A 10-Step Framework for Managing Risk

featuring Brett Tucker as Interviewed by Suzanne Miller

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.

Suzanne Miller: Hello, my name is Suzanne Miller. I am a principal researcher here at the SEI, and I am here to welcome today my colleague Brett Tucker, who is a manager in the SEI CERT Division. He is the creator of the OCTAVE FORTE [Operationally Critical Threat, Asset, and Vulnerability Evaluation **FOR T**he **E**nterprise] model, which is a model that is dealing with enterprise risk management (ERM) and prioritization; in particular, enterprise risk.

I want to welcome you to our podcast, Brett. As we get started, I just want to have you tell people what it is about this work that drew you in and a little bit about your background, so people understand where you are coming from.

Brett Tucker: Sure, thanks Suzanne. I really appreciate you having me. Like you said, I am Brett Tucker, and I arrived at the SEI about three years, almost four years ago now. I came from industry. I was working at Westinghouse. We built nuclear power plants there. In my time there, around a decade or so, I helped them build their global risk-management program. In doing so it gave me great exposure across the entire enterprise as to how risks knit together. Then I came to the SEI, which had far more of a cyber focus, recognizing that these connections needed to be made between the folks who are always saying, *Hey, we need more resources for cyber risk and addressing our cyber risk*, and the overall executives who are saying, *Look, you need to converse with us more in a dollars and sense, like business sense, more than that bits and bytes stuff that we are not getting.* My history brings me from more like private industry, and I had some public-sector experience too, in federal government. I was in the Department of Defense, and then I was in the intelligence community, so I have seen both sides of that. I think I brought those elements here to help develop this new process to get that enterprise-risk focus for any organization, actually.

Suzanne: Let's talk about that gap that you mentioned. The gap between say the cyber, but it is not just the cyber, it is practitioners across a myriad of areas, safety engineering. I think of the routers and all the security issues with those. That is not just the computer people. That is the whole way that is built, that makes some of the risks visible in those kinds of things that people hack into. That disconnect between the practitioners and the executives, say a little bit more about what your experience is.

Brett: Yes.

Suzanne: What is underneath that and what do we need to be aware of as practitioners, when we are working with folks like that?

Brett: Yes, so two big things really resonate as you ask me that question. One is for sure that I think that a lot of us who come up in the technical ranks of cyber especially, we think a lot in technical terms: the bits and bytes, the coding, the tools. We really geek out on tools. Controls and all that great stuff, and executives, they want to hear crisp decisions that they need to make. Like I said, they are very much in the return-on-investment mindset, where we are not necessarily thinking about that at all times. In the cyber community we are thinking about whatever it costs, we need to insulate our information, our facilities, our people, whatever asset we are speaking to at the time.

Suzanne: Some of that comes from the fact that as practitioners, we have a deep understanding often of really just how bad it could be.

Brett: That is right. The doom and gloom…

Suzanne: That is the thing that is kind of hard. I mean, thinking of my own experience. It is hard to translate that into dollars and sense.

Brett: It is.

Suzanne: How do we help people do that?

Brett: It is. So good business impact assessment is important here. And there are elements of that in FORTE, but it is part of a greater process. I think, let us step back yet again. It is not just about that. It is understanding that there is a whole lifecycle here for risk. All the way from very beginning in the makings of a program where they need to have fundamentals, they need to have a governance structure. So the people who are making the decisions around these technical risks or other global risks in the organization, they have an appetite. So, they are communicating with each other in that governance structure of, *Hey, what risks matter more to you and why?* Because of the dollars-and-sense piece, maybe because of operational factors, whatever the case may be.

We have to document that somehow in a policy, because this is kind of like the idea of, if a tree fell in the woods and no one was there to hear it, does it ever really make a sound? I go with a different analogy here. It is the idea, if nothing is written down in an organization, will it ever really get done? Will people ever really follow the policy?

Suzanne: Yes.

Brett: Policy and procedure are very important, telling people the why and the how. OK, another thing that really resonated in your question there, is this idea of cyber tends to be the silver thread or silver bullet, if you will, that threads through a lot of different risks. Throw a risk at me. A good example here would be like a merger acquisition kind of a thing. There is a lot of opportunity risk as much as threat risk related to merging or acquiring another organization. But think about that. They bring all of those assets with them to include information, people, technology, facilities. We have to understand what their risks are related to those assets, inherent to the ones that they have. Maybe they do not have the same control sets or practices that we do, and they are bringing into this organization now, we are effectively accepting those risks. So, communication needs to be had there, between the CISO the chief information security officer, and the chief risk officer, and the chief strategy officer. What we are trying to do with this enterprise-risk take on this practice is to get all those folks talking in that same language. We can do this with a series of tools that is provided within FORTE. A good example, and this is just a real, easy one, kind of like the softball of enterprise risk, would be a risk tree or a bow-tie analysis, where there is a line on, *hey, what are the trigger events or what are the things that are going to happen that are going to kick this risk off and make it happen? What are the conditions necessary for that risk to take place?* And then, *How do we feel the pain, and what are the consequences?* A simple tool like that is the way that you can make that gap, without maybe necessarily even having to have that dollars-and-sense conversation. So, bringing it back to your question there again, this notion of yes, it is hard to get it to dollars and sense, but there are some tools that can qualitatively help as much as quantitatively.

Suzanne: OK. All right. So, FORTE is an evolution of other operationally focused risk work that we have done at the SEI. It started back in early 2000s with something called OCTAVE. Some people may know that, yes. Operationally Critical Threat and Vulnerability Evaluation.

Brett: That is right.

Suzanne: That evolved into something called OCTAVE Allegro. Now, we are working with you on OCTAVE FORTE. Tell us a little bit about that evolution. What have we learned from that first OCTAVE to where we are now?

Brett: Great question. It has been a journey, Suzanne. We would be remiss without talking about the fact that OCTAVE has been around for a while. And the Alberts-Dorofee textbook really captures a great, solid process. But as things evolved, and as customers tried to adopt the process, they said, *Hey, this is really heavy.*

Suzanne: Very heavy.

Brett: Yes, and it almost kind of died on the vine, if you will, because organizations were not willing to pick up all that capital that comes along with it. All the investment that…

Suzanne: True.

Brett: …to make it work. So OCTAVE S came out. That kind of worked for a while. There were some industry-specific or sector-specific examples that came out. But I think it really made another leap about a decade later with OCTAVE Allegro. You mentioned Allegro. That is a process that is a lot lighter. It is about seven or eight steps, and what it does is it really focuses on information assets, and they said, *Hey, look. If anything, we really need organizations. We need the practitioner that is at the desk, who are identifying everyday risk, to give them a base set of tools that they can use to get a base, qualitative analysis going. Maybe a little bit of quantification, and understanding as to how they can respond.*

Suzanne: Right.

Brett: Admittedly, when I first saw Allegro, in my mindset, and this is just speaking from a risk professional's perspective, it needed a little bit of buffing up. It needed some primping, if you will.

Suzanne: A little polish.

Brett: It did. It needed some polish. The polish that it needed was, if you look at the OCTAVE Allegro process, if you will, it is not a closed cycle. It really ignores a fundamental point of risk— the fact that you can never really get rid of all your risk. You will always have a residual left over. So, you have to go through this iterative cycle of continuing to understand how that risk is evolving, and how the actions you are taking in response possibly, are maybe bringing that risk exposure down. But once again, *Is there anything left that we need to address?* And we convey that with what we call risk appetite. There is this idea of an organization's willingness to take on so much risk. An appetite statement, which that is another tool, by the way that we provide in the FORTE process, and was touched upon in Allegro, but not in a holistic or broad sense across an enterprise. An enterprise may think of risk in different ways. How are we going to feel pain in terms of revenue loss, or if you are in the public sector, maybe how are we going

to think about it in terms of a budget, or operational disruption, or like you said, safety is another great example.

So in FORTE, we kind of picked up Allegro, and we said, not only do we need something that the practitioner can use at their desk, we need to have them have a conduit, or a means of communicating what their analysis gave them, with the executive branch and make that case to say, *Hey, we need controls. We need resources to purchase those controls. Or we need resources to hire more people*, or whatever the case may be. So that was where FORTE picked up Allegro, ingested it, and now it [has] this nice, 10-step process, where you are going to see elements of Allegro, because there is a large discussion about assets and containers and how all that works and how we map that. But now, there is a greater discussion of, OK regardless of the analysis that you use, and by the way, FORTE is very accepting and uses it, and I would endorse and encourage the use of FAIR, Allegro…There are elements of the risk management framework that can certainly be knit into FORTE if you are a risk-management framework shop, in the public sector, let us say, that you can bake in and actually use other elements of FORTE, such as the projectization of response plans, where a lot of these processes somewhat fall short. They decide they have a great mitigation plan, and then they do not put a schedule to it. They do not put a budget to it, and things just become shelfware, we call it. It gets purchased and never gets implemented. FORTE provides that discipline, and why I am doing this by the way, FORTE has that nice process model. It is a circle, and that response piece is on the, oh, 7 to 8 o'clock side, as you are going up to finish or round out that process.

One more element I want to point out here that is important, Suzanne, to focus upon. Allegro, it did have some small elements, but I think FORTE tries to drive home a lot greater piece of measurement. It is important to understand not just the performance of your risk program. That is one thing altogether. You know what I mean? *What is my engagement? What is my awareness across the culture?* But it also is to look back at the individual risk and understand how the exposure is being brought down with each individual risk that could also be a good indicator of how the program is performing. There is that discussion, as well.

Suzanne: OK. You have hit on a couple of different elements of FORTE. Why don't we step back and give our viewers sort of a summary. We will have a graphic for them to show them. Just give us a verbal summary of OCTAVE FORTE, so they have an idea of where all these little things fit together.

Brett: Absolutely. To keep things simple, OCTAVE FORTE is a nice, convenient, 10-step process. In the graphic, you will see that it is a continuous circle. There is no end. There is no head or tail to this process. I want to make it clear from the beginning, some organizations may already have maturity at some of these steps. And, they may forgo or not necessarily need FORTE to help them with asset management, for example. Maybe they have that down. But let

us say that you have maybe a more nascent organization or one that is new to this whole risk-management game, and they need that.

Let us start at the very beginning. Let's go to Step 1, and say that the Step 1 lays the foundation for following the process. It is really important to recognize there are three fundamental pillars that need to be addressed when building a risk program. The first one I mentioned is governance. You have to have a management team, an executive team, that endorses and advocates for risk management to be done in the enterprise, to have it be done properly, and to allocate resources so that things can get done. You are not going to get anything if the car does not have any gas in the tank. A governance structure is very important, and that is emphasized in Step 1.

Another pillar is, like I said, risk appetite. You have these different layers of a governance structure and by the way, it is scalable and tailorable to the size of your enterprise, and its need and function. Let us just say that we have a pyramid-like structure, and we have maybe an executive board, a risk committee, and a subcommittee. They need to communicate with each other. Some levels may want to address risk, and some may say hey, especially with the executive-board level, the whole idea of deciding if you need to have a—I am being very basic here—a firewall for a computer, that kind of thing. That is not what we get paid to do. That is in the CISO [chief information security officer] organization, somebody way down in the ranks is doing that. Well, that is all conveyed with that risk-appetite statement. So to have that quantifiable tolerance of different strategic objectives in the organization, that is captured in appetite, very important. Finally, like I said, policy is also very important. It gives the organization the *why*, and the procedure gives the *how*. How are you going to execute this process? That is in Step 1. So, clearly Step 1 is very important.

Steps 2, 3, and 4, what you are going to see here is a large overlap, with not just OCTAVE Allegro, but also our Resilience Management Model, RMM, where there is a real high emphasis and premium placed on managing your assets. In review, let us remember that our assets are people, the information that we have in the organization, the technology we have in the organization, and possibly the facilities. There is also an element of supply-chain risk there, too, because we do not want to neglect the third-party vendors that are important in this discussion as well. Either way, steps 2 and 3 or so, what we are doing is we are trying to understand what those critical services are in the organization—in other words, what we are doing, what we are delivering upon—and trying to map what assets are holding up those services. If we were to take any one of those assets out what would happen? We would have some kind of major disruption. OK, so what we are trying to do is we are trying to get a critical process map. We are trying to map together what assets are contributing to those critical services.

Then, once we know that, we understand, or we start to identify, what our needs are in terms of making those assets more resilient. We also recognize too, especially around Step 4, that we

already have controls in place. We are already doing great things, and we don't want to lose the value of those great things. We also don't want to replicate and reinvest in resources that we already have. Try and measure those current capabilities, and with that, we are going to try and understand what gaps we have.

Now you are getting into Steps 5 and roughly 6, where what we are really trying to do is understand what the threats are to the organization, what the vulnerabilities are, or those gaps that we talked about to those assets. We really are going to start prioritizing those risks. Once we start prioritizing, we are going to start understanding too where our greatest needs are. When we do that, when we understand where our greatest priorities are, we go back to that governance structure, and we make appeal to them. This is where that magic of FORTE comes together, where you are making that case to that governance structure, saying, *We do need resources to address these risks. Here they are. Here are our plans*.

Around Step 7, now we are starting to talk about what do those response plans look like? Are we accepting risks? Are we avoiding them? Are we transferring them? Or, are we truly establishing some kind of control framework that would constitute a mitigation around those risks? Then like I said once again, we do not want to just buy a tool and just let it sit on the shelf. We have to actually have someone own that. We have to actually have a response plan that is projectized and implemented. That owner if you will, that response-plan owner, risk owner—they may not be one and the same thing, by the way—is going to come back to that governance structure and regularly provide updates as to how things are going. To do that, they need to relate the measure, or how it is that they are going to demonstrate that those processes are being ingested by the organization, being accepted.

The metrics discussion starts coming up in Step 9. How are we measuring the effectiveness of reducing the exposure of that risk? Around Step 9 and 10, there is yet another discussion of measure. What we are trying to do is measure our system and how it is performing. We are trying to measure how the whole program is performing at large. What is our culture in our organization? Does it have a notion of what risk is? Does it have it defined? Does it have that policy understood, and everybody is following the rules, if you will? So, in a nutshell, there [are the] 10 steps and how they come about.

Suzanne: I want to come back to the iterative nature of this for a minute.

Brett: Yes.

Suzanne: The example that immediately comes to mind is I am a DoD program or a development acquisition program of some type, and I am running along, and I have security classifications, and I have suppliers and all that. and then the quote, *COVID quarantine*, comes

around. Now that to me is kind of the quintessential reason why we have to do this iteratively. Because we may have had a fantastic risk-mitigation profile, up to the point that we hit quarantine. Now, all of a sudden, I have people needing to use personal computers, because they have never worked from home before, and they do not have a government laptop. All the things that bubbled up because that environment changed. That is why we have to keep looking at this, because otherwise…I actually did a podcast a little while ago with somebody about, what are some of the threats inherent in working from home? That kind of thinking is necessary, so that we do not let go of one, opportunities, and so we aren't able to respond resiliently to really drastic changes in the environment that sometimes happen. They are not always drastic. This one was. I mean I could give you another example, but the other examples that are not as dramatic are also impacting in many cases.

Brett: Yes. That is a great example. What a very relevant, first of all, example. But I will say, another thing that FORTE points to is thinking about that incident response. How is it that we maintain business continuity? There is that discussion there. COVID of all things is kind of an ironic example in a sense too, because a lot of times organizations have maybe some kind of disaster-recovery plan, and it points more strictly at operations. Like, *We had a fire in a facility*, or, *We lost a major server farm or something like that*. Really, you may not think of that bio-danger to your workforce. And maybe the fact that they all do have to start working from home. Ok, so everybody's remote working, teleworking. *Can our VPN even handle that? Have we even tested it?* So yes, absolutely.

Suzanne: Well, and, *Are we ready for it to continue?* I think that is one of the things that the COVID case has pointed out to a lot of organizations, is they have what I will call pinpoint risk mitigations. *A fire happens, done, now we recover from it. A flood happens, it is done, we recover from it*. This is a flood that never goes away. We have to figure out how to work in the water for eight months plus, and that changes your thinking when you are going from a single point failure kind of example to, *We have a change in the environment that is going to affect us for a long time.* So, tools like this give us a systematic way of saying, *OK, how are we going to deal with this on a…*

Brett: That is absolutely right.

Suzanne: We need those.

Brett: The other important thing to recognize there too, the threats shift as that continuity-operations discussion is going on. The bad guys and girls, they are out there, and they are thinking, *OK, so people working at home, what can we do differently?*

Suzanne: *How can I take advantage?*

Brett: *I can take advantage of this situation.* Once again, that iterative nature of FORTE is necessary, or any risk-management process is absolutely necessary to stay ahead of the game if you will. Because they are thinking, and we need to stay ahead of that wave.

Suzanne: There are smart people on the threat side, and that is one of the things we have to continually recognize when we are dealing with risk. They are not stupid.

Brett: That is right.

Suzanne: All right, so I got somebody's attention out there. They went, *Oh, I have not been paying attention to this stuff.* We have a technical report. We have a blog post that you have written. What other kinds of resources to help people adopt this approach to risk do we have available that we can share with them and help them to deal with these things?

Brett: Great question. So, yes, you are right. We have the tech note. We have a blog post. We have several, actually, blog posts and discussions that have been out there historically that have kind of teased it. But I think more importantly, if people want to engage the process and learn more about it, we have some training offerings that we provide through the SEI. We have our next offering, I think that is going to be coming up summer/fall timeframe, I think, accounting for the COVID possibility? We are thinking of also web-enabling that training. But I am also happy, and I have several customers who have brought me to their site. We have done broad trainings for their workforce, so that way they could have some executives on hand as well as some people who are going to be practitioners, that we can do some hands-on training, not only just to orient them with OCTAVE FORTE, but also to do some facilitated workshops to help them develop policy, help them to design or build a governance structure that may work for them, to show them how to facilitate the development of a risk-appetite statement. So those facilitation sessions, I am happy to help, just reach out to the SEI and find me, and we will be happy to help people get more into the process and understand it, and give them the little details.

Suzanne: I will say that having worked with OCTAVE 15 years ago, and a bit involved in some of the early training, I will say two things. One, some of the training scared me more than I ever expected because it just brought up things that I had never really considered as being risk elements or really thinking about the ongoing consequences of certain kinds of risks. So that alone was just an amazing epiphany for me. The good news is, but then the training helped me build some strategies, so like it is not this hopeless case. It is not, *I can't deal with this ever, I will be in a risk morass for the rest of my life*.

Brett: Right.

Suzanne: I do really believe this is an area where education and training may have more impact than some of the other technologies where I can just go to the web and look at a bunch of tutorials. Because you have to get past our complacency is how I would put it.

Brett: Yes.

Suzanne: *The bubble we are living in, even though the bubble is not as comfortable as it was before March, I have figured out how to make this bubble work. But there is still a bunch of stuff that I probably should be paying attention to, that I am not.*

Brett: Suzanne, you bring up a great point. Risk management, the challenge with it, especially cyber risk management, we think so much in terms of technical tools, things we can download, things that use code. I would like to say that risk management in general is actually social engineering as well. You are trying to get an organization to understand, you are trying to get people to behave in a certain way. Behaviors are tough to try to drive in your organization. How do you have proper advocacy for that? That is absolutely a good point.

Another thing I would like to point out about the training that is really good is, come to the training program and meet people who are in the same boat as you. Network. You are going to have a confluence of folks that you are going to meet who are facing a lot of the same situations. That is a great thing to have, people—a Rolodex if you will—of people that you can contact and ask questions. In that regard, I would like to also offer that I am the technical sponsor at Heinz College at Carnegie Mellon. That is our School of Public Policy Information Security, leading up their Chief Risk Officer Program, and their Chief Risk Officer Program also provides the FORTE framework for the program. So, not only do you get training from other executives and former executives, also from myself, so that way you can learn to be that chief risk officer, or maybe you are budding or aspiring to be that.

Suzanne: No, no, I am not.

Brett: There are multiple avenues.

Suzanne: I like to sleep at night.

Brett: Right. So there is the more discreet training that you can get through the SEI, and I can give you focused training there. If you want more extensive training, that is also available is what I am saying.

Suzanne: For those that have the appetite, the risk appetite. I do not have that much risk appetite for being a chief risk officer.

I really want to thank you for joining us today and giving us this window into some new tools that are available. I am one of those people that really focuses on sociotechnical issues. I resonate very much with we have got to get the connection between the practitioners and the enterprise leaders, so that we can get everybody out of that complacent place and move forward with resilience strategies.

Brett Yes.

Suzanne: Thank you very much for taking the time for today. Do not forget, for our viewers, we do have a tech note out on this. You know where to find those. Blog posts, easiest thing to do is to go to insights.sei.cmu.edu and search under the author's name, which is in this case, Tucker. Thank you again for joining us today to talk about this. Thank you to our listeners for joining us today, from one of our COVID podcasts, remote. Eventually, we will get to be able to be in the same room together, but we are figuring out how to do things safely, securely, and remotely.

Brett: Yes.

Suzanne: Thank you very much, all of you for joining us. As always, we will have links to the resources we have mentioned in the podcast, which will be in the transcript. That is where you will find those.

Brett: Yes. Thank you so much for having me too, by the way. That is great.

Suzanne: You are absolutely welcome.

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.