The Future of ERP

Compliance Made Simple: Understanding Cloud ERP's Role in Shared Compliance with KPMG

[00:00:00] **Brian:** The ERPs, especially SAP, have an amazing integrated transactional database, meaning it's been built to handle these transactions that ripple across multiple layers of traditional old school singular activities. That database is full of knowledge. Full of capability. The future of ERP is AI agents on top of that ERP, that take away the gooey transaction responsibilities for employees. Employees are still gonna be involved to handle issues, but AI is the future of ERP.

[00:00:34] **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 today I'm joined by my wonderful co-host Oyku.

[00:00:46] **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 are chatting with Brian Jensen from KPMG about Cloud ERP's role in a shared compliance model. [00:01:00] Brian, great to have you here today. Could you please introduce yourself and your role at KPMG?

[00:01:05] **Brian:** Excellent. Thank you. Welcome everybody. Brian Jensen. I'm a managing director in Dallas, Texas. My focus at KPMG is the trusted application estate with a specific focus on SAP. In that world, we blend traditional compliance and risk management with cyber to help our clients enable and protect the organization through the applications.

[00:01:29] **Richard:** Maybe we can start with a level setting just to get a definition of what you mean when you say compliance, 'cause it could be in several different things. So, what do you mean when we talk about compliance in the context of a business system?

[00:01:42] **Brian:** So I've always had the concept around compliance that we first start with managing risk as an organization, so we have risk, and then we have techniques to mitigate those risks. The compliance angle comes in when organizations throughout the world, be it governmental or private [00:02:00] organizations, set a standard where they expect companies to manage those risks effectively. And so that standard generally has rules and requirements and policies and procedures. I find that organizations, if they focus on the

compliance standard for their risk program, for the risk mitigation program, they'll end up checking the compliance box, but they'll miss the goal of those compliance requirements. The goal is to ensure they're doing their required responsibilities in managing risk effectively. When it becomes a check-the-box exercise, compliance becomes something expensive and a mandatory activity that doesn't seem to have any value. When you take a step back and look at compliance, and realize that there are a number of organizations that have those policies in place and requirements in place, and as you operate in different countries, but if you simply set a standard around understanding your risk holistically and then mitigating those risks in an effective way, compliance is easy. [00:03:00] When it comes to checking the box, it's a cost. When it's an enabler and a process improver and a protector, then it's much more effective.

[00:03:09] **Richard:** And I think the advent of cloud has only increased the complexity of compliance. So we talk about a shared responsibility model. How does this change the way companies handle compliance with the cloud ERP system?

[00:03:23] **Brian:** That's a great question. So if you're not familiar with the shared responsibility model, jump out to a chatbot and ask to explain it, or ping me on LinkedIn. But the shared responsibility model is something we really didn't have to deal with when we owned the full application stack, and when I say we meaning organizations, when we own the application and installed it on servers in our network, we fully managed and were responsible and accountable for the activities of that application as we partner in the cloud world, be that a full SaaS partnership, and I'll talk about that in a [00:04:00] second. Or simply moving that application to a server running in a hyperscaler's environment. We have to acknowledge that we now share the responsibility with our business partner. Now, what's interesting is that while we share the responsibility, we still maintain the full accountability. So if our business partner does something wrong and that device or server's compromised, we're still accountable. We still have to answer to the public, regulators, or the compliance evaluators. We still have to answer what happened. And so when you look at shared responsibility, it's simply the division of activities and tasks throughout the layers of your chosen application, enablement suite. So in some cases, you own the full application, and your hyperscaler simply runs the servers. And so their SOC reports cover the running of the servers. In other situations, like with SAP's private cloud, there are three layers. There's you. [00:05:00] There's SAP, and I say, you're doing application enablement. Application configuration. You're providing the data. Then the next layer is SAP. SAP is providing the large-scale basis work and the infrastructure work, the database management work, and the coordination with the third layer, and I'll talk about that in a second, but they're really managing that SAP environment for you. You're simply providing data

and users. And the direction of what they're supposed to be doing. And then the third layer is that hyperscaler layer where they're managing the network connections for that environment. They are managing the servers, et cetera. And those three layers, even in that explanation, are somewhat complicated. And that's a simple version of it. Those three layers are orchestrated together. They're covered by SOC reports, but they're orchestrated together, meaning that they have to, each layer has to understand what the other layer is responsible for. The key with the shared responsibility model is across your application estate, knowing for each application, what you're responsible 00:06:00 for, and what your business partners are responsible for, because you are accountable.

[00:06:05] **Oyku:** You just started talking about these layers, and sometimes I think it can be a little bit confusing to understand who is responsible for what in a shared compliance model, which compliance responsibilities are handled by the ERP vendor, which ones fall to hyperscaler, and what do companies need to manage internally, for example. So, where do these boundaries lie between compliance and support?

[00:06:29] **Brian:** That's a great question, and what's genius about that question is whether it combines operations and compliance? When you look at a shared responsibility model across the application estate, it's imperative that organizations look at the individual application and understand how the layers are divided and who's actually responsible for the operations. The associated compliance requirements start to kick in. Once you understand the operational layers, as you go through those layers, there's 00:07:00 not a simple definitive guide you can get for each application; you actually have to go into the application, look at your contract. Look at the SOC reports and then look at any other agreements, like data privacy agreements or data management agreements, to construct a shared responsibility model for that application. That shared responsibility model will define who is operating what task at what level, and it will also define what documentation supports the combined requirements in a three-tier model. Which is more traditional to a private cloud environment, and SAP, the hyperscaler, has its task. Then SAP has its task. Well, those tasks are grouped together and managed through the SOC reports from a compliance perspective, but more importantly, the data privacy agreements, the SLAs, and the contract will define what tasks they're responsible for, at what level? What I find is most [00:08:00] companies make an assumption that because they're using cloud, everything's covered by the SOC report and SAP, i.e., the cloud provider with their hyperscaler is doing everything. Sometimes they make an assumption that nothing's changed for them and their customers, and the customer's doing everything. That confusion leads to breakdowns in operations, breakdowns in uptime, and breakdowns in compliance. The other thing we see is that companies don't go and decompose and define the shared responsibility

model for that single application. When it comes time for the auditors or anybody from a regulatory perspective to look at that application, they simply think they can give the SOC report as a get outta jail free card, and that's not true. What they should be doing is defining upfront what the responsibilities are by layer, having a very clear understanding from an operations and compliance perspective, and then going through and building their model, a forward-looking model going forward with that consideration, not at the [00:09:00] end.

[00:09:00] **Richard:** Another big, what I believe is a misconception when we're talking about cloud solutions, is that the security and safety of the data, controlling the data, and owning the data. So how can companies keep control over their sensitive data and also user access within this shared responsibility model?

[00:09:20] **Brian:** Let's start with user access. Transactional user access is handled by the company. They have to name the user, they have to set the limitations of what that user can do, using roles and permissions and entitlements and authorizations, and they have to manage those users in a way that matches their business requirements. And that's at their level of the shared responsibility. As you go down a level to SAP, the sensitive data is stored in the database, and SAP is responsible for that. And SAP is using a privileged access approach for managing that data. That's not where the problem generally lies. We don't see issues at that [00:10:00] layer. What we see issues with is that the organization is managing access. The organization is providing data, but it is also connecting that application environment to other data sources. And those other data sources are data in and data out. Where we see the challenges is that the wrong people make the wrong updates, which is the client's responsibility. The wrong data comes in, or data that comes out is not managed in a compliant risk-mitigating fashion. And it's all because people treat this new cloud environment as a fix-all, meaning that everything is covered. We're moving to the cloud, so we don't really have to worry about data, we don't have to worry about data security. In reality, as they better understand the shared responsibility model, they're actually able to construct A user management lifecycle program and a data security program more effectively and not make assumptions.

[00:10:52] **Oyku:** And whether it's data security, whether it is sustainability reporting, or other requirements, regulations keep changing [00:11:00] and sometimes it can be hard to follow, right? So, how does Cloud ERP help companies stay compliant with industry rules and regulations?

[00:11:09] **Brian:** First off, SAP is going to be managing their cloud solutions, because it's their fiduciary responsibility, they're gonna be managing and

monitoring those regulations at a level that most companies do not. And so they're gonna update their SOC reports, their SLAs, and their operation procedures as those regulations change. One advantage of cloud for applications is the ability to scale. They have dozens and hundreds of clients that are having to comply with these regulations. So SAP has a program to manage this that's often far more advanced than the clients. As these regulations change, it is incumbent upon the client to do two things. Number one, at the beginning, establish the shared responsibility framework for that application. So they clearly understand at the beginning what it is, what their responsibility is, not only for operations, but 00:12:00 for compliance. What documents are associated with that, like the SOC reports, and then start operating from the beginning with that structure as they manage that. There are two inflection points. Number one is yearly. That document should be reviewed yearly to make sure it's complete and accurate and represents what the true shared responsibility model looks like and what the requirements are, so there are no surprises. But throughout the year, they should have multiple inflection points for their significant compliance requirements. In states like SOX and PCOB, they should be monitoring any changes with those so that if something does pop up, they don't wait till the end of the year cycle to review it. They actually address it right at that stage. Those two points. That's a mature operating model, right? A yearly cycle and a monitoring system. What clients can't do is think that they can blame SAP, that something changed, and that SAP should have told them, right? They need to be proactively managing that as well because you can count on SAP and their associated [00:13:00] hyperscaler partners to be doing that just because they have to. Their organization is much more mature than most clients are.

[00:13:07] **Richard:** You made a great point there in that the shared responsibility model enables companies to focus on their core competencies. When you talk about new rules and regulations coming out, business systems need to keep up with these rules and regulations so that they can support all of their customers and all of their customers can be compliant. It means that it's done once and everyone gets the benefit of it, which enables the manufacturing company, for example, to focus on manufacturing. Not on the rules and regulations because they're built into the system.

[00:13:38] **Brian:** Yeah, that's right, Richard. That's the beauty of cloud. If you look at a manufacturing organization to employ a full stack, meaning fully responsible for all layers of the application management and compliance, that involves employing people who aren't core to your organization. As you move to the cloud, you get to avoid that. You get to say, look, [00:14:00] SAP has the experts who know how to operate SAP and their hyperscaler partners to operate this in a very efficient way. And so as a result, you're not having to worry about

having the most minute NIST expert in cyber managing the network for SAP. And that's the beauty of cloud. That's one of my favorite parts about the cloud.

[00:14:19] **Richard:** Right. You also mentioned earlier that compliance can be leveraged as a business advantage. So let's talk about how it can be leveraged as a business advantage. What advice would you give to companies about how to turn compliance into a business?

[00:14:35] **Brian:** That's the eternal question. We look at compliance as a cost and an inconvenience in something we have to do, when, in reality, the mindset of managing risk in an enabling and protective fashion is highly effective. I actually just gave a speech on this yesterday. When you look at the word compliance or controls, people see that as an internal auditor, external auditor, risk management, [00:15:00] privacy person's responsibility. In the IT world, we simply call that requirements. The more that it acknowledges that those requirements from compliance standards and risk management standards are there and bake those into their solutions, the more effective we're gonna be. One of my favorite compliance requirements is when you go to a website and you start filling out the address that you are gonna ship your product to, and the website starts filling in the address for you. Well, that looks like a convenience to the customer, but in reality, that is a risk management compliance function in the sense that the credit card company that you're about to charge that to is making the business be compliant by confirming who that person is to make sure there's no credit card fraud. But they also have a risk management function, which you're gonna get a better ship location when you do that. Now, sure, people can pick the wrong address, but when you have to type in the full address, you're going to make mistakes [00:16:00] and you're gonna type in that address in a different format than the consistency requires. Well, that's an example where the business actually addresses two issues. The customer's happier because they're not having to type everything in again. But then the business and the credit card provider are happy too, because the shipment's gonna go there where it needs to go, and the first time credit card validation's gonna be more accurate. If businesses look at compliance that way, where it actually is protecting the integrity of the data, protecting the value, and the accuracy of the transaction. Then, as opposed to, we have to do this because the auditors say so, they're gonna get a better outcome. We've always had Richard, the concept of bad data in bad data out. Right. Compliance tells us we should have good data, but good risk management and good risk controls programs actually ensure the data coming in is gonna be clean.

[00:16:46] **Oyku:** We often talk about how important this continuous innovation is, but is it really possible for companies to keep pushing out new

innovations quickly while they're still sticking to the [00:17:00] strict compliance rules, and how do they find that balance?

[00:17:02] **Brian:** So I find that to be an excuse. We can't innovate because of compliance, when in reality they're not able to innovate because, number one, they don't invest and understand the technology associated with the innovation. Or number two, they have so much technical debt because of bad decisions in the past, which have layers of complexity that make innovation almost impossible to move forward with. You know, I'm obsessed with AI. Anybody who knows me knows I'm obsessed with AI. As you look at this AI journey, I see these organizations that have baked in so much confusion that not only does it make compliance difficult, but it makes change difficult. They've so over-architected. They don't understand their inventory. You know, my session I led yesterday, I was referencing a minute ago, the moral of the story is you have to know your users, your process, and your data, and your applications and your infrastructure, your shared responsibility. When you don't know that, or if that's overly complex, it's [00:18:00] sure hard to change, and that's, we use the term technical debt to cover that. But when I look at compliance requirements, I don't see things that delay innovation. What I see is adult supervision that minimally tells you what you should be doing with risk and compliance, and sure, does that add cost, yes. But for an automobile, brakes, airbags, safety features, windows that don't harm you, right? Extra, um, metal and doors. Those are all things that are good. Sure, you can manufacture a car without all those things. A car without brakes is cheaper, but it's not the car I wanna drive. And it's the same analogy for applications and innovation, right? We wanna bake in risk management, security, and cyber compliance programs into our innovation cycles so that we don't innovate without breaks.

[00:18:49] **Richard:** Brian, you just opened the AI floodgates by mentioning AI. 'Cause I, I have a question around AI. We made it 20 minutes without talking about it, which is quite impressive in this podcast. [00:19:00] Yes. But how will technologies like AI and automation change how compliance is shared between companies and the cloud providers?

[00:19:10] **Brian:** That's a question we are still answering, number one. Number two, my entire career since 3oF and SAP has been defined by automation, innovation, and new things that reduce human activity. When we went from procurement that was manual with triplicate forms and in-office mail and catalogs to SAP procurement, which was all digital, we innovated, right? We had to think through what the risks are and what the compliance requirement impacts are. When you go to pure digital, people can work in silence. When you fill out a form, somebody has to put their eyeballs on it. And

so there are these layers, and as you consider AI, there are parts of AI that are simple workflow and tasks. You have to look at the DevSecOps, meaning you have to look at those AI agents and the AI configurations to make sure that [00:20:00] those agents, just like with code, are performing the tasks they're supposed to. You have to limit those agents' access to an SAP environment. You would never let an agent call SAP with an interface of conversion ID, or a system ID, or a SAP, all ID, right? You would constrain the agent's access. It's the same thing; it goes to a concept called completeness and accuracy for the data the agent is using. The large language model appears to be magical. When you look at AI in a large language model in alignment with a business process, that magic is scary. But in reality, as you code agents, we're using small language models or data sources that have been trained for the purpose to mitigate that risk. If you simply say, go perform this business function like a PO approval and use a large language model, you may get positive results, right? The large language model will look and see something scary, or something's inappropriate, or something looks [00:21:00] good. But if the context of that is a large language model, if you wanna prove SAP POs using an agent, you want to use the context of your organization and the small language model, meaning your historic purchasing data, your procurement rules and standards to make that decision. AI does support that. It's just that so many people in AI right now are using it as a magical term, when in reality, it is the concept of code, and what we've been doing with workflow has been around the entire time since the mainframe days. You just have to acknowledge it's not magic, and you have to understand how it works and then use it appropriately.

[00:21:37] **Richard:** Yeah, we have to move away from the term, the answers, AI. Now what's the question?

[00:21:42] **Brian:** Correct, correct. And so my peers in the consulting world will jump out and use AI in a prompt fashion and say it doesn't gimme the right data. Well, if you use the right prompt, it will give you the right results. You just have to talk to it correctly. It's not magic, it's just, no different than SQL for those who've written [00:22:00] SQL statements, right? You will get bad reports if you write the wrong inputs and the wrong requirements for that report using a SQL statement.

[00:22:07] **Richard:** And it's not just the inputs, it's also having confidence that the data is accurate. Because if you do leverage AI on top of bad data, you'll get bad answers.

[00:22:16] **Brian:** A hundred percent. Those small links, that's right, Richard, those small language models where you upload your historical purchasing

information. Well, if you skip a year, when you run that upload, you're gonna have bad data.

[00:22:26] **Richard:** Yep.

[00:22:27] **Brian:** Right. Its completeness and accuracy have been true my entire career, and as we go into AI, completeness and accuracy are different, but it's still a requirement.

[00:22:36] **Richard:** If not more of a requirement. Brian, you've provided some great examples, advice, and guidance so far, but if the listeners want to learn more, where should they go, and how can KPMG help?

[00:22:51] **Brian:** So when you look at trusted advisors like KPMG and our peers, we are here to help in a way that sometimes you don't [00:23:00] always appreciate, meaning you come to us with a question, and we may have more context come to us with a challenge, not a question. That challenge is how do I address compliance with my ERP, not how do I address separation of duties. Look at it as a holistic, because one of the things that we all provide is an experience that's professional or hopefully professional. It is insightful in the sense that we have exposure to a lot more companies than you have individually as your organization, but we also understand things at scale. And so when you come and ask us questions and inquire. Talk to us in a way that is a larger challenge than something simple. Ask us, what are the impacts of compliance for my new SAP private cloud environment? No, can you help me understand the SOC report? Because if you ask the larger question, just like with AI, we will decompose all the sections in the areas that you are struggling with, or you may wanna know more information, or you want help with. If [00:24:00] you allow us to show you the context, you'll get a better outcome. And so when you look at KPG, obviously, you know all of our LinkedIn pages, my LinkedIn page, my peers' LinkedIn page, or the local KPG person that you're working with. But also our webcast, our websites. Our white papers. But more importantly, develop that trusted connection. And then when we start providing that detail, appreciate that. It may be larger than you're thinking of, and you may want a bullet point list, but take a step back and say, Well, let me understand the context, and then let me dive into the details, because that's how you best take advantage of our knowledge. What we're the worst at is when you send us a message that says, I need you to tell me this one thing and tell me the price. We'll give you the price, and we'll tell you the one thing, but the outcome you want is ultimately not gonna be part of that. Challenge us. Challenge us to think big and act small.

[00:24:53] **Oyku:** Brian, we are coming to the end of the podcast, and we have one last question that we ask all of our guest speakers. So in a [00:25:00] sentence or two, what is the future of ERP?

[00:25:03] **Brian:** The ERPs, especially SAP, have an amazing integrated transactional database, meaning it's been built to handle these transactions that ripple across multiple layers of traditional old-school singular activities. That database is full of knowledge. Full of capability. The future of ERP is AI agents on top of that ERP, that take away the gooey transaction responsibilities for employees. Employees are still gonna be involved to handle issues, but AI is the future of ERP.

[00:25:36] **Richard:** That's a great answer, Brian, and we took 20 minutes to mention AI.

[00:25:42] **Brian:** Well, I mean, Richard, I'm obsessed with AI, but I do think a lot of people use it generically

[00:25:48] **Richard:** I couldn't agree more. You've gotta work out what the business problem is you're trying to solve, and then work out if AI is part of the solution.

[00:25:54] **Brian:** Well, I mean, it could be a simple report that SAP provides out of the box that you would never go [00:26:00] recreate with AI, right? From a control's perspective, you would never go build an agent to address a control. That's a configuration in SAP.

[00:26:08] **Richard:** So true. Hey Brian, this has been a great conversation. I've really enjoyed it. Learned a lot, and thanks so much for spending the time.

[00:26:16] **Brian:** Thank you so much. It's been enjoyable. Please let me know if you have any other questions.

[00:26:20] **Richard:** And we'll make sure that we share your contact information and some of the webpage that you were talking about in the show notes as well, so people can get in touch with you on KPMG. 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 Brian, Oyku, and me, thanks for discussing the future of ERP.