Comparing IT Risk Assessment and Analysis Methods
Transcript

Part 1: Risk Assessment Methods and Comparison Factors

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division is part of the Software Engineering Institute. We are a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a principal researcher at CERT working on operational resilience. I'm very pleased today to welcome Ben Tomhave and Erik Heidt. Ben and Erik are research directors with Gartner Technical Professionals. And I think you'll find today's topic pretty interesting; it seems to be popping up in all kinds of interesting places.

We'll be talking about the criteria for selecting an IT risk assessment method that is a good fit or best fit for your organization. We'll also be comparing and contrasting a range of assessment and analysis methods that Ben and Erik and their colleagues have analyzed and get into the meat of some of these methods and the criteria applied against them.

So with no further ado, welcome to the Podcast Series, Ben.

Ben Tomhave: Hey Julia.

Julia Allen: Really glad to have you today and Erik, very pleased to have you join us today. Thanks for your time.

Erik Heidt: Thank you, it's a pleasure to be here.

Julia Allen: Okay, so for a little bit of a stage setting, as a community we have all struggled with this whole area of risk management, risk assessment, how to take the risk pedagogy if you will that's been applied to so many other parts of running and managing our organizations, and now apply it to information, information technology, cybersecurity, to try and help the people in those positions better identify and assess their operational risks.

So Ben, if you can get us started, how does this work that you and Erik have done contribute to trying to get us a little bit closer to this sweet spot?

Ben Tomhave: Yes, so it was an effort that came driven largely out of client requests. A lot of our focus is servicing end-user clients in our community, and a lot of people, especially technical professionals, oftentimes come back and ask, "Okay, I need to do risk assessment. I've been told I need to do this now. Where do I get started?" Or alternatively we'll get requests around specific risk assessment methodologies and then they'll ask, "What other methodologies should we be considering? What factors go into making a choice about the best fit?" Things like that, and so it leads to typically a larger conversation about overall risk management practices as well.

And what we find, of course, is that a lot of the interest tends to be driven by a combination of compliance desire, especially as we see much more growth in the compliance regimes, but also it can be an offshoot of vendor marketing and PR (public relations) spiel. So a lot of

vendors have been using risk and flogging the term "risk" around in a lot of their product sales lately. So it's a good time to engage on this topic. Don't you think, Erik?

Erik Heidt: Yeah I do. And another thing, Julia, that I think we really wanted to address that's a real common problem here is that frequently people start with very idealistic criteria when they are trying to select their risk management and risk analysis process.

And one of the things we try to do in the reports is really ground people in the fact that at the end of the day there are some decisions whether it's to change the status quo about how a control operates, or whether it's some new decision that's being presented to the enterprise.

There are some decisions that this is supposed to help improve. And keeping in mind exactly what it takes to just simply provide a better decision, one with adequate quality that is a good fit for the organization may be more important than methodologies that need certain other more idealistic criteria or that might be more appropriate for different decisions.

Julia Allen: Well that makes sense because I know as a security community and as professionals we all struggle because we know we can't do it all. Every time we escalate or ratchet it up, the attacking community is always seems to be several steps ahead of us.

And so for me, one of the things that I view risk management, risk assessment as being ideally positioned is to help us prioritize and help us make the right choices. And Erik, is that what you meant by informing decisions?

Erik Heidt: Well absolutely. Sometimes it's a question about what next year's information security budget should look like. Maybe it's a question about whether or not a particular new business feature is appropriate or not -- fits within the risk tolerance of the organization -- or maybe the question is being inspired by an outside party.

You may have a regulator or a compliance-driven requirement to do a risk analysis. But really at the core of that requirement is that they want you to take action on or be able to discuss the results of that risk assessment.

So even in a situation where you have an external regulatory requirement to perform the risk assessment, there is an implied decision that that compliance body wants you to make with the results about whether or not the current controls are adequate or not.

Julia Allen: That makes sense. So Ben, in your analysis, you review a very rich range of IT risk assessment and analysis methods or methodologies. And I was wondering if you could briefly introduce our listeners to some of those that you have dug into and done some analysis on?

Ben Tomhave: Sure, so from an ordering perspective, ISO 31000 -- we included at least from a summary perspective and the driver for that really was because it's pretty broad, it's referenced in a lot of cases. What we also found from a research perspective is a lot of the methodologies out there are starting to converge around ISO 31000 as a reference standard.

We also then looked at other risk assessment methodologies such as that contained with ISACA's COBIT 5. We looked at MAGERIT, M-A-G-E-R-I-T, which actually comes out of the Spanish government environment but it's starting to be used a little bit more broadly throughout Europe and has some pretty interesting attributes to it.

We, of course, looked at NIST 800-30, which is the risk assessment portion of the overall risk management framework and risk management process that NIST has developed overall. And, of course, one of the reasons we are talking with you today is because we included OCTAVE Allegro in that analysis as well.

And then the one that I haven't mentioned thus far and I think it stands out a little bit differently and really applies more as a risk analysis method rather a risk assessment method is FAIR or what used to be known as Factor Analysis of Information Risk, which has just become an open group standard through its roots are of a much more proprietary nature up to this point.

Julia Allen: Great and for our listeners' benefit we're going to get into a couple of these a little bit further when we talk about the factors and criteria that Ben and Erik used to apply to these different methods.

So with that as the lead in, Ben or Erik, can you say a little bit about the factors, the criteria that you use to compare and contrast each of these methods -- kind of rank and stack them?

Ben Tomhave: Sure, absolutely; so a couple different sets of criteria. First of all, just from a broad search perspective, we wanted to make sure that we were as inclusive as possible so we looked very broadly.

And once we looked at very broadly across risk assessment and risk analysis methods, we came up with a number of key attributes that we felt really were common across all of the methods or at least good differentiators. (1) The first key attribute there would be method type -- whether it was a risk assessment framework or whether it was actually risk analysis methodology.

And the key difference there being that risk analysis methodology tends to be very focused on performing a specific set of analysis functions, whereas risk assessments frameworks overall may include a risk analysis capability or instructions for that, but they also serve to provide a larger risk assessment process framework as it incorporates into an overall risk management process.

And so if you look at something like an ISACA COBIT 5, for example, that's a very large governance framework and we actually looked at the COBIT 5 for risk document and pulled out the appropriate risk assessment components there.

Julia Allen: So Ben, let me just ask so would it be fair to say that a risk analysis method or methodology would generally fit within the context of an overall framework or process? Is that the right relationship?

Ben Tomhave: Yes, so if you want to look at the overall hierarchical structure, risk management program or risk management process is kind of the overarching grouping. Risk assessment is a subset underneath that, and then risk analysis is a discreet subset or step underneath risk assessment.

And that is consistent with how ISO 31000 articulates the overall risk management process and the risk assessment process. That provides a pretty good frame of reference for looking at all these other methods and frameworks.

Julia Allen: Great, so please continue on with the other factors.

Ben Tomhave: Sure, so some of the other factors we looked at were (2) whether or not the methods were quantitative or qualitative in nature or possibly both. So MAGERIT, for example, provides a number of examples of risk analysis methods. Some of them are qualitative in nature, some of them are quantitative. (3) We also looked at what sort of cost am I to be associated with getting it so you can't just go down the ISO documents, for example. You actually have to pay a licensing fee to get a copy.

And similarly there have historically been requirements to pay for at least as the supporting documentation for some of the other methods over time although nowadays a lot of stuff is now moving to freely available.

(4) We did look at whether or not tools were readily available. And we didn't necessarily include things like GRC (governance, risk, and compliance) tools, IT GRC tools and things like that but whether or not they were actually native tools.

So again, pointing to OCTAVE, they have spreadsheets available to support the process, worksheets for that process. MAGERIT has a few tools that are actually binary executables that you can download and license quarterly but there's a cost associated with that as well.

And similarly ISF's IRAM (Information Security Forum Information Risk Analysis Method), which I didn't mention in the previous list, was one of the methods we also included. And they provide both a set of spreadsheets that you can use or they also now have a Web interface that you can reference as well.

(5) We then also looked at the type of skills that were required to operate the frameworks or methodologies. And this is where we started seeing some pretty interesting correlations in terms of the prescriptiveness of the methodology and whether or not it was designed for a general audience or whether or not you really actually need to hire a pretty experienced risk analyst or at least send somebody through some decent training.

(6) Similarly we looked at method flexibility; how easy it was to incorporate it into an environment, whether it required a lot of customization, how much time it took really to get up to speed and how much depth and knowledge. And there's a pretty strong correlation there between the specialized skills and how flexible or prescriptive the overall methodology or framework was.

(7, 8) And then the last two things that we really keyed in on, which also had an interesting correlation value, were what we described as "ramp-up time" and then "cycle time" -- so ramp-up time being how long it takes to go from start to finishing the first analysis. And then cycle time was the time it requires to then complete each subsequent analysis.

And the thought being there that the first time you decide to go and use specific methodology you're going to have to invest a fair amount of time into learning how to use that method, use that framework or process, and then adapt it to your organization accordingly. So that typically is going to be a longer period of time than subsequent iterations through the process.

Julia Allen: Great, so Erik, would you like to add anything to those factors or points or anything that really stood out for you?

Erik Heidt: Well one of the great things about the research that we do is that we get an opportunity to really go out and talk to people in the field and to have conversations of significant depth.

And there are a couple of things that appear to be very, very important. And that seems to be number one, no matter what your process is, it has to be a good fit for the decision that's being made. And one of the things that we discovered was that most of the organizations that we spoke to did not have a one-size-fits-all assessment approach to risk.

Most organizations had a baseline procedure that they used to do most of their risk assessment work and potentially which was used to identify when things were not a good case for the baseline or when they had significantly high, maximum impact characteristics or high residual risks or weren't a good fit for the baseline method.

And then they would move to some other method, usually using more specialized staff to perform the risk assessment. So I think that really speaks to something that I think is kind of a broad misconception. I think a lot of people have an impression when they come in and they ask, “What's your risk assessment process?” they really expect that the organization is going to have a single monolithic process for assessing risk.

Ben Tomhave: And just to hop in and build on that too, that was actually one of our key findings here was that-- or key recommendations I should say that using kind of a two-tier approach really seems to be very sensible. And it's something that I think most of the frameworks really were flexible enough to allow.

Essentially you can't run every single decision through an in-depth quantitative risk analysis that takes potentially days or weeks to perform and gather data. It's very important to have some sort of initial vetting process if you will or a filtering method up front that's very lightweight that allows you to decide, “Okay is this really something truly high-risk and important that we need to do a deeper analysis on?

Or is this something where we can have some cookie-cutter templates and decisions so we can just document that okay, this has happened and this is important but it doesn't necessarily rise to the level of something that's material to the overall wellbeing of the organization.”

Julia Allen: That makes a lot of sense and I really like this set of factors because there were some for me that were counter-intuitive or were things like, “Oh yes, I could imagine why this would be really important, like special skills required.”

How often when we're picking a method or picking a tool or picking an approach do we actually look at the requisite skill set that's going to be required to not only deploy it but to use it, to maintain it, to make sure that it's got traction and becomes part of the operational way of doing business.

Part 2: Tradeoffs – Methods vs. Factors

Julia: So we have some time and what I'd like to do, Ben or Erik however you want to prosecute this, is if you could take maybe your favorite factors, a couple of your factors and maybe one or more of the methods that were noteworthy from your point of view, and just on a sample basis, could you give us an idea about how some of the methods stacked up against some of your factors? I'll leave it to you as to how you want to go about that.

Ben Tomhave: Sure absolutely. So one of the pairing that I'll talk to and maybe Erik can talk to the ramp-up time and cycle time. So the specialized skills and method flexibility I found particularly interesting. And we actually went through and went back and forth on how to properly name it because -- and then described these especially the method flexibility topic.

And really what that one came down to was how prescriptive a given framework was. Was it more prescriptive or less prescriptive? What we found was that there does seem to be somewhat of a correlation sometimes between the two though not as much as we might have believed originally.

But the more prescriptive methodologies, for example, oftentimes -- I should say well most of the time; how about we go with most of the time -- were relatively straightforward to understand and potentially implement. Where they however became more difficult was when it came to customization -- and COBIT 5 is a great example. COBIT is huge as an overall governance framework.

And they recognize this and this is why they produce separate documents such as the COBIT 5 for Risk document as well as the enabling processes and the enabling information supporting documents too.

It's very, very prescriptive. I mean they go to a great depth of coverage in terms of the specific processes you should follow and so on and so forth. But the one point that ISACA really drove home with us is that while it is prescriptive, it's also designed to be heavily customized to meet the needs of an organization. They don't expect anybody to go out and wholly implement COBIT within their organization.

And so in that regard, it really does take somebody with a reasonably high level of skill both with risk management overall and also with the COBIT 5 methodology to be able to parse through and know what pieces are important, what really need to be followed, where customizations can be done, how customizations work most easily so on and so forth.

Julia Allen: So I would assume with those two factors and the tradeoff being if you think that this risk management, risk assessment process or method that you are intending to deploy is going to have some longevity to it and some broad applicability to it, then it may make more sense to do the upfront investments to get to a customizable approach that really fits your organization. Would that be one of the factors to think about?

Ben Tomhave: I definitely think that very much something worth thinking about is how much are you willing to invest upfront to get something to best meet your organization's needs versus looking for something that's quick and easy and more cookie cutterish? So a couple contrasting examples to COBIT 5 -- ISF IRAM, for example, is more prescriptive but it's designed essentially just to be run out of the box.

FAIR (Factor Analysis for Information Risk) -- it's a risk analysis method and it's very prescriptive but there's really no opportunity for customization. It's true that you need to go through a fair amount of training because of the nature of quantitative analysis tool like that, but in terms of customization which you don't have to do much with it.

OCTAVE on the other hand, is a much broader, much more general framework. And it provides I think a great basis for organizations to -- especially engineering-minded organizations who kind of already fit with the style of writing and the style of thinking that CERT is known for.

Being able to take OCTAVE and customize it to your organization I think is pretty straightforward because it doesn't tend to be quite as prescriptive in nature but again you still need to then have somebody reasonably skilled who can understand the principles that are discussed and the processes that are discussed there in order to match it to your organization's needs.

And what you'll find too that goes along with this -- and I think Erik you might want to hop in here and comment as well -- but if you don't invest that time up front, you're not going to be as successful overall. And you may find that whatever efforts you do end up undertaking relative to risk assessment, risk analysis, it's not going to last very long if you don't actually take the time to tie it into your organization.

Julia Allen: Got it. So Erik, why don't you take some of the air time now in response to Ben's handoff and also maybe talk with us a little bit about ramp-up time and cycle time.

Erik Heidt: So it's cliché but you really do need to start with the end in mind. Something that is really of critical importance here also to understand is that you will likely have multiple other processes or tollgates that require some type of risk assessment in your organization.

So I had a conversation with a client about two months ago who needs to do 2,000 risk assessments on existing third-party suppliers per year. So immediately you know that you have time and resource constraints and there are limits to what you can do with those time and resource constraints.

And so one of the things to keep in mind early in the process is what do you want out of the assessment on the back end? And sometimes you want to make that a go-no-go decision. Other times you're trying to identify where are you going to put your risk management and mitigation work. How are you going to categorize and prioritize the areas where you want to focus on improvement? And so those can be very different demands in terms of what the organization needs from you on the back end.

So also critically -- I think this is a good lead in to this other discussion -- that has a big impact on what kind of ramp-up time as well as cycle times are going to be acceptable for you, ok? If you are a large organization or an organization that is highly regulated or that has very, has occasional super high risk activities that you participate in, investing the time and energy in a methodology like FAIR which deals very well with those types of problems, would be very well spent.

On the other hand, if you have a situation where due to a regulatory change or a compliance finding you need to perform hundreds or thousands or tens of thousands of risk assessment across a population in a very short period of time, you're going to have to make some decisions and potentially some compromises about the methods that you use. Because you may not have the liberty of selecting methods that, say, are going to require formal outside training.

You may have to have methods which can be automated through tools so that self-assessment risk questionnaires can be used to collect most of the data. Again, you're probably going to take a look at those scores and sampling strategies to make sure that those self-assessment questionnaires are meaningful and are effective measurements. But again, if you have to do very large numbers of these things, you may need a method which can in fact be automated.

So these things become real critical to the overall success of the effort in terms of how long do you have to make things happen -- which in most organizations your executives would like your risk assessment process done yesterday so they can make these decisions and move on to other things.

And when you embed these things in tollgates or when they get applied to large populations like suppliers, like BIA (Business Impact Analysis) that may be repeated on a periodic basis across your services and applications, and so on.

How do you size those so that the cycle time and the resource requirements can actually fit into the time and energy of the resources that you have? And/or how can that effort generate results that allow you to demonstrate that the process is effective or that you need to commit more time, energy, or resource to a process to improve its effectiveness? These are all real important starting considerations that you want to think about.

Julia Allen: So Erik, on the ramp-up time which is time to complete the first analysis and cycle time which is the time required for subsequent analysis, with respect to some of the methods that you and Ben have been talking about, could you give us some examples on methods that are at the extremes? About maybe short ramp- ups, short cycle versus longer ramp- up, longer cycle?

Erik Heidt: Well I would say that the qualitative methods in the report tend to have shorter ramp-up times and the methods that are either more qualitative (meant to say quantitative) or that have very, very large scopes have longer times.

I don't have them stack ranked in front of me, but the things like, for example, NIST and probably also OCTAVE I would say can be on the relatively short path to adoption in terms of ramp- up. COBIT because of its size and scope has a tendency to be longer.

Julia Allen: That's great. And as I was listening to you talk about the tradeoffs that you need to make, I was also thinking about you said executives want the risk analysis results yesterday.

The organization, when you're starting to embark down this path may not have a lot of tolerance for waiting and so you may need to grab something that give you a quick win early so you can grab the attention and generate some momentum for the initiative. Did you find that in your analysis as well?

Erik Heidt: Generally items which generate quick wins are generally ad hock in nature. They generally will predate or be used to justify a more formalized process.

Julia Allen: Okay, okay.

Ben Tomhave: If I could just jump in for a second and follow up too. So pardon me Erik for correcting you but with the chart in front of me here, it's reinforcing what he said. The qualitative methods tend to be easier and shorter to ramp up. The quantitative methods tend to take a little longer time just because you have to have a little more specialized skill to support them.

Overall we found that frameworks like COBIT 5, for example, really has the longest ramp- up time because there's so much customization and there's so much stuff there to do. NIST 800, OCTAVE, and MAGERIT both seem to have reasonably middle-length ramp- up times.

And then the cycle times can vary widely depending on how well you have everything tuned down. OCTAVE, for example -- we list it as having a medium long cycle time just because of all the analysis that goes into each assessment.

But if you talk to someone like Lisa Young from CERT about it, there are ways to shave off a lot of that time and short-circuit things, especially as a team or an analyst goes along and becomes more accustomed with things.

Some of the other methods on the other hand will be much shorter. And even FAIR; for example, tends to have a shorter cycle time once you get through that longer, slightly longer ramp-up time. And that is because of the tools associated with it that you essentially learn how to go through and do estimation and calibration and plug numbers into the tools. And there's less to it overall process-wise.

Erik Heidt: Another thing to keep in mind there is that some of these processes lend themselves to a more iterative approach than others.

Julia Allen: Good point.

Erik Heidt: So FAIR in particular gives you the ability to figure out what size hazards, threats, and potential impacts you're dealing with early in the process and then allows you to make a decision about when you've reached a decision of granularity.

So it can be applied iteratively which some of the other more questionnaire-oriented processes, you're kind of one and done. But again, I think that in the vast majority of situations the risks that come out -- having high residual risk to the organization or otherwise stand out from a potential impact perspective, are almost always going to get some type of additional analysis.

Ben Tomhave: That's a great point, Erik, and something that I think is worth driving home too which is there seems to be a common misperception within the industry still -- it's finally starting to go away -- this mythology of the annual risk assessment. There are cases where perhaps you do an annual risk assessment. Supply chain risk for example comes to mind where you're assessing your vendors maybe in the healthcare context for compliance with HIPAA or something along those lines.

But overall, risk management isn't a once-a-year type thing, right? It's an ongoing thing so this is where that cycle time really comes into play that maybe you need to do a risk analysis or a risk assessment on key systems, key applications -- even potentially integrate it into the development process. Now we're starting to see a lot of good tool integration that is starting to potentially move that the needle forward on doing integrated risk assessments as part of application security testing as one example.

But it highlights the point that this is an ongoing thing and risk assessments really should be a continuous deployment model, not a one-and- done or annualized type approach.

Part 3: Important Characteristics for Selecting the "Best Fit"

Julia Allen: Excellent point. Well Ben, you are headed in this direction so let's see if we can net this all up for our listeners in terms of the things that they really need to think about as they embark on this journey or perhaps fine tune the things that they are already doing.

So could you start us off by talking about -- across all the factors that you considered and across all the methods that you evaluated -- what things did you find were really essential for selecting the right risk assessment approach for an organization?

Ben Tomhave: Right. Yes, so the true differentiator that we found surprisingly -- I think this is actually very surprising -- is because of the primary direction towards converging on the ISO 31000 overall model or reference framework, that there's not a lot of difference qualitatively in terms of how these frameworks all function.

And so really where a lot of differences come into play is how they fit better with your culture -- so that cultural fit. This can be maybe foreign to some people in terms of what do you mean by cultural fit? Well Again, when I look at OCTAVE and I read through it, it's got a very nice logical structure to it that fits very well with an engineering mindset or an analytical mindset.

COBIT 5 having its roots coming out of the audit community tends to have language and stylisms that fit much better to that audit and compliance and governance mindset. As such it might fit better into some organizations that already function in that type of cultural manner. And in particular we see this in financial services, right, because they are very heavily committed to doing audits within their organizations and very audit-centric security practices.

Similarly FAIR is great for people who are very numbers-oriented. MAGER-IT, MAGERIT -- however you want to pronounce it -- may also be a very nice fit. Again it's oriented around ISO 31000 but it provides a lot of good structural guidance while giving flexibility for deploying multiple methods so that might also be a good cultural fit for an organization.

The other ones that jump out at me too -- and I'm sure Erik will agree on some of this too -- scalability is a huge key, right? So that ramp-up time and that cycle time is very important in keeping that end goal in mind is really very critical. You can't afford to spend a month or three months on each assessment cycle typically especially if you're under a lot of demand in order to get these done very quickly.

And incidentally in talking to some of our end user references around this topic one of the things that we found on scalability is that a good methodology will actually allow you to choose between a centralized and decentralized approach as well. So rather than having to have just a single centralized team that everything comes through, there are possibilities of being able to essentially distribute that analysis function and providing supporting tools accordingly. But that then ties back into that specialized skills topic as well and that flexibility topic.

So if you want to do distributed and embed risk analysis functions into different parts of the organization, then you need to be able to provide reasonable support for them. So that all goes to scalability.

And then of course again on Erik's point about having the end in mind -- meaningful output. Just because you can do a risk analysis and get some sort of output doesn't mean that it's going to be useful or meaningful to your organization. And this is something that's been historically problematic with a lot of the qualitative methods especially the older ones that get back to, go back ten years or more.

We're thinking about things like CRAMM, for example, and even the IATRP program (Information [Security] Training and Rating Program) that used to be run out of the NSA's assurance program. Qualitative can be okay but when you're looking at high, medium, low labels and trying to then differentiate between, “Okay, I have ten high findings. Which one is actually more important?” That leads to the point where it's not necessarily meaningful output. What do you think, Erik? What were some of the more important characteristics there for making a selection?

Erik Heidt: One thing that's very important by the way in terms of your communication as a risk management professional with the rest of the organization is distinguishing between the risk management activities you perform with these methods and compliance checks because a lot of people get that mixed up -- not a lot of risk management professionals, but a lot of the people you engage with in the business and so on.

And then the second thing is we're all overbooked. And so something that I'm strongly emphasize is don't just keep the end in mind with how are you going to use this data to fulfill the immediate need, but also how are you going to use this data potentially in the future.

Can you modify this particular risk assessment task that you have been handed -- especially if it's one that does one of these activities that goes out to a large number of individuals or across the large population -- and can you add things to it so you can get more value and more leverage out of it in the future in terms of it helping you to either identify hazards to the organization -- they need to be mitigated -- or to classify and stack rank and prioritize risk management efforts.

Julia Allen: Excellent. Well, gentlemen, I'm going to need to bring our conversation to a close as much as I regret doing that because we could go on for quite a bit longer. So I'd like to leave you with one last question, is do you have some pointers or references for where our listeners can learn more on this subject?

Ben Tomhave: Absolutely. So this report is available to subscribers on the Gartner for Technical Professionals side of the research house. The report is titled "Comparing Methodologies for IT Risk Assessment and Analysis". And the Gartner document number is 256964, again 256964.

If people are not Gartner subscribers, then they can certainly hit the Gartner.com website and click on the link to explore becoming a client. And oftentimes Sales will provide access to documentation as part of a proof of concept through the exploratory process.

Julia Allen: Okay and Erik, anything you'd like to throw in here?

Erik Heidt: No. The thing I like to do when we do these research processes is we talk to a lot of end user organizations who for confidentiality reasons we're never allowed to name and we just have a tremendous amount of gratitude and appreciation for their participation and for their making this research and all of our other research possible.

Julia Allen: Great, and also for our listeners' benefit, I will include in our show notes links to all of the publically available methods that we have discussed to include FAIR and COBIT and ISO 31000 so check out the show notes for additional references.

Well Ben, let me first thank you for this excellent body of work and for your time and preparation today. We really appreciate having you on the podcast series.

Ben Tomhave: Thank you very much, Julia.

Julia Allen: And Erik, great to have you with us and appreciate the hard work that you and Ben are doing and your team is doing to bring these methods to our community for practical application. So thank you for today.

Erik Heidt: It's our pleasure and our passion.