FEDERAL TECH PODCAST

EP48 Deadlines, CMMC, and the Defense Industrial Base

Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. today. Our guest is Igor vola vich. He's the Vice President compliance strategy at a company called cumulus QMU LLS and we're gonna talk about cmmc cmmc 2.0 and everything you need to know About CMC. But first, I have to tell you, we're recording this from monk's barbecue in lovely downtown Percival Virginia and have to as eager so what are you going to order after the interview here with your brisket for me? Whoa, wow,

01:05
gotta be the brisket.

01:06
garbled beans in there. Gotta have some maybe mac and cheese. It's great. Absolutely. Purcellville has monk's and you should have come down here as well. Okay, let's jump right in here. People in software development people and cybersecurity people and everything to do with the Pentagon and the DoD know about cmmc. If you can, can you just paint a picture of Siemens see for me exactly what it's where it started and where it's at today, then we'll dive in with more seriousness.

01:32
Well, I think that's actually probably not a fair characterization. I think a lot of people are confused about CMC. In fact, I think a lot of people think of this as a new mandate. We see that a lot out there. And the reality is, it's not a new mandate. It's just a new way of assessing against existing mandates. So when you think about CMC, what it is, is just a program for figuring out if you are in compliance or non compliance with things like SB 801 71, and 172. So it's not a novel thing. And I think a lot of folks need to kind of get get up to speed on that the requirements for or the requirements are you going to be successful under same MC 2.0. They've been there for a long time. So this isn't anything new.

02:11
Let me try to put it in perspective, someone like me, who's just an outsider. So around 2020, people looked at the defense industrial base, the 300,000 companies that supply the Pentagon, and they said, hey, that's like Swiss cheese, we got a lot of Hoelscher, we got to improve the cybersecurity. So they came up with this pretty fancy document, CMC with five trim levels. And then for some reason, they took off 2021. Maybe they're all at Monk's eating barbecue, or something I don't know, in late 2022, they came up and they must have been working on the rules since then. And they changed some of the requirements. And they pretty much have the rules pretty much intact now and what they're doing now we're in 2023, and is anticipated sometime between now and November of 2023. They're going to release the CMC 2.0 rules and start taking contracts based on in

fact, that could happen a lot sooner than that. So we have a situation where there are many companies, Igor, that are putting your feet up on the table, smoking a cigar and waiting until November, and then they're going to start the compliance. What could possibly go wrong?

03:08

Well, everything right? So for once, you really shouldn't wait, first of all, this idea that we have to wait around and figure out well, what the cmmc 2.0 mean, to me, you've known all along, all those requirements have been there for a long time, the same as C 1.0. We had five levels now has been simplified. Now we have three levels. So things are a little easier. But what's really important to understand is you can't wait because your competitor is actually moving ahead. And what we're seeing out there is its compliance, basically becoming a point of competitive advantage. What does that mean? You know, we heard 3040 years ago, it becoming a point of competitive advantage. Right? And that's people were slow to update on that one, right? And compliance. That's really a foreign concept. How can compliance be a point of competitive advantage? Well, the truth is, with cmmc compliance is now table stakes, you can no longer afford to defer compliance. You can't wait to demonstrate compliance. You can't do these never ending poems, right? You have to actually demonstrate compliance in real time. And the sooner you can get there, the better position you're in to compete for contracts, because basically, it's table stakes. If you cannot show compliance practically, you can't even bid for the federal business anymore. And so when we're talking about a number of contractors who could be in scope of this, in the end, we're talking about, yeah, the entire scope of the defense industrial base, which is about 300,000. Companies. What's interesting is you hear these estimates range from 80,000 to 300,000. We don't really even know because there's these cascading kind of the Russian nesting dolls not to use the Russians, but it's kind of a Russian nesting doll of complexity. You've got primes, you got subs, you got subs of subs. So this is multi level. And you know, a single bolt and nut assembly that goes into a fighter jet could be coming from some Mom and Pop sitting in Texas, and they still have to comply because they're holding some level of CUI they confidential and classified information. So the real story of who's going to be in scope of them when it's it's very complex. And the reality is, nobody can wait doesn't matter which level they find them and how far from that trough they are from DC, right? how close they are to the prime if they are the prime? Absolutely they can't wait. And so as you mentioned earlier, the federal government finally woke up and realized the supply chain presents an enormous level of problems. For us. It's a huge exposure, the attack surface is virtually unknown. And so with the self assessment scores being what they are SBRs system, we've allowed this system kind of to persist for a long time. And the contractors took advantage of it. Right. And this isn't to say the federal government was asleep at the switch. But the reality is, they weren't necessarily diving in deep to figure out where exactly those controls were. And then you're given time. So they relied on the contractors kind of self certify. And what we wind up with as this big unknown, it's this huge risk fog of war. And so that's something that CMC 2.0 is basically intended to resolve, and really get a lot more credibility, a lot more transparency. And doesn't that process, I'm trying to

05:48

come up with a, an analogy, a metaphor, or a story that would maybe crystallize this for this whole idea is that people who are listening to us provide software for the federal government, we know that they're competing with each other, we know that and they all try to hire good people. And they all try to do good work. We know that that's an assumed, but you're in a race. And my avocation is distance swimming. So I compete notion

races on the East Coast and West Coast. And I was once in a race in the Great Lakes. And I was with a pod, and they shot the gun is about to start and someone kicked me in the head knocked off my goggles. So I had to go back to the pier, climb up on the pier, ask someone for goggles, I gotten the goggles, then I jumped back in the race. Well, guess what? I was 100 yards behind everyone in the race. And that's what's going on today. There are people listening to this. They're saying, Yeah, I'm here with Randy software. And we're just going to wait until the all the rules are finished here in November, and then we're gonna jump in and get compliant. But you know what, Randy software, you're gonna get killed by, you know, cod software, whoever your competitor is, because you're behind in the race already. Let's face it, you know, the rules are there, the rules aren't going to change a whole lot. I mean, this is pretty much the concrete form, they're just waiting for to cure. So they pretty much know what the rules are. So why not take and take advantage of the situation, you have to beat that guy who puts his feet up and waits to the last minute. I mean, this is a lesson from today is that don't wait to the last minute,

07:11

don't wait at all right. And here's the funny story. So we have a good friend of ours, Jacob Horne, who is actually over at seven, seven is a big cmmc guru. Here's a guy who basically dedicated himself a couple of years back and said, I will become the same MC industry expert. And he is he reads the forest, he goes deep down into the controls. And what he says because he he's reaching the market all the time, he's talking to people in the marketplace, what he found out is a lot of companies say publicly that they're waiting for the rules to really hit before they do anything about it. In the meantime, they're working furiously, to get compliant as fast as possible, because they actually understand this is a point of competitive advantage. And the faster they can get there, the better they can compete, they want their competitors asleep, they want them thinking that they need to kick their feet up, wait a second, you know, wait for the rules to be completely federally accepted. And and that's not the option anymore, you really can't do that. So we seeing this sort of this public face, I've seen mostly compliance where people are saying, Yeah, we're gonna I'm gonna wait, but really, they're going home and telling everybody in their system shop and their risk shop and our compliance shop, audit shop, get to work, right. So some of the stuff could be kind of subsurface, you know, we're not seeing that effort. But I think eventually, it's all gonna come public, right? But folks are going to start competing for bids, one cmmc 2.0 is in place. Once those contracts actually folded into the scope of compliance for CMC 2.0 That's a everybody's gonna be on the same footing, we will have to wait a couple of years for that to completely permeate the marketplace. But for now, if your contract winds up to be in that first batch of contracts that are coming, were similar to when I was coming into force, it's a might be an unpleasant surprise,

08:41

Igor, I spent many decades in radio, so I have to do my radio stuff here. So if you want more information on Igor, you can go to qmuls.com for lots of information on cmmc. And if you want to find out who the 2023 best beard in the World contest winner is go to YouTube and type in Jacob horn, J. LB HR any because he has a beard that makes yours look pretty shabby. Their ego looks pretty shabby and roaches Isn't this amazing?

09:09

I have to admit, you know, this is something that's actually a great analogy because you can't train for the beard contest. Or you can train for it. But you certainly can wake up the day before and go, I forgot to train for it. I have to plan I haven't

09:20

I think you know, most tuck it into his pants. It's so long. It's an incredible beard. So let's so let's say time machine, they start releasing in June and your company applies. And hey, you're all caught up and you're fully compliant. And you get a deal. Okay, everyone's happy. So Randy software gets the deal. Randy's happy. Everyone's happy. Well, you know, you can't just put again, put your feet up in the chair. You know, there used to be a TV show where this guy named Ron Popeil. he'd sell his chicken cookers and it was set it and forget it you know, it was great. Yeah, it set and forget to put that chicken instead and forget he saw a lot of on TV. I don't watch much TV anymore. But I think about that. I think what people the next step is see him and see his Oh, yeah, yeah, I know that Igor guy we hadn't come out and we're all compliant now. And we're just gonna, you know, not do anything, not do anything next five years. Really? This, this is another trap,

10:11

isn't it? Well, the reality of compliance is people don't think to think of it as a snapshot in time. And historically, that's what compliance has been. If we roll the clock back to the first real known compliance mandate, we're going back to the times of Hammurabi, right, the first building code that went off, you know, if you don't build a building, right, and it collapses, well, we'll collapse the billing on to you pretty draconian, but for the time was pretty fair, right? If you kill people? Well, I guess, you know, it gets pretty biblical pretty quick. And so we've always looked at compliance that way, historically, we've looked at compliance as this deterrence measure, right, you know, we tried to find non compliance, as a way to predict proactively manage risk, and then deterrence, in fact, should be there, right. So if you are not doing right, they should be punished, and it should be public. So this deterrence models, compliance has really driven the design of compliance systems or compliance models for a very long time, and it really hasn't changed much. The problem with that was built into that model, it's you're always looking backwards, you're looking always looking at past acts. So you're waiting for something bad to occur. So you can actually enforce that that compliance measure, right. So the idea is, how do we move forward? How do we actually bring compliance with the real time? We haven't had that? Right? We haven't had that, because compliance has always been kind of this audit function, which we borrowed from where the financial industry, right, financial audit firms became cybersecurity audit firms. And that's kind of the same idea. Well, you'll look at things that happened, you capture them, you report them, it's always this kind of historical reporting function, it doesn't work. Because today, the threats are moving too fast. The bad guys are not looking your compliance reports, not worrying for the quarterly report, they're not waiting for your annual report. Look, in the federal space, we have a tios, that period of time is three years, you have to reassess. And, of course, you have to come back and recertify. But that snapshot, entire look, we've talked to a lot of federal agencies that when they say, Look, I just can't even have a faster cadence than once every three years. So if you're looking at things right annually, and the bad guy is looking at the real time now, what value is that compliance report? Right? It's basically a cya exercise. Mostly right? It's for somebody to go in front of Congress, like Colonial Pipeline, good example, and say, Well look at that compliance report. And here comes the whistleblower, and says, Guess what those compliance reports they were bogus, right? So you have these layers of complexity? And layers of well, let's say it untrustworthiness. Right, you don't even know

what's in that compliance report because of how complex it is. And there's a built in lag, right? I call it the compliance lag or compliance latency. So you don't, you can't really rely on that as a reflection of what is your current state of controls or your current state of risk, your current risk posture for the enterprise? So we keep doing compliance that way keep we keep trying to get different results out of it, right. And it's also considered a different animal, right? Here's compliance. Here's security, we treat them differently. We think of them as different functions, different values that deliver to the enterprise. My personal opinion is, and I think we've we've said this quite a few times. And I think some people, I think, starting to think that way, is that compliance, security shouldn't be thought of as different things, you know, we accept this compliance latency on the compliance side, we would never accept it on security side, imagine your sock security operation center running on data from three years ago, it could never work the bad guys operating in the now. So if we could bring compliance into real time, do it continuously, which means we have to do it with automation. And we can talk a little more about that. That's really the ticket. That's really the way to do it. So instead of taking snapshots at some periodic cadence, bring compliance into real time, make it continuous, right. And this isn't a novel concept. Look, CDM program has been in existence for over a decade. So we've got continuous monitoring as an idea has been around for a long time. We just really have never taken it on board as certainly not in the federal space. So that's my thesis.

13:43

I have a friend who has a podcast about sports. And they talked about basketball. He thinks he knows everything about the NFL, you know, he really does, you know, and here's what I know about the NFL, sometimes a quarterback gets the ball and he hides the ball. No, no, he's got the ball. Okay, kind of football one on one. Well, when it comes to cmmc, they ain't hiding the ball, this. This isn't a secret mumbo jumbo that no one knows about. Now the ball is out there, you can go to NIST and download the requirements today and start right so you can get a little checklist out yourself and started so. So I don't want to hear this Igor software saying, Oh, well, I didn't know anything about it until November of 2023. No, no, they're not hiding the ball. This is right in front of you, isn't it? I mean, you can that all the regulations are there.

14:23

Exactly. So it's not you know, nobody's got an advantage in terms of what they know what they don't. We have complete informational parody. Everybody else on the same page, everyone knows what their requirements are. There's really no excuse, right? You know, you show up to a bid and you're not compliant. You're not gonna get a deferral. I don't care if it's mission critical. I don't care if you're, you know, the only source of something. Guess what, in today's day and age, especially in the cybersecurity space, you've got over 4000 operating vendors, there's always a choice. Every category is full of competitors. So if you think that your unique proposition is somehow so compelling, that you can get away with not compliance that somebody will give you a deferral or some kind of low risk acceptance letter that's not going to All right, so get compliant. Get there now. And also think about this SEMA MC is just one thing, right? This is not one set of requirements that's unique and different and somehow so special that you just have to figure out a different way of doing it. It's just It's same SB 801 71 172. Show, it's been updated. It's actually 171 is being updated right now. But the way you do compliance is something else you have to think about. So I think there is a kind of a meta conversation about your compliance program maturity, not just your compliance maturity against a specific set of controls and standards. But really, it's more about what is your capacity as an Enterprise Compliance and

Risk and security management program? What is your agility? How quickly can you adapt to these different requirements and how quickly you can demonstrate your compliance with those requirements on an ongoing, continuous basis? Because these things keep coming out, right? We've seen executive order 1402, eight, it's spawned many different mandates, you know, OMB, M 2131, comes to mind, am 20 to 18, that's a supply chain security, one, etc, etc, they will continue to emerge. So if you're always jumping from one foot to the next, trying to figure out well, how do we comply with this next thing? Right? These are the conversations that are happening within the enterprises right. Now. Here's Here comes another one. How are we going to do that? How are we going to deal with that? That's not the question, right? This isn't a question about how you deal with it. cmmc specifically, of course, it hits people in the p&l, it will stop business. So that is so critical. It's creating a sense of urgency, which is great, right? It's driving a lot of intensity around this, this conversation. But it's not just about TMC, it's about how do you comply with anything that's around the corner. And you I mean, you can read the files, and you can read the Federal Register, and you can figure out what's coming down the pike, you're gonna do this kind of predictive modeling of what comes down from a regulatory perspective. But ultimately, it's about your ability to know where you stand at any given time. And again, we go back to the continuous monetary controls. If you can't do that, if your program is incapable of doing that, then cmmc is just a litmus test. This is just one thing that you will fail amongst many others.

16:50

In a previous podcast, I quoted Niels Bohr. And then I quoted Yogi Berra. And this podcast for monks. I'm gonna quote an author from England, and he wrote it, no man is an island. No man is an island himself. And if we apply this to technology, it means that even if we have Randy software, and he goes through all the compliance procedures, he is still interconnected with other companies. And so I think step one is, you know, understand what the requirements are because not hiding the ball. But second, number two is you're not hiding who you're connected with, you know who your partners are, you're going to have to go to each one of your partners and go, okay, there, Joe software. Tell me what kind of liabilities Do you have? Where do you stand in cmmc? Okay, Pete Smith, okay. Jeff kalamar, where do you stand with CMC? And so the first step is understand it. But the second step is, you're not doing this alone. You're integrated with other people you have everyone's got partners. There are interdependencies

17:37

here that need to be mapped out. And the Nexus here is CUI right. Oh, some people call it kind of funny. kuih. Right. But it CUI is confidential and classified information. That's also FCA federal contract information. If you hold it, where you hold it, you have to figure that out. And you have to figure it out quick. And if you also need to understand your data flows, right? What do you consume? Where do you get Cui? Where does it come from? How does it enter your environment? What does it sit? And so it to me, it's reminiscent of the conversation we used to have about 15 years ago with PCI DSS, you know, where am I enclaves? Where am I holding cardholder data? You're trying to figure that out pretty quick. And, you know, the sooner you can do that, the sooner you can figure out what kind of controls you can place around it, because that will create the priorities for your compliance strategy. Right? And when people talk about what compliance strategy, what does that even mean, right? You got to comply? Like, what's, what's the strategy? Where's the strategy? Well, you got to figure out which of your business activities are the most critical, which ones are going to be most likely impacted by things like CMC 2.0, right? If this will be disruptive, from a revenue perspective, that's where

you got to pour your resources, right, you can be compliant everywhere at once, I would say if you're investing into this, if you're thinking about prioritizing, on the one hand, invest into a program, make sure that you have maturity in your program, you have a jewel in your program, that you understand how this information comes to you. How do you even know what you know? Right? And I have to get philosophical on this. But a lot of folks are taking their existing data and their existing compliance reports at face value. I'm gonna pose this question to the audience. How do you know this? How do you know that what's in that compliance and audit report is actually true? Because when you think about it, a lot of data goes through a lot of hands, right, that control statement that somebody has to interpret that analyst to ISO Information System Security Officer, they have to make a judgment call that auditor have to make a judgment call, right? So what they're looking at is these these failure and non failure statements, you know, whether those controls complying or not, think about extrapolating that to a level of system down to a level of a system of systems then to level an entire enterprise. Now, you've got you know that one piece of data becomes a pixel on that dashboard that your sister reads or your audit board reads, how did it get there? Right? How truthful is that pixel? Can you trust? And is there credibility built to that model? And so if you understand opinion, subjective opinion versus fact, how much factors in your compliance program versus opinion, right, how much data versus subjectivity, these are the kinds of questions you should ask so you can get down deep into the controls. But at the macro level, I think that's something to ask. And when you kind of look, I'll give you an anecdote I stood with a head of risk of a large federal agency, and we looked at their pool of ISOs. You know, they had about 250. And we stood on his doorway. And I said, How do you know what you know about risk? And he was the head of risk, right? And said, How do you know what you know about risk? It says, Well, this is it. We pull these compliance reports. And we we compile them and figure out that that's what a compliance posture is. So But you do realize there was a lag built into this model, right? And it says, Yes, I do. I said, you realize that there was a subjectivity built into each one of those decisions. But each one of those is a sales for each one of those systems, each one of those controls. And he says, I do, but this is the best we've got. And this is the best they had. Right. So there is a better way, there's a better way to think about it. I think people need to start asking more of these questions, where they're investing their resources. It's not just technology. It's not bottom up. It's not, you know, tech first, you know, what, what's the latest tech that we acquired to make this easier for us? It's not about that. It's about where are my resources pointed? How much truth is in those statements? And can I increase that truth whether it's the trustworthiness of that data, that credibility build of the program, invest in that

21:00

ego? Are we recording this at monks barbecue and lovely downtown Pearl Seville, two blocks from here? Mike Bridges has an auto repair shop. And what happens is, let's say Randy from Andy software brings his car in there and needs brakes, as they say, Hey, Randy, got you two weeks here and you get some breaks. Okay. Then Randy gets some bakes and then he passes inspection straight. So let's talk about cmmc. So Little John Gilroy waltzes in, and I don't pass the criteria. So what about the deferrals? Do I get a deferral here? What happens then? No deferrals what was my car inspection?

21:35

No, no, it's not safe. It's not safe on the road. Look, we had not not to get morbid here. But we actually had in our neighborhood, we had a terrible accident. The guy had uninspected vehicle. It was actually a van he was using as a food truck. And he went down the hill. And he skipped about it past the stoplight, he couldn't stop,

his brakes went out. And he killed people. And now we actually have a different stoplight there. It's a different system. But it took a year and people kept writing about it. They said, Look, this is a bad intersection, somebody's gonna get killed, and it took that one unexpected truck, and he was unexpected for years and years. So this is the reality CMC sorry, isn't it? Right, as they say, Mercy story, right, you know, you don't get inspected, you get a deferral. And that's why this federal government is getting away from that, right, because that deferral, basically, what you're effectively doing is extending that window of risk, that window of exposure. And that's exactly that's that classic OODA Loop conversation, right? The bad guys operating inside of OODA loop. And we need to constrain it, we need to decrease that the time that it takes to identify a control failure, understand how to fix it, apply the fix, and then check it again, make sure that stays in place. We think about it that that way on the security side, like vulnerability management, we definitely do it in real time we tried to make around those scans every day pen test, we tried to automate those very quickly, right. But for compliance, we just accept this lag, like well do this data from three months ago, three years ago. Who cares? Check the box move on. But it's about risk. Compliance was really created to manage risk. It's a consistent model for risk management, nothing else. It's not a paper exercise.

23:02
Let's take this risk management topic and flip it on its side. So little, John Gilroy, spends 500 hours on an RFP submits, it turns out that he's not seen as he complied. And they can help out here. I mean, there's situations where people are spending 1000s of dollars, and they're kind of like shrugging the shoulders. Now there's going to be a filter, it's going to be go home, John, we're going to look at Igor because he's compliant. This is this is this is serious business system cost you money.

23:27
Absolutely. Absolutely. I mean, it's impacting the revenue. If we were about to publish a white paper about actual impact, a p&l, we're doing an analysis on this right now. And if you're a federal contractor, you'd like to continue being a federal contractor, and continue to be making money, you got to worry about this, right? Because you can have a great product, you can have a great solution, you have a wonderful value proposition for your clients. But the problem is, they simply are not allowed to do business with you anymore. And so no more deferrals no more, hey, you know, we're going to have a sole source contract, and you're the only one who could provide it. We're talking software, this is whole fungible, right. So anybody can do software, anybody can do cloud, and it's just not going to play anymore. table stakes, and you got to get there now. So you don't want this, you know, bad old compliance to really torpedo your chances. And I did, right, let your product speak for itself. You have the software to speak for itself. It's service speak for itself. Give him a chance, a fair chance. Because you don't want to like you said, you don't want to be thrown out the door because you can pass EMC compliance. Okay,

24:21
two thirds way the podcast I'm thinking how the blocks first block is learn about CMC learn about Ms. Learn about their clients. Next, see about your part and see where they stand. And the third part really is that, oh, I'm behind the game. I gotta go call up eager and haven't helped me. Well, guess what? Either could be booked up. So then you can't bid so your hands are going to be tight. And so what you have to realize is that if you do these basic steps, and you still need help, at the end, you may be able to call up Q M U L OS and they can

help you but it could be you know, this shelf is bare. There's no time that this is a bad bad situation to be in. But it's true,

24:56

right? So that's why we think about scalability right? How do you scale compliance. And typically, well, in the federal space, especially, especially federal contracting space, we throw bodies at it, right? That's how people traditionally do it. Those armies ISO sales, a lot of them are contractors, there's a nice fat margin on those. Right. So you know, the the big contracting firms out there, they're interested in continuing to perpetuate that model. And this is not to slag off on them, right. This is the model that's worked for years, we thought of it differently. We a lot of our folks came from the federal space. In fact, our company was founded by a federal executive who was at DHS when they were starting the CDM program. So we're very familiar with that space. When this Stan how the economics work, what we tried to do is be a little disruptive and actually quite disruptive. What we tried to think about is how do you scale compliance at the enterprise level, to any framework, any amount of data anytime, and really be proactive and predictive about any any mandates that come down the pike. So what I'd CMC 2.0 is something else that emerges out of the executive order 1402, eight, you're always ready. Again, we're talking about compliance, agility, and compliance readiness, right? That being kind of proactive compliance, it's a novel idea, it's a novel term, the only way to do it is through automation, you can throw bodies at the problem, you can't hire fast enough, we still have 3.4 million cybersecurity jobs that are open. That's the latest study from ISC squared that just got published, we've got a lot of churn. Last year, we've hired somewhere around 470,000 new people into cybersecurity. And yet, we're still have more to hire. So that's problematic. So you can't teach people fast enough, you can't keep them there fast, you know, long enough. That's the other problem, you know, and I SSL will stay there, you know, a couple of three years, and then they go to that next job, they want to double their money and they can't write. So you have a lot of problems, thinking about it as just a manual solution, you have to do automation. How do you do automation? Well, you have to understand what automation means within this space. A lot of folks do what we call workflow automation. So you know, the ServiceNow is of this world, right? They They're experts at that. So they lean into those kinds of models, we think about as full lifecycle automation, how to actually automate your entire compliance lifecycle. But first, you have to understand what that means. So from the moment that piece of data becomes an indicator of that control status, right, when it fails, or it passes, and how that becomes an all the way that I traveled all the way down to that dashboard, it becomes that pixel where it turns green, yellow, red, or whatever, right? How do you map that chain? How do you understand that data flow that data architecture? And how do you ensure there's credibility across the way and so you try to minimize the amount of hands that touch that data, because you try to again, eliminate subjectivity. So you want objective, you want data, you want real time you want a continuous, and you want it so adaptable and agile, that you can comply with any framework. And anytime something else comes out that comes around the corner. So what we're ready for it because we understand how to monitor these controls. And it doesn't matter to what framework so you kind of flipping it around a little bit. Right? You talking about the data? First you talking about objective objective facts. First, you try to get away from while subjective opinion. I call it opinion farming at scale, most compliance programs are doing that they're just opinion farming at scale. And I don't care if you have 500, ISOs, 1000, ISOs, it doesn't matter, right? It's an infinite type problem, what we're trying to solve for his time, right? It's credibility. Absolutely. Well, so we're trying to solve for time, no matter how many people you have, you cannot look at those controls every day. You cannot look at them every minute. And you certainly can't

make those decisions consistently. You have posed that question to many folks in the federal space. I'll give you that same example, my client at the federal agency, when we started his doorway, and looked at that arm, yeah, why so so as I said, How do you know that they're making these decisions consistently, when he looks at that control on Monday, and he comes back three months later, he looks at that control on a Wednesday. And guess what, on Wednesday is a bad commute day for him. And he woke up on the wrong side of the bed. And that same control, you look at it hard enough, and maybe not passes, but it really should have failed. And so you have this false negative. Now you don't even know that you've got a problem. And you keep working like you don't, right? scale that out. extrapolate that out. Now you got that big problem at the enterprise grade. Now you don't know what your risk posture is. So this is what we're trying to solve for and shorten that cycle. know as soon as you can. Because guess what, the bad guys there? No, they know this now their operating environment right now.

28:59

People have listened my podcast in the past, I have a go to phrase my phrases. Show me the money, Tom Cruise, show me the money. And I'm trying to figure out the money on something like this. And I read different estimates and everything else. And we know FedRAMP is just you know, pick a number to three years for FedRAMP. But for some like this, I'm trying to get a level one number I'm trying to get like a level three number. I'm guessing maybe under $5,000 for level one, maybe 50,000 100,000 for level, but it varies from company to company. Are there any kind of horseshoes and hand grenades and estimates we can have here for compliance cost?

29:32

Well, they vary, right. So typically the estimate so the estimate is usually we do it as a percentage of revenue, right? So for of course, federal agencies that have revenue have budget to different story but for commercial environment, commercial enterprise, compliance costs are usually somewhere between three to 8% of their IT costs. And there it costs however, somewhere between three to 5% of their top line revenues. That's good. So guess what security is also about three to 8% of their IT budget, which is frightening given how much attention would pay Security, it's only three to 8%. Because they think of it as a technology acquisition problem, right? It's more of portfolio management, most security operations, actually portfolio management operations. But that's the time for another podcast, they will talk about them at different times. So when you look at compliance investments and the ROI, they can actually recognize that it is very hard to quantify because while compliance has never really been keeping people away from doing business, very rarely, and I've had those personal experience myself where I've tried to kind of ring the bell and sound that alarm and say, Look, if we're not compliant, we can't do business in this particular area, typically, in a very highly regulated industry, you know, health care, financial, you know, for instance, nydfs, you know, New York DFS rules, especially now with the new addition of corporate responsibility, personal accountability for executives, it's becoming the kind of that sense of urgency is there. But traditionally, compliance is kind of you can defer it, you can kind of negotiate it away, right. And so like, we'll get there, right, but at this point, it's not an option, you're gonna see people actually asked for compliance reports to be done earlier, for compliance assessments to be done early, you don't want those surprises, walking in the door with a great product and then being knocked out. So when I think it's going to start hitting people in the actual p&l, when they start suffering actual losses, when they start losing bids, for no other reason, than they can pass compliance, I think it's gonna wake a lot of people up. And

also what we're seeing is a case for convergence. And I'm a big proponent of convergence between compliance, security and risk management, a lot of those investments tend to be fairly similar. When we look at kind of investments, we're doing security space, what we want real time controls, we want real time preventive detective responsive controls. In compliance, we tend to think of it as a historical reporting function. If we converge that thing, you convert that mindset and say, Look, I demand my compliance to be real time as well. Right? Why should I accept three year old data? Why should accept three month old data, three day old data, I will data now Security wants it compliance shoot habit, if you think that way, you realize a lot of that data comes from the same controls, same kind of technology. So instead of investing separately into compliance, and separately into security, and separately into risk management, and governance, et cetera, you can actually converge on that. You can say, well, let's not look at it as a risk or governance or compliance platform. Let's look at it as how do we manage risk? How do we know what we know? Guess what, I have firewalls, I have DLP. I have antivirus and anti malware having to run somewhere. I have things in the perimeter, I have things that they actually have things in the cloud, I have things telling me things, I can just ask them in a different way. So it's about applying a different lens. So take your security investments, apply a compliance lens to them, and doing it real time. Now you've got extra ROI, you're leveraging out of your existing investments, enormous ROI. And by the way, now you can actually map it to maybe not proactively driving revenue, but you're certainly enabling revenue. And when you talk about cash flow velocity, which is another great business metric, right? How quickly can you close those deals, if you can demonstrate compliance very quickly. Now, that's a whole different problem, right? You are compliant. But to demonstrate that you are, you have to go through an assessment, you have to go through an outside audit, you have to pay somebody to do that. It might take months, what if you're compliant, and you can show at any given time, if you can show it on demand, it's a dashboard, it's a report, you hit the button, it's there. You show credibility, you show trustworthiness, you show maturity, it matters, right. And so if an auditor comes from your third party supplier, or you or your partner or your prospective client, they say show me that you are compliant, and you show them that's a different story that positions you differently. It shows you as a mature environment. And I think it positions your products and services in a better light because security is considered more and more as a dimension of the business, not a separate function. You know, I want to secure a product. I don't want a product with security bolted on it. Well, I

33:35
mean, we could probably due to our show just about acquisition and zoom saying this is a deep topic, but I think the walkway today is don't wait to the last minute Get started today because if it's the last minute bad things happen. You have been listening to the federal tech podcast with John Gilroy I'd like to thank my guests Igor Ivanovich, Vice President compliance strategy at cumulus.

33:54
Thanks for having me, John.

33:58
Thanks for listening to the federal tech podcast. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcasts.