The CMMC Level 3 Assessment Guide: A Closer Look

featuring Andrew Hoover and 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.

Andrew Hoover: Hi, and welcome to the SEI Podcast Series. My name is Andrew Hoover. I lead the Resilience Engineering Team here in the SEI's CERT Division at Carnegie Mellon University. I would like to welcome my colleague, Katie Stewart. Katie is a senior engineer also in the SEI's CERT Division. In today's podcast, we are going to focus on the Cybersecurity Maturity Model Certification or CMMC, Level 3 Assessment Guide.

First, we are going to tell our guests a little bit about ourselves. Again, I am Andrew Hoover, been at the SEI for about eight years. I mainly focus on cybersecurity architecture, cyber resilience, and critical-infrastructure protection, which is how I got into the CMMC. I have been a member of the model-development team since the very beginning of the project.

Katie, can you tell us a little bit about yourself?

Katie Stewart: Yes, sure. I am Katie Stewart. I have been with the SEI about seven years, primarily focused on risk and resilience as well as measurement and analysis. Like Andrew, I have been involved with the CMMC model team since the beginning. I am really excited to continue the discussion around assessment guides.

Andrew: OK cool, thanks Katie. For the members of the audience who are new to CMMC, we have done a bunch of blog posts, webcasts, podcasts, and other things that provide a really good overview of CMMC and the work we have done on it. We will link to all of those resources in the transcript of this one, so people can find it. Let's get started on the podcast for today.

Today we are going to discuss the CMMC Level 3 Assessment Guide. Our last podcast, we did a deep dive into the Level 1 guide; today we are going to primarily focus it on the differences between the Level 1 guide and the Level 3 guide.

As I said, we have a previous guide that focuses on the Level 1. We talked about how organizations at Level 1 are only authorized to store, process, and transmit federal contract information; that is FCI data. So therefore, the Level 1 guide only focuses on protecting FCI. One of the major differences in the two guides is that with CMMC Level 3, an organization is authorized to store, process, and transmit controlled, unclassified information or CUI. So that is the big difference and the big distinction between the two guides.

But Katie, can you tell us a little bit more detail, not only about FCI and CUI, but also the distinction between the guides?

Katie: Yes. When we talked last time about the Level 1 guide, you did a really good job stressing how important it is to read the upfront matter. If our listeners have gone and done that, with the Level 1 guide, and then they open a Level 3 guide, they will see a primary difference immediately in the guide.

First and foremost, the Level 3 guide has detailed information specifically around scoping a Level 3 assessment, and Andrew just explained that. A Level 3 assessment is looking to get certified to process, store, and transmit CUI. So, an organization can think about achieving a Level 3 certification for two different use cases.

Andrew: OK, so I assume, Katie, that the first use case is the entire enterprise, right? Basically, an organization would have CUI spread out everywhere across their enterprise; thus, the whole enterprise is in scope. Is that right?

Katie: Yes, that is exactly right. Then, if you think about use case number two, this would be where an organization would store, transmit, and process CUI within an enclave. Perhaps they have FCI in their entire enterprise boundary, but they really sectioned off in this enclave where they are going to handle CUI.

Andrew: OK, so that is interesting. In that scenario then, so that I understand it, the entire organization would have like a Level 1 CMMC certification because they have FCI data. But, then, they have segmented off some systems where they store, process, transmit CUI data. That enclave is the only area that would be applicable to the Level 3 certification because that is where the CUI is?

Katie: Yes, exactly. We encourage organizations to really think through how they are going to segment their network for these certifications.

Andrew: Yes, that is a really important concept. There is a lot of interest in that, so we are definitely going to deep-dive into that, in a future podcast, where we talk about Appendix A and scoping the assessment. Katie, can you tell us what else makes the Level 3 guide different from the Level 1 guide?

Katie: Yes, building off of the boundary discussion that we had earlier, when an organization receives a Level 3 certification, that means that they are authorized to process, transmit, and store CUI. The reason why is because they meet all of the 110 security requirements that are outlined in NIST 171. Now, the CMMC model, if you have listened to our other podcasts or are familiar with the model, there are additional requirements on top of that, but fundamentally, the ability to have CUI is given because they meet all 171's strict requirements, and those are all outlined in the Level 3 assessment.

Andrew: OK. Just to be clear here, when we say, *satisfied*, we mean that the organization has successfully implemented that practice, right?

Katie: Yes, that is right. And as we talked about before, when we say, *implemented a practice*, that actually means that you have satisfied all the defined assessment objectives for that specific practice. Just like in the Level 1 guide, for the 171 CMMC practices, those assessment objectives will be verbatim from this special pub 171, Alpha (NIST Special Publication 800-171, Rev. 1), which again, is the assessment methodology for NIST 171.

Andrew: OK, good. So that brings up the next point that I want to highlight, which is the next really big difference in the L3 guide. Do you want to go into it a little bit more?

Katie: Yes, I touched on it earlier. There are additional requirements, so it is not just what is in 171. And those fall into two categories: we have the introduction of delta practices, which you will see at Levels 2 and 3—so obviously, they will be in the guides—as well as process maturity.

Andrew: Right. So, firstly can you remind everyone what a delta practice is? I mean, that is kind of our internal term, right? What do we mean when we say, *delta practice*?

Katie: Right. We use it to describe the practices that are not verbatim from 171. There are 20 practices at Levels 2 and 3 (they are spread out over the two levels) that we felt needed to be added to the CMMC model to round it out for good cyber practices. You will see the assessment objectives and the objects and the methods. The structure will be exactly the same as the NIST 171 practices, but these were developed by the model team using some of our key references. In some cases, if we felt we needed to add to it, we developed it just as a model team. But again, the structure will be identical to the 171 Alpha structure, which is also the CMMC assessment-guide structure.

Andrew: Right. So, that is the delta practices. Now, something else to mention here, I think, is that in Level 2, we introduced process maturity, which carries over into Levels 3, 4, and 5. So, Levels 2 and 3 in this guide, are going to have process-maturity requirements as well. When you say delta practices, you said there are 20 of them; that does not include the process-maturity practices. So can you talk a little bit more about that?

Katie: Yes, sure. At Level 2, there are two maturity processes for each domain, and at Level 3, there is one for each domain. Now, we kept the structure the same. For each of these process-maturity processes, we have defined assessment objectives as well as the methods and the objects and the discussion. The process-maturity component of CMMC will follow the same structure as the CMMC practices. There is a lot of information there, and I think it is really important for our listeners to think through how are they going to tackle process maturity? The assessment guide is actually one of the key resources to start with, because there is so much information around each of the maturity processes within CMMC.

Andrew: All right. Just to summarize that, the Level 2 and 3 assessment guide is a great tool for organizations to get a handle on, and understanding of, how they are going to be assessed for process maturity in CMMC. It is probably also useful for Level 1 organizations, right? Because a lot of Level 1 organizations will eventually progress or want to progress to a higher level. So even if an organization is at Level 1—they have used the *Level 1 Assessment Guide* to get there—they can use this guide to understand not only the practices that are required at Levels 2 and 3, including the delta practices, but also the process maturity that is going to be there. Process maturity takes time; it takes time to implement, it takes time to institutionalize, and so the assessment guide is a great place to start, if not the best place, for an organization that wants to implement process maturity to get started in understanding what the requirements are.

Katie: Absolutely, and just like the practices, we list out the artifacts, various people that could be interviewed, and things that can be examined, which really helps, I think, clarify the types of activities that need to go into prepping for the process-maturity component of the CMMC assessment.

Andrew: Yes. Well, you know, Katie, this was a great overview of the differences between the Level 3 guide and the Level 1 guide. I really appreciate your time here, and I am really looking forward to the deep dive into the scoping activities, which I think is going to be really helpful as organizations start implementing these things.

Katie: Absolutely. It is one of the most important concepts around the CMMC assessment, so it should be a good discussion.

Andrew: OK, Katie. Thanks again for being here. As a reminder to the audience, we will put the links in the transcript to the other podcasts and the other content that we mentioned. Stay tuned for more podcasts focusing on CMMC. The next one will focus on the Appendix A or the scoping appendix. As always, if there any questions, reach out to Katie or me through the SEI email at info@sei.cmu.edu or you are welcome to find us on LinkedIn [Andrew] and [Katie]. We would love to hear from you. Thanks and have a good day.

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.