

## **ERM VIDEO INSIGHTS**

### **Transcript of Rick Moyer and Don Pagach**

#### ***Integrating ERM, Compliance, and Audit to Provide a Comprehensive View***

**Don:** Hi, I'm Don Pagach. I'm the Director of Research for the Enterprise Risk Management Initiative here at NC State. And it's my pleasure today to welcome Rick Moyer, who is the Chief Risk Officer at Stanford University. Rick, thank you for joining us today.

**Rick:** Don, I'm glad to be here.

**Don:** Maybe you can just start off by telling us a little bit, many people just probably think it's Stanford University, as just the university. What do you all oversee at Stanford?

**Rick:** Yeah, so Stanford is a large complex enterprise in addition to being a large university. We have a health system, that includes three hospitals, physician networks, the school of medicine, which is part of the university. We have a department of energy laboratory, SLACK, and we have a large management company that manages our endowment. So it's a very diverse set of operations that we provide risk oversight for.

**Don:** So when there's so many diverse elements of risk, you have student housing, you have athletics, you have the medical school and all the different things that happen there, and then you have compliance with endowments. What's the benefit of having all those under one leadership structure for risk management?

**Rick:** Yeah, so maybe I could start by telling you the functions that I'm responsible for. I think it's a bit unique in a chief risk officer operation. I actually have six functions. I started at Stanford as the chief audit executive, so internal audit reports to me, I now have a chief audit executive who reports to me. I have an ethics and compliance function. I have the enterprise risk management function. I have risk management insurance function. I have information privacy and then also, information security. Now information security is actually the one that's unique in that, that function reports to me and the chief information officer. The others all report to me alone. For internal audit we provide that service to all those Stanford entities. For enterprise risk management, which I think we are primarily interested in today, I serve as the chief risk officer for the university but I'm in a leadership role supporting all the other Stanford entities in my risk role.

**Don:** So I know that in our past discussions, at Stanford you have an integrative review of functions to help the better understand their risks. Can you touch a little bit on the integrative review process?

**Rick:** This is a process we implemented, Don, about three years ago. As I looked at these various functions, which, you know the reason we pulled them all together is they really all have a risk-based focus, they also all closely align with our board and our senior leadership oversight. So the integrative review report approach, the idea is to pull together these various functions and rather than doing separate assessments, reviews, activities in each of these areas is to try to pull them together whenever possible to have a more integrated, holistic approach, looking at risk. And my real focus is to try to be efficient in our support of our leadership in our organization and to the board. So we can bring one more comprehensive look at risk than if we did all these reviews separately.

**Don:** Okay, so you do both internal audit and ERM and sometimes those don't always go together in terms of what their end goal is. How do you manage the boundaries between two items like that?

**Rick:** yeah I get asked that question occasionally, but you know, what's interesting, Don, is I've actually never been asked that question by the board and I've never been asked that question by our leadership. So what I have though, I think it's important to point out is each of those six areas has a senior leader that leads those areas. And I make sure that each of those six leaders has direct access to the board and makes direct presentations to the board about their respective areas. So for example, the chief audit executive at every board meeting, makes a presentation. In enterprise risk, either I or my director report in that area gives a report, my privacy officer, my information security officers, my insurance leader, all of these folks, my chief ethics and compliance officer, they have a chance to report directly to the board. The other thing we've done; is we've had independent reviews periodically of our functions. So in the internal audit space we are required to have a quality assessment review every five years, which we do, but in addition to that, I've asked when we do those reviews for them to look at our other activities. So in the last review they looked in enterprise risk management, they looked at ethics and compliance and they gave us an assessment of those areas. And so there's a number of things we do to make sure that these functions have independence and objectivity but at the same time we are trying to coordinate the activities to be more efficient and provide a more holistic view to the organization.

**Don:** has this been some sort of process under your leadership? Do you think that there is anything that you can give to the viewers that would say, this is one thing that has really helped as I've gone through this process?

**Rick:** well, you know, first of all it's been an evolution. So I started at Stanford twelve years ago, as the chief audit executive and the chief ethics and compliance officer. These other functions have been added over time. You know first of all, I'd say they don't have to all be under one leader to be effective, but I think the message that we could give to everybody is, these functions, I believe, will be more effective if they are effectively coordinated. So whether they're under one leader or not, I think it's the idea of coordinating the activities, to give again, that more complete view of risk to the board, and to senior leaders. Stanford, we talked in the beginning about the complexity of the organization. We actually have many boards we report to. So there's a board for the university, the board of trustees. We have three hospitals; each has a separate board of directors. We have physician networks that have separate boards. SLACK or department of energy operation has a separate board, and the management company has a separate board. So we do lots of reporting to lots of different boards. And I think it's another reason it makes sense to coordinate these activities.

**Don:** I appreciate you've been able to find time to speak with us, and this has been great. Really good knowledge about the process that you've gone through. Thank you again.

**Rick:** Thanks Don.