# NICE Framework in Focus – Wintana Girma

**Marian Merritt,** lead for industry engagement, the National Initiative for Cybersecurity Education (NICE): As part of our series *Framework in Focus*, it is my pleasure to speak with Wintana Girma today. She is a Governance, Risk, and Compliance Analyst with Rush University Medical Center in Chicago. Hi Wintana Girma. It’s nice to speak with you and learn more about your career in cybersecurity and, in particular, how your role relates to the NICE Cybersecurity Workforce Framework.

**Wintana Girma**: It’s nice to speak with you, Marian. Like you said, I am a Governance, Risk, and Compliance (GRC) Analyst. My specialty area is third party risk management. I do vendor onboarding for the hospital and university as well as some GRC team metrics and reporting and other projects as needed. I work with the medical device security team, IoT team, as well as security awareness and training.

**Ms. Merritt**: That’s quite a portfolio you have in front of you. Who do you report to at Rush University Medical Center?

**Ms. Girma**: I report to a GOC director as well as to our CISO.

**Ms. Merritt**: How big is the overall cybersecurity team and what kind of roles do you find that you have in a training university and a medical center?

**Ms. Girma**: The team is about 25 people, split between operations under one director and GRC under another. My role is primarily in GRC, but I work with the whole team. The GRC side is about 11 people. We’ve got a 4-person IAM team; a policy and ERM integration analyst; a data flow analyst; a medical device engineer, as I mentioned before, who works closely with clinical engineering; two analysts – one for the database and myself; and also an attorney, who dual reports to us and legal.

**Ms. Merritt**: It sounds like a number of roles from the NICE Cybersecurity Workforce Framework have been represented right there. Would you say that is a typical size team in healthcare? How mature is your operation if you compare it to other organizations?

**Ms. Girma**: I would say we’re pretty firmly middle of the road. When I first started, I thought if felt very immature to me. Our CISO had just been brought on a couple years back and was building a team from scratch. He was pulling from the rest of IS to populate his team, but a lot of people had been doing security work, just not under a formal CISO and cybersecurity program. As I compared it to other similarly sized organizations around us – Loyola, Northwestern, the other hospital/university combos – I think we’re just about middle of the road in terms of maturity and size.

**Ms. Merritt**: We’ve talked about this. Your career pathway to your current role as a GRC analyst is not that typical. Perhaps you can share a little bit about how you got into this field.

**Ms. Girma**: I had already worked in healthcare for quite a while. I used to be a program manager for a surgery suite at a hospital in Boston, and so I had been working directly with clinicians in administrative and program planning role. I loved being in healthcare but wasn’t really married to that in terms of career progression. So when the opportunity came to move to Chicago, I knew that I wanted to look specifically at academic medical centers (AMCs) just because I really enjoy working with educators and feel that, personality-wise, it works well for me to learn from the people I’m working with. When I first came to Rush, I actually came in on a temporary contract role as the executive assistant to the CISO. He was just starting out and had only been here a few months and was starting to build his team. As his EA, I was working very closely with him on projects and contracts and helping him with scheduling interviews to build his team. As he was filling these roles, he found one that he thought would suit me. He moved me in as an analyst and taught me quite a lot at the beginning and then surrounded me with other teammates who would continue to teach me. That’s how I ended up originating third party risk management program lead role.

**Ms. Merritt**: That’s great. As you’ve been able to observe him build out this pretty robust team over the last few years, would you say that your colleagues have similar backgrounds, or do they come from more traditional cybersecurity pathways?

**Ms. Girma:** I would say it’s a pretty good mix. The first 10 or so employees that he brought in probably all came in with computer science degrees and had already had a professional interest in cybersecurity and maybe had moved up the ranks from help desks, which is typical, I think, for most security engineers. The newer additions have all come in from disparate places. He got his med device engineer from a clinical engineering team. He brought in a lawyer to work with us on policies and things because we work so closely with legal in putting cybersecurity contracts and information into agreements at the onset. I think he was very strategic about bringing in the right mix of skill and personality. The personalities hired came from all sorts of backgrounds.

**Ms. Merritt**: He sounds like an individual with a well-honed sense of aptitude and attitude in terms of identifying talent.

**Ms. Girma**: Agreed. Absolutely.

**Ms. Merritt**: Have you had a chance to look at the NICE Cybersecurity Workforce Framework to see how well it describes work that you’re doing?

**Ms. Girma**: I did, yes, and I located one of the places where I would put myself. In the category of Securely Provision, I think part of my role at least would fall into the specialty area of risk management.

**Ms. Merritt**: I have to admit that when I was preparing for our talk, I used a tool over at the NICCS portal where you can just type in search terms. I typed words like *policy* and *vendor* because those came up in our conversation, and those led me to the area of Oversee and Govern. There are roles like cyber policy and strategy planners, and those also could describe some of your work roles.

**Ms. Girma:** Absolutely.

**Ms. Merritt:** Tell me how you envision how the NICE Framework could be used to guide your own personal career or maybe as a tool for your whole department.

**Ms. Girma**: I would say that personally it’s nice to see the specific tasks and skills that associate with different kinds of roles. It takes the guesswork out a bit about whether you’re qualified for something or what kind of training specifically you should target. Especially being a person who does a lot of self-directed learning – reading, watching videos – as opposed to formal training programs, it’s nice to be able to target my search in that way to learn about specific things. In terms of team-building – and that’s always something that we’re working on – it’s nice to see really targeted descriptions to make job descriptions. When we’re hiring for a role, it’s very easy to just think of the primary function that you want that role doing. But being able to put together a good mix of the skills and tasks that would relate to that role is just going to get you a much more targeted applicant and might decrease the hiring process by quite a lot in terms of time – not wasting your time and not wasting the applicant’s time when you’re looking for something really specific.

**Ms. Merritt**: Do you find that there are particular types of cybersecurity skills or jobs that are difficult for you to fill on your team?

**Ms. Girma**: I would actually say it’s easier to find talent who understand the technical aspects of the roles we’re trying to fill because it’s upfront on someone’s resume what technologies they’ve used before, what systems they’ve used, what technical training they’ve had, what programming languages they know and all of that. What’s more difficult is finding folks who understand the environment. Even if they’ve worked in healthcare before, academic medical centers are a whole different beast because we’ve got the healthcare aspect where we see patients; we’ve got the research aspect where there’s a lot of groundbreaking work going on using technologies that are new and emerging or maybe being built onsite; there’s also the university and all sorts of data implications for having students who live and work onsite on the network. I think one of the nice things is finding the right talent in terms of the technical skills that they need makes it easier to then pivot to looking at personality and culture match.

**Ms. Merritt:** You’re an example of somebody whose CISO spotted talent. You have different lived experiences and different education background, but you definitely didn’t have a cybersecurity degree. Is this part of a bigger trend, do you think?

**Ms. Girma**: I do see that, absolutely. It feels like the earlier additions to the team when it was first being built were people with the standard cybersecurity pedigrees. But now it seems to be moving toward degrees being on the nice-to-have list and being secondary to things like really targeted learning through certifications or actual work experience or transferrable skills. I think that learners are able to spot those transferrable skills and understand how they would relate. You could have an easier time bringing in good talent and differently thinking talent.

**Ms. Merritt:** You mentioned certifications. How have you been keeping your skills up or developing your skills?

**Ms. Girma**: I was actually really lucky to be able to attend a SANS course about a year ago. I did the 301 level, which is cybersecurity fundamentals, just to get myself up to speed on the network and cryptography and all that people who learn cybersecurity traditionally in school have the background in. It was a really good experience. It was a week-long intensive course. I think at the end of it, I was a little more comfortable with a lot of the terminology. That’s the one professional cert that I have. And then I’m always studying for others. I’ve got a ton of textbooks on my desk and whenever I have free time I look through them. I’ll continue to get professional certs because I think they’re a really good way to test my knowledge in certain areas that are related to my job.

**Ms. Merritt**: That’s great. When you look across the team of 25, how does it look from a diversity point of view?

**Ms. Girma:** I would say this is the most diverse team I’ve ever been on, and I don’t think necessarily think that was my CISO’s aim. I think it was really the way that he hires in that he’s looking for the culture match as opposed to the formal pedigree. I’ve never worked with people from so many countries, who speak so many languages. I’ve never worked with so many women, which I know is unusual in IT and especially in cybersecurity. It’s been really pleasantly surprising how diverse this team actually is, even with only 25 of us.

**Ms. Merritt**: What would you say you enjoy most about the work that you’re doing at Rush and any particular role?

**Ms. Girma**: I love my role because I get to see what’s being worked on before it’s announced to the hospital or the community at large. In my function of third-party risk management, we sit within legal and we’re part of the contract review process. When someone wants to bring in a new vendor, they get vetted by my team first. We look at architecture, security controls, and all of that before contracts are signed. Sometimes we’re involved earlier like with the RFP and the procurement side of things too. I get to see the cool things that our researchers and our physicians and even the university are working on before they become public knowledge, and I always find that really exciting. We’ve got this huge new cancer center being built, and the kind of work that they’re doing and the way that they’re revolutionizing virtual visits for cancer patients. It’s very cool to be in the room discussing how they’re going to make things work before they become public knowledge. I think that’s really fun.

**Ms. Merritt**: I think that does sound very rewarding. Your enthusiasm is contagious. It makes me want to be part of that too. If you could give advice to somebody starting out or somebody even just thinking about a cybersecurity as a potential career, do you have any advice to give someone?

**Ms. Girma:** I would say the most important advice that was given to me was not to be intimidated. It’s really difficult, I think, especially in IT if you don’t have the same training or background. You could be put off by all the acronyms, and it really just sounds like a foreign language sometimes when two people are having a work-related conversation around you if you’re not fully involved in what they’re doing. But I learned the most from listening. Just being in a room with engineers who would talk over my head, sometimes I would just stop doing what I was doing and listen to their conversations, and I learned a lot. A lot of that has been lost now that we’re all working from home. But what has been cool for me – and I wish I had done this before I even joined Rush just to have some lean-in background -- social media and conferences are also a great way to see and hear the conversations that are happening without having to participate at first. You can just be quiet and read the conversations and you end up getting a lot more out of them than you think. I think that’s been really cool for non-technical, non-textbook learning.

**Ms. Merritt**: That sounds like really good advice. As we wrap things up here, is there something you want to add that I didn’t ask you about or closing thoughts that you’d like to share?

**Ms. Girma**: I think one of the cool things in terms of the diversity of the workforce is that managers who have been more focused on bringing in people who are going to be a good culture fit and understanding that most of the training happens on the job – which you have to do anyway, right, like you might be doing the same kinds of work but using a different technology or vendor. Bringing people in who have the exact keyword matches on their resume may be fine. But if you’re willing to teach someone who may not have that technical background but has the enthusiasm and ability to self-study and the hunger to learn more – I think that’s how these really interesting and diverse workforces are built. I’m finding that we are all really benefitting from it, especially the diversity of thought in our group. We’re all so different that conversations in which things happen or decisions get made are just very interesting because everyone’s bringing up things that everyone else wouldn’t necessarily have thought of because they’re not coming from the same place.

**Ms. Merritt:** That’s terrific. Thank you.