Documenting Process for CMMC

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 would like to welcome Andrew Hoover. Andrew leads the Resilience Engineering Team within the Software Engineering Institute's CERT Division at Carnegie Mellon University. Today we are here to talk about some of the process-maturity requirements in the Cybersecurity Maturity Model Certification, more commonly known as the CMMC.

Our discussion today will focus on documenting practices. But first, we are going to start off by telling our guests a little bit more about ourselves and our backgrounds as well as what brought us here to SEI. Again, I am Katie Stewart. I have been with the SEI for about seven years now. My work primarily focuses on risk and resilience management as well as metric and measurement development. So, Andrew, do you want to tell us a little bit about yourself?

Andrew Hoover: Yes. Certainly. Thanks, Katie. I have been at the SEI for eight years, like Katie, primarily working on risk and resilience in the Cyber Risk and Resilience Directorate. My background is in auditing and technical vulnerability assessments, and I have been able to continue that work while at the SEI.

Katie: Great. Thank you, Andy. For members of our audience who might be new to the topic of CMMC, we have done a bunch of introductory blog posts and some other webcasts that can provide you with a nice overview of the model, and we will include links to that in our transcript.

So, let's get to it. One of the requirements at Level ~~Two~~ 2 in CMMC is the documentation of practices. Andy, can you tell us a little bit more about this process-maturity requirement?

Andrew: Yes, so it is in Level 2, like you said, and basically it requires that all practices up to the level that you are being certified at be documented.

Katie: Yes. That is a very important activity for organizations. Can you talk about why it is so important?

Andrew: Yes, sure. An organization should build its cybersecurity practices by documenting them and then practicing them as documented. Right? So, in other words, say what you do, do what you say. What this does, it enables an organization to execute them in a repeatable and consistent manner, but also to achieve the outcomes that they are expecting, which becomes the foundation for continuous improvement, which is why we built the maturity component into the CMMC so that organizations can continue to improve.

Katie: I think continuous improvement is critical for organizations when they are trying to build a cybersecurity program. You put it in place and then you iterate, and the very first part of that is documenting your practices. Can you actually tell us what that might look like? What does it look like when you document a practice?

Andrew: The level of detail of the documented practices can and will vary from organization to organization. Some organizations are going to likely have handwritten desk procedures, and other organizations are going to have formal SOPs or standard operating procedures. It is really up to the organization to document them however they feel like it is going to work best for them.

Katie: So, if I am a smaller company, maybe just five people, I can just have simple procedures defined?

Andrew: Yes, as long as the documented procedures define the practice in such a way that the activities are repeatable, then that would work. We would expect the complexity of the documentation to kind of grow as the organization grows. So, the smaller organizations, like you said, they are going to have kind of very basic documentation, whereas when you get to larger multi-national companies, you are likely going to have very formalized SOPs for everything that are regularly managed and updated and used throughout a massive enterprise.

Katie: Right. That makes sense. Let us turn specifically to CMMC. Do I have to document all of my CMMC practices?

Andrew: Up to the level at which you are being assessed. How you document them is going to vary. I assume some organizations will likely have an IT security policy, right? And they would be able to document them there. Other organizations might look to document them in their SSP

[System Security Plan] and still other organizations may have very specific SOPs for the individual area of the practice. It is really up to the organization, but there is no process maturity at Level 1. So, at Level 1 it is not required, but when you move up to Level 2, the model is cumulative. So, not only do you have to document the Level 2 practices, you also have to document the Level 1 practices in order to be certified at Level 2 or higher.

Katie: What about organizing my practices? If I am going for a CMMC assessment, do I have to organize my practices by the CMMC domains?

Andrew: No, that is a good question. The organization of the documented practices does not matter. What does matter is that you should just do what is easiest to use. The most important component of a documented practice is that they are followed, and if the documentation is too complex or too difficult to find or too difficult to follow, it is not going to be followed. So, it does not matter if you organize it based on the CMMC framework, which you can, but you could also organize it in another way that works best for you. Like we said, maybe in an SOP, maybe in your SSP, or any other way that you think you would get the most value out of the documentation.

Katie: Just as long as the practices are followed, right? That is the most important.

Andrew: Exactly.

Katie: What about updating practices? What are the requirements to update documented practices?

Andrew: There is not a real defined requirement in the CMMC to update them. However, if the practice is being followed and the organization changes the way that that practice is implemented, then the documentation also should change with it. The CMMC assessors should be looking to ensure that the practice is being followed, not just that it is being documented. You are not getting any value out of documenting something that you are not using, and so hopefully the CMMC assessors will be ensuring that not only is it documented, it is also being used throughout the organization that it was intended to be used for.

Katie: I just want to reiterate a point you made earlier, that the documentation of practices is key to establishing continuous improvement.

Andrew: I will add that in a previous podcast we talked about establishing policy, which drives the establishment of the documented practices, and so I would encourage our listeners to go find that one and tune in to that one as well. In later podcasts, we are going to talk about managing and measuring these activities for effectiveness and then standardizing and optimizing all of this documentation for your organization.

Katies: Great. It will be good to continue the discussion. So, let us close by talking about the resources that are out there and where those can be accessed. We have already mentioned a few, and once again we will include all the links to the resources in the transcript of this podcast. And this podcast as well as the others that we have recorded are available on the SEI website at sei.cmu.edu/podcasts and anywhere that you get your podcasts, including iTunes, YouTube, Stitcher, SoundCloud. As always, feel free to reach out to us. You can reach out to us on LinkedIn [Andrew's LinkedIn profile and Katie's LinkedIn profile] or, if you have specific questions, please just email us at info@sei.cmu.edu. 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 don't hesitate to email us at info@sei.cmu.edu. Thank you.