Transcript

Hi, my name is Allen Keele. I'm a Principal with Certified Information Security and today I would like to bust a myth that the Board and C-Suite have no role in cybersecurity, at least that's what I seem to run into an awfully lot.

So the reality is that cyber risk is pervasive throughout the enterprise. Wherever Internet technology exists, not just in the server room, meaning that operations, technology, and Internet of Things, any device that we use within our organization that has Internet connectivity in some way is essentially a cyber risk entry point. So expecting that a small IT or Infosec team can manage something as important and complex as cybersecurity on their own is not only unrealistic, it's just flat out dangerous, and it doesn't conform to cybersecurity framework 2.0 by NIST, which is another problem when. We have people that are assigned the role and the job to set up and manage NIST CSF 2.0 as a cybersecurity framework. But they don't have the authority to actually assign the roles and responsibilities. They don't have the authority to provision the resources for the cyber security that is recommended in this CSF 2.0. So in other words, they can't even get the program properly started without participation and input. And decisions from executive management at board at C-Suite. Cool. So in this short video, I'm going to show you some of the tasks that NIST CSF requires to be completed by the board and C-Suite before the cybersecurity program can be designed and operated to manage cybersecurity risk throughout the organization as part. Of its overall enterprise risk management, not separate from. So that's right. Top management's failure to properly initiate the strategy, scope, roles and responsibilities and ongoing oversight completely bottlenecks setting up a proper cybersecurity program fit for purpose to the organization's unique needs. And the new NIST Cybersecurity Framework 2.0, released on February 26, 2024, makes this clearer than ever.

So how so? Well, the previous NIST CSF 1.1 really addressed the process of cyber security risk management, the risk identification and assessment mitigation, incident detection response and recovery in the five functions called identify, protect, detect, respond and recover. However, NIST CSF 2.0 that was just released realized that all those CSF 1.1 addressed the process of risk management and had not done a very good job of establishing the actual risk managing program for cyber risk. To design, operate and oversee cybersecurity risk assessments as part of the organization's overall enterprise risk management. So as with proper enterprise risk management, the new NIST cybersecurity framework now begins with a function devoted to establishing cybersecurity governance to initiate, manage, oversee the cybersecurity programs, risk assessment process of assessing, managing, responding to. And recovering from cyber risk. So establishing A cybersecurity program in an organization begins with active participation from the board and executive leadership in the C-Suite to create the strategic goals and objectives for cyber risk management, as well as then scoping the program and assigning roles and responsibilities. Appropriately, after all, it's hard for me in the cybersecurity function within an organization to

assign roles to the Board of Directors and to the C-Suite, as is required by NIST CSF 2.0.

Hold on, I'll show you. So let's go ahead and take a look at the new CSF 2.0 reference tool. NIST is made available online so I can show you the kinds of activities that NIST CSF 2.0 recommends to be performed prior to actual cybersecurity risk assessments controls implementation and even incident response and recovery. OK, so this is the roles, responsibilities Excel template that I created for assigning roles responsibilities throughout the organization using the racy. Little. Now obviously we don't have time to go through all of that because after all, it turns out that we have 367 recommended tasks. That are actually allocated across. 103. Desired outcomes throughout the six functions. OK, so just like we were able to expand these desired outcomes into. Further tasks I've done the same thing in this, but again it has the additional benefit of being able to assign these across the positions you see in the blue bar from the senior most board of Directors, Strategic Committee and Chief Executive Officer, Chief Operations Officer, Chief Financial Officer, Chief Risk and Compliance Officer. Chief Information Officer, Chief Technology Officer, all of these senior folks until finally we get to the necessary tasks for compliance managers, the information security manager, the OT security manager, the Data Protection Officer. The business continuity coordinator, the HR Manager, communications director or manager, the IT director or manager, facilities managers, and then finally there are cyber security tasks that need to be assigned to the risk owners. The department heads the business process risk owners. That's right, this is going to be integrated along with other operational risk management. In the enterprise risk management program. Perhaps driven by ISO 31,000? So which I also teach, we go on and look at again this is we have roles, responsibilities that of course need to be assigned to specialty risk assessors, auditors, customer relations managers, supply chain manager as well as employee staff and even there are tasks that are assigned to the external suppliers and vendors. Because we have a whole category of desired outcomes within governance devoted to. Well, managing cybersecurity supply chain risk. Wow. All right, so again, don't have time to go through all of this. This is an awful lot of information. But again, just to show you how this needs to be properly allocated. Is beyond the authority of someone that is actually seated in Cybersecurity. We don't have the authority from cybersecurity to assign these roles and responsibilities, so again, taking a look at that GV.RR-01, that we see again in the RACI model, the group that is actually accountable for senior leaders agreeing upon roles, responsibilities well, the only boss of them is the board of directors. They're the ones who are accountable and then we have the responsible parties, these directors and senior leaders. Such as the CEO, CEO. Perhaps the chief risk and Compliance Officer, CIO, CTO again, how is someone from? Some. Cybersecurity information security to assign these people those roles. I just don't see how that could happen. So to sum things up, that board and C-Suite play a critical role in initiating, operating and managing cybersecurity risk throughout the organization. And the NIST Cybersecurity Framework 2.0. Introduces a new component devoted to establishing cybersecurity governance up front, which requires upfront active participation from the board and executive leadership in the C-Suite to create the strategic goals and objectives for cyber risk management.

I'm Allen Keele. Thanks for joining me.