



Optimizing Process Maturity in CMMC Level 5

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 with [SEI's CERT Division](#). I would like to welcome my colleague [Andrew Hoover](#). Andrew leads the Resilience Engineering Team at the SEI's CERT Division at Carnegie Mellon University.

Today, we are going to continue our discussion around process maturity requirements for the [Cybersecurity Maturity Model Certification, or also known as CMMC](#). We are going to focus today on the Level 5 process maturity requirements, which are standardizing and optimizing a documented approach for CMMC. But first, we are going to tell our guests a little bit about ourselves and our background, and what brought us here to the SEI. So again, I'm Katie Stewart, I've been with the SEI about seven years. I've primarily focused on risk and resilience as well as measurement and analysis. So, Andy, can you tell us a little bit about yourself?

Andrew Hoover: Yes, sure. Katie, thank you. I'm Andy Hoover. I have been at the SEI for eight years, most of that time in the Cyber Risk and Resilience Directorate. I mainly focus on cybersecurity architecture and cyber resilience assessments, which is how I got involved with CMMC.

Katie: Thank you. Okay so, for the members of our audience who might be new to CMMC, we have done a bunch of introductory [blog posts](#), a couple other [webcasts](#) and [podcasts](#) that should give you a good overview of CMMC and our work that we have done on it. We will link to all of those resources in the transcript of this podcast.



SEI Podcast Series

But today, we are just going to focus on the Level 5 process maturity requirements within CMMC. I said it before, but at a Level 5 for process maturity those requirements are *standardize* and *optimize*. Andy, can you tell us a little bit more about this process maturity requirement?

Andrew: Sure. All organizations who are trying to achieve Level 5 in the CMMC model should have a mechanism in place to ensure their practices are standardized across the organization and then continuously optimize for improvement.

Katie: OK. Can you say a little bit more why that is important and why it was included within CMMC?

Andrew: Yes, certainly. Keep in mind—we will say this a few more times probably throughout this podcast—but this is a Level 5 process. So, this really applies only the most mature organizations who are trying to achieve the highest level within CMMC. Now standardizing a documented approach is all about getting consistency in your activities across the organization. At this level, organizations should basically standardize their approach to each of the 17 domains within the CMMC model. Now what this gives you is that you get consistency because all operating units are meeting a minimum standard, which is established by the highest level of the organization.

Katie: OK. So when you talk about consistency at the highest level, does that mean that every individual operating unit would have to adopt that practice verbatim?

Andrew: That is a good question. The standard approach that is defined and documented should constitute kind of the minimum that is required by each of the operating units. Now, the operating units can, and probably should, take that and customize it to fit their unique operating circumstances. They should tailor the approach to kind of fit their operations as long as they continue to meet the minimum that was defined at the highest level. This way, you ensure consistency because all of the operating units are continuing to meet the minimum, but they also have flexibility to adjust the standard approach to kind of fit their unique operations.

Katie: OK, that makes sense. So, let's switch to the second part of Level 5, which is the optimizing. Can you describe what optimizing a process looks like?

Andrew: Yes, so, as I said earlier, the standard approach constitutes the minimum that all operating units need to follow. Now they can, however, modify this to fit their unique operations as long as they are again meeting that minimum approach. When they tailor this approach and they identify a success in their implementation—maybe it is a software product that has helped streamline their operations or a new procedure that they have implemented that is really a success for that particular practice. Well, there should be a way for them to share that success with the rest of the organization. So, think of it as like a feedback loop back into the standard



SEI Podcast Series

process that then allows all of the other operating units to adopt that success. So, therefore you have got this continuously optimizing approach.

Katie: Right, which sets the stage for continuous improvement.

Andrew: Yes. And, like we said before, this is Level 5, and this continual optimization really represents the highest maturity that an organization can achieve, certainly within the context of the CMMC.

Katie: Right, you mentioned something I would like to circle back to in that span of control. What we mean by this is, in a very large organization the standard approach may be implemented at the highest level of the organization or at a sub-unit. But, regardless, all subordinate organizations would need to adopt and use the standard approach, but they would just tailor it appropriately for them.

Andrew: Yes, exactly. Thanks for clarifying that. It really depends on the makeup and the hierarchy of the organization, you know how these things get implemented. Because when you think about it, there are a lot of organizations, especially at this level, that are going to have business units and operating units that are essentially run as individual companies themselves. In some cases, the operating unit or the division may be the level where the organization chooses to establish that standard approach. It is important to keep in mind that this is Level 5. So, again—we have said that a few times now—at this level most, if not all, companies are going to be very mature already. Considering the DoD is estimating 70 percent to 80 percent of organizations that adopt the CMMC are only going to need to achieve Level 1, we are talking about a very small number of companies who are actually going to have a need, or a requirement, to achieve Level 5.

Katie: Well, good. I think this was a great discussion, and I hope our listeners have enjoyed all of our podcasts on process maturity. As a reminder, today we focused on Level 5, but we have podcasts specifically at Levels 2, 3, and 4 that are also available. In addition, I said at the beginning, we have a large set of resources around the CMMC, and we'll provide links to this material in the transcript of this podcast. As always, if you have any questions, please don't hesitate to reach out to [myself](#) or [Andy](#) on LinkedIn. Or you can email us at info@sei.cmu.edu, and 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



SEI Podcast Series

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.