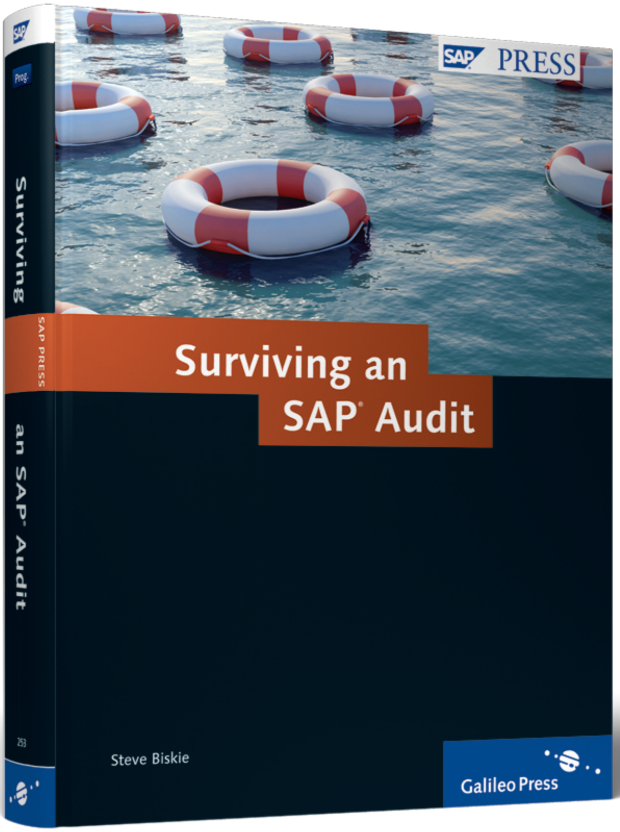
Steve Biskie

Surviving an SAP® Audit



Galileo Press ®

Bonn • Boston

Contents at a Glance

Contents

"You can discover what your enemy fears most by observing the means he uses to frighten you." — Eric Hoffer

1 Introduction

To survive an SAP audit, you must first understand the rules. Despite occasional appearances to the contrary, there is actually sound logic to the way auditors work. Once you understand the audit approach, and recognize what the audit is intended to achieve, you can be better prepared for audit success.

This chapter is the linchpin for everything we will discuss in this book — helping you understand the basic audit concepts that ultimately affect the nature, scope, timing, and requirements associated with an SAP audit. We provide an overview of the different types of auditors as well as different types of audits, both of which directly impact the nature and scope of your audit. We explain why auditors do what they do, and review techniques they may use during the course of their reviews. We also discuss ways of working with your auditor, including the types of discussions and negotiations that can influence the final content of the audit report. By the end of this chapter, you should have the knowledge required to work effectively with your auditor toward a positive audit outcome.

1.1 Audit Overview

We often think of audits, and auditors, with negative connotations. It may be hard to find the positive in certain types of audits, such as a personal tax audit, where the outcome may be discovering that an inaccurate calculation has resulted in an underpayment (and loads of penalties and interest). Sure, you may walk away with the knowledge required to avoid similar mistakes in the future, but the fines associated with the audit finding, however, cloud the benefits received. Jokes about auditors abound, and in many cases for good reason.

In a business context, however, audits can have tremendous value. We work hard in our organizations to ensure the accuracy and integrity of information and our business processes. We are proud of the increased efficiencies and control that SAP can provide, and an audit can turn skeptics into believers by independently demonstrating that we've met that objective. An audit can support the diligence and quality that we‘ve put into our work as much as it can be an indictment of poor work. And if done well, an audit can provide valuable feedback and commentary that allows us to continuously improve our operations.

In their *International Professional Practices Framework*, the Institute of Internal Auditors (IIA), defines internal auditing as:

> *Internal auditing is an independent, objective assurance and consulting activity to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*

While this definition is focused on internal auditing (a concept we‘ll discuss in the next section), it can broadly be applied to audits in general. Audits are fundamentally designed to improve processes. They do this by taking a fresh look at operations, and providing insight that may not be readily apparent to those who are close to the process. Audits are not about finding problems; they are about identifying opportunities for improvement. These opportunities may result from identified problems, but what drives the audit ultimately is the desire to make processes better.

Examples of High-Value Audit Findings

Depending on the area under review, a good audit can have measurable value. This value may come indirectly through process efficiencies or cost savings identified during the audit process. In other cases, an audit can have a direct and positive impact on the bottom line — finding revenue leakage or recoverable overpayments, for example. Because audit results can be sensitive and politically charged, results such as these often go unnoticed outside the audit community.

1.2 Types of Auditors

The common thread to any audit is the auditor. Auditors are bound by a set of rules, and those rules govern how an audit is conducted. To be effective at an SAP audit, therefore, you must first understand the characteristics that define those who are doing the auditing.

As discussed in the preceding section, the goal of the auditor is not to cause problems. Conversely, the goal of the auditor is to identify where potential problems *might occur* or *have occurred*, and communicate sufficient information to interested parties so that informed decisions can be made. 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 high level, auditors generally fall into one of two categories: *internal auditors* and *external auditors*. Both internal and external auditors may also be categorized into specific audit specialties, or disciplines. In this section, we discuss not only the category of auditor, but more importantly, the impact a specific type of auditor may have on your audit.

1.2.1 Internal Auditors

Internal audit is a function within an organization, and the goal of the internal auditor is to protect management and the board of directors. Internal audit departments may exist as the result of regulation in specific industries or market segments, or from desire by management to have an independent set of eyes within the organization. Most internal audit functions report to the audit committee of the company's board of directors, although many also have an administrative reporting relationship to the CFO. Internal auditors provide the board 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 by management 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 assure that its directives and objectives are being carried out appropriately.

Internal auditors are employed by the organization; however, they may not always be part of 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 like SAP auditing, through the use of outside resources — often called *co-sourcing.* Regardless of who ultimately pays a specific auditor‘s salary, an internal auditor is ultimately employed full time or on a contract basis by your organization.

Because an internal auditor reports to the board, internal audit reports are primarily viewed inside an organization. They are rarely distributed to external parties. This is an important distinction between internal auditors and the external auditors we'll discuss next.

1.2.2 External Auditors

When most people think of external auditors, they think of financial statement auditors, typically employed by large accounting firms that opine on the integrity of a public company's financial statements as part of the year-end financial reporting process. For purposes of this text, we'll refer to external auditors in the broader, more inclusive sense, consisting of the various types of auditors an organization may encounter who are not ultimately employed by an organization.

The most common type of external auditor is the financial statement auditor. In the United States, an accounting firm is paid by an organization being audited (creating a lack of pure independence, which arguably has resulted in some of the accounting scandals seen in recent years); however, the external auditor officially represents the interests of investors (e.g., company stockholders). External auditors may also represent banks and report on issues such as compliance with loan covenants. They may represent governmental agencies such as tax authorities and report on compliance with specific laws and regulations (these auditors are sometimes called *governmental auditors*). Certain industries, such as financial services, pharmaceuticals/chemicals, and utilities (to name a few) also have industry-specific auditors that report 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 right-to-audit clause in contracts, particularly related to services such as outsourced IT or HR/payroll functions. In this case, depending on the specifics of your contract with the customer, they may periodically send a team of their own auditors into your organization to review a specified function. For organizations that perform services-related functions for many companies, the customers‘ desire to periodically audit these service-related processes can become particularly burdensome (imagine if every one of your customers decided to send their own audit teams to audit your SAP processing). As a result, some companies may choose to hire independent audit firms to issue what is known as a *service audit report* (also known as a *SAS-70 report* in the United States). Depending on circumstances, this report may be used by customers to gain assurance as to the effectiveness of operations in lieu of having to send their own audit teams to perform independent audits.

While at times the external auditor's fees may be paid by the organization being audited (as in audits governed by certain regulatory agencies), the ultimate goal of an external auditor is to protect investors, customers, or other interested external parties. Similar to how an internal auditor provides the board with objective information that may not be received directly from management, external auditors provide these external parties with information and insights that may not be received directly from your organization.

During the audit, the external auditor may at times make observations that he reports to management as additional value-added services (e.g., suggestions for improving SAP observed while performing other audit procedures but not relevant to the context of the audit being performed). These recommendations, sometimes included in a document called a *management comment letter*, are typically for your organization only. Be aware, however, that no matter what type of external auditor is working with your organization, or what type of audit he is performing, one important fact remains constant: Reports from external auditors (when serving in an external audit capacity) are issued outside the walls of your organization.

External Auditor Providing Internal Audit Services

Organizations looking to outsource or co-source all or part of the internal audit department often look to firms that provide external audit services. An organization is typically restricted from outsourcing its internal audit function to the same firm it uses for the external financial statement audit; however, it's possible from such an arrangement that the co-sourced internal auditor working in an organization's internal audit department is also an external auditor for another organization. When this is the case, the reporting relationship and report distribution procedures follow the function that the auditor is performing, independent of the type of auditing the auditor in question typically performs. If the auditor is operating in an internal audit capacity, his report is for internal use even if that same auditor performs external audits for another organization.

Knowing the type of auditor you're working with, and how the resulting audit report will be distributed, is important whenever you're going through an audit. Audit findings are never desired, but audit findings from an external auditor can be particularly problematic. In the case of a financial statement audit, the final report may be issued to the public as a whole, and is thus accessible to anyone with access to public records (including your competitors). Financial statement audit findings can have an almost immediate negative effect on stock prices, and depending on the finding, can turn into a public relations disaster.

In the case of certain types of audits (such as those conducted by your financial institution or by a customer), the distribution of the audit report may be limited to specific organizations. Negative external audit findings can be problematic even if the final report is not issued for public consumption. Failure to comply with financial covenants could result in credit lines being dissolved. Failure to conform to customer service level agreements could result in the loss of a key customer. In essence, certain audit findings can haunt an organization for years.

While it's always important to work with your auditor to ensure that the issued report is relevant, factual, and fairly stated, the nature of the distribution of external audit reports makes this an even greater concern. Many auditees don't realize that they can work with an auditor to negotiate the specific wording and even the severity rating for audit findings. We'll discuss the process of negotiating with your auditor in Section 1.6.3, Negotiating Issues.

1.2.3 Specialty Auditors

In the same way that individuals within many organizations become specialists in certain functions, both internal and external auditors often specialize in different audit disciplines. A typical internal audit department, for example, may contain multiple specialists. Some auditors may focus on financials statements and specialized reporting (e.g., tax reporting). Other auditors may focus on operational efficiency. Some auditors may specialize in technology, whether from a general technology management viewpoint or a specific application or hardware viewpoint. Other auditors may focus on areas such as internal investigations and fraud.

Depending on how audits are conducted within your organization, you may be subject to multiple audits with different focuses. Many audit departments are moving toward more integrated audits, where multiple disciplines are combined into the same audit. This helps to save time and may reduce the "pain factor" of the auditee as well.

Some auditors, typically *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. Of course, there are also auditors who specialize in auditing specific computer-based applications such as SAP. In general, the more specialized the auditor, the higher the internal/external cost, and thus the more likely your organization may not be able to afford their services full time. For this reason, organizations seeking a thorough audit of their SAP systems often turn to outside organizations or individuals for assistance.

Are They Capable of Auditing SAP?

If you've ever been through an SAP audit, you've probably at some point been frustrated by how little your auditor actually knows about SAP. You may be convinced that you know more about the system than he ever will. The reality is that you probably should. You know how SAP is being used in your organization, you probably have an understanding of how it was configured during the implementation, and you very likely use SAP more frequently than your auditor.

> If you're lucky, you may find yourself with an auditor who at least understands the basics of SAP. In many situations, however, you may find that your auditor has little to no SAP experience at all. Perhaps he is merely following a standard SAP audit checklist, and, as such, try to apply questions and tests to your organization that are, in your mind, clearly irrelevant. Maybe his SAP experience is in a different component and he has only cursory knowledge of configuration options of the component you work with. The sad truth is that those auditing SAP typically have limited SAP audit experience.
>
> This situation is unlikely to change in the near future. Given the complexity of SAP, the number of configurable variations, the differences between components and industry-specific functions, and even the ongoing improvements released by SAP, expecting any auditor to be an SAP expert in all aspects of your system is unrealistic. Even if an "expert" team of auditors could be brought together, few organizations are willing to make the financial investment it would take bring them in.
>
> Fortunately, any good auditor (even one with limited exposure to SAP or other ERP systems) can lead an effective assessment of SAP. The key lies in the auditor understanding how SAP works in a general sense, and in learning to apply traditional audit techniques to the SAP system and related processes. A good auditor is like a good private investigator — he knows what questions to ask! A good auditor learns to ask key questions from the SAP experts already housed within your organization, and adapt the audit appropriately based on their responses and independent validation of data within your SAP system.

1.3 Categories of Audit Objectives

Not only are there many different types of auditors and audits, there are also many different types of audit objectives. A commonly used internal control framework known as *COSO* (Based on a 1992 report from the Committee of Sponsoring Organizations 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.

Using this same categorization for audit objectives, Table 1.1 presents a small sampling of audit objectives that may involve an assessment of SAP.

Category	Example Audit Type	Example Audit Objective	Typical Audience
Strategic	Software Selection	Verify that the software selection process follows standard practices and is conducted in a well-controlled manner	Board
	Organizational Planning	Assess the effectiveness of processes for ensuring the SAP system will continue to meet the organization's objectives over time	Management
Operational	Implementation Review	Review the SAP implementation process and ensure project status reports and other communications are an appropriate reflection of reality	Management
	SAP Processing	Ensure SAP administration and operational processes effectively support service level agreements	Customers
	Maintenance and Change Control	Verify that all changes to SAP are appropriately designed, approved, configured, tested, and reviewed prior to movement into the production instance	Management Customers Regulators
Reporting	Financial Reporting	Assess the reliability of SAP data used to generate financial reports	Investors
	Tax	Assess the ability of SAP tax calculations and reporting sufficiently for accurately represent tax liabilities	Management Regulators
Compliance	Sarbanes-Oxley	Ensure SAP and related manual controls and processes effectively support Sarbanes-Oxley compliance	Investors
	Privacy	Review compliance with HIPAA, GLBA, and other privacy-related regulations and ensure access to key SAP transactions and data is appropriately restricted	Management Regulators

Table 1.1 Audit Objectives

Clearly, the sheer possibilities related to what an SAP audit could be looking to achieve are countless. Because the audience of various reviews is different, the auditor performing the review may also be different. Considering the number of different types of auditors and the wide variety of potential audit objectives, is it any wonder that some audits of SAP look different from others?

Every SAP audit has the potential to be different, and, as such, you must prepare comprehensively in advance of an audit. Depending on the context of the specific review, something considered important for one audit may be completely ignored in another. For example, consider an audit of SAP security. For Sarbanes-Oxley purposes, the security assessment will likely focus on segregation of duties, and also examine a few basic SAP security administration and management controls. If the SAP security review is part of a HIPAA privacy audit, however, heavy emphasis will be placed on the ability to users to see sensitive information, the encryption of that data both in SAP and in transit between SAP and other systems, and the processes for identifying protected information. Two different audits, two different approaches and concerns relative to SAP security.

Key Observation

Success (or failure) in a prior SAP audit has little bearing on success or failure in a future SAP audit, particularly if those audits serve different purposes.

1.4 Auditing Principles and Considerations

Before we discuss the SAP audit, understand some key audit principles. These principles often require auditors to behave in ways that seem foreign to those new to the audit process. Understanding these principles will better prepare you for and react to the audit.

1.4.1 Independence

Professional standards require that the audit function be independent. Audit independence generally refers to reporting relationships and communication channels, and grants the auditor department (through the chief audit executive) unrestricted access to the board via direct communication channels. Given that an auditor performs an important and sometimes sensitive function on behalf of the board, audit independence is intended to ensure that the auditor is free from interference in all aspects of his work.

The concept of audit independence can sometimes come up during an audit. For example, the internal audit department may determine that an SAP audit is warranted. In particular, he may wish to review new functionality currently being configured, and he may wish to conduct this review just before a critical deadline. The SAP project manager may object to the time or the scope of the review, even to the extent of escalating the concern all the way up to the CIO. Even in an organization where the CIO has a higher title than the head of the audit group, the CIO dictates neither when the audit occurs nor what information the auditors have access to. Most auditors would be reasonable with such a request, and if the request did not affect the ability to meet the audit objectives, the auditor would likely change at least the timing of the review. If the auditor, for whatever reason (perhaps because of a time-sensitive confidential analysis at the request of the board), does not want to change the audit, he is in no means obligated to do what the CIO requests — or even what the CEO requests, for that matter. Audit independence grants them that right, and professional audit standards require that they disclose formally in writing if that right has ever been violated.

Another common issue that can raise concerns about audit independence relates to system and data access. An organization's SAP system can house a lot of sensitive data, and companies spend significant effort securing that data. Because of the nature of audit work, normal data access restrictions do not apply to the audit function. Most auditors are allowed access to any data they request (although the head of the audit department may put restrictions on who in his department can request what type of data), and preventing that access can raise scope restriction concerns that have to be reported to the board. Internal audit departments operate in different ways, however, so it's always good to understand the way that yours works.

The actual specifics detailing the work that your internal audit department is charged with performing, the nature of the information they have access to, and other similar information can be found in what is known as the *audit charter*. This formal document, approved by the board and mandated by the IIA's International Professional Practices Framework, will describe the purpose, responsibility, and authority of your organization's internal audit department. If you're interested in learning more about the internal audit function in your organization, most auditors are happy to share the audit charter with you, and in many organizations, it's even posted on the company's website for investors and other interested parties to see.

1.4.2 Objectivity

Professional standards also require each auditor to be objective. Objectivity is different from independence in that, whereas independence is associated with the audit function in general, objectivity is applied to the individual auditor. An auditor working objectively is free from bias, and is impartial in fact and appearance to the outcome. His professional judgment is not influenced or impaired, and he is not in a position where his judgment could be influenced or impaired. This last point is important, because a conflict of interest can arise even if no unethical or improper behavior occurs, and conflicts of interest that could affect objectivity must be fully disclosed.

Seeking auditor advice during an SAP system implementation or upgrade is common practice, and can benefit the implementation team by helping ensure audit concerns are addressed before the system goes live. Auditor involvement as part of an implementation has the potential to impair the auditor's objectivity, however, so auditors are often cautious as to their specific levels of involvement. As an example, an auditor who was involved in designing or configuring the SAP ERP Financials solution of SAP would be prohibited from later auditing that solution (because his involvement in the implementation would make it appear as if he was not objective, even if he attempted to audit in an objective and unbiased way).

The Institute of Internal Auditors, Practice Advisory 1120-1

"The internal auditor's objectivity is not adversely affected when the auditor recommends standards of control for systems or reviews procedures before they are implemented. The auditor's objectivity is considered to be impaired if the auditor designs, installs, drafts procedures for, or operates such systems."

If you're looking for advice or assistance and your auditor is hesitant to provide it over concerns related to objectivity, work to an acceptable scenario. What you may be specifically asking for may compromise the auditor's objectivity if he provided it; however, often, you can work to a compromise where you still gain insight but not in a manner that compromises objectivity. Coming to such a compromise can be a win for your organization. Rather than asking the auditor to give you the answer, consider using him as a coach or a mentor — providing you with structure and tips on considerations for your decision-making process but not making the decision for you.

1.4.3 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, per audit standards, he cannot trust you without additional evidence. Auditors are required to operate in a mode of professional skepticism, which is a manner of operating objectively. Professional skepticism suggests that an auditor cannot merely trust what someone says, and must gather additional evidence to support (or potentially refute) what he 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 (Figure 1.1). As such, the auditor's beliefs (or the beliefs of the individuals who the auditor is working with) should not influence the outcome. Audit evidence must stand on its own and support the conclusions of the audit.

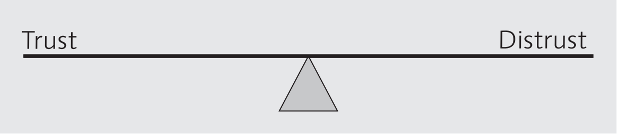


Figure 1.1 Professional Skepticism Requires Being Neutral

This standard may initially seem harsh, but we've seen first-hand how lack of professional skepticism can have a serious impact on an organization. A number of years ago, there was a company that practically revered one particular employee for his ability to reconcile SAP General Ledger accounts during period-end. This individual typically had the fewest number of outstanding reconciling items and comparatively very few dollars outstanding at any given point in time. In fact, management began looking to this person to coach others in how to effectively reconcile SAP. It wasn't until after an audit, however, that this person's true success mechanism was revealed — once the reconciliation was "close enough" (relative to the overall account balance, which was a very sizeable number), he merely created a journal entry to clear out the remaining items. In essence, this "SAP reconciling superstar" only appeared good on the surface.

You may wonder from this example how professional skepticism is relevant, because the problem was caught during an audit. In this case, professional skepticism was used during the audit, which is why the individual's actions were detected. Where professional skepticism failed was as part of the management's review processes. The issue persisted for years, despite processes that should have detected the problem. Managers were supposed to review every reconciliation to ensure completeness and accuracy. Unfortunately, this individual's manager was not operating in a neutral position on the professional skepticism scale — in essence, trusting the integrity of the employee's ongoing work based on results that appeared reasonable in the past. As a result of this lapse, the organization lost a sizeable amount of money, a large effort was required to go back through history and clean up the mess, and management was left looking foolish. We encourage every manager (not just those in audit) to apply professional skepticism in his work as well. Review the work of your SAP developers, periodically assess the accuracy of your SAP security setup and maintenance processes, determine whether those reviewing SAP exception reports are following through on identified items appropriately — whatever the role, spend some time validating your own assumptions about performance.

If We Can't Trust Our Employees, Who Can We Trust?

We're not suggesting that you completely distrust every employee. Professional skepticism is not about distrust — it's about neutrality. Clearly, you should be spending more effort reviewing the work of those employees who have proven to be inaccurate, incomplete, or otherwise problematic. Newly trained employees may also warrant more attention than seasoned employees. We are merely suggesting that you do not wholly ignore your most trusted staff and rely on faith in their continued performance. While you may choose not to review everything they do, you may consider periodically, for a selection of their work, examining what they have done to ensure that your trust in their performance is still based on reality and not on a historic perception that is no longer accurate.

1.4.4 Evidence

The concept of evidence proves to be problematic in many organizations. For audit purposes, evidence must stand on its own — meaning that a second independent auditor looking at the same information would come to similar conclusions regarding the test results. To some extent, evidence requirements are part of the topic of professional skepticism discussed previously.

In the early years following the U.S. Sarbanes-Oxley Act, some companies were shocked when their external auditors issued significant deficiencies (a type of statement that appeared in public reports) merely because the companies were unable to show evidence of signed documents — even though they performed related reviews. Some auditors went a step further by declaring "if you can't prove it, it didn't happen." Obviously, this is a little extreme, but the reality is this: If you don't have sufficient evidence to prove it, an auditor cannot independently attest that it happened. Thus, "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, lack of evidence also begs the question of how management can be assured that processes are working as intended. If, as in the example from the section above, management is merely relying on 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 operating as management intends — both for audit as well as for management.

Electronic Evidence

Many people, particularly those in IT, dislike the "paperwork factor" often associated with evidence. The reality is that evidence can also take the form of electronic evidence. The key with effective electronic evidence is in having appropriate controls, assuring that (1) the "who" (e.g, originator, approver) is the person we believe; (2) the evidence hasn't been changed or modified in any way from its original state; (3) the data contained cannot be wholly or partially removed; and (4) the evidence can be appropriately associated with what it is being used to prove. Of course, the other key to effective evidence is being able to find and retrieve it when you need to — hence, sometimes it may be easier to maintain hardcopy documents in readily-accessible files unless strong electronic document management procedures are in place.

1.5 Understanding the Audit

Now that you understand some of the common audit principles, it's time to look at several common audit techniques and processes.

1.5.1 Risk-Based Auditing

The scope of many audits is often determined by applying a *risk-based* approach. There are many different approaches and techniques of risk-based auditing, but fundamentally it's a technique for focusing more attention on organization-specific risks with a higher likelihood and/or impact than other risks (Figure 1.2). Using an SAP example, an insurance company using SAP Treasury and Risk Management applicationas well as SAP Project Management services may find that significantly more attention is placed on SAP Treasury and Risk Management, with potentially little-to-no attention on SAP Project Management. This makes sense, because the risks in an insurance company typically center more on cash and the tracing and flow of money than on projects. Conversely, a company whose primary business is construction may find their SAP audit having the exact opposite focus.

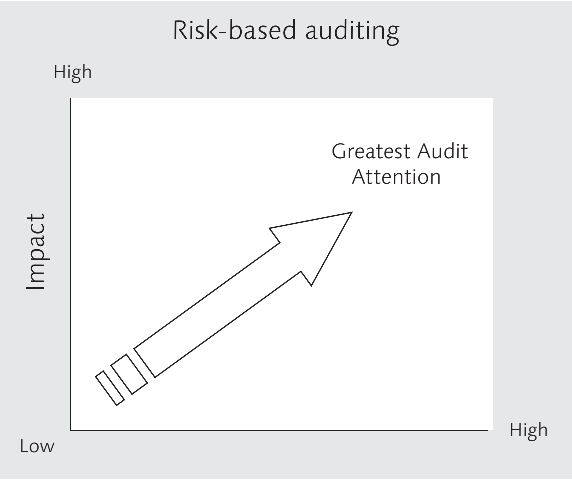


Figure 1.2 Essence of Risk-Based Auditing

1.5.2 Internal Controls

A concept related to risk is that of control. When dealing with an audit, or, even more broadly, the entire field of governance, risk, and compliance, the words *internal control* or simply *control* are used frequently. We've used the term several times in this chapter already. There are a number of different definitions for this term.

COSO, a framework mentioned in Section 1.3, Categories of Audit Objectives, suggests that: "*Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: 1. Effectiveness and efficiency of operations, 2. Reliability of financial reporting, and 3. Compliance with applicable laws and regulations.*"

The Institute of Internal Auditors defines a control as: "*Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.*"

ISACA defines internal control as: "*The policies, plans and procedures, and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.*"

A Simpler Definition of Internal Control

A control is a process or activity designed to prevent "bad things" from happening, or to detect these things within a sufficient time to stop unacceptable damage from happening.

While this definition is concise, the specific words are important. Understanding the concept of internal controls is absolutely essential to understanding the audit process, and preparing yourself for an eventual audit. Let's look at each component of this definition separately.

"A Process or Activity"

A control is active, not passive. Something specific is occurring, and that something may be as simple as a single action, or as complex as a multi-step *process*. The focus on the action in this definition is important — without action, a control does not exist.

Let's look at a specific example. SAP contains numerous exception reports that allow users to review the results of processing and follow up on potential issues, such as the report showing goods invoiced but not yet received (RM07MSAL). The mere existence of this report is not a control. The control comes when someone reviews the report and determines what type of action to take on the information in it.

By this same definition, policies and procedures are not controls (despite being referenced in many texts, and even one of the definitions above, as being such). It's the *communication* of those policies and procedures in a way that the recipient understands their responsibilities and can take appropriate action, and the *enforcement* of the policies and procedures that are the controls. The evidence as to the effectiveness of these controls (in this case, the communication and enforcement separately) is indirectly demonstrated by the right action being taken when that policy or procedure needs to be applied.

"Designed"

A control must be intentional. Because it's intentional, a control is *designed* with a specific purpose in mind. Accident does not make a control. The control, rather, comes from thoughtful consideration of the processes or activities needed to mitigate a risk, and the effective construct of those processes and activities to do just that.

Imagine that a purchasing clerk is entering contract details (for a contract that has already been initiated) into SAP and mis-keys the price on one of the line items. If the vendor associated with this particular purchase order (PO) is set up in SAP as an ERS (Evaluated Receipts Settlement) vendor, the vendor invoice will not be compared to the PO and thus the common three-way match control will not detect this mistake. Now imagine that another employee catches the mistake before the organization pays the vendor. Obviously, the fact that the mistake has been caught and corrected is a good thing. But is this the result of a control?

If the employee who found the mistake in this case did so by accident, perhaps inadvertently finding the pricing difference while he was looking into something else, then the activity that exposed the problem would likely not be considered a control. If, however, the employee who detected the issue did so as part of his designated responsibilities (perhaps he was part of a quality assurance function), then it would be the result of a control.

"Prevent or Detect"

Controls tend to fall into two categories: those that stop a potential problem from occurring, and those that allow problems to be identified if they have occurred. These are often known as *preventive* and *detective* controls, respectively. Some auditors may also refer to a class of controls known as *corrective controls*, which fix an identified error after it has occurred and before it results in harm. Corrective controls typically rely on detective procedures, however, so for the sake of this text, we will consider detective and corrective controls to be the same.

SAP security is an example of a preventive control. Thinking of this in terms of the action required for a control to exist, the fact that "Upon login, SAP verifies that the user ID is valid and that an appropriate password has been entered for that user ID before the user is granted access to the system" is a preventive control. SAP security prevents a user who does not have a valid ID/password combination from logging into an SAP system, which is designed to ensure that only authorized individuals can process transactions using SAP.

A manager reviewing the RM07MSAL report (where an invoice has been received but corresponding goods have not been received) and investigating outstanding items is an example of a detective control. If the review occurs when it's scheduled, it's likely to detect payments that have been made or are about to be made when contract terms have not been fulfilled.

"Bad Things"

Controls are not intended to, nor could they ever, prevent (or detect) every possible unintended situation. Effective control design balances the cost of the control with the benefit of that control. A situation can be less than perfect but still not be *bad*. Controls in the context of this definition are those controls that are designed well — focused not on every condition that is less than perfect but on those where the impact has the potential to be harmful in a magnitude that is not desired. The definition of this exact point is a judgment call.

Using one of the examples used earlier, let's say that the purchasing clerk who mis-keyed a price on the PO was off by $1. Is that "bad," and should a control be designed to prevent or detect this type of occurrence? It all depends on the organization. If the purchasing clerk is a buyer for the retailer Dollar Tree, and the PO is for a large quantity of goods being purchased for ultimate sale for under $1, then the situation is clearly "bad" and one for which a control should be in place. If, however, they are the buyer for an aircraft manufacturer and the item in question is a multi-million dollar part, then it makes little sense (unless required by contract or regulation) to design a control to detect an amount so miniscule when compared to the overall purchase.

"Sufficient Time to Stop"

Detective controls occur after-the-fact, and thus it's important to understand the time frame at which the detection is likely to occur. The value of detection is limited if by the time the problem is identified, significant harm has occurred to the business. For a detective control to be effective, problems identified from the process must be both stopped from future recurrence, and fundamentally resolved. The specific time frame associated with the phrase *sufficient time* depends on your organization and the specific risk being addressed.

Continuing on with our example of a mis-keyed price on a PO, the ideal timing on the quality assurance process would ensure that the incorrect payment amount is not paid against that PO. In the previous example, the contract had already been executed and thus what was keyed into SAP would not affect what we legally owe the vendor, so some organizations may also allow the detection window to extend beyond payment but within sufficient time reasonable to still expect to recover the funds from the vendor. In a more typical situation where the issuance of the PO to the vendor may create a contractual obligation, we'd likely want the detective control to occur in time to stop the incorrect PO from being sent.

"Unacceptable Damage"

The notion of damage or harm caused to the organization is also tied in to the analysis of the timeframe before which detective controls should catch a problem. Damage could be direct (such as payments exceeding contracted rates where an employee chose to make a purchase outside the normal purchasing process), or indirect (such as loss of customer goodwill, which could eventually result in future revenue loss). Like the discussion regarding "bad things," *unacceptable damage* recognizes that there is a level of harm that may not be desired but which still has not reached the level of being unacceptable. Detective controls do not need to stop all damage, but they should certainly be designed to ensure that if the organization is harmed that the level of harm does not exceed a reasonable threshold.

Internal Controls are Everywhere

Every organization has internal controls, and you deal with these controls frequently (even if you don't recognize them as such). Edit checks configured within SAP to prevent erroneous input are one example of internal controls. Other examples of internal controls include processes designed to prevent duplicate payments, procedures to ensure the confidentiality of pricing/purchasing arrangements, management reviews of SAP exception reports that facilitate the identification and investigation of potential problems, and training and education programs designed to reduce the likelihood of user error.

1.5.3 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 and pessimistic, but in reality there is simple logic behind most audit concerns. The key lies in continuously asking "What could go wrong?," taking that answer, and asking, "And then what could go wrong?" Considering risk-based auditing, you would then gauge the impact/likelihood of the event/issue to determine whether this warrants attention and investigation (not every auditis risk-based, however, so at times your SAP auditor may be concerned with issues that do not seem likely or impactful). For the items deemed important enough to warrant further consideration, you would then think through "Given that this could go wrong, what do we do to prevent it from happening, or detect it in a timely fashion if it does?"

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

- What could result in a payroll adjustment in SAP being invalid?
- What could result in checks cut from SAP having inaccurate amounts?

- What could result in the information we use to calculate liabilities being incomplete?
- What could cause goods receipts to not be entered into SAP and processed in a timely fashion?
- What could result in the information used to determine write-offs being irrelevant?
- What could result in sales being recorded in the wrong period?

As mentioned above, for each of these questions, you would then list possible causes and the impact/likelihood of occurrence for your organization. Taking the question "What could cause goods receipts to not be entered into SAP and processed in a timely fashion?," a partial list of potential causes and their impact might include:

1. 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).
2. The receipts file transmitted nightly from warehouses not running SAP was not received (low likelihood, moderate impact).
3. The receipts file transmitted nightly from warehouses not running SAP was not processed in SAP (low likelihood, moderate impact).
4. Third parties who receive and store goods on behalf of the company to not submit file for processing within corporate guidelines (high likelihood, low impact).

Lastly, you should have sufficient processes to ensure these potential causes are either prevented, or detected in a timely fashion if they occur. These processes may differ by type or category. Taking the first potential cause, you might have:

- For goods of type X: RFID tags automatically update SAP inventory records upon receipt into the warehouse (preventative).
- For all goods (both type X and not-X): All employees whose job responsibilities include entering or transmitting goods receipt information are required to 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.
- For all goods (both type X and not-X): Every week, managers review reports of invoiced items that have not been received, and investigate items that have been outstanding for more than "Z" days (detective).
- For all goods (both type X and not-X): Physical inventories are performed quarterly and inventory adjustments are made in SAP based on actual physical count (detective).

Of course, just being able to list processes that detect/prevent is not enough. Show that these processes would prevent errors above a cumulative magnitude that would cause key stakeholder (management, supplier, investor, etc.) concern, or detect such problems in sufficient time to correct them before uncorrected errors would cause stakeholder concern. In the example above, you primarily rely upon detective controls for goods receipts that are not of type-X (although there is a preventative control listed, it's fairly weak — all organizations have periodic employee performance problems). Determine whether these controls are sufficient to reduce the level of overall risk to one that is acceptable. Upon evaluation, you may need to increase the frequency of certain controls, or add additional controls. We'll discuss the principles of designing effective controls in SAP in Chapter 3.

1.5.4 Applying Audit Investigative Techniques

The audit process can be compared, in some ways, to the scientific process. In science, you have a theory that you work to prove. The audit investigative process is similar. The controls (each of the items identified that could prevent or detect the potential problem from occurring) can be considered management's theories. The auditor attempts to gather evidence to prove (or in many cases, disprove) management's view as to the effectiveness and reliability of these controls.

Related to these controls, the auditor looks both at the design (if it's operating as intended, would it sufficiently mitigate risk to the desired level), and subsequently the operation (now that he's comfortable with the design of the control, can he determine whether it's performing as intended) of the control. Throughout the process, the auditor is gathering evidence to support the conclusion.

Note

Different from the scientific process, the auditor is not looking to prove absolutely. 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 reviews. In order of reliance, the first is *corroborative inquiry*, which ensures that the people interviewed (formally or in casual conversation) during the audit share the same belief. The second is *observation*, in which the auditor observes whether the intended process is occurring consistently based on how he sees people or systems performing their required actions. The third is *direct examination of evidence*, in which 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 their result of evidence 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 own SAP audit. We discussed how auditors are attempting to prove or disprove management's theories, and there is certainly no reason why you can't (or shouldn't) do the same in advance of your own audit. Let's talk about how each of these techniques could be applied to investigate one of the controls we identified in the example earlier — that every week, managers review reports of invoiced items that have not been received and investigate items that have been outstanding for more than "Z" days.

Corroborative Inquiry Example Tests

Discuss the process with the managers who are responsible for reviewing the invoiced-not-received report in SAP. Determine how frequently they 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.) are involved in those actions. Assess based on their description of the process and the report whether they are following company policy.

Have discussions with the "who else" involved in the actions above to determine how frequently they have been contacted, and assess whether this is appropriate given the frequency of items appearing on the report.

Observation Example Tests

Ask to watch the manager review the report. Observe that he selects appropriate items for follow-up. Also, observe how readily he navigates to the correct report in SAP, and that he appears familiar with the report's contents.

If possible during the course of the review, observe other instances where the manager is reviewing the report (when he is not aware that you're observing).

Direct Examination of Evidence Example Tests

Review for report sign-off, tickmarks, 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 with issues resulting from the review. If security settings allow, review in SAP the last date the manager executed the SAP transaction that calls the report, and determine whether it's consistent with how frequently he should be reviewing the report (e.g., using RBE – Reverse Business Engineering in versions prior to 4.6).

Re-Performance Example Tests

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 these same evidence-gathering techniques to determine if appropriate follow-up occurred (e.g., discuss with receiving dock employees, look for supporting emails, etc.).

Be objective and use professional skepticism when performing these and similar tests in your own 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.

1.6 Audit Reporting

The result of the audit is, of course, the *audit report*. The audit report is the culmination of the entire audit process. Interestingly enough, while the audit report is typically discussed singularly, the final audit documentation typically includes numerous reports. We'll discuss these in this section.

The audit reporting process can be specific to the type of audit or the category of auditor preparing the report. Talk to your auditor about the nature of the report and the reporting process that will be used in your SAP audit.

The Tone of the Typical Audit Report

As discussed earlier in this chapter, a common audit objective is to find opportunities for improvement. The report from such an audit is likely to appear negative. To recommend opportunities for improvement, the auditor must identify real or potential problems in the current system, and present them so the need for change is obvious to the reader. While some auditors may do so out of courtesy, it's typically not the auditors job to identify those things that are going well.

1.6.1 Reporting Process

The audit report typically goes through a series of stages before release. The auditor often draws some preliminary conclusions early in the audit process, and, depending on your role in the audit, may share those with you in advance of report creation. Once the auditor begins to document findings, preliminary findings and issues are often shared with management over the area being audited. At this point, you can influence, to a limited extent, the content of the report.

1.6.2 Responding to Preliminary Audit Issues

If an auditor has made you aware of preliminary issues or concerns that may appear in the report, you've been offered an opportunity. Your auditor will typically solicit your feedback. Depending on the time spent on report development, there could be several iterations of report drafts. You auditor will (almost always) adjust facts or representations if they are inaccurate or misleading. The auditor will typically also add commentary, if you've provided it, on what is being done with the issue. As such, it's useful to understand how your feedback will be used and when the final report will be issued. If you know, for example, that the auditor discovered a configuration problem with an SAP setting, let the auditor know it's been fixed so that he can include that information in the report as well. You'll also typically be asked to respond to each of the issues with information about what will be done to resolve the problem.

1.6.3 Negotiating Issues

The audit reporting process can at times be contentious, but it's important for you to be diligent as the report is being drafted. In Sections 1.4.1, Independence, and 1.4.2, Objectivity, we discussed how the auditor must express his professional opinion without undue influence. Many auditees believe that, as a result, little can be done if there is disagreement on issues. In reality, there are at least three items you may be able to influence.

- **Facts**. These are the most straightforward part of an audit report. If you find yourself in disagreement with your auditor, separate facts from opinion and make sure the facts are accurate. Provide the auditor with details related to the facts you believe to be accurate — it's possible the auditor received outdated or incomplete information.
- **Risks**. The risk related to the audit issue is one of the most common points of disagreement. The auditor may believe that the issue exposes the organization to a large amount of risk, and you may believe it to be otherwise. While the assessment of risk is a very subjective process and entails a great deal of professional judgment, the basis of risk should be a set of facts. If you have facts to support your differing assessment of risk, show the factual evidence to the auditor and discuss why you believe it impacts the risk. The auditor may not have been pro-

vided with all the information you have, and as such may be basing his opinion of risk on an incomplete set of facts.

- **Cause**. Depending on the nature of the audit in question, the auditor may also be asked to document the cause of the issue identified. Usually, the auditor will work with you or your team to understand what happened, but if the audit process was rushed, it's possible the analysis was not as thorough as it could have been. Similar to what we discuss with risks above, provide the auditor with facts that support your conclusion about the cause. Auditors are allowed, and encouraged, to adjust their reports if new facts emerge — it's only when opinions are cited as the basis for adjustment that auditor independence and objectivity can be compromised.

Sometimes, even after negotiation and presentation of your side of the issue, you and your auditor may not reach a consensus. If this is the case, you can request that your auditor document your position in his report. The auditor is not obligated to do so, but many will take this step to ensure the final report is balanced and the reader has sufficient information to draw his own conclusions.

1.6.4 Report Distribution

The final report is typically a combination of multiple reports. You as the auditee will usually get a copy of the report, as well as the specific detail supporting the audit findings. For example, if the report indicates that the auditor found 25 terminated employees who still had access to SAP, you would typically be provided with the names of those 25 employees so you can clean up the issue with user access.

In addition to your report, a copy of the report will also typically be presented to the head of the department or division, sometimes in a summarized fashion. Given the scope of most organization's usage of SAP, it's not uncommon for an SAP audit report to make it up to your CIO and the CFO. This is why it's important, as previously discussed, to work closely with your auditor to ensure all facts are correct.

Reporting to the Board

Internal audit departments, as previously mentioned, typically report to the audit committee of the board of directors. Depending on the desire of the board, however, the audit committee may not see every detail of every audit report. In many organizations, the head of the internal audit department will summarize the audits performed during the period and report to the board only those audit issues corresponding to the highest organizational risk.

1.6.5 Management Response and Follow-Up

If the audit report for your SAP audit contained findings, you'll typically be charged with making sure the corresponding issues have been resolved. When finalizing the audit report, you likely provided your auditor with a *management response*, describing how and when each of the issues will be addressed. Follow through on what you've indicated as the result. Depending on the nature of the audit and the audit findings, your auditor may periodically check in with you, and may even perform some additional focused testing to independently verify that the issue has been resolved. If for some reason you determine after audit report issuance that the way you intended to resolve the issue is no longer practical, keeping your auditor informed of your new plans and rationale will make the post-audit process easier for everyone.

It's Not My Responsibility!

Often after an SAP audit, certain employees, such as SAP project managers or administrators, may feel they've been blamed for things that are not their responsibility. The audit report is not about blame, nor is it about you. The audit report is about issues and opportunities for improvement, and likely covers the entire SAP system, which includes areas that are end-user and manager responsibilities.

1.7 Rules of Engagement

Now that you understand the audit process better, a few additional tips will help you get through your SAP audit smoothly.

1.7.1 Understanding the Audit Objective

By now, you recognize that your upcoming SAP audit could be different from your last, and both of these could be different from those at another organization. As soon as you learn that your SAP system is being audited, determine the objectives, scope, and timing of the audit. Many auditors will provide an audit kickoff memo that will detail this information, although, like everything we discussed, this depends on your specific audit. Talk to your auditor well before he comes on-site, so you have a clear understanding of what will be required and when you'll be required to provide it.

1.7.2 Working with the Auditor

Auditors sometimes get a bad rap. Some of it's deserved, and some is not. Just remember that your auditor is a person, he has a job to do, and the quicker he gets it done, the sooner he will be out of your hair. Treat your auditor with respect, and you'll typically get respect in return. Make his life and the completion of his tasks easy. Provide him with what he needs when he requests it, and eliminate any roadblocks that could get in the way of his progress. The sooner he completes his audit, the earlier you'll be able to get back to focusing on your own work.

1.7.3 Establishing the Audit Environment

Have an audit-ready environment set up and ready for your auditor when he arrives. This may include having space available near the SAP team where the auditor can work, enable IDs within SAP that the auditor may use for the review, update and reconcile a non-production environment for certain types of audit testing, and other similar activities.

1.7.4 Do's and Don'ts

In addition to making sure your SAP system is ready for the audit, prepare your own employees for the audit as well. Your interest in this book is a great start, and provides you with some great ideas and tips for your employees. We recommend, at a minimum, that you provide your employees with a list of do's and don'ts for working with the auditor.

- Do answer all auditor questions openly and honestly.
- Don't speculate on the answer to a question if you do not know the answer.
- Do direct the auditor to the right team member if you're not in the best position to answer a question.
- Don't joke about things that may not be happening.
- Do take time to research and provide the right information.
- Don't provide more information than the auditor asks.
- Do clarify what the auditor is looking for if you do not understand.
- Don't take pointed audit questions as an indication you've done anything wrong.

At a minimum, having such a list can help spark a valuable discussion within your team, and ensure that everyone understands and is prepared for the upcoming review.

1.8 Summary

In this chapter, we discussed auditors and the audit process. We shared some of the principals that an auditor must follow, and provided a few tips on ways to think like an auditor that can help you ready your SAP system well in advance of any audit.

We also walked through the audit reporting process, and suggested ways to ensure the accuracy of reported audit findings. You should have a better understanding of why auditors do what they do, and the things you can do to make the audit process easier.

In the next chapter, we'll look at the SAP audit process, including the primary areas typically reviewed. We'll also share a few common problems that exist in many organizations, and the things you can do to alleviate audit concerns.

Index