

## The Keys to Sarbanes-Oxley Compliance (and Project Staffing), Part II: A Special SAPtips "Round-Table" with Three SAP® Compliance Experts

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

### Part II of a two-part interview

*Editor's Note: In part two of our interview with the core members of our Sarbanes-Oxley team, we get into the nitty-gritty of staffing these projects. The guys talk about the best approaches to Sarbox staffing, and how to tell at a glance which resumes are going to be strong and which ones to put at the bottom of the pile. In an SAP environment, Sarbox compliance is both a business and technical project, so it comes as no surprise that the ideal Sarbox team requires a range of functional and technical skills. Can one person wear all those hats? Read on and find out. Another good discussion topic is the question of "who owns the data," the IT staff or the business staff? The guys have some strong opinions on this, but find common ground. The interview concludes with a really interesting section on the connection between new privacy regulations and Sarbox requirements. Greg Robinette, who happens to be an expert on upcoming privacy regulations, explains how work on Sarbox can dovetail nicely with upcoming privacy regulations. More than any other point, what we took away from this interview is David Ashley's belief that the work done for Sarbox compliance is not just about satisfying new regulations: done the right way, there is a lasting business value that can be taken from a strong Sarbox initiative.*

**Jon Reed:** What does it take to staff SAP-Sarbox projects? What is the best approach?

**Ken Asher:** One of the challenges we have in staffing comes back to the perception that Sarbanes-Oxley is just another security project. Some companies initially say things like, "We need more security processes in place, so let's hire a bunch of security people." A couple of the companies I worked with went out and did just that. They went out and hired a bunch of additional SAP security resources because they anticipated a total revamp of their security procedures, including redefined roles and responsibilities.



**One of the challenges we have in staffing comes back to the perception that Sarbanes-Oxley is just another security project.**

– Ken Asher

And of course, that does happen in due time. But what they miss in this initial knee-jerk reaction is the need for leadership-level meetings with the business process teams, such as the financial team. These folks need to closely define their process flows and access issues before they pull a security team together and execute at the security level. Another thing, in terms of immediate issues to tackle, is that there is a need for an experienced project leader who can guide all these teams through the initial Sarbox project plan. Now, whether that person needs to be around all the time as the project goes will vary, but you have to get that plan in place before you go out and ramp up your security team. (Editor's note: this was Ken Asher's last comment before he left the interview for a client meeting.)

**David Ashley:** That's one of the reasons it's so important to sit down and talk about a company's needs on the front end. In many situations, the first step is indeed to lay out a project blueprint and come up with a resource plan for the overall staffing needs.

**Greg Robinette:** On my recent engagements, I have found that the focus is often very implementation-oriented, as opposed to looking at operations support in an ongoing way. You tend to have a group of experts who are very good at the implementation phase but haven't really looked down the road. A lot of the teams I've worked with have

been like that—very focused on their specific implementation roles, and not on the bigger picture. From their viewpoint, they have a transactional piece that they have to put in, and that's their focus. They do a great job on that, but especially with Sarbox, that work is just the starting point



***I think when companies get through their first filing deadlines, they will look at the whole big process and say that there were some very good things that came out of it.***

**– David Ashley**

During my own implementations, I have always rocked the boat a little bit because one of my pet peeves is that you have to plan for authorizations and security as you design. If you don't, you're going to run into problems. I've actually run into the opposite problem that Ken has run into: I've seen a lot of situations where companies save the actual authorizations until the end. I was on this type of project recently, and when we went live, the authorizations weren't right. This wasn't something

that should have been saved until this point in the process, and there were a lot of glitches—people at one plant could see the pay of people at another plant, for example. It's a lot harder to reinvent the wheel once you've put all your data in. But this is where I really agree with Ken: you cannot go in willy-nilly. If you tackle these issues upfront and integrate them into the plan, you'll get a lot better result.

The Big Four go in from the perspective of the audit plan, but that's only one part of it. The business process folks go in from the business process angle, and the systems folks go in with their systems plan. Companies can't step back and see the forest because they're caught up in the trees. Somebody really needs to look at it from the big picture, and that's a very important aspect of staffing for a Sarbox project: you need someone who can come in and pull all three of these secondary plans into one master plan for compliance across the business. Whether it's a consultant or somebody within the company, somebody with executive authority needs to step in and pull these teams together. It may be more work for the left hand, but both hands come out ahead at the end of the day.

**Jon Reed:** You guys have talked a fair amount of about security, but when I think about Sarbanes-Oxley from the outside, I think about satisfying federal reporting guidelines more than I do about internal authorizations and roles. Can you tell us more about why security and authorizations play such an important role in Sarbox compliance?

**Greg Robinette:** From an HR-payroll point of view, it is fairly straightforward, and commonly-accepted auditing practices bear these things out. In SAP, for example, if I go into the system, "hire somebody," and set up a direct deposit arrangement, then

when the normal payroll runs, that person is automatically picked up—nobody looks at it. What we need to have are security methodologies that prevent someone from doing that and keep the "segregation of duties" in place. There also needs to be some way to audit that. I'm generally not a big fan of third-party tools in SAP, but in this case, the SAP tools require a lot of contact time in order to go in and run screening reports and do comparisons. There are some pretty good products out there that can do that for a company, especially for a large company with complex processes. From an HR perspective, that's how I see the nuts and bolts of security in the Sarbox world. And, as I've pointed out, these kinds of access problems can be avoided by planning correctly.



***During my own implementations, I have always rocked the boat a little bit because one of my pet peeves is that you have to plan for authorizations and security as you design.***

**– Greg Robinette**

**David Ashley:** We have noted already that this is a long-term effort with a long-term benefit. I think when companies get through their first filing deadlines, they will look at the whole process and say that there were some very good things that came out of it, because it forced them to go through some things they don't necessarily like to do—like process documentation and the tightening of security and data access. But the end result of documenting those processes is a big improvement in process efficiency and a clarification of individual roles. With SAPtips, I'm excited about continuing the long history Andy Klee has established on the JDEtips side of assembling mastery-level talent and bringing them onto ERP projects. And this is exactly the kind of approach that is going to be so effective in terms of tackling the wild world of Sarbanes-Oxley.

**Jon Reed:** Agreed. Guys, when companies are looking to bring in qualified Sarbanes-Oxley consultants for their SAP projects, what key questions should be asked? And is there something in particular you look for in the resumes of good Sarbox people?

**David Ashley:** One thing I like to do is to probe more deeply into the nature of their Sarbox experience. Everyone knows that Sarbox is hot, so they all put Sarbanes-Oxley buzzwords on their resumes. But when you ask them specifically about their project roles, you find out that some of these folks were really just on the periphery and didn't get their feet too wet. I like to get a clearer sense of how long they were on a particular project, because with Sarbanes-Oxley, if you move around too quickly, you might not get enough depth of experience. You need to make sure there is a customer out there that was satisfied with them enough to keep them around.

**Greg Robinette:** When I get involved in evaluating HR-Sarbox folks who are going to be touching on system security, I look for people who have an understanding that it's not enough to just go into the profile generator (TCODE PFCG) and generate the profiles. You also have to understand the enterprise structure and the underlying objects. Regular Basis persons who are told to do HR security are at a huge disadvantage, because they have no knowledge of how the system was designed. They may not even know the enterprise structure and how the company is set up in terms of how the employees are divided into different groups.



**When companies are looking to bring in qualified Sarbanes-Oxley consultants for their SAP projects, what key questions should be asked?**

– Jon Reed

For most Basis folks, there really isn't that much requirement that they know the underpinnings of the HR functionality, and they're not likely to know their way around this stuff unless they have a functional person sitting with them. I've had projects where I was more responsible for the functional org management side, and not as heavily involved on the secu-

rity side, so I would always look for a Basis person that had a good understanding of the HR functional side—at least in terms of how the company is structured. Sometimes the best person for this role is a long-term employee of the company who has a deeper understanding of the systems that are in place. That's what I like to see when I'm working on this kind of project.

The other thing I like to see is: do they know some basic tools other than the standard ones in SAP? For example, if you're designing a role, can you go out and grab the SAP-defined roles, and can you go in and run a trace if you're running a workbench in payroll? If you give the system an authorization just for the transaction code and the things that appear on the surface, you won't be able to run that kind of trace—and a lot of folks don't know that. So my question to them is, "If I wanted you to give somebody authorization to the offcycle workbench, how would you recommend researching that to determine what authorizations need to be granted?" The answer I want to hear back is: "ST01, the trace, with authorization checks, so I can define it." That's a very specific example, but that's the kind of thing I want to hear when I'm involved on these kinds of decisions.

**David Ashley:** What Greg is saying is exactly right: knowledge that spans the functional and technical sides can be important, but on the flip side, you also want to be careful of the "know it all" type of profile. This kind of project can involve a number of specialists: HR specialists, FI specialists, Basis specialists, and someone who says, "I can do it all," probably can't. The best folks are specialized but also see that big picture and can work within the approach needed for this kind of project. Beware the "super-individual!"

**Jon Reed:** That makes a lot of sense. We've heard from a number of consultants who want to be involved in our Sarbox practice, and when I look through the resumes of so-called "SAP-Sarbanes-Oxley consultants," what I'm not seeing enough of is guys like Ken and Greg—guys who have come up from a deep SAP specialization, and have been lucky enough or fortunate enough to get pulled onto Sarbox projects from the perspective of the SAP expertise they've developed over these years.

This kind of Sarbox person really understands the intersection points between Sarbanes-Oxley and SAP, and these are the kinds of folks we're bringing into our practice. Some of the resumes we've gotten in are from people who worked for SAP until the year 2002 or so, doing programming or whatever, and then they got involved in some non-SAP projects doing Sarbox-related auditing work. I'm not saying these people have nothing to offer, because obviously, when you're building a team, there's room for "role players." But when you're talking about the core guys who are going to make a huge difference for SAP projects, it's going to be people like Greg and Ken, who can themselves be guided by a guy like David who can oversee all of it.

***This kind of Sarbox person really understands the intersection points between Sarbanes-Oxley and SAP, and these are the kinds of folks we're bringing into our practice.***

What's clear is that Sarbox compliance is totally embedded in SAP systems issues, and if your hiring managers don't understand that, your hires are not going to be very effective. SAP specialists who understand how compliance touches on their area of specialization are the key to successful Sarbox staffing. There are not that many folks out there who bring that to the table, but we've been able to bring in some good ones. And that's part of why I'm excited about this practice: we're offering an affordable alternative to Big Four Sarbox pricing but we're still providing the same caliber of individual, if not better. One of our criteria, in fact, is that we want to be able to send out our team members on their own—so they better have the depth of experience to be able to make a difference without leaning on a bunch of other consultants.

**David Ashley:** Absolutely. And that's something you do run into, as we've talked about, with the larger firms, where you might have some 24, 25 year old team members who just don't have the industry depth that the senior guys we have on board do. We're committed to putting the right people in—people who really know what they're doing.

**Greg Robinette:** I was thinking about something that Ken said before about forming good project teams. He mentioned how you wanted functional people who understand the technical side, and vice versa. I'm primarily a functional person, but out of necessity and because I wanted to master it, I went out and learned SAP security. I now consider myself as good a technical security person as most people I've met, but I don't consider myself a technical consultant. By the same token, there are technical people I know who have gone out and incorporated functional knowledge into their skills. I know one HR programmer who has done

a lot of CATS and time management programming, and she felt she didn't have a good enough understanding of the functional concepts that were affecting her coding assignments. So, she went out and mastered the functional concepts, and now she's as good as any time management person I know.

What I don't like is that stovepipe attitude. I hate hearing: "It's not my job." On this kind of project, things overlap, and everything is your job, even if it's not your specific assignment. Of course, David is right that you do want people who have a strong industry depth and specialization—but they need to be able to see beyond that specialization and connect their expertise to other areas. I look to hire people who have a clear understanding of their core responsibilities but are willing to help out anywhere and ready to tackle new areas. If you can find that kind of person, they're worth an awful lot of money.

**Jon Reed:** It's also important to keep in mind that the same person isn't a good fit on every project. When you talk about project staffing, you don't want to take the approach that every company needs the same thing. So often with SAPtips, we find ourselves plugging in one or two missing pieces that make a huge difference. And let's face it—not every company is at the point where their staffing needs are mapped out strategically. And not every company has the same amount of internal SAP expertise either. Some companies are fairly new to SAP, whereas some have been investing in SAP for years and even have their own internal "center of excellence" for skills training.

And then you have companies where everything is in place except for that one missing piece—for example, they need someone like Greg who can tie HR security issues into an overall compliance plan. We hear

from that type of company a lot, and that's another thing that may separate us from the Big Four—we don't need to have a huge team in place to make a big difference for our clients. Sometimes one key subject matter expert is all that's required. We're in a position with our Sarbox practice where we can say, "You want a one-time check up? We can do that. You need a specialized resource? We can do that. You want an ongoing plan for compliance and systems optimization? We can do that too."

**David Ashley:** That's true. We have a lot of flexibility in terms of the kinds of resources and the size of the team we can provide. One approach to consulting is to try to get your foot in the door so you can place as large a team as possible and "milk the account." Another approach is to go in with the mindset of solving a specific problem or issue and providing only the resources necessary for that situation. It's probably clear by now which approach we are partial to.

**Jon Reed:** Shifting gears from the staffing side, Greg, in the first part of this interview, you mentioned how Sarbox is just one example of the kinds of regulatory guidelines companies are facing. You mentioned some others, like HIPPA and privacy-related issues. Can you tell us more about that?

**Greg Robinette:** Sure. The attitude of the country towards financial mismanagement and corporate malfeasance was: "Do something, and do it now!" And as a result, Sarbanes-Oxley came out of it. HIPPA had a different origin. Some people think that the rampant growth of identity theft and the violations of privacy from a technology standpoint spawned HIPPA, but that's not accurate. What it really came down to was that insurance companies got tired of so many different formats,

and that got piggy-backed onto the privacy issues. Here's how Sarbanes-Oxley and HIPPA are related: people are looking at how Sarbanes-Oxley has been implemented, and they are saying, "HIPPA should be handled that way too."

I serve as a member of the Virginia General Assembly on the Committee of Technology and Science, and I was appointed to the Privacy Advisory Committee last year, and we've seen many different cases of gross violations of privacy. These happen not so much because businesses don't care about privacy, but because many businesses are unsure of how to approach the issue. What Sarbanes-Oxley does is provide a framework, and I can see that same framework being applied for issues like privacy. From the business side, it's important to look down the road and say, "Sometime, by the end of 2005 or 2006, there's going to be federal legislation mandating how social security numbers can be presented on documents."

***That's another thing that may separate us from the Big Four—we don't need to have a huge team in place to make a big difference for our clients.***

There's no question that people want changes. For example, there are counties in Florida where you can walk in

and get all kind of private information on any homeowner in the county. You can't usually get their social security number anymore, but you can get just about anything else. And here's the thing: before you had to walk into a courthouse to get that information, but now, you just go online, and it's all at your fingertips. There's a whole mass of private data out there, and it needs to be dealt with. Compliance-wise, the framework that COSO has provided for the handling of data for financial reports will translate relatively easily into the privacy arena, and I think it's something companies should be looking ahead to.

**Jon Reed:** Greg, that's very interesting. Reading between the lines, it sounds to me like you're saying that some of the hassles that go into "becoming compliant" are going to pay off in terms of addressing these issues on multiple fronts.

**Greg Robinette:** Exactly. And the documentation you do—just because it's for Sarbanes-Oxley—doesn't mean that it can't be applied to privacy. Of course, you have to have a privacy policy in place, and you have to chart out who should have access to the data. The inclusion of the privacy policy into the Sarbanes-Oxley code of ethics is, to me, just a natural next step. And the systems support for that is also a natural next step.


**Jon Reed:** Greg, thanks for that look ahead. And I'd like to thank all three of you for providing such an in-depth view into the challenges posed by Sarbanes-Oxley for our readers. From the project staffing side, it's good to know there are people out there who have already been through the nitty-gritty and come out the other side. We look forward to hearing from our readers on this piece, and we'll be sure to respond to any of your follow up questions.

*End of Part II of our Sarbanes Oxley round-table interview.*

**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's email address is [Ken.Asher@SAPtips.com](mailto: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. 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](mailto: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's email address is [David.Ashley@ERPtips.com](mailto:David.Ashley@ERPtips.com) 

# 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.*