CMMC Scoring 101

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, and I am a senior engineer in the SEI's CERT Division. I am joined today by my colleague, Andrew Hoover, who leads the Resilience Engineering team, which is also in the CERT Division at SEI.

So, today, we're going to talk about scoring within Cybersecurity Maturity Model Certification, more commonly known as CMMC. So, if you are new to CMMC, a quick background. It was created by the Office of the Undersecretary of Defense for Acquisition and Sustainment to protect controlled, unclassified information, or CUI. The idea with the CMMC is that it will apply across the DIB supply chain, or the Defense Industrial Base supply chain. It is a new certification.

There is a lot of information out there. We have put out a number of blogs, podcasts, and webinars on our website, so we will link all of those in our podcast transcript. There is also the OSD, the DoD [Department of Defense] website, which is the authoritative source on the model, and you can also reference the CMMC Accreditation Board website, which we'll link as well, which can give you up-to-date information about the accreditation process for CMMC.

Today, we are going to mainly talk about scoring and how the CMMC model will be scored for these organizations. But before we dive into that, just a little bit of background on myself. I have been with the SEI about seven years now, primarily focused on risk and resilience and measurement and analysis, supporting the CERT Division. Like Andrew, I was one of the key architects of the CMMC model. Andy, do you want to give a little bit more of your background?

Andrew: Yes, sure. Thanks, Katie. I have been at the SEI for about eight years. I am a team lead on the Resilience Engineering team, which is part of the Cyber Risk and Resilience Directorate. Like Katie, for the past year and a half, I have been working on CMMC. Katie and I are two of the chief architects of the model itself.

Katie: Great. Thanks, Andy. So, we are going to just dive into scoring CMMC. If you are not familiar with CMMC, it has five levels. So, just at a high level, Andy, can you tell us a little bit about each of the five levels and why it matters for organizations to think about what level they want to pursue?

Andrew: Yes. That is a good question. So, organizations really need to determine the best level for them to be at. It is really going to depend on what sort of contracts they want to bid on for the DoD. So, the required CMMC level for each contract will be set by the DoD program managers, and it will be listed in the RFP [requests for proposals] and the RFIs [requests for information] for those contracts. Just a reminder: the DoD thinks around 80 percent or so of organizations are just going to need to achieve Level 1, which is compliance with the basic safeguarding requirements in the FAR, the Federal Acquisition Regulations.

Level 2 is then just a transitional step. DoD has come out and said a few times now that they don't really anticipate Level 2 being included in many contracts, if at all. It's just a step to help organizations that are at Level 1 that want to ultimately achieve Level 3 and progress through the maturity model.

At Level 3, an organization has accomplished all of NIST 800-171, and they have also accomplished 20 additional practices that we added to the model. This is the level that organizations will need to be at if they want to store and process and have access to CUI data, or controlled unclassified information. Then Levels 4 and 5 are reserved for DoD special programs. They primarily consist of proactive and progressive practices, more advanced things that are not going to be applicable to most organizations. All organizations are going to need to achieve at least CMMC Level 1 in order to be awarded a DoD contract. So, again, that is probably going to be at least 80 percent of organizations.

Katie: Yes. I think that is good. I think you hit on some good points there. Another thing I would add is the model, it has two sides to it. There is the process side, and there is the practice side. When you are pursuing one of these levels that you talked about, an organization must demonstrate achievement on both the practice side and the process side. If you are familiar with the model, you know at Level 1 there is just demonstration of practice. But for Levels 2, 3, 4, and 5, the organizations are going to have to show that they can do both the practice side and the process side in the model. So, I think that is a key point in the scoring as well.

Andrew: Yes, that's a good point, and I'm glad you mentioned that, because it is kind of a misunderstood aspect of the model, but you'd have to do both at Levels 2 through 5. Something else that is important to note is that the model and the practices are cumulative. So, just for example, an organization that might want to achieve, say, Level 3, which is where you are going to have to be to have access to CUI data, not only do you have to complete the practices and the

processes at Level 3 but also at Level 2 and the practices at Level 1. So, it's cumulative. You have to accomplish everything at that level plus the lower levels in order to move forward. The same, of course, goes for Levels 4 and 5. In order to achieve Level 4, you not only have to accomplish the Level 4 practices and processes, but also those at the lower levels.

Katie: One last thing that I'll add is that, yes, there are two sides, and you are going to be assessed on each side, but you are actually only going to receive one score. So, if the organization is pursuing Level 3 like you described, but they complete all of the Level 1, 2, and 3 practices but only show process maturity at Level 2, that organization is only going to receive a Level 2 certification. I think that that is important to understand. Your awarded CMMC level will only correspond to the lowest level achievement on either side of the model, regardless of what you set out to pursue or to achieve when you go for your assessment.

Andrew: So, Katie, I think what you are saying there is that if an organization attempts to achieve Level 3, but say they haven't implemented one of the practices or processes at Level 3, they are not going to walk away empty, right?

Katie: No, they will walk away with a Level 2. So, it will be the lowest level that they achieve. So, that, I think that's another good point, that Level 2 is really a transitional level. If an organization is seeking to get a Level 3 certification, but they fall a little short, they will be awarded a Level 2 if they meet those requirements and can demonstrate that they are working towards the protection of CUI, or controlled unclassified information.

Andrew: OK, cool. Just to recap the three big main points that we covered here: organizations are assessed for practices and processes at every level except for Level 1 because Level 1 only contains practices. Scoring is cumulative. So, you not only have to achieve the practices and the processes of certification but also the levels below that. Then finally, you only achieve one CMMC level, which corresponds to the lowest of the two scores between practices and processes.

Katie: Yes. I think that covers it. Thank you guys for listening. We will include all links to the resources that we mentioned in this podcast. Again, there is a lot of information out there that we have put out that dives into a lot of the different aspects of CMMC, not just scoring. So please don't hesitate to reach out. You can find us on LinkedIn [Katie] or [Andrew], or you can email us at info@sei.cmu.edu, and you will find this podcast available off the SEI website and anywhere else you would find your podcasts, including iTunes, YouTube, Stitcher, and SoundCloud. Thank you very much.

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 don't hesitate to email us at info@sei.cmu.edu. Thank you.