are the assessor having no, or limited, knowledge of the organization. In addition, organizations can reach out to a third party to conduct either a gap assessment or a mock assessment. These activities help identify any areas the organization may have overlooked before going for formal assessment.

2. ACCOUNT FOR EACH COMPONENT:

Include SMEs for each component and ensure they are available and prepared. When formal assessments occur, these SMEs will be expected to respond to questions and demonstrate the objectives are actually in place. Often, cybersecurity assessments are thought of as involving IT or IS only. However, CMMC requires all areas of the organization to be included.

One of the components that is often overlooked is Human Resources (HR). While most organizations understand that when it comes to personnel screening HR will be involved, they often overlook the fact that when determining how authorized access is granted, how training is being tracked, or even how systems may be sent to colleagues or returned in a remote work environment, HR also plays an important role.

Additionally, looking specifically at AC-22 or certain Investor Relations (IR) activities, these items may be accomplished by the Marketing or Public Relations department. Looking specifically at AC-22, this speaks to ensuring Controlled Unclassified Information (CUI) information is not posted on publicly accessible systems. Most organizations account for DMZs, but the processes and procedures around how organizations ensure CUI is prevented from being posted to social media or organizational websites usually are the purview of the Marketing department. Make sure that when you are rehearsing for the assessment, these business functions are accounted for, and they know what objectives they will need to provide evidence for.

3. PRE-GAME:

a. When we are saying pre-game, we don't mean the activities most associate with a sporting event. What pre-gaming means here is that the organization should know where the specific configurations are located and how to get to them.

   One of the easiest ways to accomplish this is by having bookmarks or shortcuts tagged to the individual objectives they satisfy by whoever is going to be presenting them. This allows the organization, when asked the question, to quickly and easily navigate to where the item(s) are located. Organizations can also do this with any of the artifacts that have been provided. By having the artifacts, and how they were provided to the assessors, prepared, organizations can quickly and easily reference them during the interview portion of the assessment.

   While assessors are limited to only three methods to assess the objectives, which method will be used is determined by the assessor to meet the adequacy and sufficiency requirements. Do not simply presume that because an artifact was provided

the assessor may not ask for a live demonstration or potentially a test to ensure the criteria are being met.

4. INCLUDE NON-TECH FOLKS:

a. We mentioned earlier to ensure you include HR and Marketing when planning for the assessment. However, these are not the only individuals in your organization that you need to include.

   One of the most overlooked areas for inclusion is the physical security staff. These are the folks who are on the front lines regarding the physical protection of your environment. For instance, does the security which may be at your front desk understand everything that they should be doing anytime someone comes in? How often are they reviewing their policies and procedures to ensure they are being followed?

   As an example, on a recent assessment, the front desk security acted like they knew the assessors when they walked in. Could this mean they may overlook some of the steps in the process? What about if it was a delivery person in a familiar uniform?

   Another example of why you should include non-technical folks is that when conducting the physical walkthroughs, assessors may ask a question to someone sitting at their desk or that they see in the hallways. Do they understand what they are supposed to do if they encounter CUI? It may seem excessive, but it builds credence to the organization's awareness and training activities.

   One more example of why this is important can include ancillary employees who are not commonly viewed as part of the security function. Think of warehouse individuals who may have separate video systems. Do they review the cameras regularly? Do they understand where the cameras they are responsible for are located? What about if they see someone who is un-badged or not in company attire? Have they been trained to challenge them or report them to official security?

5. PLAN FOR THE SURPRISES:

a. Despite any organization's best efforts, there are always unknowns that tend to occur in assessments. It could be a door left unlocked, a respondent not understanding their responsibility, or even someone suddenly not being able to join the assessment that was expected to be an SME. These happen and often offer a first-hand view of how an organization responds to these events. Does the organization have vetted processes to address them?

   What about technical issues that always pop up? In an assessment, let's say that someone cannot get to a resource from their account, or their system goes down. In these scenarios, what is the backup plan? Can the organization pivot to ensure the evidence the assessor(s) need is still able to be conveyed? Systems go down from time to time and, according to Murphy's Law, this will probably happen during the assessment.

In the cybersecurity lexicon, these types of events speak to an organization's contingency planning. Has the organization identified how to ensure the mission, in this case, the assessment, is still accomplished? While it may seem like this is something trivial in the grand scheme of things, it speaks to the confidence the assessor(s) can gain in the organization. By not "freaking out" or throwing their hands up, the organization provides evidence of maturity in what they do.

Pro-tip in this case is to complete a risk responsibility matrix. This activity identifies who has primary responsibility in particular areas as well as identifying the backup. For purposes of an assessment, what this allows is:

- Identification of who will be answering the questions
- Backup in case the primary responder is not available
- The organization directs the assessment

Additionally, what can be included in the matrix is a summary of where the artifacts and documentation that address each practice are located. In doing so, the assessors know directly where to apply the evidence received much like what was mentioned earlier.

6. TAKE OWNERSHIP:

What the matrix we just talked about allows is for the organization to take ownership of the assessment. It ensures that each SME that is going to be speaking or presenting understands that he or she is going to be responsible for driving the review of their particular area. As an example, when looking at AC 3.1.1, assessors are going to want to ask questions about how the organization identifies authorized users, processes, and devices. If you have rehearsed the assessment based on the objectives, then the SMEs can provide the specific information needed.

Additionally, the SMEs should be able to speak to the documentation and artifacts provided. In doing so, the assessors are stepped through the evidence provided which ensures evidence provided is not overlooked. Plan for this as for each system or service in scope, if it is a CUI asset or Security Protection Asset (SPA), then each practice has to be satisfied. One of the ways some organizations have gone about preparing for this is by providing an outline of the items to everyone who will be in the assessment. While this can be burdensome to some extent, it keeps everyone on the same page while the assessment is occurring. Having the outline also allows notes to be taken both for any additional evidence the assessors require as well as for preparation the next time the organization has to be certified.

In summary, think of it as a conversation:

- Organization "X" can you talk to us about how you authorize the users, processes, and devices?
- Yes, for our authorized users, these are identified via "Y" as documented in our SSP/Policy/Procedure. Each user is limited by "this mechanism" for these systems/services as evidenced in artifact "Z"
- To confirm this is in practice, "This Admin" will provide a screenshare of "these items" to verify the users are limited to only those authorized.

This conversation would repeat for the processes and devices that are within the scope.

7. EDUCATE THE DEFAULTS:

Earlier we spoke about the unknowns and how inevitably they occur in every assessment. In addition to the unknowns, organizations have to be aware of any defaults that are enforced by their systems or services. In this instance, the defaults are items that cannot be changed and often are seen when using third-party services. These instances are where shared responsibility matrices come in, but also the organization has to provide evidence of their due diligence with the practice and objective.

If these items are enabled and the organization cannot change the setting, then two things should occur in the assessment.

The first thing is that the organization identifies upfront that they cannot change the setting. Also, evidence should be provided showing the vendor explicitly states that the setting cannot be changed. This is usually through a website or some other type of documentation. If the default is set based on an industry benchmark, ensure you identify it to the assessors. An example of this could be how the vendor established the user provisioning and authentication of the system or service. Perhaps the third party defaulted to authentication configurations based on NIST SP 800-63b as an example.

The second thing is that if the defaults do not satisfy the objective, then the organization has to provide evidence showing what has been put in place to meet requirements. An example of this could be additional configurations for MFA, utilizing VPN technology to protect the CUI in transit, or even having offline storage for particular items. Remember, the onus is on providing the assessors with the proper evidence from an adequacy and sufficiency standpoint to satisfy each objective.

8. EXPLAIN THE NUANCES:

Nuances speak to situations where the expected configuration is not in place. Using SharePoint as an example, to ensure any CUI stored at rest is protected using FIPS 140-2 validated encryption, the expected way to enforce the setting is through a specific Group Policy Object (GPO). However, in certain configurations, it may be operationally necessary for the specific GPO to not be set. In these situations, the organization should identify why the expected configuration is not set (e.g., operational necessity), identify what has been put in place, and address if the nuance is based on an authoritative source.

Keep in mind that operationally necessary does not mean the same as operationally convenient. Also, authoritative sources may not mean vendor documentation. In the SharePoint example, has the nuanced configuration been defined in a DISA STIG, CIS Benchmark, NIST Guidance, etc.? If so, then provide the justification to the assessor, speak to the configuration in place, and ensure the evidence supports guidance.

To this point we have been speaking of mostly technical items via the evidence. However, another nuance could be procedural documentation. This is where the shared responsibility matrix comes into play as activities normally conducted by the organization may be the responsibility of the third party.

As of this writing, the specific scoping guidance under the final rule is not known. Once it is known, then there may be specific requirements on what the third parties have to go through for use in a CMMC-validated environment. This could include the third party having to go through CMMC validation itself, reviews by a 3PAO (FedRAMP equivalent of a C3PAO) for cloud service providers, or other items that will be specified. In this case, keep abreast of what the rulemaking process defines.

9. DON'T FORGET THE DETAILS:

Somebody famous, or at least infamous, once said, "The devil is in the details". This is never truer than when going through a CMMC assessment. The details are what is expected and should be included in the objective evidence.

An example of this is when addressing AC 3.1.3, Control the Flow of CUI. Often, organizations identify that they are controlling the flow, there are VLANs in place, conditional access policies in place, or any other number of items. However, organizations often neglect to identify if there are Access Control Lists (ACLs) on the VLANs, how they identified what conditional access to put in place, or specifically how they control the flow.

Additional details could be in the background checks or offboarding procedures. This doesn't mean assessors expect to see actual background checks or offboarding actions. Instead, this speaks to identifying what occurs in each of these activities under Personal Security. As a reminder, this domain brings in the SMEs outside the IT/IS function. They may not be aware of the level of detail assessors ask for nor what they should provide as evidence.

For instance, do the background checks identify the nationality of the individual? Is the background check benchmarked against a well-known standard (e.g. Office of Inspector General)? Do offboarding procedures remind folks of their ongoing responsibilities to the confidentiality of the CUI they were exposed to? What about recovery processes for equipment in a remote work environment?

Another detail that could be overlooked is the physical protection of CUI in remote work environments. You may be thinking, "We address these when working at customer locations." While this is a valid point, in a post-COVID world, accounting for homework environments should also be addressed if the organization authorizes access to CUI remotely.

10. REHEARSE AGAIN:

So, you have gone through the steps, you have reviewed all the documentation, met with all the SMEs, and rehearsed the assessment. Now, do it again! In the sports world, successful teams understand that if the team puts in the work during practice, then the game is easy. This holds for a CMMC assessment as well.

Rehearsing again ensures that all the items you put in place have been accounted for. It provides the practice needed to accomplish the mission, which in this case is passing a CMMC L2 assessment. Speaking from personal experience, when Redspin was getting ready to be assessed, we:

- Reviewed all the artifacts and documents
- Matched it to the configurations
- Walked through the objectives via a checklist
- Brought in a third party to review everything
- Scheduled targeted review sessions with each SME
- Constructed playbook outlines for everyone who would be in the assessment
- Went back and did it again!

Doing this cadence helped us uncover any items we may have overlooked. This also helped to provide confidence for our SMEs that may not have been through an assessment like this before. Using the third party allowed for a fresh set of eyes that had not spent days and months looking at the same information. Reviewing the information in a targeted format provided the SME with experience in answering questions, moving between different pieces of information, and handling the curveballs that the SME may not have thought of. While I know this item has used a good deal of sports analogies, a CMMC assessment is much like a sporting competition. That's why having playbooks helps immensely, especially for those who are nervous. Now, doing all that, we went back and did it again, and again, and again until the actual assessment happened.

A CMMC assessment can be strenuous for any organization. Passing the assessment means that the organization can continue to bid on and be awarded contracts. By working through each of the steps above, the organization should be in a good place once the "Game" starts. While throughout parts of the above, we have used sports analogies to help illustrate each item the individual elements can be compared another way. "'If you know the enemy and know yourself, you need not fear the result of a hundred battles." (Sun Tzu). What this means is that the more you understand what the assessors are going to ask, the more you know what you have in place, and then you should have no fear for your CMMC assessment!

WHY REDSPIN

- Over 100 security advisors and assessors, ready to scale with you as needed
- Possesses the know-how from performing over 1,000 assessments in highly regulated industries, including the first successful Joint Surveillance Voluntary Assessment Program (JSVAP) assessment
- Uplifts its service offering to validate your security, giving you the confidence that your people, processes, and technology are effective
- Our team understands CMMC requirements and follows professional conduct to help you on your journey to becoming CMMC-ready and certified.

Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies for the Defense Industrial Base. Our exclusive focus on tailoring our CMMC assessment, training, consulting, and managed services for each client delivers peace of mind by lowering the risk of a security incident or breach, and meeting/maintaining compliance regulations. Since our founding in 2001, we've become a thought leader in IT security, helped countless clients control their security risk, develop their security strategy, and avoid a breach headline.

Redspin
A Division of Clearwater

40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
800.721.9177
www.redspin.com