

The Keys to Sarbanes-Oxley Compliance: A Special SAPtips "Round-Table" with Three SAP® Compliance Experts

In this exclusive cover story, SAPtips Managing Editor Jon Reed interviews SAPtips Sarbox Director David Ashley, SAP Technical Compliance Manager Ken Asher, and SAP-HR Compliance Manager Greg Robinette.

Part one of a two-part interview

Editor's Note: To kick off another year of SAPtips, we wanted a special cover story, and we got one. There may be no single issue in the SAP community surrounded by as much hype and confusion as Sarbanes-Oxley compliance, so it was a privilege to interview our core Sarbanes-Oxley team and ask them about the challenges posed by Sarbox compliance. In this freewheeling interview, David, Greg, and Ken give SAPtips readers their honest take on how Sarbox and other regulatory requirements are affecting SAP users. Most importantly, they explain why compliance is not just an accounting problem—it's an ERP problem. These three guys have the distinction of completing some of the earliest SAP and ERP Sarbox projects, and throughout the interview, they inject specific project examples into the discussion. By the time we're done with Part I, we've learned about the "three pillars of compliance," and we've witnessed a lively discussion about who is most responsible for managing the process—IT or business users. And yes, there may be a knock or two against the Big Four somewhere in this interview. :) At SAPtips, we pride ourselves as shooting straight about the good and bad in SAP, and this interview is no exception. We don't claim to be the final word, but we intend to spark a debate. One of the most compelling things I took from this discussion was that Sarbox compliance efforts are not just about damage control and avoiding jail time. As the guys explain, implemented and monitored properly, Sarbox initiatives bring a great deal of business

value to an SAP project. There's no way around it: sooner or later, most companies are going to be impacted by regulatory requirements like Sarbanes-Oxley. Some are going to learn the hard way that compliance must be tied into the ERP systems. By sharing their perspectives and "lessons learned," Greg, Ken, and David have also made a great case for the value of SAP-savvy Sarbox experts who can link systems, controls, and business processes.

Jon Reed: David, Ken, and Greg, thanks for joining us today. This "Sarbox round-table" is a chance for our Sarbox team to share lessons learned from some of the first SAP compliance projects. To get us started, give us a brief overview of your background and how you see the future of Sarbanes-Oxley compliance in an SAP (or ERP) environment.

David Ashley: As the Director of Sarbanes-Oxley for ERPTips, I'm excited about the chance to take what I've learned on my own compliance projects and share it with the SAP community. On my last Sarbox project, what I realized is that the need for Sarbox support is not a one-time thing, but an ongoing need that companies have to address as part of a continuing process. This isn't something like Y2K that you can deal with as a one-time fix, wash your hands, and wonder where all your money went. With Sarbanes-Oxley, there is a quarterly review required, and there are thousands of companies that are going to have to comply with these guidelines.



This isn't something like Y2K that you can deal with as a one-time fix. Sarbox support is an ongoing need that companies have to address.

– David Ashley

About a third of them had to do it last year, and this year, in addition to a larger group of companies in the states, there are companies listed on the stock exchange that are foreign-owned and that now must comply. There's going to be a wave of mid-size and smaller companies that will also have to comply, and these are firms that often turn to SAPtips already. It's a natural fit between us and the next wave of companies that are facing compliance.

Greg Robinette: I'm a senior HR consultant, and I met Jon while writing HR articles for the first editions of the SAPtips Journal. Since then, I've been involved in a major Sarbanes-Oxley audit and implementation project. We've been through the entire audit and mitigation process, working with one of the Big Four, and I've been able to see first-hand how Sarbanes-Oxley impacts companies from an SAP-HR perspective.

I've learned a lot of different things going through this. From the HR/payroll perspective, one of the main things is that HR as a business function is disengaged from defining controls and defining business processes. Where HR overlaps into financial reporting, in such areas as compensation, benefits, and benefits liabilities (in addition to the direct payroll connection), a company needs to improve its processes. And I mean from the beginning of the processes all the way through to the Sarbox Section 404 controls, which reflect the improvement in the processes.

That's a big issue for HR departments, because this is not their typical mindset. Their mindset tends to be oriented more towards people than numbers, and the audits they've gone through in the past have been less direct in terms of what they need to complete. All of the SAP clients I've talked to are concerned about this. Also, I think HR is in for more compliance issues going forward with the addition of HIPPA and privacy regulations. A lot of people are looking towards the Sarbanes-Oxley controls and COSO controls to set the tone for how any technology-related compliance projects are going to go.

Ken Asher: I've been an SAP technical consultant for a long time, and Jon and I have known each other for many years. My area of expertise in Sarbanes-Oxley is in the technical

area, enforcing the controls at the IT level. For SAP-specific projects, of course, that would be at the Basis level. On my recent Sarbanes projects, I find that SAP users are learning that there's a gap that Greg has just alluded to, where you have functional teams that are focused on their own business processes, but those processes are not tied into the technical systems in the way they must be to ensure systems compliance.



You must define the policies and procedures that will affect the company on a corporate level, and then you have to enforce those at the Basis level and the security level.

– Ken Asher

Each of these departments tends to think in terms of their own business processes, so what's needed is really a collaborative effort between the functional teams and technical teams who can actually execute the enforcement strategy. This means you must define the policies and procedures that will affect the company on a corporate

level, and then you have to enforce those at the Basis level and the security level. So, everyone looks to IT to address all this, even though the IT department doesn't "own" those business processes. Sarbanes-Oxley really pushes the ownership to the business units themselves, and asks each unit to be responsible for who has access to that information within its area.

So you have to have a good understanding of the technical architecture and how you're going to enforce these new policies and procedures, how you're going to enforce separation of duties, and how you're going to "trap and capture" anyone who's tries to manipulate the system. That must all be administered on the technical level, and that's where I come in as the interface between the technical architecture and all the functional areas. Beyond SAP, I also help companies to address any of the cross-application issues that are involved. Depending on how deeply a company is invested in SAP, you could be talking about integrating anywhere from one to one thousand external systems, and each one of those interfaces has a potential risk, because you could manipulate the data before you pop it into SAP and affect how the numbers are going to come out.

Beyond that, a more elaborate issue that we're dealing with on my current client is that you don't want somebody to be able to manipulate numbers outside of SAP and then have a certain function within SAP, where they can create a vendor on the inside and route funds to that vendor. To address situations like this, we've isolated each functional and technical area—something that all companies are going to have to do. Then, they will have to take a step back from that, and look at how all these areas are affected from a cross-application standpoint.

They can't look at these different business areas as silos of documentation and policies—they all have to be assessed from the vantage point of compliance on a broader perspective. And then on an ongoing basis, you have to look at systems maintenance. At least on an annual basis, all of these access points are going to have to be reviewed. So another question that companies face is how IT is going to provide the infrastructure to do that.

David Ashley: Jon, I'd like to add to something both Greg and Ken touched on. Having come from a management background where I've overseen a lot of different functional areas on ERP suites, often times I've seen that people really are focused on their own little world. They don't look at how changes in certain functional areas or controls are going to impact someone else. To be successful with a Sarbanes-Oxley project, there needs to be some oversight in place, so that you can anticipate how changes in one functional area will affect another.

Greg Robinette: One concept that I've used pretty successfully is to set up a project plan where there are people who own certain data, who have the responsibility for it, and that data ownership remains the same even as the data moves into different areas and systems within the business. So, data ownership doesn't exist simply within a single system. The owner of that data has the responsibility to be in touch with all the people who will potentially touch that data throughout the business. They may not need to know the detail information about what the object-level maintenance in SAP is, and what the FTP file going out to some bank is, but they need to know that when you're talking about System A, System B, and System C, they have some accountability to those systems because they own the data that flows through them.



The data owner has the responsibility to be in touch with all the people who will potentially touch that data throughout the business.

– Greg Robinette

To ensure this is handled properly, the people who own the data need to participate in the business process side that supports IT and the IT controls. If you do that, and document that, it takes you right through the key provisions of Section 404. That's what we ended up doing extensively on my current project—utilizing the data ownership concept and involving the business process leaders in the establishment of IT controls.

Ken Asher: That is probably the biggest challenge that we've faced at both of the Sarbanes projects I've been on: getting people to accept ownership. Ultimately, any business process you can name crosses over functional areas, inside and outside of SAP. But at the end of the day, who owns that data? That's a corporate approach that has to be decided upon and agreed upon, and deciding which business units are responsible

for which data is actually a huge challenge that has to be addressed before any of these controls I'm talking about are put into place.

David Ashley: Ken, the point you raised reminds me that the challenges brought on by Sarbanes-Oxley bring both headaches and benefits. On the one hand, whenever you put these kinds of tight controls in place and designate ownership of data, you're going to have some griping, but I can also see some good coming out of Sarbanes-Oxley. One benefit is that you have now established a continuing plan for data ownership. It's not like you do an initial implementation and certification and walk away from it. The hard work you put into developing a data ownership model becomes a real corporate asset. The other good thing is that you see management stepping forward and taking ownership of some of these processes on a continuing basis. So, there are some real good things to come out of Sarbanes-Oxley as well. Again, it's not like Y2K, where you spent a ton of money to address problems that may or may not have had any long-term value for your business.

Greg Robinette: To support that, on my current project, when they went through the payroll process and actually forced themselves to define what they do and define who owned the data, and then did what they defined, the end result was that they now have transparency at a bunch of positions that were fairly critical for making sure that the payroll went out the door. They were able to spread out the workload and increase the efficiency of the business process. I don't have the numbers in front of me, but we did some pretty decent metrics, nothing too in-depth, but enough that we were able to take those numbers to the executive team and tell them that we had increased efficiency by twenty or thirty percent.

People were even able to take vacation around Christmas, and previously, at this company, you didn't get much shutdown time because of year-end close. Now, they were able to give easily fifty percent more people time off. We tracked that backwards to figure out how they were able to do that, and it was because the business processes had changed and become more efficient. This was just in the last year. When they were done, they were able tie functions directly to each person, and it was Sarbanes-Oxley that drove that whole process.

Jon Reed: That's a funny image: to think of someone getting some extra time over the holidays, and while they're driving home, they're thinking, "God bless Sarbanes-Oxley."

Greg Robinette: (laughs) I don't know if that's the image, but that's the reality of what happened there.

Jon Reed: Guys, are there any publicly-traded companies that are not going to be impacted by Sarbanes-Oxley sooner or later? I know there's been a staged rollout of compliance requirements so far.

David Ashley: The rest of the publicly-traded companies will have to go through the certification process by the end of the next fiscal year. Those mid-size companies that were under the initial equity cap of \$75 million must come into compliance this year, and then also your foreign-owned companies on the stock exchange are required to come into compliance this year. And the thing we need to emphasize here, Jon, is that it's not just the publicly-held companies that are affected by this. Private companies that are major suppliers to these public companies will be affected, and certain financial institutions and insurers may have compliance guidelines for companies as well. So there's going to be a big trickle-down effect

with Sarbanes-Oxley that's going to impact privately-held companies as well.

Jon Reed: And as for companies that aren't fully aware of these requirements yet, one thing you've already noted is that addressing Sarbanes-Oxley is not a one-time concern—it's a lifelong process of implementing controls and assessment tools that will help companies stay on track with these guidelines.

David Ashley: That's right. And to me, Jon, that's one of the reasons that SAPtips offers something special to SAP customers in terms of Sarbanes-Oxley—SAPtips has a long-term commitment to SAP users, and our business is built around the long-term relationships we establish with our user base. One thing that companies need to keep in mind is that the auditors and the firms that do the documentation and testing cannot be the same.

Greg Robinette: That's something I was going to mention also. In the "pre-Enron era," before Sarbanes-Oxley, the previous model for this kind of auditing process was that Big Four firms would go in and advise and test the systems. Now, that whole process must be split. Companies are now saying, "I don't want to have to pay a firm like KPMG to come in and do my audit, and then pay Deloitte to come and do my follow-up testing and advise me at whatever ridiculous billing rate they're charging." Companies are pushing back.

David Ashley: And from the war stories I've heard so far, we know that these big services firms, being in major competition with one another, have different methodologies that are not necessarily compatible. So you get a firm like Deloitte to do the initial audit, and then a firm like KPMG to do the follow up, and the second firm is likely to fuss and bicker about



It's funny to think of someone getting some extra time over the holidays, and while they're driving home, they're thinking, "God bless Sarbanes-Oxley."

– Jon Reed

what the first firm did. So they're stepping on each other's toes quite a bit in a rush to get this business, and the best interest of the end-user is not always taken care of here.

Greg Robinette: This is my prejudice coming out, I'll say that right upfront, but I've worked with a lot of these large consultancies in my years in the SAP world, and they sell their services at a certain level, and then the people that they actually send out to the implementations are often junior-level. In the past, it was to the point where you wondered if these junior consultants could even spell the word SAP. I don't think that this lends itself to a job done well. Maybe they do a better job on the auditing side, let's hope so, but that's my prejudice coming out. I just think that companies need alternatives from the larger firms when it comes to any kind of SAP services, and Sarbanes-Oxley is no exception.

David Ashley: What I've run into with some of these larger firms is that they do have the accounting know-how, but they might not be tuned into how that knowledge translates into an ERP environment. And as Greg and Ken have already mentioned, for a company that is heavily invested in any kind of ERP system, SAP included, you need to be able to help them tie these accounting practices into the logic of their enterprise systems.

Jon Reed: That raises a really good point I'd like you guys to address: why is it so important for companies running ERP systems to look at compliance issues from within their ERP environments?

David Ashley: In my opinion, ERP runs the business now. For most companies, when you take a look at their business processes (how they operate on a day-to-day level, how they generate public reports), you see that they are deeply tied into an ERP infrastructure. And that's what Sarbanes-Oxley is all about. You have to have the proper controls set up within the ERP system in order to satisfy these new requirements. And these days, most ERP systems are so complex, and have so much underlying technology, that unless you really understand that technology, there are going to be a lot of big holes in that ERP system that allow people to get in there and do things that they shouldn't be doing—things that affect the bottom line on the financials side, and in turn, possibly affect officers and get them to spend time in places they don't want to be—such as jail.

Ken Asher: It's correct that ERP systems and technology are fundamental to Sarbanes-Oxley compliance, but one thing that I've noticed being on the ground on these projects is that people tend to look to their IT departments to solve all these problems.

They think that IT owns the security process because they enforce it. But IT doesn't own that process. That's been a big obstacle for us on the projects I've been on, trying to explain to the functional teams that they actually own the process. You don't want to let them believe that IT owns that process, because we don't—we just enforce it. I'm not taking away from the fact that IT people are integral to the overall process, because, for most companies, they are; but if you put the burden entirely on the IT teams, you are not going to succeed.

David Ashley: That's the reason that we've decided to go in with a methodology that says, essentially, you start by looking at the financials and work backwards. What I mean by that is: when you start with the financials, you say, "OK, what are the huge risk items we're dealing with? And where are the controls located? Are they in the back-end ERP systems, or other application systems, or are they in manual systems? And how do they all fit together?" Ken is exactly right, keeping that in mind is very important.

" People tend to look to their IT departments to solve all these problems. They think that IT owns the security process because they enforce it, but IT doesn't own that process."

Greg Robinette: On that point, to make it simpler for me, since I'm not the brightest person in the world,

and I need pictures, what I did is that I sat down and looked at the problem graphically. If you can think of compliance as a broad line across a lot of different areas, and I add into that equation leveraging that compliance for value (I always look at value, not just compliance, whether it's Sarbanes-Oxley or any other new initiative), there are three major components needed to support that, and they need to be integrated.

The catch is that people don't like them to be integrated; they want to see them as separate. Those three major pillars that support the entire "compliance and value" effort are:

- your audit area—that's the people who are going to look under the hood and test your current controls;
- then there's the middle part of that, which is your systems people;
- and then there's the third part, which is your functional teams that run the actual business processes.

Unfortunately, there's no one group that really says, "How do I go in and serve all three of these areas to meet the compliance and value needs?"

That's where I think, from a consulting standpoint, there's a need to be able to go in and fill in the gaps. There are very few people who can go in and do all that. There's plenty of people to go in and do security audits; there's plenty of people who will help you do your audit testing, and there's lots of people who will help you structure your business processes, but you really have to tie all three together to achieve both compliance and value.

And Ken, you said that IT can't be the owner, and I agree with you, but a lot of times IT departments will say, "I'm only responsible for the techni-

cal part,” but that’s not true, because they also need to think about the business implications and add value in a non-technical way. They have to realize that the data owner is going to partner with them, and that this combined partnership will give a greater value to the project than either one of them can achieve alone. If either one of those two parts of the support system decide that they’re only going to do a certain amount, then they will devalue the whole chain. So these projects need to be a lot more integrated than people think. They don’t like it to be more integrated, because it requires more communication, and that’s probably one of the hardest challenges in business.

David Ashley: Greg, I agree: we have to remember that there are really two aspects of Sarbanes-Oxley compliance: your business systems or accounting side, and your IT side. It takes experts from both sides working together to arrive at that final product that someone is signing off on. We have to be willing to rely on the expertise of people we may not be used to working with. There’s no such thing in this world anymore as an expert in everything.

Ken Asher: Greg has laid out the three main pillars, and I’m glad he also mentioned the importance of collaboration between the IT and business side, because that’s crucial to the success of these projects. But between the three main pillars Greg mentioned, there are so many smaller areas. For example, a huge force for us on this project is the corporate controls—not the people who are running the audit, but the people who assess risk to the company. Whether they are looking at who has access to sensitive personal data in HR, or who has the ability to go in and manipulate the financial numbers, they are helping us to define the standards that we must then go

End of part one of our Sarbanes Oxley round-table interview. The interview will conclude in the April/May edition of SAPtips.


Kenneth E. Asher is a technical SAP consultant with 15 years of experience in Information Technology. His career started as a Basis Consultant where he developed a fundamental understanding of SAP’s technical architecture. Ken’s technical knowledge of SAP led to many implementation and technical management roles for a variety of clients and industries. Ken has lived and worked in several countries, which contributes to his ability to bridge the various departments, geographies, and cultures of corporations to ensure collaborative success. In his current role, Ken is functioning as the Sarbanes-Oxley Technical Compliance Manager, where he’s responsible for SOX compliance for the entire SAP product suite. Ken.Asher@SAPtips.com

Greg Robinette is an SAP-certified human resources application consultant. His most recent projects have involved HR security and enterprise compliance control, software product development, and serving as the organizational management lead for an SAP pharmaceutical implementation, and developing output management and reporting strategies.

out and enforce, whether it’s through policy, security, or a combination of the two.

But you’re right, Greg, the success I’ve had is that I’ve been able to come in as a techno-functional SAP manager and bridge these different groups of people together. I’ve been able to help them develop the processes and security procedures that met their needs. And I think that’s a

He has led projects in payroll in SAP and other software packages. Greg has a varied background including packaging system design, service, and installation, hotel engineering management, and business development for mechanical contracting and veterinary hospitals. Greg’s email address is Greg.Robinette@SAPtips.com.

David L. Ashley Jr., CISA, CISM. David has over 25-years experience in Information Management. His duties over these years have included assignments at various levels as programmer, analyst, programming manager, and business systems manager, where responsibilities have included overseeing business applications, technical support, computer operations, information security, business continuity/disaster recovery, information systems policy, regulatory compliance, and information systems audits. His responsibilities have been to users at the corporate level, user communities at locations across the United States, and international sites. Working with these many cultures has given David a unique perspective in dealing with people from all walks of life and at all levels of the corporation. David has published in several periodicals and has addressed audiences ranging from C-level officers to college graduate students. David.Ashley@ERPtips.com 

different kind of service than you can get from the Big Four. As the project goes along, we see these different groups putting their heads together and realizing that they can only be successful if they can tie the security issues and the business process issues together. That’s when I know I’ve done my job right, and that’s the kind of approach we can offer with our SAPtips Sarbanes-Oxley practice.

SAPtips *Journal*

The information in our publications and on our Website is the copyrighted work of Klee Associates, Inc. and is owned by Klee Associates, Inc. NO WARRANTY: This documentation is delivered as is, and Klee Associates, Inc. makes no warranty as to its accuracy or use. Any use of this documentation is at the risk of the user. Although we make every good faith effort to ensure accuracy, this document may include technical or other inaccuracies or typographical errors. Klee Associates, Inc. reserves the right to make changes without prior notice. NO AFFILIATION: Klee Associates, Inc. and this publication are not affiliated with or endorsed by SAP AG. SAP AG software referenced on this site is furnished under license agreements between SAP AG and its customers and can be used only within the terms of such agreements. SAP AG and mySAP are registered trademarks of SAP AG. All other product names used herein are trademarks or registered trademarks of their respective owners.