(DONE) Who Owns What? Clarifying Identity and Access Management Roles in Cloud ERP

[00:00:00]

[00:00:00] **Aditya:** The future of ERP cybersecurity is identity first and zero trust. AI will drive real time threat detection, dynamic policy enforcement, and security orchestration across the ERP landscape.

[00:00:15] **Richard:** Welcome to the future of ERP, a podcast where we discuss hot topics, best practices, and the latest innovations in today's global business. I'm Richard Howells and I'm joined by my wonderful co-host, Oyku.

[00:00:28] **Oyku:** Hello everyone. I'm Oyku Ilgar, a marketer, blogger, and podcaster in the ERP and supply chain area at SAP. In this week's episode, we chat with A ditya Thakurdesai from Infosys about cloud security and the evolving role of identity and access management. In other words, I am. Hi, Aditya, great to have you here. Could you briefly introduce yourself and your role at Infosys?

[00:00:51] **Aditya:** Thanks, Richard and Oyku, and hi everyone. Thrilled to be here. They say that in the cloud, ownership can get foggy, so let's clear the air [00:01:00] together. I'm a Kuai director at Infosys. I spent nearly two decades in identity and access management, watching security evolve from backroom concern to a boardroom imperative. At Infosys, I lead SAP Risk Management Practice for manufacturing, media and Technology. And I also head Transformation Center of Excellence, where we drive automation, innovation, and increasingly AI led security. My current focus is on Agent TKI, and I'm excited about how it's making ERP security not just smarter, but truly intelligent. Who owns what? Because as organization move to cloud ERP. Clarity in roles and responsibility isn't just important. It's non-negotiable.

[00:01:44] **Richard:** It's great to have you on. Let's start with hopefully an easy question and just to get, set a level playing ground for everybody listening to the podcast, what is Identity and Access Management? And from now on I will use the acronym IAM [00:02:00] to describe it. So what is IAM and what and why should businesses know about it?

[00:02:06] **Aditya:** Identity and access management, or IAM is how a company controls who gets access to what in its digital world. Think of it like running an office. You wouldn't give every employee a master key. HR gets access to personal files, finance to accounts, and vendors only to the delivery area. Everyone can do their job. No one can walk into the wrong room. Businesses need to understand IAM because every digital transaction depends on trust. If access is too open, you risk data leaks, fraud, and fines. If it's too restricted, operations, slow down. I am strikes that balance keeping systems secure while allowing people to work efficiently. In simple terms, identity isn't just about security. It's the operating model that lets businesses run safely and at speed.

[00:02:59] **Oyku:** [00:03:00] Why is it important to understand who owns what when it comes to identity and access management strategies in Cloud ERP?

[00:03:09] **Aditya:** Today's ERP world is complex, multiple clouds, hybrid systems, and many teams all connecting to same apps. And this very complexity is the enemy of security. It's what allows ownership to blur and risk to slip through. Many thing that moving to the cloud means vendor does it all wrong. Providers like SAP, secure the underlying infrastructure and provide an IM framework and tools. But customers are responsible for setting up user roles, defining who can access what, and ensuring ongoing compliance. This shared responsibility isn't a hover, it's a handshake. Clear ownership mix. I am a governance enabler, not just a technical control. While infrastructure and services may be managed [00:04:00] externally, the responsibility for access decisions and security governance remains firmly with the organization. Simply put in the cloud, you don't give away responsibility. You share it. Knowing exactly who owns what in IAM is what keeps your business safe and audit ready.

[00:04:19] **Oyku:** Mm-hmm. This shared responsible model is not just about splitting the work, it really shifts how customers need to think about managing access, permissions and security on a daily basis. So how exactly does this shared responsibility model affect the way customers approach their daily activities?

[00:04:40] **Aditya:** Under the shared responsibility model, the provider secures cloud infrastructure, data centers, network virtualization. While customers are responsible for what happens inside the cloud, their data access controls and configurations in day-to-day identity and access management, that changes [00:05:00] everything. Customers no longer manage physical servers or network firewalls. Instead, they focus on defining who can access what. Enforcing multifactor authentication, rotating credentials, and applying principle of list

coverage becomes central task. These are no longer optional. They are the front line of security. Think of it like renting an apartment. The cloud provider is the landlord maintaining building doors and fire alarms, but you still lock the doors and decide who gets a key. Shared responsibility doesn't reduce IAM it reshapes it. The customer's job shifts from securing machine to securing identities.

[00:05:44] **Richard:** You obviously speak to many customers. What are you seeing as the common challenges that customers are facing and how does it change company from company about how they drive the [00:06:00] decisions?

[00:06:00] **Aditya:** Most customers I speak with have a clear goal. To secure their systems without slowing down the business. But part to that goal is anything but straightforward. One of the biggest challenge I see is roll sprawl. Over time user roles multiply. Some are outdated, some grant excessive access, and many lack clear ownership. It's like handing out spare keys without keeping a log. Eventually, you are not sure who can open which door and why. Then there is what I call audit anxiety. During compliance reviews, organizations struggle to answer basic questions, who access what, when, and why? The data exists, but it's scattered across systems and stitching it together becomes a time consuming puzzle. And when companies move to cloud ERP, the issues tend to surface even more. Many assume their [00:07:00] on-premise I practices will carry over, but they don't. It's like switching from driving a car to flying a plane. The destination might be the same, but the controls, risks and responsibilities are entirely different. What's driving decision today is the realization that I am isn't just about locking things down. It's about enabling clarity, control, and confidence. When customers truly understand who owns what, they're not just safer, they're smarter, faster, and more compliant.

[00:07:31] **Richard:** I have a follow question if you don't mind. It was really interesting you mentioned that concept of role sprawl . It's just as important to keep up to date with who's doing what at all times and revoking authority in some cases, if people are no longer responsible for that particular function, so that they only have access to what they need for their given job at a given time, would that be a true statement?

[00:07:56] **Aditya:** Absolutely. And. It's not just about [00:08:00] access, because this roll sprawl not only affects your maintenance, it means additional access risk, and more importantly, in the new context, it impacts your licensing. You possibly end up paying far more than what you had expected.

[00:08:15] **Richard:** That's probably very much like what it's like at my house with the monthly bills for subscriptions. Be using certain things, but I'm still paying for it.

[00:08:25] **Aditya:** Yes, indeed.

[00:08:27] **Oyku:** And do we have any cases that you can share with us that demonstrates how security model has helped customers?

[00:08:33] **Aditya:** Yes, and what I love about this shared responsibility model is that it helps every customer in slightly different way, depending on what matters most to them, security, agility, or efficiency. Let me share two quick stories. The first is a global pharmaceutical company running its R&D and supply chain on SAP's Cloud. They work with external research partners across continents. [00:09:00] So data protection is absolutely critical. The shared responsibility model helped them draw a clean line. SAP took care of deep level cloud security, the infrastructure, encryption, and compliance framework. While the company focused on managing who gets access to what, using SAP's identity tools. That Clarity gave them the confidence to collaborate globally without losing control of sensitive data. Access for outside researchers became secure, time-bound and fully auditable the result. Faster innovation cycle, fewer compliance worries, and complete peace of mind. The second story is quite different. A large supply chain using SAP SuccessFactor in Ariba Cloud. The pain point wasn't research security, it was speed. They hired thousands of seasonal employees and manual user setup was hitting up days. Here, the shared responsibility model helped by letting SAP handle [00:10:00] the infrastructure level security, while the customer focused on automating access management through SAP's IM services. What used to take days now takes minutes with accurate compliant access every time. So whether it's a pharma company protecting data or retailer streamlining operation, the shared responsibility model helps in different ways, but always deliver the same core benefit, clarity, confidence, and control.

[00:10:27] **Richard:** That's two great examples of trying to solve that security issue for completely different purposes. But you can see how that would translate into many industries, many companies, many different companies, lots of companies have seasonal workers have, different times of the year have to bring people in to do different services. So, thanks for those great examples. We've long way through this podcast, and we haven't mentioned the AI word or not in any detail at least.

[00:10:56] **Aditya:** Absolutely.

[00:10:57] **Richard:** Technology can be both a great [00:11:00] benefit when we talk about security, but also a risk. So how is AI transforming business processes across all industries? The roles and responsibilities are evolving and the use of AI for both good and bad is increasing. Is that the same when we talk about IAM?

[00:11:18] **Aditya:** Great question. Richard. AI is transforming identity and access management, just like it's reshaping every other part of business. Everyday security task. Reviewing access records, spotting unusual logins or handling user queries are now getting an intelligent boost from AI in SAP's ecosystem. Cloud identity services are moving from automation to adaptive intelligence, learning from user behavior, predicting risk, and suggesting smarter role design. AI is also becoming an assistant instead of end users waiting for IM teams. For simple access questions, conversational tools within SAP can now respond [00:12:00] instantly. Saving time and effort. And with GRC 4 HANA 2026, AI driven analytics will soon detect access conflicts and anomalies long before audits. Two. This shifts freeze. IM teams to focus on strategy, managing risk, strengthening compliance, and aligning access with business goals. But as you said. AI is double-edged sword. It makes IAM faster and smarter. Yet it also introduces new risk like AI powered phishing or automation errors that grants wrong access. So IAM roles are evolving. It's now about governing this systems using ai, ensuring intelligent oversight, ethical use, and security across both automated and traditional processes. The modern Im professional needs to pair deep identity expertise with new skills in ai governance, analytics, and cybersecurity to stay [00:13:00] ahead.

[00:13:00] **Richard:** We are coming to the end of the podcast and we do ask all of our guests the same question, so hopefully you're prepared for this one. So, in a sentence or two, what's the future of ERP from a cybersecurity perspective or risk perspective?

[00:13:16] **Aditya:** The future of ERP cybersecurity is identity first and zero trust. AI will drive real time threat detection, dynamic policy enforcement, and security orchestration across the ERP landscape.

[00:13:32] **Richard:** I love a short, concise answer that summarizes everything we've just talked about. Thanks very much. And Aditya, thanks for a great conversation. It's been really interesting.

[00:13:42] **Aditya:** Thank you.

[00:13:43] **Richard:** Welcome back anytime, and thanks everyone for listening. Please mark us as a favorite and you can get regular updates and information about future episodes. But until next time, from a Aditya, Oyku and I, thanks for discussing the future of [00:14:00] ERP.