Q&A

Karen Hardy, Founding Member, the Association for Federal Enterprise Risk Management and Board Vice President.

ERM AT THE FEDERAL LEVEL

By Russ Banham

RIMS

There's no bureaucracy like government bureaucracy, making the U.S. agencies ripe for a centralized approach to risk management. When Karen Hardy began her work in the government space in 2005, she began with a clean slate approach, given the immensity of the task ahead.

Not only did Hardy need to integrate ERM into one of the agency's strategic decision-making processes, day-to-day operations and budget cycle, she was responsible for creating and overseeing the implementation of ERM frameworks across 29 bureaus, including the National Cancer Institute—to scratch the surface.

RIMS sat down recently with Hardy to discuss her general observations for implementing ERM in large government organizations. She is the author of the Award-winning seminal book, "Enterprise Risk Management: A Guide for Government Professionals," (John Wiley & Sons 2014), and holds a MBA and a Doctor of Education degree (from Nova Southeastern University in Florida).

RIMS: Thanks so much for taking the time to chat with us this afternoon. As challenging as ERM projects are and remains, it appears your earlier ERM work with the NIH was equally demanding, given the 27 institutes and centers under its purview, comprising some 18,000 employees in all.

Hardy: Yes, it would seem I take on the tough jobs, but I have to say I've always enjoyed a challenge.

RIMS: How did you end up at NIH, given your background in education?

Hardy: Actually my undergraduate work was in journalism and communications, which helped me with everything that followed. One of the benefits of having studied communications is that it gives you the uncanny ability to interpret many things with ease. That has come in handy in the field of risk management because though it is technical, the edge is being able to convey it in a manner that makes sense to everyone. After previously working at Citi and eventually completing my MBA, over time I heard that the NIH was looking to get out more in front of issues and do things in a bigger way. While at NIH, I made contact with one of the NIH directors who headed up internal controls at Office of the Director (OD). I stayed in touch with him and when a position opened at NIH OD in risk management in 2005, I applied and got the job. What interested me was that risk management was moving toward enterprise risk management, and I'm the type of person who likes to get ahead of the next big movement. I basically had a blank sheet of paper to design it from the ground up.

RIMS: That sounds both exciting and scary. What gave you the courage to start filling in that blank sheet?

Hardy: I started doing research into ERM to learn all about it. At the time, there was no ISO 31000, which didn't come about until 2009 (at present, ISO 31000 is an internationally accepted standard for the management of risk in 57 countries). And then in 2008, I met Carol Fox from RIMS. (Fox was then-chair of RIMS' standards and practices committee and is today RIMS vice president of strategic initiatives). I just picked up the phone as a total stranger and asked Carol about ISO 31000, what it was and would it be useful to my work at NIH. She was so gracious and helpful.

RIMS: How did Ms. Fox assist you?

Hardy: She invited me to be a part of RIMS' efforts on behalf of ISO 31000. I accepted and joined the Technical Advisory Group looking at the first draft of the standard. I also attended various summits on the subject and was involved in developing a seminal survey (on ISO 31000). I suggested to RIMS to consider including feedback from government practitioners of risk management because often the public sector is not at the table during these policy developments. This makes it hard to implement, especially if your industry's perspective is not part of the conversation. So, I was able to share the survey with the right people. Ultimately, we were able to include ISO 31000 language in the policies of the OMB (Office of Management and Budget), the largest office within the Executive Office of the President.

RIMS: Well done! What happened afterwards?

Hardy: What happened is that a director at my current agency came across the survey and called me. He told me they'd been thinking about ERM at the department and that two of their larger bureaus had it on their radar. He asked me for a briefing on what I was doing at NIH. I went over there and next thing I knew, he'd created the position of Deputy Director for Risk Management and asked me to apply for it. I said I was interested, but there were three obstacles. One was that I would need to establish that I was not a "shadow" auditor. The second was that they needed to understand that "risk" was not a bad word. And the third was to accept that project risk management was not ERM.

RIMS: So he agreed?

Hardy: Yes, and I took on the position. I was charged with creating this broad ERM implementation just as the Obama Administration was getting its footing. I had a whole list of priorities, but at the same time I realized the sheer massiveness of an ERM implementation in an organization with so many moving parts. I needed to scale down my ambitions to make things more manageable.

RIMS: What did this entail?

Hardy: I decided to create engagement first, reaching out to the bureaus and their program managers and division leads to introduce them to the concept of ERM. I wanted to get them involved in active learning—to understand this is something that would help them do what they already did, only better.

RIMS: After you cultivated these relationships, did you then create the ERM framework?

Hardy: I had an outside contractor working with me at the time who added his expertise in COSO (one of the most widely recognized and applied risk management frameworks) to my knowledge of ISO 31000, and we came up with our own framework. We then introduced it to the division heads as the principles and the tools of ERM. But, I want to emphasize that what was most important was the fact that we had developed a rapport first. That was the foundational strength of our success.

RIMS: What did you talk about in these conversations?

Hardy: I'd ask things like what makes your business tick, what makes it a success, what are your concerns, and what are you afraid might happen in the future—questions like that. I didn't even use the word "risk" in these early conversations. I just tried to engage them. It's my belief that's how you earn people's trust. In the back of my mind, I knew what I needed from them, but I wanted them to feel ownership in our journey. It's the human factors that make a project a success.

RIMS: Is there a milestone during this journey that stands out as particularly successful?

Hardy: One that comes to mind immediately was the establishment of our enterprise risk policy, which required significant consensus building. We had to identify various stakeholders across the multiple bureaus to come to an agreement on the risk policy. There were some things we felt were absolutely critical and others we were willing to trade off. For example, we believed it was crucial for each bureau to develop a risk inventory that was frequently updated to make it dynamic and not static. And we wanted risk to be incorporated in all their decision-making conversations and part of their management teams' agenda.

RIMS: Any other "must-haves?"

Hardy: Yes, we had developed a risk maturity assessment tool—basically a survey of about 80 questions across five attributes of risk—we wanted them to respond to on a regular basis. We'd benchmarked the tool against a variety of different industries and organizations like the State of Washington Risk Management office, and then tailored it to our needs. Similarly, the categories were broad—covering executive leadership, integrating ERM into the bureau's culture, applying ERM principles, the fundamentals of risk management, and integrating ERM into strategic operations. But, the questions within each category were specific. For example, under the "fundamentals of risk management," one question was "Are high severity risks being tested using risk-based controls?" The respondent checked "yes" or "no" and then provided the reason and corresponding evidence. The survey responses are then rolled up to my team for comparison with prior years' surveys and possible action.

RIMS: Any other milestones you'd like to touch on?

Hardy: One is the establishment of our ERM Council. Because of resource constraints, I decided to duplicate myself at each of the units. I made it a requirement that each unit have a risk management officer, headed up by a facilitator championing ERM expectations in that organization.

RIMS: What's coming down the line for ERM in Government?

Hardy: Honestly, just rinse and repeat. The key is to get to sustainability—where you have the full commitment and resources to do what we've been doing, embedded it in business operations' decision-making so it doesn't make a difference whose running these organizations in the future. ERM will simply be a part of the culture.

RIMS: Are you pleased to have accomplished so much in such a short time?

Hardy: Honestly, seven years ago, people saw me coming and ran in the other direction. Fast. Today, they're all open arms. They look forward to discussing their efforts and are eager to offer up different perspectives. I love diversity of thought, as I truly believe it results in more and better ideas. But, I'd be fooling myself if I didn't say there are some frustrations across the board in government. Sometimes, things do not move fast enough. But, we are all very tenacious and committed. ■