Audits and Regulatory Reviews — Will Your SAP Project Make the Grade?

Steven W. Biskie

Steven W. Biskie is an assistant vice president for a large insurance corporation, where he focuses on compliance with recent financial regulations. Previous to that, he ran the Implementation & Process Improvement practice for Jefferson Wells International. Steve is a certified information systems auditor and has worked in all areas of the systems implementation process.

(complete bio appears on page 88)

Implementing an SAP project has always been challenging. Anyone who has gone through the process of gathering requirements, designing solutions, testing them with users, validating them with third parties, and driving them to completion under often unrealistic constraints knows what a Herculean task it can be. Now new forces have conspired to complicate things even more — regulations.

Over the past five years, federal and state governments have put more than 10,000 new regulations on the books. Many of these regulations go directly to the heart of how a company conducts its business. Because our SAP systems also directly affect how we conduct business, it does not take long before the average SAP project manager comes to realize that this new regulatory environment poses a tremendous challenge to any SAP implementation, expansion, or upgrade.

This article shows project teams a way to simplify the decisions and tasks that are required of you to address the mounting number of requirements posed by a rapidly increasing number of regulations (e.g., Sarbanes-Oxley, FDA, HIPAA, the Gramm-Leach-Bliley Act, the Patriot Act) and how to navigate the array of potential interpretations of these regulations by management, lawyers, and auditors. The trick is understanding the common themes of these requirements, which typically fall into four categories:

- Security and confidentiality
- Data accuracy and integrity
- Business continuity and recovery
- Communications and training

Thinking about the requirements in this way helps you minimize the time your team spends on activities peripheral to the true implementation, reduce project redundancies caused by distinct yet often overlapping requirements, lessen the ongoing cost of maintaining compliance-related documentation, and ease the burden of future internal and external testing activities. In short, understanding the common categories for varying requirements and knowing how to apply their implications to your project will save you time, reduce both your initial and recurring costs, and keep your staff focused on activities more enjoyable than constantly dealing with auditors and regulators.

In this article, I offer ideas for how to tackle the extra security, data management, business continuity, and communication and training requirements that come with the mounting wave of new regulations, how to extract helpful information from your auditors at the outset of a project, and how to test and document your activities to ensure your effort passes audit scrutiny.

Two important caveats: I am an auditor by training, but I am not *your* auditor, and my opinions may not be shared by your auditors; I am also not a lawyer (nor do I play one on television). Consult your own auditing and legal teams for specific advice and direction. Consider that to be my first and most important piece of advice. If you check with your auditors and legal teams from the outset, and cross-reference your documentation to their recommendations and expectations, you will save yourself and everyone else significant time, money, and energy.

Remember When Projects Were Simpler?

Think about your very first significant SAP implementation or upgrade. You probably sat down with management, who told you that this implementation is "really, really, really critical to our business." They explained that they were giving you an opportunity to change the entire company. You would be working closely with executive management and looking at the business in part and as a whole. And by the time the project is complete, they said, you're going to know more about the company than almost anyone else, and "that's going to make you more valuable than any other single employee." You probably became excited about the opportunity, and you probably went home and celebrated over it.

Shortly thereafter, reality set in. The tone of certain managers changes from one of great opportunity to one of "you'd better not mess up." Maybe you inquired about a new salary to go along with your new responsibilities and were told, "We'll take care of you when it's over." That might be the point when they tell you that go-live is January 1, so you might as well forget about being home for the holidays!

Next, you meet with the business teams. Up until a few days ago, these were your compatriots. Now they look at you with suspicion and ask, "Why do you have to change the way we do things?" "Why can't we just customize SAP?" When you come looking for critical project team members and ask for Bob, management frowns and says, "Bob is pretty valuable. How about John (who is drawing a large salary and this is just the excuse we need to move him out)?"

We've all been there, and despite all the obstacles, we've managed to successfully complete our SAP projects. But those were simpler times. On top of the already-existing challenges associated with every implementation and upgrade, we're now faced with a new and growing pool of challenges: regulations.

10,000 New Regulations and Many More to Come

In the past five years, the regulatory environment has exploded with nearly 10,000 new state and federal regulations. The speed at which regulations are passed, and the resultant impact on teams who work with systems such as SAP and who must respond to these regulations, has increased exponentially.

Knowing how these regulations apply to your project is the first step toward being able to manage your resource constraints. Newly imposed rules and regulations don't come with canned marketing campaigns geared toward raising management's awareness of the increasing burden on your project team. The regulations themselves don't lobby your executive sponsor to give you more time and money, nor do they tap project teams on the shoulder and suggest that they pay attention to them. If you're not careful, you may find a host of under-funded, under-estimated, under-resourced requirements awaiting you as you move closer to your implementation deadline.

At the outset of any new SAP project, you need to know what regulations to factor into your activities. For example, an online retailer implementing the SAP Sales and Distribution (SD) module and planning to deliver goods to consumers in California needs to understand the impact of California legislation on consumer privacy, the relationship of up-front sales processing to the controls required for financial statement reporting under Sarbanes-Oxley, and the records that may be necessary to comply with sections of the Patriot Act — in addition to myriad sales tax and other commerce-oriented regulations. A financial institution selling investment and insurance products may have to deal with HIPAA and Gramm-Leach-Bliley on top of the same regulations that affect the retailer. And a company with international reporting requirements may have to deal with not only US regulations but also country-specific regulations that, while similar, may each have differing requirements.

To get your hands around the requirements that will affect your project, I advise project managers to start with the following steps:

1. Meet with management and the legal department (preferably together) to discuss both current and pending regulations affecting the system or related process, focusing on the following questions:
   - How are these regulations addressed in today's environment (if applicable)?
   - What parts of the legislation are subject to interpretation, and how are other companies addressing this uncertainty?
   - How can the SAP implementation/upgrade improve the way we meet these requirements?
   - How important is it that our compliance activities be system-enforced (vs. driven from manual processes)?

2. Meet with your internal audit department to discuss the effectiveness of the steps enacted to meet current regulations, and learn the typical root causes of any prior compliance failures. Brainstorm ways the implementation or upgrade can address these issues.

3. Get in contact with other organizations affected by the same regulations. Learn both what has worked well and what "great" ideas turned out to be "not-so-great" in retrospect.

4. Conduct your own independent research to better understand regulations and how the market is reacting to them. The following sources may be good places to start:
   - www.complianceweek.com — This is the site for Compliance Week magazine, which is dedicated to compliance-related issues.
   - www.theiia.org — Since many internal audit organizations get involved in auditing compliance activities, the Institute of Internal Auditors (IIA) site can be a good place to go to understand what may be important to an auditor.
   - www.isaca.org — Similar to the IIA, the Information Systems Audit and Control Association (ISACA) is focused exclusively on the systems side of auditing and is a useful source for understanding what is important to systems auditors.
   - http://corporate.findlaw.com — This is a portal for researching corporate compliance laws and news. It is designed for lawyers, so be prepared for some exciting bedtime reading.

Regulatory Requirements Generally Boil Down to Four Key Concerns

After following the previous steps, you've probably identified numerous regulations that could affect your implementation or upgrade. Fortunately, you may already have existing business processes that address some of the identified areas of concern, and your SAP system may inherently address some other requirements. However, you're still probably left with a fair share of requirements that will affect how you design, configure, and implement the system. Don't panic. When you start to look at the dozens or even hundreds of requirements in the context of an SAP project, you will see that the requirements pretty much fall into four categories:

- Security and confidentiality
- Data accuracy and integrity
- Business continuity and recovery
- Communications and training

Let's take a closer look at each of these categories and the steps you can take to address the related requirements.

Security and Confidentiality

Directly or indirectly, security is a component of almost all regulatory requirements affecting SAP implementations. Directly, security provides a means to meet the confidentiality requirements of laws like HIPAA and Gramm-Leach-Bliley. Indirectly, security supports requirements in the other three categories (i.e., enabling data integrity by restricting users of certain key transactions to only those who have the experience, background, and training to execute them appropriately). Most of you probably know that setting up security within an SAP system is an intensive, time-consuming, multi-faceted exercise that is often wrought with problems. As a result, an early focus on security will go a long way toward lessening post-implementation headaches.

While the requirements of each regulation are different, focusing on the following will give you a leg up on addressing the security-related issues associated with most of them:

- **Data classification:** Have you identified the key data elements associated with the implementation/upgrade, and have these elements been categorized into levels of sensitivity based on a company-wide standard (and in light of the applicable regulations)? Has security been implemented around this classification? For example, it's very common to limit access to employee data within the SAP HRM module to employees within HR, but under HIPAA, further restrictions may need to be placed upon employee healthcare information.

- **Conflicting transactions/authorizations:** Have you identified transactions or other SAP authorizations that, based on your business processes, should not be granted to the same user? Have you ensured that no SAP profile contains any of these conflicting transactions? Have you confirmed that no composite profiles (multiple profiles assigned to a user) have created additional conflicts? Do you use your matrix of conflicting transactions to validate changes to profiles and additions to user access? For example, under Sarbanes-Oxley, the same user should not be able to initiate and approve transactions that result in direct GL postings (possibly above specified tolerances). If a manager "approves" additional access for this user, would you know that a segregation-of-duties conflict has been created? And if so, do you have a process for obtaining secondary authorization?

- **Powerful transactions/authorizations:** Have you appropriately restricted your powerful transactions and roles? Do you periodically monitor the use of these transactions? In regard to Sarbanes-Oxley, these transactions often bypass built-in process-related controls and thus should have controls of their own. Don't get caught in the trap of excluding certain transactions from your analysis simply because they are "read-only." While it may seem innocuous to give transaction SE16 access to an auditor or analyst to allow them to download tables for transaction testing, it could pose problems for any regulation where data confidentiality is important.

- **Security setup and maintenance:** Once you've covered the previous three items, how do you maintain these processes over time without degrading your security? How strong are the processes for updating access when an employee leaves the company? Is the same rigor applied to an employee transfer (in many cases, more risky than a termination since that employee may now have additional responsibilities that, if added to their prior responsibilities, could create a conflict)? If you're upgrading, have you included additional transactions and authorizations in your matrix of conflicting transactions/authorizations? Are you periodically monitoring access privileges to ensure nothing has fallen through the cracks, and if so, do the people performing the monitoring have the right knowledge to perform what you expect of them? For example, a business manager may easily be able to tell whether someone is in their department, but he or she may not have the requisite knowledge to say whether transaction MR8M creates a segregation-of-duties conflict when combined with transaction MR1G.

I'll go into more detail later about getting through an audit successfully, but until then, remember one very important point: The actual practice is more important than the policy. Don't get me wrong, policies are important, but most audits are looking for what you actually *do*, not what you *say* you do. Don't operate under the false presumption that a strong security policy will get you through the audit. While it may help with some audits, and may get you past an inexperienced auditor, you run a greater risk of failure by focusing on the policy more than the process. Focus on ensuring people are actually doing what you expect of them (with the policy serving as a means for communicating expectations). An auditor who finds that processes are not consistently aligned with written policy will begin to question management's effectiveness at creating and maintaining a strong control environment.

Data Accuracy and Integrity

Many regulations also focus on the accuracy of data and how you maintain the integrity of that data (as it is processed and maintained) over time. Sarbanes-Oxley is a good example — it focuses not on whether a company has made sound financial decisions but rather on whether the accounting data and related footnotes have been presented accurately given the financial events that actually occurred throughout the reporting year. For other regulations, data integrity has an indirect impact. For example, the security and confidentiality issues discussed previously are dependent upon the integrity of certain data (the data classification scheme must be accurate and current, user profiles must be set up and maintained accurately, and data about employee status must be accurate).

Within this second category, it is important to consider inputs, processing, and outputs. The premise is this: We must first start with good data, we must process that good data accurately and completely, and we must take the results of this processing and record them accurately and completely. Let's look at each of these pieces separately.

Inputs

If your implementation or upgrade is around a process where data will be input directly into your SAP system, you are fortunate. The SAP system has some strong data input and validation capabilities, and the control around this input will be within your authority to influence. If the SAP system will be receiving data from other sources (data transfers, Microsoft Excel spreadsheet uploads, etc.), you have a slightly larger challenge. Many companies operate in silos, and it's easy for an implementation team to assume that it's the responsibility of the originating system or process to ensure the accuracy of what is passed to the SAP system. Unfortunately, regulators and auditors do not generally care *who* is responsible for the integrity of the data input — rather, the concern is that the input has integrity (independent of who has been assigned that responsibility).

Generally, your input will fall into two categories — input that is entered online by a user, and input that is fed from another system.

For input entered online, consider the following two areas of focus:

- **SAP-configured tolerances:** Within the SAP system, you can often flag transactions that meet certain criteria and force a secondary review before that transaction is processed. For example, you can configure SAP to automatically block all journal entries over $X and limit the ability to unblock these journal entries to only certain people within the organization. In many cases, the SAP system provides defaults already configured in the system. Make sure these tolerances have been configured to fit your business. A common "red flag" from an audit perspective is noting that tolerances have not been changed from the SAP-provided defaults.

- **Exception reporting:** SAP provides a lot of great exception reporting, but merely having a report available is not a control. A control is someone's periodic review and follow-up of the report. Key to success in this area will be focusing your training and education processes beyond "how to get to this report" and into areas like: a) how often should this report be reviewed; b) what should the reviewer be looking for; and c) if something questionable is found, how should the reviewer be leveraging the SAP system to get it resolved.

For input fed from another system:

- **Data transfer controls:** The use of file headers/footers containing record counts, checksums, and other such identifying information can help to ensure that all information sent by the originating system has been received by the SAP system. Additionally, similar controls can help ensure that a) all files expected were received; and b) a file is processed only once.

- **Job scheduling and monitoring:** Many file transfers are automatic, and thus the auditor will look to ensure that the job schedule itself is accurate and that someone is actively monitoring the completion status of scheduled activities to ensure everything was run to completion.

- **Exception reporting:** The exception reporting mentioned for data entered online also applies to data received from other systems.

One final consideration on data input — focus on a means to monitor the proper classification of that data, particularly if that classification will drive how that data is processed. For example, entering a sundry invoice goes through a completely different set of controls than a traditional three-way-match invoice. As such, someone could intentionally (or unintentionally) circumvent the controls you have built into your process merely by improperly classifying the transaction. It happens more frequently than you may think. While working on a post-implementation audit for a client a number of years ago, we discovered that 70% of the invoices being processed as sundry invoices actually should have been processed through the traditional PO-matching process. Why was this happening? A group of accounts payable clerks didn't like the number of screens required to process the invoice by matching to a PO and found it "quicker and easier" to simply enter all invoices as sundry invoices. Whenever there is a "quicker and easier" option, there is a higher likelihood that someone may try to circumvent the intended processes. To detect this, look for ways to monitor the accuracy of how transactions are classified.

Processing

Once data is input into the SAP system accurately and completely, you need to make sure that data is then processed accurately and completely. Your first reaction may be that since the SAP system is doing the processing (and since thousands of companies are using SAP), there is limited risk here. In reality, unless you have implemented a purely "vanilla" SAP system, where you do not make any modifications to the system or customize it in any way, a typical audit will focus heavily on your change control process.

The premise here is that the configuration and customization changes you make to your SAP system are the biggest points of exposure that could cause the system to process transactions in a way that does not maintain data integrity.

To button-down your change control process, focus on the following areas:

- **Authorization:** Maintain a list of employees who are allowed to approve changes to the SAP system. Require written (or electronic) documentation supporting this authorization. Set up a process whereby a change cannot be made without this authorization.

- **Requirements:** Ensure that requirements are documented and agreed upon for all change requests. Consider standardizing a request form or other means of change communication to stimulate thought around control-related requirements (e.g., security/confidentiality requirements).

- **Testing:** Ensure all changes are tested from both a technical and a functional perspective. Develop a quality assurance process to ensure all required test steps are actually included in the test plan (particularly for user-conducted tests). Map initial requirements to test steps. Maintain these test results for all changes and document the follow-up to any test exceptions.

- **Transport:** Obtain official approval to move changes into production post-testing. Define a process to ensure that the code actually tested and approved by the user group is the code that gets moved into production.

- **Data cleansing and conversion:** If you will be performing any data cleansing (i.e., adding data elements not required previously, validating existing data elements, populating additional fields, etc.), enact procedures to provide an audit trail from the original data to the new data. Tightly limit the number of people who can update this data. Set up a process to ensure that only data that should have been modified gets modified and that it is modified accurately. If the data being cleansed ultimately affects financial reporting, expect a fair amount of audit scrutiny under regulations like Sarbanes-Oxley.

- **Segregation of duties:** Define job functions and security authorizations to separate the ability to modify code from the ability to transport changes into SAP production. Eliminate (or at least limit and monitor) programmer access to production.

- **Emergency changes and other exceptions:** It’s perfectly acceptable to have a process for dealing with emergency changes and quick fixes that streamlines the previous items. However, make sure the objectives of the prior items are covered post-change if you do have exceptions to the standard change process.

The strength of your change control process is key to meeting the requirements of many regulations, including Sarbanes-Oxley. Once you’ve defined the process, make sure it is consistently followed. It’s easy to let some of these processes slide over time, particularly since the desire to please users may cause some support staff to circumvent controls that may seem to hinder the process of getting a user request implemented quickly. Expect to spend a fair amount of time integrating this process into the support culture, and enact some strong monitoring processes early on to detect whether the rigor around the change control process starts to slip.

Outputs

Controls over outputs will closely follow controls over inputs — particularly those for input fed from another system. While the tendency from a project management standpoint may be to consider the successful receipt of the output the responsibility of the receiving area or system, the auditor is not concerned with such details. The key question is this: How do we know all records that should have been output were actually received, were received accurately within the necessary time frame, and were protected from unauthorized disclosure? In addition to electronic feeds, don't forget to consider the confidentiality effects of printed reports or electronic downloads (which could affect how/where information is printed or saved).

Business Continuity and Recovery

While a few regulations directly affect business continuity and recovery, many have an indirect impact. For example, while Sarbanes-Oxley explicitly excludes disaster recovery (since it is a potential future event that has no impact on current financial statements), the controls you have in place for data handling during the recovery process may very well have an effect on the integrity of your financial reporting if you have a recovery event, and thus they may be "in scope" for Sarbanes-Oxley. Additionally, confidentiality-related regulations such as HIPAA and Gramm-Leach-Bliley may influence your data recovery strategies and controls during the recovery process.

Key questions include:

- **Confidentiality:** Do the regulations provide for an exception to confidentiality requirements during a disaster scenario? Do my backup and offsite storage processes provide for appropriate controls over this media in light of security and confidentiality requirements? Do I need to consider separate facilities or develop additional roles to deal with information now considered sensitive from a regulatory standpoint? What media destruction processes should be enacted at the hot/warm site post-recovery to ensure the confidentiality of my data is not compromised?

- **Data integrity during recovery:** How do I ensure that the accuracy of my data is maintained during the recovery process? Should additional monitoring processes be enacted during recovery or post-recovery to ensure unauthorized changes or inaccuracies are not introduced into the system? Is management aware of the additional segregation-of-duties risks exposed during the recovery process, and have they accepted this risk?

- **Completeness and integrity of interim processes:** How do I ensure accuracy and completeness for the data collection and processing that occurs manually until full system recovery? Once the system becomes available, how do I know that what was captured/processed in the interim gets into the system? Can I detect whether the information entered into the system post-recovery shows a different result than what was generated from the interim manual process (i.e., user mistake), and if so, what additional follow-up with customers/suppliers/etc. should occur?

In many cases, your disaster recovery and business continuity processes serve as an insurance policy. If they are enacted, however, these processes tend to bypass many controls built into your standard business processes. Be prepared to show that, at a minimum, you have detective processes in place to ensure errors are not introduced into the system or confidential information is not disclosed during a recovery event.

Communications and Training

Several regulations require communication of key business events within specified time frames (such as Sarbanes-Oxley Section 409's "rapid and timely" disclosure of material business events, or California Senate Bill 1386's disclosure of potential security breaches). For regulations such as these:

- Determine what indicators exist that would allow you to recognize that such a business event has occurred.

- Identify or develop reports within SAP or other systems that give you visibility into these indicators.

- Assign responsibility and expectations (including frequency) for monitoring these reports.

- Trigger workflow and other email-type notifications, where possible, to automate the detection process.

Communication relies on good information, good processes, and the ability to report on that information. Effective communication is also dependent on effective training, since employees need to understand what they are responsible for and how it needs to be communicated. This is particularly important related to the controls you've put in place to address regulatory requirements.

Consider, for example, a monitoring process over exception reporting. For this to be effective, the responsible user needs to understand a lot more than just how to navigate to a particular report (which, unfortunately, is often how people are trained in SAP). To rely on this as a control, the user must also be educated in a) how often this report should be reviewed; b) what they should be looking for in the report; and c) how they should leverage SAP or other systems to follow up on any potential issues they identify from this review process.

Of course, almost all regulations will necessitate some form of user training. Under Sarbanes-Oxley, employees need to understand the controls they are responsible for and how they fit into the process, managers need to understand the risks that need to be addressed when changing a process or implementing a new process, and some staff need to understand how to facilitate an audit walkthrough. For HIPAA, employees need to understand how to recognize protected information, how that information can and cannot be communicated, and what additional forms of protection (i.e., email encryption) need to be placed on the information if it leaves the company. For California Senate Bill 1386, security administrators need to understand the type of monitoring that must occur and the internal and external communication processes for potential breaches.

Suffice it to say that training issues could easily fill an entire book. The key takeaway related to communications and training is this: Deficiencies in this area are likely affecting you today. As a former IT auditor, I can guarantee I would find security holes in your SAP instance, problems with your change management processes, outdated business continuity procedures, and a host of other issues that could present risks if certain events were to occur. Unlike the majority of these situations, however, the difference with communications and training is that employees doing something unintended today are likely affecting the quality of your information and processes now — not at some potential future date. A perfectly designed SAP system will fail if users do not know how to use it. Poorly trained users will affect other users upstream and downstream and will have a huge impact on business today. Furthermore, poor understanding or use of systems by users can hinder the effectiveness of controls within the SAP system. Don't skimp on training. Switch your focus from "How to use SAP" to "How to do your job right using SAP" — there is a difference.

By recognizing and focusing on the four major themes regulatory issues tend to revolve around — security and confidentiality, data accuracy and integrity, business continuity and recovery, and communications and training — you are well positioned to respond to both current and future regulations.

Use the Right People to Address Your Requirements

By this point, you are probably overwhelmed by the potential impact regulations can have on your SAP implementation. If there is one thing that should be clear, it is that you will need help. You cannot do this alone. You need to expand your project team to include the knowledge and skills to proactively address these regulations in your SAP project.

You will need someone who knows regulations, someone who knows your existing policies and procedures, and someone who knows how SAP will affect them. To address many regulations, you will probably want someone who understands risks and controls. You will also need someone who understands security in an SAP environment.

As for skill sets, a key skill is the ability to produce clear documentation. While all of us are

Increasing the Chances You'll Pass the Audit

As there are a wide variety of audits (Sarbanes-Oxley Internal Control, compliance audit, SAS-70 Service Provider, HIPAA, tax, operational effectiveness, and others), the following steps are not specific to any particular one, but they should apply to any of them.

To successfully weather any audit, remember to:

1. Communicate
2. Evaluate
3. Prepare-uh-ate
4. Facilitate
5. Celebrate!

Communicate

Meet with your auditor beforehand and agree on scope and documentation technique. Define exactly what documentation is required for which audit and agree upon key terminology (i.e., what is considered a "deficiency"). Auditors hate surprises, so make sure you are all speaking the same language.

Evaluate

Understand the business processes covered by your project. Focus your documentation around those processes and transactions determined to be "significant" and "material," per your auditor, based on the type of review.

accustomed to documenting our SAP implementations from requirements through go-live, many regulations require that your documentation live and breathe beyond the implementation. You may think that the documentation you've already produced will suffice, but I recommend against it. Consider additional

✓ ***Note!***

Recognize right away that what will be expected of you will differ depending on the type of audit, the type of regulation, and the particular auditor involved. Two different auditors performing the exact same audit at very similar companies may have two different approaches and two different sets of expectations. Accept this. Complain about it behind closed doors, cry about it over a glass of wine, threaten to expose the whole audit industry for what it is, but at the end of the day, be prepared for an evolving set of expectations with vastly different requirements to make the auditor happy.

Identify and test your internal controls. Internal controls safeguard your systems from waste or fraud, oversee the accuracy and reliability of your financial systems, and ensure compliance with internal policies and procedures, not to mention external laws and regulations. Pay careful attention to those controls that depend upon or affect other controls, as this will affect the design of your testing. For example, SAP Workflow can be a great control, but it depends on the integrity of your workflow authorization tables, which in turn depends on communications processes surrounding employee transfers and terminations.

Address gaps and weaknesses. If you find gaps and weaknesses, and you will, you must either come up with an effective compensating control or remediate the deficiency.

✓ ***Note!***

You never want your auditor to find something you missed, so consider testing more than required.

✓ ***Note!***

Don’t forget to allow time for retesting after changing controls!

When evaluating, there are certain areas that represent potential trouble. They are:

- The process by which you handle exceptions
- Complex, non-routine processes
- Change control (over IT applications)
- Security administration, particularly SAP segregation of duties, transition employees (transferred, terminated, hired), and non-employees such as contractors
- Cross-departmental process changes, such as procurement/accounts payable
- Anything related to system configuration, either SAP or legacy systems

(continued on next page)

documentation written at a higher level and geared toward a non-technical audience that may not be familiar with SAP. The level of detail traditionally created during an implementation often greatly exceeds the level of detail required for an auditor to understand the process. More important, providing too much detail could cause additional questions (which take up both your time and theirs), which may have no bearing on the actual audit itself.

Next, I’ll show you how to package the documentation of your processes in a way that minimizes rework for separate audits and makes the audits themselves as hassle-free as possible (see the sidebar above for some additional tips on improving your chances for a successful audit).

Multi-Purpose Documentation Is the Key to (Relatively) Painless Audits

> *“The issuer must maintain evidential matter, including documentation, to provide reasonable support for management’s assessment of the effectiveness of the issuer’s internal control over financial reporting”*
>
> *– SEC Final Sarbanes-Oxley Section 404 Ruling [emphasis mine]*

If you’re like me, you’ll learn to love the precise, descriptive language in many of these regulations — phrases such as “reasonable support” … “more than

(continued from previous page)

Prepare

This stage takes *your* information, *your* process, and *your* employees and prepares them for your *auditor's* assessment:

- Documentation checklist — have you:
  - ☑ Clearly addressed all elements required by your auditor?
  - ☑ Linked documents, where applicable?
  - ☑ Clearly documented all decisions?
  - ☑ Resolved all open issues?
  - ☑ Documented all key process changes?
  - ☑ Indicated who was responsible for evaluating the results of tests?
  - ☑ Evaluated and classified all deficiencies?
  - ☑ Satisfactorily retested remediation items?
- Systems checklist — have you:
  - ☑ Set up a thorough test environment enabling walkthroughs?
  - ☑ Reconciled the test environment to production?
  - ☑ Established audit IDs and profiles for use during audit testing?
- Employees checklist — have you:
  - ☑ Sufficiently educated employees on their respective business processes and related controls?

inconsequential" … "in the most expedient time possible" … "rapid and timely." So, what documentation should you keep? What qualifies as "reasonable support"?

The average SAP implementation or upgrade accumulates a considerable amount of paper, such as:

- Project plans
- Interview notes
- Exception lists
- Policies and procedures
- Test plans
- User requirements and use cases
- Test plans and test results
- Workflow charts
- Remediation plans

I could list many more, but you get the idea. There are some schools of thought that maintain it's best to keep everything so that no one will accuse you of not having enough detail. Saving everything comes with a price, though: space on your network or in your

☑ Prepared employees for the audit? For example, have you educated them on the do's and don'ts of answering audit questions:

- Do be honest.
- Don't joke around.
- Don't speculate if you don't know.
- Don't exaggerate.
- Don't get angry, but if you do, keep it to yourself (and especially refrain from any sort of inflammatory language in email messages or other published communications).

☑ Held practice walkthroughs?

☑ Practiced communicating potential issues?

Facilitate

This final stage is all about making your audit easy. In a nutshell, it involves packaging your documentation so it makes gathering, understanding, and testing your information easy for your auditor. By focusing on the four major themes of regulatory requirements discussed in the article — security and confidentiality, data accuracy and integrity, business continuity and recovery, and communications and training — you now have a single repository that addresses all potential regulations. Rather than giving the entire repository to each auditor, attribute your controls and process documents to the audits they address. Your auditor may have a checklist or other similar set of standard expectations they are auditing against. Map your documentation to your auditor's checklist, so they can get through their process effectively. As an example, if for Sarbanes-Oxley you have identified 36 control objectives related to IT, and your auditor's standards have them looking at 23 control objectives, provide a mapping from your information to their "view of the world." This may require a database or other similar reporting tool, but nirvana for this stage is the ability to, by regulation, quickly pull together only the documentation and policies that apply to the regulation at hand.

file cabinet, maintenance time, increased time finding what you need, and when you become completely overwhelmed, the need for a project to manage projects, such as the implementation of a multi-million dollar document management system.[1]

The best approach, I believe, is to inventory the types of documentation collected and create rules for each category of documentation. Differentiate between those documents you will require in the short term and those in the long term, and then set retention practices for each. For example, you might separate project documents like this:

- Long term
  - Scoping and decision-making documents
  - Process descriptions
    - Flow charts

[1] SAP offers a management solution that integrates documents, transactions, workflows, and data in a single view. SAP Records Management is available as part of SAP Web Application Server 6.20 and higher, though it is licensed separately. For more information, see the articles "Consolidate and Integrate All of Your SAP and Non-SAP Documents, Transactions, Workflows, and Data with SAP Records Management" (*SAP Professional Journal*, January/February 2005) and "Improve the Efficiency of Your SAP Records Management Implementation with Automated Record Updates" on page 89 of this issue.

10 Common Documentation Mistakes

1. **Failing to understand how all parties will use the documentation.** For example, under Sarbanes-Oxley, your auditor is required to perform a process walkthrough. If your documentation is department-focused and does not easily follow the end-to-end business process, the time and cost of your audit may increase. Talk to your auditors and seek their counsel as to what form your documentation should take.

2. **Forgetting to document what's not documented.** For example, it may be just as important for an auditor to know why you decided *not* to do something as much as why you did it. If you decide not to do something because you determine it's "out of scope," be sure to document that decision. If anything, this shows something was not documented as an intentional decision, as opposed to it being missed or forgotten.

3. **Including poor links between required components (e.g., accounts/assertions/processes/controls for Sarbanes-Oxley).** If your documentation fails to elaborate on how components are related, your auditor will probably ask. And that means more time with the auditors and, almost certainly, higher audit fees.

4. **Overusing hyperlinks or referencing.** This may seem to contradict mistake number 3, but you can over-reference, particularly if you provide links to objects that change over time, such as policies and procedures. Since most audits are of a point-in-time or over a period in the past, if you hyperlink to a policy that changes before the audit, you've lost the ability to show what existed during the period in question.

    + Narratives
    + High-level overviews
    + Risk overviews
  - Control details
  - Test plans and results
  - Conclusions and logic
- Short term
  - Project planning and task-management details
  - Preliminary issues logs
  - Prior versions of process descriptions
  - Meeting and interview notes supporting process descriptions

I'm a firm believer that it is better to be smart and more discriminating about what you keep. Ask your auditing partners, understand their requirements, and map your documentation to those requirements. Since your documentation needs to be sufficient for multiple audits of different regulations, you will have more than necessary for any one specific audit. Your goals should be to:

- Maintain your required regulatory-related compliance documentation centrally for ease of ongoing maintenance.
- Catalog and attribute this information for ease of filtered dissemination of only what is necessary for a specific audit.
- Minimize the amount of redundant information while balancing the need for different views of similar information (i.e., the benefit of having a high-level security overview for Sarbanes-Oxley with very technical detailed overviews for HIPAA security may outweigh the cost of having two different presentations of similar information).

5. **Documenting processes instead of controls.** A process would be, for example, the SAP system generating an exception report. Auditors are more interested in the control, meaning proof that someone actually reviews the exception report and what action they take to resolve identified issues.

6. **Providing insufficient details on controls.** It's difficult to test if control specifics are not known. You should standardize control details, if possible, such as making sure you always use the specific name of the report being used, the role name or transaction code being segregated, the name and location of the Microsoft Excel file used as a control, and the specific action being performed.

7. **Failing to implement reasonable versioning controls.** When you have many iterations of the same document, it can only lead to confusion unless you have a system in place to keep track of the most up-to-date version.

8. **Failing to keep consistent documentation.** If the information in one document differs or contradicts that of another, it will likely increase questions. Set standards for documentation early. This is particularly important for regulations such as Sarbanes-Oxley, where the audit is recurring and your processes may change between audits.

9. **Documenting by department instead of process.** An audit knows no corporate boundaries, so be sure to show the flow of transactions, or, at the very least, link the handoffs between departments.

10. **Failing to agree early on what the final documentation will look like.** Make certain the format you select for documentation meets the approval of all your auditors, both internal and external, or risk headaches throughout the audit.

Remember that the documentation is first and foremost your documentation, and its secondary purpose is to allow you to facilitate the audit. As such, it should be easy for you to manage and maintain, while sufficient to provide the detail requested by an auditor.

Helpful Hints

☑ Switching on your SAP implementation without proper testing, training, or documentation because you are "out of money, out of time" no longer applies. If you have a concern that the controls are just not there and you are about to go-live, you must act. It is no longer responsible to simply give super-user rights after go-live so users can do their jobs, even if you intend to tighten access later. I recommend you use the threat of big penalties to persuade those in charge of your project to increase the budget or resources or push back the go-live date. Your CEO and CFO may be more amenable than he or she might have been before, because now he or she could go to jail.

☑ Customizations can pose a challenge and require careful attention to design and custom configuration documents. Testing of custom functionality also becomes critical and should be properly documented.[2]

☑ SAP systems are not just objects of compliance activities; they can be enablers as well. SAP systems can, for example, enable the rapid disclosure of relevant financial information, such as that required by Sarbanes-Oxley. You can apply SAP technology to monitor access of critical customer information to determine whether it has been

[2] See the article "Test and Manage Your SAP Configuration the Smart Way: Start Using Your eCATT Test Scripts and BC Sets Together!" (*SAP Professional Journal*, March/April 2005) for some pointers on how to do this.

viewed by an unauthorized individual, as required by California Senate Bill 1386. SAP now has a number of compliance-related tools and modules such as the Whistle Blower portal, Management of Internal Controls (MIC), and an improved Audit Information System (AIS).

☑ The responsibility of conforming to laws and regulations falls to every employee, not just IT and the auditors. Consider an ongoing awareness program for all employees, and develop a process to include new and transferred employees as well.

☑ While it may be convenient to have audit-specific documentation, over time maintaining separate repositories will become time-consuming and cost-prohibitive. Look to automated tools such as SAP MIC or other third-party corporate governance systems to serve as a single repository for all your compliance-related activities, and attribute these by regulation to provide for easy reporting and exporting for specific audits.

Have You Hugged Your Auditor Today?

The regulatory environment is not going away anytime soon. Changes to your business are now under greater scrutiny than at any other time in business history, and your SAP system goes right to the heart of your business. Accept it, if for no other reason than you have no choice. Only by understanding how regulations can affect your SAP implementation, and by having the skills and expertise on your project team to address them, can you come to a place where regulations don't control your project but where your SAP implementation can actually manage regulations.

Steven W. Biskie is an assistant vice president for a large insurance corporation, where he focuses on compliance with recent financial regulations. Before that, he ran the Implementation & Process Improvement practice for Jefferson Wells International. Steve is a certified information systems auditor and has held management positions at Deloitte & Touche. He has a Master of Business Administration degree from Michigan State University and is a certified public accountant.

Steve has been involved in implementations for SAP, PeopleSoft, Oracle Financials, QAD, and GEAC SmartStream. He has worked in all areas of the systems implementation process, from initial requirement analysis and application selection through post-implementation troubleshooting and review.

Steve enjoys the widespread appreciation lavished upon those running compliance-related initiatives and hopes to one day graduate to other highly appreciated fields such as IRS auditor, airport security screener, or collections agent. He can be reached at anmsualum@yahoo.com.