Q&A

Dr. Lianne Appelt, Director of Risk Management, Oracle Cloud Infrastructure

BENEFITS OF A CLEAN SLATE APPROACH TO ERM

By Russ Banham

RIMS

Oracle Cloud Infrastructure is a set of complementary cloud services provided by tech pioneer Oracle that enables a company to build and run a wide range of applications and services in a hosted environment. The infrastructure-as-a-service (IaaS) offering gives businesses the opportunity to migrate their traditional mission-critical applications to the cloud, instead of maintaining them in on-premises servers, as well as build new native cloud applications.

Lianne Appelt started at Oracle in 2015 as the director of enterprise risk management for its public cloud operations. She built the ERM program from the ground up, establishing standards and operating procedures, developing risk and reporting methodologies and recruiting a team to perform operational risk assessments. In April 2017, Appelt migrated to the new Oracle Cloud Infrastructure organization as first director of risk management. She brings years of experience in project management and governance, risk and compliance (GRC) to her new job, in addition to a doctoral degree in information and interaction design (from the University of Baltimore). RIMS sat down recently with Appelt to discuss her approach in creating an ERM program from scratch.

RIMS: What was the mandate before you when you joined Oracle's public cloud operations in 2015?

Appelt: We needed to get our ISO 27001 certification and to do that you need to have a risk management program, which we didn't really have at the time. I came in under a small GRC team to build the program to obtain the certification (ISO 27001 is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes).

RIMS: How did you proceed in building the ERM program to acquire the certification?

Appelt: I asked for guidance from Oracle headquarters, and was given the name of a gentleman from our global information security team. He gave me the corporate risk management policy on our information assets, which was similar to OCTAVE Allegro (a methodology to optimize the assessment of information security risks). It was useful, but not what I would call ERM. A few months later, he left Oracle and I was essentially on my own, with a clean slate to build an ERM process from scratch.

RIMS: What was the first order of the day?

Appelt: Previously, the focus was on passing the compliance and audit requirements, which resulted in sort of a piecemeal approach to risk management. I wanted to provide uniformity to the process. So step number one was to create a risk management standard that included things like how we identified, perceived and treated risks. Eventually, I brought in two people to assist me, and then this new baby came along.

RIMS: By "new baby," you mean the new position with Oracle Cloud Infrastructure?

Appelt: Yes, it was a golden project founded by a small group of ex-Amazon folks wanting to put together an IaaS cloud product that would compete with Amazon Web Services. They called themselves the "bare metal group" and had been working on it in a lab setting for quite a while to see if it would take off. The product launched with a very aggressive pricing model that made us very competitive. It turned out to be a great idea for a startup, going from a handful of people to about 6,000 today—in just two and one-half years. Basically, I was recruited to do the same thing I had done in our public cloud group.

RIMS: Two fast-track major projects in two years is a lot to ask of a person. How did you jump from one ERM project to another?

Appelt: Well, the first thing I needed to do was to get to know the environment. As before, there were all the compliance and audit requirements, but nothing in the way of a formal enterprise risk management program. They asked me if I could do what I had done previously and I said yes. I eventually brought my team over to the new business, after they had trained people to replace them at Oracle public cloud. Once they moved over, I hired some additional people. We needed to learn how this new environment was different to modify the ERM program accordingly. In both cases, we have sort of a hybrid ERM program that includes traditional risk management, most of it information security-related, and compliance. I've been trying to socialize the idea of more strategic risk management. One of the first exercises I did with my team was to identify our top five risks globally, and then determine if these risks resonated with our leadership team.

RIMS: Can you tell us what these risks were?

Appelt: We had a lot of discussion about them, but eventually narrowed the list down to reputation/customer confidence, legal and regulatory compliance, finance, technology, security, and health and safety. We were effectively a startup looking to acquire customers, and that was leadership's primary concern which made great sense. The responsibility for this fell primarily to marketing and sales teams. We were entrusted with assisting our information security team to identify and manage technology risks, and with helping the compliance team address regulatory risks. We also work closely with the business units to provide operational, service-specific and data center risk assessments.

RIMS: What does this latter work entail?

Appelt: We perform a combination of questionnaires and interview-based assessments to understand the functional objectives of each service, team and sub-team, and then do a pretty deep dive into the risks associated with achieving those functional objectives. The business unit SMEs (subject matter experts) now have an avenue to report on risks they see in their respective areas, making our services quite valuable. We offer an outlet for team members at every level to communicate and report concerns they have and to surface the issues that keep them up at night. In a way, we're like their therapists.

RIMS: What a great analogy.

Appelt: Honestly, it often feels like that's part of our role. Afterwards, we put together and provide them a completed risk assessment documenting the risks. This gives them some ammunition to request additional funding for tooling or additional headcount. In turn, this helps us cultivate a strong relationship with the SMEs—to our mutual benefit.

RIMS: What happens to the risk assessments after you present them to the SMEs?

Appelt: We work with the SMEs to track the risks and help them develop mitigation plans. We also share the assessments with their managers, who roll up all the risks from the varied teams under their supervision to senior leaders. Other managers do the same. This way there is a comprehensive view of all the operational risks to the organization. My hope is to eventually report on strategic and other risks, as well. I want to see the whole picture and senior leaders need to see it too.

RIMS: Is this in the works?

Appelt: I haven't bridged that gap yet, but let's just say it is my cause *célèbre*. At this stage of maturity in the organization, the focus is on keeping things simple and nailing the basics. My hope is that as we evolve, the value of more strategic risk management becomes evident and we are then able to expand our scope to become a truly enterprise risk program. ■