CMMC Level 1 Assessment Guide: A Closer Look

Featuring Andrew Hoover as Interviewed by Katie Stewart

Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Katie Stewart: Hi, and welcome to the SEI Podcast Series. My name is Katie Stewart. I am a senior engineer with the CERT Division at Carnegie Mellon University. I would like to welcome my colleague, Andy Hoover. Andrew leads the Resilience Engineering Team at the SEI CERT Division at CMU.

So in today's podcast, we are going to talk about the Level 1 Assessment Guide for the CMMC or the Cybersecurity Maturity Model Certification. But first, we are going to give our listeners just a little bit of background on who we are and what brought us here. So again, I am Katie Stewart. I have been with the SEI about seven years. I have been involved with the development of CMMC from the beginning. My primary research focus at CMU is in risk and resilience as well as measurement and analysis. So, Andy, can you tell us a little bit about yourself?

Andrew Hoover: Yes, sure. Thanks, Katie. So as mentioned, I am Andrew Hoover. I lead the Resilience Engineering Team here at the SEI. I have been in the organization for about eight years mainly focusing on cybersecurity architecture, cyber resilience, and critical infrastructure protection, which is how I got involved in CMMC. I have been on the CMMC development team like Katie ever since the very beginning of the project.

Katie: OK, great. Thanks, Andrew. So, if this is your first time tuning in to a CMMC podcast, just know that we put out a lot of material around CMMC, so I encourage you to go back and listen to some of our other podcasts. We also have a series of blogs that really set the stage and give background and overview of the model as well as our role in the development. So, we are going to jump right into assessment guides in this podcast, but we will link to all of the resources that I just mentioned in the transcript of this podcast.

All right, so let us get started. Like I said before, we are going to talk about the CMMC Level 1 Assessment Guide. It just came out, and it has been really highly anticipated. We are going to try and give you a good overview of what is in that guide. The first thing to remember is that a Level 1 organization will only be authorized to store, process, and transmit FCI, which is federal contract information, so when you are going through this Level 1 guide, you will only focus on protecting FCI. We are going to do a couple more podcasts, and in that next one, we will talk about the differences between Level 1 and Level 3, and that is where we will get into the distinction between FCI and controlled unclassified information, or CUI.

Our past two recent podcasts really dove into assessment guides and what they are and how they can be used. But I think it would be good to recap some of that today. So, Andy, can you just give us a quick overview, just a recap of what we talked about before around what is an assessment guide, and then really talk about, in the context of CMMC, what they mean?

Andrew: All right, so an assessment guide is a document that assessors will use to guide their CMMC assessment, obviously. But, it is also a guide that the organization seeking certification or OSCs can and should use to prepare for their assessment. The guide will document all of the applicable practices that are relevant to a specific domain as well as the details that the assessor will use to determine whether or not those practices have been effectively implemented. In our last podcast, we mentioned this would be two guides: there is a Level 1 assessment guide, and there is a second guide; it is going to cover levels 2 and 3. This podcast is just going to focus on the Level 1 guide. Now, that said, it is important to keep in mind that CMMC is cumulative. Even though we are only going to discuss the *Level 1 Assessment Guide* today, pretty much all what we are going to talk about will also be applicable to Levels 2 and 3, because the Level 1 practices have to be achieved to successfully achieve Levels 2 or 3 of CMMC.

Katie: Yes. I think that is a really good overview. I like to think about the assessment guides as, *This is the exam. But not only is this the exam, it is also all the answers to the exam*. As you are going and you are preparing for your assessment, the assessment guide will be your number one document or artifact that you will use as an organization to prepare. OK, so let us dig into it. Can you walk us through some of the specific details of a Level 1 assessment guide? I think we should start from the beginning.

Andrew: Yes. Your analogy about the exam and the answer to the exam is really good. The first thing that people should do when they are reviewing the guide is look at the front matter. Now, I know it sounds funny, and people are going to laugh, *Like, of course, we are going to start at the front of the guide*. But a lot of people are going to be very anxious to get to the practices, which make up the bulk of the guide. So they could very well just skip over the front. Please do not do that because it touches on some really important stuff. We begin to talk about scoping there. We talk about criteria and methodology, and even scoring. So there is really important stuff that

people could miss. The front of the guide really lays the groundwork and provides really good context that is needed to look at the practices.

Katie: Yes, and I think you will also see in the beginning that there are some terms that maybe you are not familiar with. The introduction does some definitional activities, walks through some assumptions that are made around assessments. So really, really give that a good read. It is so super important to do.

Andrew: Yes, for sure. Something else to mention, when we look at the front of the guide, there is a section about scoping up there, but it is pretty short. The reason that it is short is because Appendix A goes into much greater detail on how to scope your CMMC assessment. We are going to touch on that a little bit today, but we are definitely not going to focus on it a lot, because we are going to do another podcast. It is going to really deep-dive into Appendix A and how to scope a CMMC assessment. So, again, do not skip the front matter, really important stuff there. So when you open up the assessment guides, be sure to start there.

Katie: The other podcast on scoping I think will be very, very valuable for listeners. That is one of the key hot items that we get asked almost every day. OK, so, let us actually walk through maybe just one practice from an assessment guide and just talk through the different components that our listeners will find in that guide.

Andrew: Yes, let us do that. So, I think the practice that we should start with, let us go look at AC-1001. That is the very first practice in the model; it is right up front so let us start there. Now when you look at that, the first thing that you are going to see is obviously the *Identifier* and the *Practice Statement*. OK, now moving beyond that, next we see the *Assessment Objectives*. Now, this is important, because these are the specific items, the specific objectives that must be met in order for that practice to be marked as implemented. All of the objectives for a given practice have to be met in order for the practice to be implemented. That is a very, very important aspect of CMMC.

You will notice that there are a varying number of assessment objectives per practice. This one has six. You can see them listed here as a through f. Some of the practices have, I believe, up to eight in Level 1, and there are some, a handful, that have just one. So they are kind of all over the place.

Katie: Yes, so just to remind everyone, and we talk about this in our previous podcast, but the Level 1 practices are all sourced from the FAR [Federal Acquisition Regulation]. So, those are also present in 800-171. What Andy is talking about when he talks about assessment objectives, those are all taken verbatim from NIST Special Publication 800-171a. That is the companion

document to 171, which really guides the assessment of the security practices in 171. So, if you are familiar with 171, Alpha, the *Level 1 Assessment Guide* is going to look very, very similar.

Andrew: You can see right above the objective there where it says NIST SP 800-171A, if you are looking at AC-1001, you will see that right above the objectives. In the next podcast when we start on Levels 2 and 3, that is where we introduce Practices and Controls that, of course, are outside of NIST 801-71. You will begin to see references to other standards there or even reference to CMMC because remember, when we could not find a practice that we thought needed to be added to the model from another relevant standard, we wrote it ourselves, and so you will see those references too.

Katie: Right. All right, so let's go back to the guide. What is after the assessment objectives?

Andrew: The next thing you will see, Katie you have covered this last time, so we will quickly walk through it, but you'll see the *Potential Assessment Methods* and *Objects*. If we continue to highlight what we see in AC.1.001, the methods are things like *Exam and Interview and Test*. Now, this is how it is laid out in 171A, and this is how it is laid out in the CMMC assessment guide since CMMC is built on top of 171, which has adopted the way that that their assessment guide flowed. The interview, test, and examine are the ways that an assessor will determine the implementation of a practice. Now, there are also assessment objects, for each of these, and the objects are the specific items that the assessor will look at. So maybe it is a document, maybe it is a suggestion for the type of people that you want to interview, or a test that you want to see.

So, we will go back and look at AC.1.001 again. Objective A says, *Authorized users are identified*. Now, to assess this practice, the assessor may want to review a list of active system Accounts. Seems like a really good place to start. And you can see that listed under the examine method—List of Active System Accounts and the name of the individual associated with each account. So that is there. Maybe the assessor wants to see a test. In the context of a CMMC assessment, there is a bit of a nuance with the test here because that CMMC assessor obviously is not going to be authorized to perform an actual test on another organization's system, but they can observe someone that is a part of that organization performing a test. And you can see potential tests that are listed right there under that method.

Katie: I also want to make the point, we mentioned it last time, but these lists of potential objects on there to examine and folks to interview and all that, it is not meant to be all encompassing. If an organization has another set of artifacts or different individuals who should be interviewed, or even different demonstrations in the test that they think would meet the assessment objectives as they are laid out, as long as the assessor agrees that they are applicable, that is perfectly acceptable for a CMMC assessment.

Andrew: That is a really good point. It is really meant to be a starting point for the assessor and the OSC to demonstrate the implementation of a practice. All right, so, going back to AC.1.001. The next thing that you see listed in the assessment guide is the Discussion. For the Level 1 guide, the text here in the discussion comes verbatim from 800-171, Rev. 2. The CMMC development team wrote the Further Discussion section, and this is where we really tried to clarify things that we thought were a little bit unclear. Maybe something in the practice or the objectives or even in the discussion, we attempted to provide some clarifying language there. When you look at the CMMC clarification, you will notice that we included references which link back to the Practice Objectives. So, going back to our example of AC.1.001, the first sentence discusses the identification of users, processes, and devices, and it is followed by a reference to Objective [a]—you can see it there in the brackets at the end of that statement. That means that that part of the further discussion directly relates to that particular assessment objective, and that is important because we sometimes did not cover all of the objectives and the further clarification. So, we wanted to be very clear about what was covered and what statements reference back to which objectives. Then for each practice, we provide at least one illustrative example. Some of the practices have more than one, but you can see that here in Example 1. The examples also include the references going back to the assessment objectives, which we think is really helpful. Then people will know when we wrote something in there what specific objective we are referring to.

Katie: So back to examples for a second. These are not meant to be the way an organization *must* do something right? They're just representative of *a* way.

Andrew Yes, that is a good point. They are only meant to be kind of an illustrative example. So it is a way that you can do something, not a way that you have to do something.

Katie: Also, even if you do it that way, you are not necessarily guaranteed to fully pass the practice, right? Sometimes they do not include all of the objectives.

Andrew: Exactly. Like I said before, just like the CMMC clarification that we added, the examples do not include all of the objectives. Sometimes they do, but not always, and so, the implementation of a practice by just following the example is not recommended because you might not get there and there might be a better way for you to do it. Perhaps your organization is already doing it a different way that we didn't necessarily highlight in our example, but that is a way that it can be done.

So, moving on here. The next section is the Potential Assessment Considerations. These are statements, sometimes they are questions, that may help an assessor determine if an organization is meeting the assessment objectives. We include the references back to the objectives here as well. The first one in the list in AC.1.001 is a list that authorized users maintain that defines their

identities and roles. We reference that to Objective [a]; it might even relate to others. But it is important to remember further discussion examples, potential assessment considerations, these are not meant to be prescriptive or comprehensive, like Katie just mentioned, so I do not want people to misinterpret their use.

Katie: Good. So, I think the last thing that is left to talk about is, we list the key references at the end of each of the practices. As I said before, these are all sourced from the FAR, so you will see that reference included, as well as the corresponding reference to 800-171.

Andrew: Yes, so quickly, another thing I wanted to mention too, while not in a lot of detail, I wanted to quickly go over Appendix A—and, Katie, jump in here wherever you want to—but we are going to do a podcast on this directly, so we are just going to give a quick high level. If you go into Appendix A and you look at Figure 1, you will see Assessment Boundary and Certification Boundary. These are very important for scoping your CMMC assessment. The Assessment Boundary identifies the assets and the contractors' environment that need to be included or at least considered for the CMMC assessment. All right, now this is different than a Certification Boundary, which is where the CMMC practices are actually implemented. That is a really important distinction for CMMC, because there are some assets that an organization might not apply all of the CMMC practices to, but are still relevant to the scoping and the discussion around your CMMC assessment.

Katie: I think that is really good, that is a really good point. Great, well that was a great overview of *Level 1 Assessment Guide*. I am looking forward to looking at the Level 3 guide as well as the future discussion on the scoping appendix. I think that will be really good.

Andrew: Yes, I think that both of those are going to be really helpful to organizations that want to achieve Level 3, but then also, organizations that want to achieve any level in CMMC can refer back to the podcasts on scoping that we are going to be releasing.

Katie: All right, well, Andy, thanks for being here and talking us through the Level 1 Assessment Guide. For all of the resources we mentioned, we will provide links in the transcript in this podcast, and as always, if you want to reach us, feel free to email us at info@sei.cmu.edu. Or you can find us on LinkedIn [Katie] [Andrew], and we look forward to hearing from you. Thank you.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, Stitcher, TuneIn Radio, Google Podcasts, and Apple Podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally funded research and development center sponsored by the U.S. Department of Defense. For more information

about the SEI and this work, please visit www.sei.cmu.edu. As always, if you have any questions, please do not hesitate to email us at info@sei.cmu.edu. Thank you.