How to prepare for an SAP audit: What you need to do to ensure a successful result

by Steve Biskie

Steve Biskie
Founder,
SAP Audit Solutions

Steve Biskie has been involved with governance, risk, and compliance in the SAP market space for more than a decade. He is an accomplished public speaker on the topic of audit and compliance for SAP users. His 15 years of audit experience spans public accounting, private industry, and specialized risk management consulting firms. Steve is the Best Practices Program Director for ACL Services. He is also the founder of SAP Audit Solutions, a company that specializes in helping organizations better prepare for, manage, and recover from SAP audits. You may reach him at steve@sapauditsolutions.com.

Everyone hates an audit. An audit of a company's SAP systems can distract employees from their operational responsibilities, create an environment of conflict, and result in configuration changes, consuming precious time and resources. Worse, some audit findings may require costly rework — with issues becoming increasingly difficult to correct the longer they go undetected. While guidance exists for auditors who review SAP, little guidance exists for the employees being audited. Audit findings are common; fortunately, many could be avoided if employees were better prepared for the audit itself.

This is the first in a series of articles designed to help SAP project managers, administrators, and users understand the typical audit requirements related to SAP and ultimately ready these individuals for their next SAP-related audit. (For simplicity, I refer to audits of SAP systems as SAP audits; however, this does not indicate that the audit is an SAP product.) This article provides an overview of how auditors approach an SAP audit, discusses typical audit techniques, describes the common elements required for a well-controlled SAP infrastructure, and sets the foundation for ensuring success in any type of SAP audit. I also share some simple templates which, if completed and provided to your auditor before the audit, may significantly reduce audit questions and provide the basis for a quick, efficient audit. (You can download the templates for this issue from the Downloads link on the *SAP Professional Journal* Web site at www.sappro.com.)

Future articles will examine event-specific audit considerations (such as implementations and upgrades) as well as SAP module and business process issues (including training and other areas). I'll reveal certain "tricks of the trade" and examine new tools and audit techniques that auditors use to uncover problems. This series will conclude with a detailed discussion of continuous controls-monitoring techniques within an SAP environment and how effective management processes can ultimately reduce the impact of compliance requirements and improve ongoing business operations.

Disclaimer!

While I am an auditor, I am not *your* auditor. Opinions vary widely (even within the same audit firm) as to which areas of SAP are most critical from an audit perspective and how to test them. In addition, very little comprehensive guidance exists in the public domain around SAP audits, risks, and controls. Large external audit firms have internal guides they are sometimes willing to share with their auditees; however, much of the focus of your SAP audit will depend on the specific auditor (and his or her management) responsible for the review.

Throughout this article series, I will attempt to present a balanced, comprehensive overview of key audit issues in and around an SAP environment. Given the complexity of SAP systems and the number of configuration and customization options available, however, it won't be possible to discuss every potential audit concern. This first article should give you a good understanding of basic audit objectives and allow you to apply this understanding to specific issues within your organization. (See the sidebar below to find out why these articles will be important to you and your organization.)

Overview of the audit function

Regardless of the type of audit in which you are involved — SAP, financial statement, operational

Why is this series important?

A common statement among many auditors is that you can apply 90% of audit findings to any organization. While the specific number may be questionable, the sad reality is that audit findings among different organizations (even across different industries) can be very similar. Why is this? Early in my career, I thought that organizations were just complacent and didn't take the time to do things right. Now, I'm of the opinion that much of the problem stems merely from the auditees' lack of understanding and education.

Learning to be an effective auditor can be difficult. Even though my MBA was in professional accounting, my first several years with Deloitte consisted of months of additional training, supplemented by a tremendous amount of ongoing coaching and mentoring. By the time I reached manager level, I was able to effectively apply audit and control concepts to processes with which I had never worked. Reaching this level of competence, however, required years of formal development. Contrast this to the typical auditees who likely have no formal audit training and whose sole understanding of audit concerns comes from being written up on their last audit. It's no wonder that we in the audit community find many commonalities in audit issues. Historically, we haven't taken the time to educate our auditees not only on what the audit will cover, but also on why and how these items relate to the organization's risks.

This series is written for you: the SAP user, administrator, support staff, and other non-audit personnel. Rather than being written for auditors, this series is designed for those of you who may find yourselves on the receiving end of an SAP audit. My goal is to help you avoid many common audit findings and allow you to have better, more productive discussions with your auditors. As an outcome of this increased knowledge and understanding, future audit processes will hopefully take less of your time, be less painful, and result in value-added findings that can help you and your business. You may never be able to make your auditor smile, but you may surprise management with fewer findings, a more cooperative audit process, and lower internal and external audit costs. If you're lucky enough to be in an organization where your bonus is tied to audit findings (or the lack thereof), perhaps this advice can positively affect your personal bottom line as well.

efficiency, or any other variation, the common thread to any audit is the *auditor*. Auditors are bound by a common set of rules, and those rules govern how they conduct an audit. To be effective at an SAP audit, therefore, you must first understand the characteristics specific to any audit.

Contrary to popular belief, an auditor's goal is not to cause problems. Conversely, an auditor aims to identify where potential problems might occur or have occurred and communicate sufficient information to the "interested parties" so they can make informed decisions. Each of these interested parties may have different concerns relative to the process or system being audited. Thus, the nature and extent of the audit may take on different characteristics depending on the type of auditor involved. At a very high level, auditors generally fall into one of two categories: *internal auditors* and *external auditors*. There is also a wide variety of *specialty auditors*, who provide services in specific audit disciplines.

Internal auditors

The goal of internal auditors is to protect management and the board of directors. Most internal audit functions report to the audit committee of the company's board of directors, although many also report administratively to the chief financial officer (CFO). Internal auditors provide the board of directors with valuable information about the company's operations that the board may not receive directly from management due to biases, lack of objectivity, or merely a desire to look good in the eyes of the board. As a result, the internal audit function provides a system of checks and balances so the board of directors can better ensure that its directives and objectives are being carried out appropriately.

Companies employ internal auditors; however, they may not always be on the company's payroll. Smaller organizations, in particular, may choose to outsource the internal audit function to a third-party provider. Even larger organizations may choose to supplement an existing Internal Audit department's knowledge and skills, particularly in specialty areas such as SAP, through the use of outside resources — often called *co-sourcing*. Regardless of who actually pays the specific auditor's salary, your organization ultimately employs the internal auditor. Most importantly, internal audit reports are primarily for use inside the organization and are rarely distributed to external parties. This is an important distinction between internal auditors and external auditors; I'll discuss this topic next.

> ***Note!***
>
> Remember that acting in an internal audit capacity and performing internal audit functions is independent on where the auditor is employed. Some organizations choose to outsource or co-source the internal audit to a firm that also performs external audits. To maintain independence, you cannot outsource your internal audit function to the same audit firm that you use for your financial statement audit, but you may have someone employed by an external audit firm (e.g., Deloitte, PriceWaterhouseCoopers, etc.) functioning in an internal audit capacity. In this case, the auditor's reporting and objectives would align more closely with those described in the section "Internal auditors" than those in the section "External auditors."

External auditors

When most people think of external auditors, they think of the financial statement auditor, typically employed by a large accounting firm, which voices an opinion on the integrity of a public company's financial statements as part of the year-end financial reporting process. For the purposes of this series of articles, I refer to external auditors in a more inclusive way as consisting of the various types of auditors an organization may encounter that it does not ultimately employ.

Although external auditors may review their reports with management and the board of directors, their true goal is to protect investors, customers, or other interested external parties. Just as an internal auditor provides the board with objective information that it may not receive directly from management, external auditors provide external parties with information and insights that the organization may not make directly available.

The most common type of external auditor is the financial statement auditor. In the United States, the organization being audited pays the accounting firm creating a lack of pure independence, which arguably has resulted in some of the accounting scandals seen in recent years. However, in these cases the external auditor officially represents the interests of the investor (i.e., company stockholder). External auditors may also represent banks and report on issues such as compliance with loan covenants. They may represent governmental agencies (tax authorities, for example) and report on a company's compliance with specific laws and regulations. Certain industries, such as financial services, pharmaceuticals/chemicals, and utilities, may have industry-specific auditors who are charged with reporting on compliance to a governing entity.

Depending on the nature of your business, you may also have external auditors who report to your customers. Customers may include a right-to-audit clause in their contracts, particularly related to services such as outsourced IT or human resources/payroll functions. Depending on the specifics of your contract with the customer, it may periodically send a team of its own auditors into your organization to review a specified function. For organizations that perform services-related functions for a large number of companies, the desire by customers to periodically audit these services-related processes can become particularly burdensome (imagine if each of your customers decided to send in its own audit team to audit your SAP system; see the sidebar on the right). As a result, some companies may choose to hire an independent audit firm to issue a Statement on Auditing Standard 70 (SAS 70) report. Depending on the circumstances, customers may use this report to verify the effectiveness of operations instead of sending in their own audit teams to perform independent audits.

Despite the wide variety of external auditors, one important fact remains constant: Reports from external auditors are issued outside the walls of the company. Although some external auditors may provide additional value-added recommendations for your organization's management (e.g., suggestions for improving your SAP system that were observed during the audit but are not relevant to it), the ultimate audit report is issued externally. For certain types of audits, such as those your financial institution or a customer conducts, the distribution of these reports may be limited to specific organizations. For a financial statement audit, the final reports may be issued to the public as a whole and, thus, be accessible to everyone, including your competitors. While it's always important to work with the auditor to ensure that the report of findings is relevant, factual, and fairly stated, the distribution of external audit reports makes this cooperation an even greater concern. (I'll discuss negotiation issues with your auditor later in this article series.)

Specialty auditors

Both internal and external auditors often specialize in different audit disciplines. A typical internal audit department may have multiple specialists, with some auditors focused on financials and reporting, others focused on operational efficiency, some examining technology, and still others dealing with investigations and fraud. Depending on how the audits are conducted, you may be subject to multiple audits, each with a different focus. Many audit departments are moving toward more integrated audits, where one audit may combine multiple disciplines. This helps to save time and may reduce the auditee's "pain factor" as well.

Some auditors, typically called *IT auditors*, specialize in auditing technology. IT auditors may specialize in a subset of technology, such as networks or firewalls, although many IT auditors are technology generalists. There are also auditors who specialize in auditing SAP systems. In general, the more specialized the auditor, the higher the internal/external cost, and thus the more likely it is that your organization won't be able to afford these services full time.

Differing audit objectives

There are many different types of auditors and audits, and there are also many different types of audit objectives. A common internal control framework known as COSO, based on a 1992 report from the Committee of Sponsoring Organizations (COSO) of the Treadway Committee (www.coso.org), classifies an organization's objectives as falling into one of four categories:

- **Strategic:** High-level goals, aligned with and supporting the company's mission
- **Operational:** Effective and efficient use of resources, including safeguarding of assets
- **Reporting:** Reliability of public reporting
- **Compliance:** Compliance with applicable laws and regulations

My auditor doesn't know anything about SAP!

Have you ever been frustrated by the feeling that you know more about SAP than your auditor does? The reality is that you probably do. You know more about how your SAP system has been set up and how your organization is using it, and you probably use SAP more frequently than your auditor does.

Having said that, you may find situations where your auditor has little to no SAP experience at all. Perhaps your auditor is merely following a standard SAP audit checklist and is unable to identify those areas that do or don't apply to your organization or your specific SAP environment. Maybe your auditor does have SAP experience, but it is in a different module and he or she doesn't understand the configuration of the module being audited. In fact, frequently those individuals auditing SAP systems have limited SAP audit experience.

As much as you may not like it, the reality is that this situation is unlikely to change. Given the complexity of SAP, the number of configurable variations, the differences between modules and industry-specific functions, and the ongoing improvements SAP is releasing, it is unrealistic to expect that any auditor could truly be an SAP expert. Even SAP's own personnel may be strong in some areas of SAP functionality (e.g., SAP security), but have limited exposure to specific control-related functions (e.g., stochastic invoice-blocking within the Purchase-to-Pay cycle). In addition, even where an "expert" team of auditors could be pulled together, few organizations are willing to make the financial investment it would take to use such a team throughout all phases of the SAP audit.

The good news is that a good auditor, even one with no exposure to SAP or other ERP systems, can perform a successful SAP audit. I've been educating auditors and non-auditors alike for almost a decade on techniques for auditing SAP and other ERP systems. As previously discussed, it is impossible for any given auditor to be an expert in all audit and control aspects of SAP. The key is to understand how SAP works in a general sense and to learn to apply traditional audit techniques to the SAP system and related processes. Good auditors are like good private investigators; they know what questions to ask! Good auditors learn to pose the important questions to the SAP specialists already within your organization and adapt the audit appropriately based on their responses and an independent validation of the data within your SAP system. Of course, if your own organization doesn't understand how SAP has been configured to mitigate your organization's risks, that's an inherent problem, isn't it?

Unfortunately, not all auditors are good auditors; not every auditor has been educated on the fundamentals of auditing in an SAP environment; and a bad auditor or a bad audit process can have a significant impact on your time and other organizational resources.

Figure 1 provides some examples of audit objectives that can result in an SAP audit and the typical audience who would be the consumer of the related audit report.

Considering the number of different types of auditors and the wide variety of potential audit objectives, is it any wonder that some SAP audits look very different from others? Depending on the context of the audit, something that's important for one audit may be irrelevant to another. For example, consider an SAP security audit. If that audit is part of a Sarbanes-Oxley review, then the assessment will likely focus on segregation of duties (SoD) rather than key functions related to financial reporting, as well as some basic SAP security administration and management controls. If the SAP security review is part of a HIPAA privacy audit, however, there will be a heavy emphasis on the

Category	Audit focus	Audit objective	Audience
Strategic	Selection / implementation	Ensure SAP is configured to support the organization's strategic objectives	Management
	Long-term planning	Validate the long-term SAP planning processes to ensure the system will continue to meet the organization's objectives over time	Management
Operational	Project management	Assess the management of the SAP implementation for efficiency and effectiveness, and review the accuracy of project status and other communications	Management
	SAP processing	Ensure SAP processing effectively supports the integrity of customer processing and related service level agreements	Customers
	Change control	Ensure that all changes to SAP are appropriately approved, designed, configured, tested, and QA'd prior to movement into the production instance	Management, customers, regulators
	Help desk & support	Ensure the processes that support SAP effectively identify and resolve issues and proactively identify trends and resolve the root cause of problems	Management
	Pricing	Ensure the pricing processes and practices designed within SAP support management's profitability goals	Management
Reporting	Financial reporting	Ensure the reliability of financial reports generated from SAP or created using information within SAP	Investors
	Tax	Ensure SAP tax calculations, related processes, and tax-reporting sufficiently and accurately represent your tax liabilities	Management, regulators
Compliance	Sarbanes-Oxley	Verify that controls within and processes around the SAP system support Sarbanes-Oxley compliance	Investors
	Privacy	Review compliance with HIPAA, GLBA, and other privacy-related regulations, and ensure that access to key SAP transactions and data is appropriately restricted	Management, regulators

Figure 1 Sample categorizations for audit objectives

ability of the users to see sensitive information, the encryption of that data (both in an SAP system and in transit between SAP and other systems), and the processes for identifying protected information. The key takeaway here is that success (or failure) in a prior SAP audit does not necessarily relate to success or failure in a future SAP audit.

Auditing principles

Before getting into the actual auditing of SAP, you should understand some key auditing principles. These principles often "require" auditors to behave in ways that seem foreign to employees who are new to the audit process. Understanding these auditing principles enables you to better prepare for and react to your audit.

Professional skepticism

Have you ever felt that no matter how many years you've worked with an auditor and how forthcoming you've been in previous audits, you just can't seem to get the auditor to trust what you're saying? The reality is that per audit standards, they cannot trust what you say. Auditors are required to operate in a mode of *professional skepticism*. This means that an auditor cannot merely "trust" what someone says and must gather additional evidence to support (or potentially refute) what he or she has been told. Specifically, auditors must operate in a neutral position on a scale where trust is at one end and distrust is at another. As such, an auditor's beliefs (or the beliefs of the individuals with whom the auditor is working) should not influence the audit's outcome. Audit evidence must stand on its own and support the conclusions of the audit.

Initially, this standard may seem harsh, but I've seen first hand how a lack of professional skepticism can have a serious impact on an organization. I worked with a company a number of years ago that highly regarded one particular employee for that person's ability to reconcile SAP general ledger accounts during period-end. This individual typically had the fewest number of outstanding reconciling items and comparatively few dollars outstanding at any given point in time. In fact, management began relying on this person to coach others in how to effectively reconcile SAP-based accounts. It wasn't until after an audit, however, that this person's true success mechanism was revealed. After working with many of the larger reconciling items, once this person got close enough (relative to the overall account balance, which was a sizable number), this person merely created a journal entry to clear out the remaining items. In essence, this "SAP reconciling superstar" only seemed like a model employee on the surface.

You may wonder from this example how professional skepticism fits since it was an audit that caught the problem. In this case, the auditor used professional skepticism during the audit, which is *why* the individual's actions were detected. Management had failed to be professionally skeptical during its review processes. Surprisingly, management had approved this person's work for years prior to identifying the problem. The organization had a process whereby managers were supposed to review the reconciliations of each employee to ensure accuracy. Unfortunately, this individual's manager did not operate in a neutral position on the professional skepticism scale. Instead, the manager trusted the integrity of the person's ongoing work based on results that had appeared reasonable in the past.

As a result of this lapse in judgment, the organization lost a sizable amount of money, a large effort was required to go back through history and clean up the mess, and management was left looking foolish. I encourage every manager (not just those within the internal audit department) to apply professional skepticism in his or her work as well. Review the work of your SAP developers, periodically assess the accuracy of your SAP security setup and maintenance processes, and determine whether those employees who review SAP exception reports follow through appropriately on identified items — whatever your role, spend some time validating your own assumptions about performance.

Note!

I don't recommend that you completely distrust every employee. Professional skepticism isn't about distrust; it's about neutrality. Clearly, you should spend more effort reviewing the work of those employees who have proven to be inaccurate, careless, or otherwise problematic. Newly trained employees may also warrant more attention than seasoned employees. What I am suggesting is that you should not ignore reviewing the work of even your most trusted staff. Although you may not review everything they do, you might consider periodically examining a selection of their work products to ensure that your trust in their performance is based on reality and not on a historic perception that is no longer accurate.

Evidence

Another principle that can cause problems during an SAP audit involves the concept of evidence. For audit purposes, evidence must stand on its own; this means that an independent auditor looking at the same information would come to similar conclusions regarding the test results. To some extent, maintaining evidence supports the concept of professional skepticism.

For example, some companies that have to comply with the U.S. Sarbanes-Oxley Act may be shocked when their external auditors issue a significant deficiency simply because someone didn't sign a document, even though they performed the related review. Some auditors even go a step further by declaring, "If you can't prove it, it didn't happen." This may seem a little extreme, but the reality is: If you don't have sufficient evidence to prove something, then an auditor cannot independently attest that it happened. Therefore, a "lack of sufficient evidence" during an SAP audit becomes an audit issue itself. Beyond resulting in the auditor being unable to attest to the adequacy of audit results, a lack of evidence also begs the question of how the auditor can assure management that things are happening as intended. As in the previous example, if management merely trusts employees to perform as expected, this can raise broader audit concerns around the effectiveness of the control environment that management has established. In short, evidence should exist that processes are indeed operating as management intends — for audit purposes as well as for management. (See the sidebar below for information on various electronic forms of evidence.)

Understanding the audit

Before examining the parts of a typical SAP audit, let's discuss several common auditing techniques and processes.

Electronic evidence

Many people, particularly those in IT, dislike the "paperwork factor" often associated with gathering, maintaining, and keeping track of evidence. However, evidence can also take the form of electronic evidence. The key to effective electronic evidence is to have appropriate controls that ensure: a) the "who" (e.g., originator, approver) is the person you believe it to be; b) the evidence hasn't been changed or modified in any way from its original state; c) the data contained cannot be wholly or partially removed; and d) the evidence can be appropriately associated with whatever is being used to prove it. Of course, you should also be able to find and retrieve evidence when you need it — hence, sometimes it may be easier to maintain hard copy documents in easily accessible files unless strong electronic document management procedures are in place.

Risk-based auditing

The scope of many audits these days is often determined by applying a risk-based approach. Many different approaches comprise the details of risk-based auditing, but fundamentally this technique focuses more attention on those risks specific to your organization that are more likely to occur or affect your organization than those that are not. Using an SAP example, an insurance company using both SAP's Treasury module and SAP's Projects module may find that significantly more attention is placed on SAP Treasury while potentially little-to-no attention is put on SAP Projects. This makes sense because the risks in an insurance company typically center more on cash and the tracing and flow of money than around projects. Conversely, if a company's primary business is construction, it may find that its SAP audit has the exact opposite focus, with far more attention being paid to SAP Projects than to SAP Treasury.

Thinking like an auditor

Learning to think like an auditor is actually one of the best things you can do to prepare for, and ultimately survive, an SAP audit. You may think your auditor is cynical or pessimistic, but in reality, there is simple logic behind most audit concerns. The key lies in continually asking, "What could go wrong?" then evaluating that answer, and asking, "What else could go wrong?" Considering risk-based auditing, you should then gauge the impact and likelihood of the event or issue to determine whether it warrants attention and investigation. (Not every audit is risk-based, however, so at times your SAP auditor may be concerned with issues that don't seem likely to occur or to greatly affect your business.) For the items deemed important enough to warrant further consideration, you should then think, "Given that this could go wrong, what do we need to do to prevent this event from happening or to detect it in a timely fashion if it does?"

The issues that can cause problems in an organization tend to fall into several buckets, so you may see audit objectives centered on themes such as: validity, accuracy, completeness, timeliness, relevance, and recording. Asking the "What could go wrong?" questions in the context of these categories can be particularly helpful to ensure that you've appropriately addressed all the risks in your SAP system. Here are some examples:

- What could cause a payroll adjustment in SAP to be invalid?
- What could make checks cut from SAP have inaccurate amounts?
- What could result in the information you use to calculate liabilities incompletely?
- What could cause goods receipts not being entered into SAP and processed in a timely fashion?
- What could result in the information used to determine write-offs being irrelevant?
- What could lead to sales being recorded in the wrong period?

For each of these questions, you would then list the possible causes along with the impact and likelihood of occurrence for your organization. Regarding the question, "What could cause goods receipts not being entered into SAP and processed in a timely fashion?" a partial list of potential causes and their impact might include:

- Goods were received in the warehouse but not entered into SAP within the 24-hour corporate policy standard (high likelihood, low impact for parts; moderate likelihood, high impact for equipment)
- The receipts file transmitted nightly from warehouses running non-SAP systems was not received (low likelihood, moderate impact)
- The receipts file transmitted nightly from warehouses that are running non-SAP systems was not processed in SAP (low likelihood, moderate impact)
- Third parties that received and stored goods on behalf of the company did not submit a file for processing within corporate guidelines (high likelihood, low impact)

Finally, you should have enough processes to ensure that you either prevent these potential causes or detect them in a timely fashion if they occur. These processes may differ by type or category. Considering the first potential cause, you might have:

- **For goods of type X:** RFID tags automatically update SAP inventory records upon receipt into the warehouse (preventive)
- **For all goods (both type X and not-X):** All employees whose job responsibilities include entering or transmitting goods receipt information must periodically (at least once per year) sign off on compliance with receiving policies, which dictate that all receipts must be entered into SAP within 24 hours (preventive)
- **For all goods (both type X and not-X):** Every week, managers review reports of invoiced items that have not been received and they investigate items that have been outstanding for more than Z days (detective)
- **For all goods (both type X and not-X):** Physical inventories should be performed quarterly and inventory adjustments made in SAP based on the actual physical count (detective)

Of course, just being able to list preventive or detective processes is not enough. You need to show that these processes would prevent errors above a cumulative magnitude that would cause concern to key stakeholders (management, suppliers, investors, etc.), or detect such problems with sufficient time to correct them before uncorrected errors would cause stakeholder concern. You can see from the example that this organization relies primarily upon detective controls for goods receipts that are not of type X. Although they do have a preventive control listed, it is fairly weak; this organization, like others, has periodic employee performance problems. You need to determine whether your controls are sufficient to reduce the overall risk to an acceptable level. Upon evaluation, you may determine that you need to increase the frequency of certain controls or add additional controls. I'll spend a lot more time on the principles of designing effective controls in SAP in a subsequent article.

Applying audit investigative techniques

I like to think of the auditing process as being similar to the scientific process. In science, you have a theory that you work to prove. In the audit investigative process, you can consider the controls (each of the processes you identified that would prevent or detect the potential problem from occurring) to be management's theories.

The auditor attempts to gather evidence to prove — or, in many cases, disprove — management's view of the effectiveness and reliability of these controls. The auditor looks at the design, determines whether it is operating as intended and whether it would mitigate risk to the desired level. Once the auditor is comfortable with the design of the control, he or she reviews its operation to determine whether it is performing as intended. Throughout the auditing process, the auditor gathers the evidence that supports the conclusion.

> ***Note!***
>
> I should point out that, in contrast to the scientific process, the auditor is not looking for absolute proof. Most audits operate in a way to statistically target a 95% confidence level.

There are generally four different types of evidence that auditors gather during the course of their SAP review, as follows in order of reliability (see **Figure 2**). The first is *corroborative inquiry*, which seeks to ensure that the people interviewed (formally or in casual conversation) during the audit share the same beliefs. The second is *observation*, in which the auditor observes whether the intended process occurs consistently based on how the auditor sees people or systems performing their required actions. During the *examination of documentary evidence*, the auditor looks for other indications (such as paper trails or details within electronic transaction records) to further validate the consistency and integrity of the process. The final type of evidence is *re-performance*, in which

the auditor independently performs all or part of the action (review, calculation, data extraction, etc.) and compares his or her results to what actually occurred. Auditors often perform a combination of these techniques to increase the level of assurance.

Knowing these evidence-gathering techniques can be useful as you prepare for your SAP audit. I described how auditors really attempt to prove or disprove management's theories. There is certainly no reason why you can't (or shouldn't) do the same before your own audit. Let's talk about how each of these techniques could be applied to investigate one of the controls identified earlier: "Every week, managers review reports of invoiced items that have not been received and they investigate items that have been outstanding for more than Z days."

Remember the concept of professional skepticism when performing these and similar tests in your SAP environment. If you can get in the habit of thinking like an auditor and applying audit techniques to your everyday processes, you can significantly reduce the pain and duration of your SAP audits.

Example test	Questions or investigative tools
Corroborative inquiry	• Discuss the process with the managers responsible for reviewing the invoiced-not-received report in SAP. • Determine how frequently the managers are reviewing the report. • Determine whether actions taken as a result of the review are appropriate and who else (e.g., receiving dock employees, vendors, etc.) is involved in those actions. • Assess whether the managers are following company policy based on their description of the process and the report. • Have discussions with the other people involved in these actions to determine how frequently they have been contacted, and to assess whether this is appropriate given the frequency of items appearing on the report.
Observation	• Ask to watch the managers review the report. Observe whether they select appropriate items for follow-up. Also, observe how readily they navigate to the correct report in SAP and whether they appear familiar with the report's contents. • If possible during the course of the review, attempt to observe other instances in which the managers are reviewing the report (when they may not be aware you are observing).
Examination of documentary evidence	• Review for report sign-off, tick marks, or other evidence of review on any available hard copies of the report. • Review emails sent to other parties for follow-up or meeting minutes discussing issues resulting from the review. • If security settings allow it, review in SAP the last date the managers executed the SAP transaction that calls the report, and determine whether it is consistent with how frequently they should be reviewing the report (e.g., using Reverse Business Engineering [RBE] in versions prior to SAP R/3 4.6).
Re-performance	• At various dates, review the SAP report of goods invoiced but not received and determine which items, based on policy guidelines, should have follow-up. • For these items, follow the same evidence-gathering techniques to determine whether appropriate follow-up occurred (e.g., discuss with receiving dock employees, look for supporting emails, etc.).

Figure 2 Tests for gathering evidence

Overview of the typical SAP audit

Now let's talk about the typical SAP audit. Given the different types of auditors and different types of audits, a "typical SAP audit" is a bit of a misnomer. That being said, after years of SAP auditing I tend to classify components of a review into five major buckets: Project management and system administration, General Computer Controls (GCC), SAP Basis settings and security, SAP module-specific technical settings, and the business processes enabled by an SAP system.

I'll look at each of these briefly here and then discuss them in more detail later in the article.

Project management and system administration

The project management and system administration category looks at how you select, install, and make upgrades to SAP components and in general, ensure that SAP is meeting the needs of your business. When auditing in this category, I would look at issues such as how you determine the appropriate tolerance settings for SAP configured controls and ensure that they are reflected in your SAP system. This category is specific to the things you do to make sure SAP works well for your business, both in the present and in the future. In my mind, this category is more about strategy, management, and execution than about SAP or IT specifically. I generally refer to this layer as the foundation layer for the SAP audit. I'll discuss the whole area of implementing, upgrading, and managing SAP in a later article in this series.

General Computer Controls

GCC is a term used in the information systems auditing profession; it reflects a standard set of higher-level IT management, infrastructure, and process controls that should be in place to support the effective operation of any system (SAP included). This category of controls would generally look at broad issues that are not SAP-specific but would be considered in the context of SAP for an SAP audit) such as interface management, troubleshooting and support, network infrastructure, business continuity, and security administration at the network and infrastructure layers. While some of these areas may not be under the influence of employees who work directly on SAP systems at these levels, the effect that these processes have on the reliability of SAP systems is significant and, therefore, can be a large part of a comprehensive SAP audit.

> ***Note!***
>
> Depending on the framework used, the project management and system administration category I define may be included in the GCC area. For the purposes of communicating the SAP audit in a way that makes sense, however, I prefer to break project management and administration out as a separate category.

SAP Basis settings and security

This category generally addresses SAP settings that are not module-specific. It is concerned with powerful administrative functions such as backups, archiving, and mass maintenance. This category also puts significant emphasis on global security settings, such as minimum password length, passwords for default SAP accounts, log off and locking parameters, and other settings that provide the foundation of SAP's powerful security model.

SAP module-specific technical settings

This category is similar to the Basis category, but addresses those settings specific to an SAP module, such as PP (Production Planning), FI (Financials), or SD (Sales and Distribution). Audit steps in this category typically look at specific configuration settings

and defined tolerance levels to determine whether they are appropriate (e.g., examining the configured release strategy and related authorization limits for purchasing). Security in this category is primarily concerned with sensitive transactions/authorizations for that process (e.g., the ability to change vendor bank account information), as well as segregation of duties (e.g., separation of the ability to enter an invoice from the ability to approve the disbursement of funds). Depending on the extent of the SAP audit, this could be a detailed audit or a high-level audit. In subsequent articles, I'll examine a number of SAP modules in detail and the typical audit considerations associated with those modules.

Business processes enabled by SAP

The final category in a comprehensive SAP audit deals with the business processes that SAP enables. To a large extent, this set of audit procedures deals less with how you set up SAP and more with how employees use SAP in practice. In my opinion, while a lot of auditors tend to focus on the earlier categories I discussed, the most significant and critical findings can occur in this category. At this level, I am no longer predicting what could happen based on how you configure or manage your SAP system, but rather you deal with what happens currently and how it affects the business. Findings may exist where SAP is technically configured "correctly," but employees misuse functionality because they either lack understanding (training and development), require a defined process (policies and procedures), need ongoing guidance/coaching (management monitoring), or are consciously attempting to circumvent the system (fraud and abuse). Audits covering this category would find, for example, employees in accounts payable using sundry invoice processing (which needs to be enabled to pay certain invoices such as utilities and services) for payments that should go through SAP's three-way match process. Although findings in this area may not be the fault of employees supporting SAP, the SAP support function can often assist by helping management proactively identify these issues and define additional monitoring routines.

How these five categories fit together

Notice that the image in **Figure 3**[1] is shaped somewhat like a pyramid. I like to picture the components of an SAP audit in this way because a pyramid shape

[1] Copyright SAP Audit Solutions, 2007.

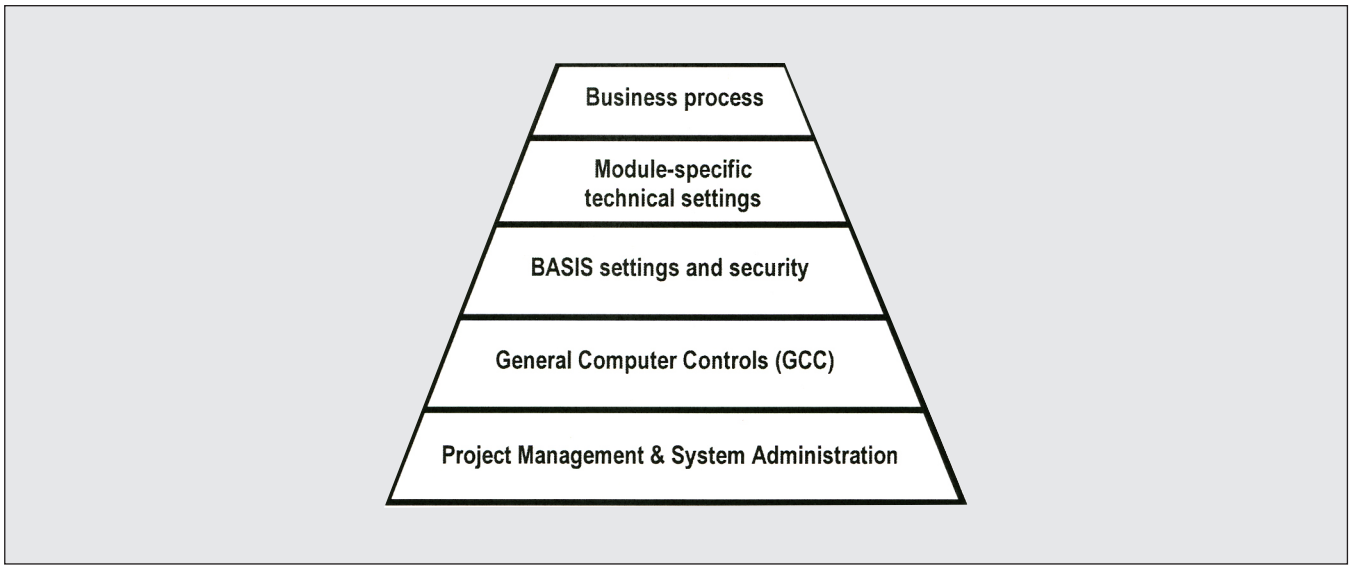

Figure 3 The relationship between the components of an SAP audit

illustrates how the lower categories support the upper ones. For example, having authorization limits set in SAP is a good start, but if you don't configure SAP security to enforce reasonable security measures at the Basis level, then it's difficult to ensure that a user and an approver are who they say they are. Similarly, if appropriate processes do not exist within the GCC environment to monitor interface processing, SAP may be processing accurately against an incomplete (and therefore incorrect) set of transactions. Finally, if you don't appropriately coordinate SAP changes with the applicable business areas, a change that seems minor may have unintended consequences and result in inappropriate decisions based on a faulty interpretation of the data. From an audit standpoint, the auditor must ensure that reasonable controls exist at the lowest levels of the pyramid before spending too much time on the upper levels. There's no point in checking the deadbolt if the back door is wide open!

The pyramid also helps prioritize audit work when time and other resources are scarce. In a perfect world, the auditor could fully validate every control setting and process within SAP. Given the complexity of SAP and the number of possible settings, however, this is a practical impossibility. If evidence can show that the right people are involved in SAP-related decisions, sufficient testing occurs for all changes, an overall control mindset pervades the organization, similar control foundation-related elements exist, and auditors can be more confident that the specific details are taken care of without having to examine each of them exhaustively.

The GCC audit

Now that you've had a fairly thorough overview of the audit process, it's time to dig into the specific details of an SAP audit. I'll discuss other components of the SAP audit in detail in subsequent articles, so for the remainder of this article I focus on just the GCC component.

You are likely to encounter some type of GCC assessment during every SAP audit. I already described how GCCs support the controls and effective processing in SAP. GCCs are also common to every system audit, regardless of application type; thus, most technology auditors, even those relatively new to the field, become quickly comfortable with assessing GCCs.

The most common IT control framework addressing GCCs from an audit perspective is called Cobit. It is published by the IT Governance Institute (a spinoff of ISACA, the leading organization for IT auditors). If you are really interested in understanding the GCC audit, I'd recommend you spend some time reading at least the Cobit summary documents (www.itgi.org). Cobit itself has multiple manuals, so it would be impossible to summarize it effectively here. Instead, I'd like to focus on some of the areas that, based on my experience, seem to be the most problematic for organizations. While a GCC audit covers more than policies and procedures, security, and change control, you can survive some of the more painful parts of a GCC audit with the tips that follow.

Policies and procedures

- **Have a formal exception process:** You can't always follow policies and procedures, so you should have a formal, defined process for approving exceptions to the policy, and document each approved exception. This shows the auditor that you are aware and have made a conscious decision about how to address the related business risks.
- **Periodically communicate and revalidate exceptions:** Having an exception process alone is not enough, particularly in an organization with employee turnover. The risk tolerance of new management may not be the same as that of previous management. In addition, advances in technology may allow you to address your risks more effectively now. Finally, the costs of compliance may change over time, resulting in a need to re-evaluate exceptions to management's defined processes.
- **Periodically self-audit against your policies, and update your policies (or approve exceptions) if they don't work for your business:** One of the

easiest findings for an auditor is determining where settings and processes don't match corporate policy. For example, if your security standards say that all passwords must have a minimum length of 10 characters and be changed every 30 days and your SAP security settings in report RSPARAM show SAP set at 9 characters and 40 days, you have an audit exception. It doesn't matter that 9 characters and 40 days may arguably provide very strong security. The mere fact that SAP doesn't match your corporate policy and no exception has been documented is an issue.

Security

- **Validate user access against a SoD matrix**: Every organization should have an SAP SoD matrix, defining capabilities that should not be granted in combination to a user (e.g., entering vendors and approving vendor disbursements). Management should validate this matrix periodically, and each capability should be mapped to its respective transactions, authorizations, and authorization objects so that SAP security personnel can effectively identify which users have which capabilities. In addition, you should check user capabilities for SoD conflicts, as well as any change to profiles and profile assignments, upon initial setup. SAP Governance, Risk, and Compliance (GRC) Access Control can greatly enhance an organization's ability to check its SoD issues.

- **Change SAP default passwords:** Hopefully, this is not a risk for your organization; however, verifying that default passwords have been changed is on every IT audit checklist. Pay particular attention to IDs such as SAP*, DDIC, SAPCPIC, EARLYWATCH, and (in some systems) TMSADM.

- **Restrict privileged access requiring only periodic use:** At times, you may need to give certain individuals access to transactions and other SAP capabilities they may not typically need (or that they should not have, given typical SoD requirements). For example, a programmer may need emergency access to SAP production to fix a time-sensitive problem. Rather than granting privileged access as part of the user profile definition (risking that these privileges could be used when not intended by management), provide a means to grant access only when needed, and audit the access actually used. SAP GRC Access Control has some useful features for enabling this that are better than historical means.

Change control

- **Use standard forms, which require consideration of security and control elements for all SAP changes:** Good business practices suggest that you consider security and control requirements for every system change. For example, when creating a custom transaction in SAP, how does it affect SAP workflow? Does the transaction create the potential for any SoD concerns? What edit checks and tolerances should be addressed to validate user input? Requiring that security and control elements be considered on the change request form ensures that they are checked consistently.

- **Maintain a pretransport checklist to ensure that you gather sufficient support prior to implementation:** Earlier in this article, I mentioned the importance of retaining evidence. The change control process includes many evidence-related items important to an auditor — from the initial change request and requirements through approvals, testing and quality assurance results, and ultimately the go-ahead for transport into production. Since any of these areas could be required for audit support, it's a good practice to make sure they are all gathered with appropriate signatures and support prior to moving any change into SAP production.

- **For emergency changes, complete skipped steps post-implementation:** Every organization experiences emergency changes, where you must move code into production more quickly than through the standard change process. Emergency changes often involve less up-front diligence to streamline

the process, and some may completely bypass controls. Following up after the change to ensure the emergency change meets production standards is critical to satisfy audit requirements. In addition, be sure to inform affected business management of the emergency change so they can monitor operations for potential impact.

- **Develop test plan details commensurate with the complexity of the change and experience of those involved in testing:** Some changes are less complex than others. For example, adding a field to a report has potentially less inherent risk than changing the essence of a calculation, but you should test even simple changes. However, the complexity of the change isn't the only factor that should affect the level of detail in the test plan. Some testers may be more familiar with SAP testing procedures than others. Your test plan should consider both the complexity of the change and the experience of the testers to provide better assurance that testing is effectively catching the issues it is meant to catch.
- **Resolve unsuccessful tests prior to go live:** Although this may seem obvious, as an auditor I've seen situations all too frequently in which organizations did not fix every problem identified during testing prior to approval and transport of the change. If management has been appropriately informed and accepts the risk associated with a test failure, document this information thoroughly — not only for audits, but also for troubleshooting and problem resolution if issues occur later.

Conclusion

In this article, I've discussed auditors and the audit process. I've highlighted the primary categories of an SAP audit, and provided tips on some of the more problematic areas within one of these categories — the GCC audit. I hope you have a better understanding of how an SAP audit works and have the knowledge to help shore up certain components of your SAP infrastructure prior to your next SAP audit.

Stay tuned for future articles in which I will provide much more detail on other areas of an SAP audit, including implementations and upgrades, module-specific settings, and audit tools and tricks.

