Reviewing and Measuring Activities for Effectiveness in CMMC Level 4

Featuring Katie Stewart and Andrew Hoover

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's Podcast Series. My name is Andrew Hoover, and I lead the Resilience Engineering team at the Software Engineering Institute's CERT Division at Carnegie Mellon University.

I would like to welcome Katie Stewart. Katie is a senior engineer also in the SEI's CERT Division. Today, we are here to talk more about some of the process maturity requirements included in the Cybersecurity Maturity Model Certification or CMMC. Our discussion today is going to focus on reviewing and measuring your cybersecurity activities for effectiveness.

So, first Katie, why don't we start out by telling our guests a little bit about ourselves and what brought us here to the SEI. I have been here at the SEI for eight years now, primarily working in the Cyber Risk and Resilience directorate. My background is in cyber auditing and technical vulnerability assessments. I have been able to continue that work here at the SEI. That is specifically what brought me onto the CMMC project.

Katie Stewart: Yes. Hi. As Andy said, I am Katie Stewart. I have also been with the SEI about seven or eight years now, primarily looking at risk and resilience as well as measurement and analysis. So, I am excited to talk today about measuring.

Andrew: Thanks, Katie. For members of the audience who are new to the topic of CMMC, we have done several blog posts and webcasts and other materials that provide a good overview of CMMC and our work on it. We'll be sure to provide links to all those materials in the transcript.

OK. So, the process maturity requirement at Level 4 of the CMMC is to review and measure activities for effectiveness. Katie, can you tell us a little bit about this requirement and what it means?

Katie: Yes, sure. All organizations that are seeking to get a CMMC Level 4 or a Level 5 certification will be required to show that they are controlling their CMMC practices by reviewing and measuring their activities. This will account for all of the activities that go into carrying out the CMMC within their organization.

Andrew: So, good point, thank you for that introduction. So, reviewing and measuring activities is really necessary to make sure that you are getting out of them what you would expect, right? It seems pretty involved. Can you talk a little bit more about that?

Katie: Yes. There are two components to it, there is the reviewing and the measuring. If you look first at reviewing, the process of reviewing activities for effectiveness simply means that you are looking at your practices to see if they are producing expected results. Within the context of CMMC, at a Level 4 or even a Level 5, you are looking at each of your CMMC practices to say, *Hey, these are performing, and they are giving me the results that I expect*. If we choose an example like access control, you may have somebody that is designated to review accounts on specific machines to ensure that your access control practices, things like limiting access to authorized users, that they are being implemented, followed, and effective. Again, when we say effective, we are simply just saying that what we are doing is giving us the output that we expect.

Andrew: Another important aspect of this process is communicating the status regularly with higher-level management, right?

Katie: Yes, exactly. Let me add to that. The reason why you do that, the reason why you review and then communicate status is so that if there is a problem that is discovered, you have brought the right people into the conversation, and they can help take action and correct any issues that you identify. For example, with access control activities, if I am reviewing them, and I realize that I am not limiting unauthorized users, I want to raise that issue to the appropriate stakeholders as soon as possible.

Andrew: So, that communication can really take different forms, right? It can be just a regular status meeting. It could be emails back and forth. It is kind of whatever works, isn't it?

Katie: Absolutely yes, and organizations should have a set of periodic reviews, right? They should be reviewing status periodically on a time frame that they define. But, there also should be a clear line for communication when issues do arise, so outside the bounds of your periodic reviews.

Andrew: So that is reviewing and communicating, which is the first part. Let's talk a little bit about the second part of this process, which is measuring for effectiveness. Now, measuring is one of those things that a lot of organizations get scared by, and they find it just very difficult. So, any tips that you can provide, Katie, on how to do this effectively?

Katie: Yes, so the measuring component at Level 4 is on top of reviewing. You are correct when you say measurement can be somewhat difficult. It can also be expensive. This is why we do see this at a Level 4 within CMMC because organizations that are committed to measuring their CMMC activities, they will require a resource investment. Some kind of examples that you would be measuring would be measurement of your actual performance against your plan. We are planning out our activities, and then you want to measure to see that you are achieving your plan.

You may measure things like the time it takes to accomplish activities. You may look at how long it takes. Is that within your bounds, within the expected value? Then you may measure things as simple as successes and failures. How often are you successful in a certain activity and how often do you fail? Then, while reviewing it is just simply looking at the results to say, *Are these within my expected values?* When we start to measure, we are actually looking at quantifying the performance of our activities, which is what drives improvement. You cannot improve what you can't measure, right? We are no longer just looking to say, *Is what we are doing effective?* We are actually looking at, *How effective is it, and can we continue to improve to become more effective?*

Andrew: Right. So in doing that, the CMMC model doesn't define any specific measures, right? It is up to the organization to kind of measure what is important to them.

Katie: Right. That is exactly right. Measures within an organization should be driven by an organization's measurement objectives. So, one organization may measure one thing because it is important to them, and then another organization may choose to measure something else. So it will be organization defined and again, up to the organization.

Andrew: Katie, another question that we get about this one pretty often is about time frames. Is there any required time frame that these activities need to take place? Do you have to perform measurement activities with some regular interval? The same with the communication. Do you have to report up to senior management with some regular interval, or is it just kind of whatever makes sense for each individual company?

Katie: Within the time frame question it is up to the organization. So, what makes sense? There isn't a standard model for how often the review and measurement activities should be performed, but you need to do it in an interval that makes sense for the organization to take action against. If your measures aren't timely, then what is the point in measuring them? So again, I would turn this back to the organization to say, *If I am looking at this measure, and I need to take action, what is the time frame in which I need to do that*? The other thing to consider is measures that have been done for a while and are engrained within the organization. *This is just something that we are doing*. You don't want to set and forget it, but you maybe don't have to look at that as

much as you do at measuring an activity that maybe is new or you are undertaking some sort of improvement. So different time frames will apply to different measures within your organization.

Andrew: That is a good way to put it. Just kind of like the well-established ones won't require as much attention, right? Because they are already adopted and people already know about them and are using whatever kind of protocol it is, or communication, or measurement, or whatever. So it probably doesn't need to be revisited quite as often, if it is something that is just well-adopted in the organization.

Katie: Exactly. Again, I have talked about this a little bit before, but your measures will change. They'll change over time. They will change based on the objectives within your organization. But if you want to tie this back to CMMC, your measurement objectives that, again, you derive your measures from, they really should align with the organization's commitment to increasing cybersecurity, right? And they should align with the CMMC practices. When an assessor is coming in at Level 4, they are really looking at those measures that are measuring the effectiveness of what you have implemented for CMMC.

In a later podcast, we're going to talk about how this measurement data can inform you and can help you optimize your practices, so that you get into at Level 5 for CMMC. We will go into more detail in a later podcast about that. Reviewing and measuring is kind of the next step and gets you towards really optimizing your activities.

Andrew: OK, great. I'm sure that the Level 5 podcast on optimizing will be really useful for the more mature organizations that need to achieve that level.

Katie: Yes.

Andrew: So why don't we close by talking about some of the resources and where they can be accessed. We have already mentioned a few. This podcast will be available on the SEI website, which is sei.cmu.edu/podcasts or anywhere else that you get your podcasts. We will link to the other resources in the script. Then, as always, if you have any questions, feel free to reach out to Katie or I on LinkedIn. Or don't hesitate to email us at info@sei.cmu.edu. Thanks.

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.