**6 Audit Methods**

1. Content Determinants and Formal Determinants

KEY POINTS •••

* Internal Audit uses a variety of content determinants and formal determinants to identify the appropriate audit method to use for a specific engagement.
* Content determinants include the audit fields and the audit approaches.
* Formal determinants include: the audit category, type, and status of the audit within the audit cycle.
* Thus audit methods are characterized by a framework of standard parameters, which allows auditors to treat different audits according to standard rules. In­dividual criteria may be added to the predefined standard parameters at any time.

When planning an audit, Internal Audit must consider several important factors to determine the appropriate audit method to use. Chapter 6 provides an overview of the determinants on which audit methods are based. Additional factors for deter­mining the audit method may be needed. These factors include the period perspec­tive and the distinction between set and freely selectable audit content. These other determinants are described in Section C, where the individual audit fields are dis­cussed.

**Overview**

For identifying the appropriate audit methods to be used, SAP internal auditors consider several important content determinants and formal determinants. The content determinants of an audit method are described first, followed by the formal determinants. Content determinants include the audit fields and the audit ap­proaches.

**Content Determinants**

At SAP, the audit universe is divided into six audit fields (for more information on audit fields refer to Section A, Chapter 6.2.i):

**Audit Fields**

* management audits,
* operational audits,
* financial audits,
* IT audits,
* fraud audits, and
* business audits.

In principle, each audit field listed above has the same significance to Internal Au­dit, as each is exposed to core business risks. These risks are measured by assessing the individual risks as part of the annual audit planning (see Section D, Chapter 3.1.2) and are monitored during the fiscal year through the risk management pro­cess. Thus, there may be a different number of individual audits required for each audit field as determined by the annual risk assessment.

**Importance of the Audit Fields**

Conceptual Basis of Internal Audit Audit Methods

Content Determinants and Formal Determinants

The content of audits is determined not only by the audit fields but also by the audit approaches that the internal auditors use (see Section A, Chapter 6.3 for de­scriptions of each audit approach). The different approaches are as follows:

**Audit Approaches**

* risk-based audit approach,
* system-based audit approach,
* transaction-based audit approach,
* compliance-based audit approach, and
* results-based audit approach.

Each audit field has its own set of specific attributes, thus the emphasis of the audit method is different in each case. Therefore, audit approaches can generally be aligned with the specific audit fields, and standardized combinations can be created for audit methods (for more information see Section A, Chapter 6.3). The correla­tion identified between audit field and audit approach thus creates a guidance framework for conducting audits, which allows auditors to quickly establish the individual audit steps required.

**Assignment of Audit Approaches to Audit Fields**

In addition to content determinants, an audit method is also shaped by formal determinants. They include audit category, audit type, and audit cycle. The audit categories are local, regional, and global audits (see Section A, Chapter 6.4). The audit typology defines audits as standard, special, or ad-hoc audits (see Section A, Chapter 6.5). The audit cycle generally consists of the basic audit, a status check, and (up to two) follow-up audits (see Section A, Chapter 6.6).

**Formal Determinants**

By combining the audit determinants into a consolidated approach, Internal Audit is able to establish the final design of the particular audit method to use. Thus, for each specific audit, the auditors must consider the following factors:

**Merging of Determinants**

* assignment to an audit field,
* audit approach,
* audit category,
* audit type, and
* audit cycle status.

The special characteristics of each formal determinant, in combination with the content determinants, allow Internal Audit to identify the appropriate audit method. For example, assume Internal Audit is planning a routine audit of the pur­chasing process at a regional shared service center and will examine various pur­chase transactions to determine whether the controls are working effectively. The auditors must define each of the determinants when identifying the appropriate audit method to use, as follows:

* audit field: operational,
* audit approach: transaction-based,
* audit category: regional,
* audit type: standard, and
* audit cycle: basic.

The following diagram shows how the audit method is determined by the content and formal determinants with their possible characteristics.

***Fo***

**Determination of the Audit Method**

**c?**

Local

Regional

Global

Standard audit Special audit Ad-hoc audit

%

**vr**

**o'**

***%■***

***% ^***

Management audit Operational audit Financial audit IT audit Fraud audit Business audit

Basic audit Status check Follow-up

Risk-based

System-based

Transaction-based

Compliance-based

Results-based

■Approach

**ants**

Fig. 17 Determining the Audit Method with Content and Formal Determinants

**HINTS AND TIPS**

• The differences between the individual audit methods must be clear-cut. Decide together with the Audit Manager in charge which audit method to use in any given case.

1. Audit Field Structure 6.2.1 Introduction

**KEY POINTS •••**

* The audit fields represent the core audit tasks of Internal Audit. Based on the Audit Roadmap, the specific audit methods are applied to the audit fields.
* There are interdependencies between the individual audit fields. It is very rare that an audit will address only one audit field in isolation.
* Increasingly, Internal Audit’s work must be viewed from a profitability perspec­tive. Thus, a cost/benefit analysis is frequently performed.

The audit fields represent the core audit tasks of Internal Audit. Therefore, most Audit Fields audit requests can be classified within the audit fields. Each of these audit fields has several Core Scopes, which in turn contain the Key Scopes at lower levels (see Sec­tion A, Chapter 5.3 and Section B, Chapter 2.1).

Management

|  |  |  |  |
| --- | --- | --- | --- |
| Finance and accounting | | | |
| TT TT \*1 | TT  TT | Tt  Tt  ^ | TT  TT |

Operations

Fig. 18 Overview of Audit Fields

The audit fields shown in the diagram above are audited on the basis of different Scopes using specific audit methods. Ultimately, however, all audits are conducted according to a standard process model, the Audit Roadmap (for details, see Sec­tion B).

At first glance, the audit fields appear to be independent of each other, but they do have commonalities. For example, a fraud audit may also include a financial audit. The same applies to business audits. And operational audits are regularly part of any audit (for combined audit topics see Section B, Chapter 5). The rest of this chapter briefly outlines the focus of each audit field. More detailed descriptions are provided in subsequent chapters.

**Basics**

**Interdependencies**

**Management**

**Audit**

**Operational Audit**

**Financial**

**Audit**

**IT Audit**

**Fraud Audit**

**Business Audit**

As part of a management audit (see Section A, Chapter 6.2.2), Internal Audit tests whether management complies with existing policies, guidelines, and proce­dures and whether its decisions and the associated internal controls are effective and efficient.

Operational audits (see Section A, Chapter 6.2.3) address issues relating to both organizational and workflow structures. They can affect almost any operational business unit. The audit normally comprises all issues of process design, internal controls, risk cover, and any relevant financial accounts.

The main focus of a financial audit (see Section A, Chapter 6.2.4) is on examin­ing the accounting and financial data of the organization. The focus is different, depending on the audit topic: Either, the accounts and financial data can be audited as a whole on the basis of an analysis of the financial statements, or the audit can be conducted on the basis of individual accounts.

The aim of IT audits conducted by Internal Audit (see Section A, Chapter 6.2.5) is to test relevant system structures and processes for their alignment with IT, in­cluding compliance with applicable guidelines and risk mitigation. This audit field covers all process-related issues, ranging from organization, structure, and proce­dures (including project management) through access authorization, data and anti­virus protection. In a software company like SAP, the entire software development process can have an influence on IT audits. Therefore, SAP’s Internal Audit has formed a dedicated global IT audit team.

Fraud audits (see Section A, Chapter 6.2.6) are aimed in particular at identifying suspected organizational and process weaknesses, investigating anonymous accu­sations or specific information on irregularities, or gathering evidence for cases of fraud that have already been proven. In this context, it is of special importance to establish whether and to what extent an incident has led to directly measurable, or at least indirectly related, financial consequences for the company.

External business relationships also give rise to audit-relevant issues for Internal Audit, because the network of suppliers, customers, and partners, relations with public institutions and organizations and even government bodies ultimately have a significant influence on the internal processes of a company. A business audit (see Section A, Chapter 6.2.7) is a preventive audit measure conducted in line with the

de-escalation strategy. Its main purpose is to ensure that processes, methods, and guidelines within a project are compliant and take third parties into account.

In today’s environment, the effect of Internal Audit’s work on profitability is in- Cost/Benefit Analysis creasingly important. Thus cost/benefit analyses are frequently performed. Cost/ benefit analysis can be performed for each of the above audit fields. In doing so, the focus should always be on the audit as a whole, i.e., if a combination of several audit fields is used, all components must be subject to efficiency measurement (for de­tails, see Section A, Chapter 6.7).

**HINTS ANDTIPS •**

* At the start of an audit, auditors must be aware of the audit field to which the audit task in question belongs.
* Especially when interdependencies exist, consistent assignment to the audit fields facilitates the structuring of the audit engagement.
* Auditors should try to gather practical experience in all audit fields in order to enhance their personal flexibility and eligibility for engagements.

1. Management Audit

**KEY POINTS •••**

* During a management audit, Internal Audit tests management’s compliance with the established policies, guidelines, and procedures.
* Internal Audit also examines the effectiveness and efficiency of management decisions and the associated internal controls.
* The effect of management decisions is a key benchmark of how successfully managers perform their management duties.
* For a variety of reasons, management audits conducted by Internal Audit may lead to difficulties, depending on the corporate culture, the role and importance of management, as well as the managers to be audited and the auditors them­selves.

When conducting a management audit, Internal Audit must determine whether all Compliance the necessary processes and guidelines have been defined in the company, enabling managers to execute their duties according to the established rules. Auditors must also investigate whether managers act in compliance with the established rules and policies.

In addition, Internal Audit may audit the efficiency and effectiveness of corpo- Efficiency rate management. Even if managers are very committed to their tasks, it is possible and Effectiveness

that the company as a whole derives little benefit from their activities. If that is the

case, the role of management should be reconsidered and realigned if appropriate. In addition to the financial effects of management’s activities, Internal Audit must consider how management’s actions affect the motivation and conduct of employ­ees. One of the key points of a management audit is to ensure that management activities are not only duly performed, but lead to the desired results and thus be­come measurable.

The two key types of management audits described above (compliance audits and management effectiveness and efficiency audits) make up the complex field of management audits for Internal Audit. During the course of a management audit, the internal auditors should consider:

**Management Audit as an Audit Field**

**Process- and Results- based Audits**

**Activities in the Interest of the Company**

**Historical and Forward- Looking Analysis**

**Examining the Process Chains**

**Guidelines and Instructions**

* Process-based assessment of all aspects of governance as well as a results-based investigation of decision-making within the company as a whole.
* The extent and the manner in which the managers concerned use the entrepre­neurial powers vested in them to the benefit of the company. This includes, in particular, the control of extraordinary management and decision-making situ­ations, as well as crisis management. It involves all the process steps of escalation (and conversely, of course, de-escalation) procedures across various manage­ment levels. The audit assesses the existing and required management and com­munication tools, and how the tools are used to communicate with both superi­ors and subordinates.
* Management’s past leadership and areas for future improvement, e.g. moving from a problem-based to a solution-based management approach.

In summary, the main focus of a management audit is the entire management pro­cesses, including internal controls. Thus a management audit is mainly about exam­ining all the process chains that managers deal with as part of their strategic and operational tasks. The management audit focuses on the manager’s willingness to accept processes and their internal controls and to apply them accordingly. For as­sessing leadership qualities, employee satisfaction, and the efficiency of the manag­er’s personal management behavior, there are other, more suitable tools, such as management evaluations performed by the human resources department.

When implementing these audit requirements, Internal Audit makes use of a number of existing procedures, documents, and external specifications. For exam­ple, Internal Audit should examine whether corporate-wide policies and guidelines are implemented and applied. This includes whether each employee has a clear un­derstanding of the company’s strategic and operational objectives. It is the only way to justify and enforce certain courses of action among employees and to align and commit all involved parties with the basic objectives of the company. On the one hand, this may involve general principles, such as standard rules of conduct for all employees. On the other hand, however, special guidelines can also be drawn up for individual business areas or operational units and functions, such as general secu­rity and IT security.

Management audits also examine compliance with legal and financial reporting requirements. If these external requirements demand entrepreneurial action and company-internal implementation, the audit work of Internal Audit ensures that the relevant processes are compliant, complete, and correct. This allows Internal Audit to help minimize the company’s exposure to legal risks.

In the context of a management audit, an employee survey or the general moti­vation of the team assigned to a manager may provide clues as to the degree to which the responsibilities of a management function are met.

**Legal and Financial Reporting Requirements**

**Personnel Management**

**Management Controls**

**Special Challenges of Management Audits**

**Mistrust**

**Impact on the Standing of Employees**

The examination of management controls is of high importance for compliance with policies, guidelines, and procedures. Management controls must be estab­lished for all activities, including objective-setting, process development and ap­plication, decision implementation, and information and documentation activities. Internal Audit must investigate and verify whether these controls are adequately defined and documented and working as intended. This includes management’s responsibilities for compiling and tracking minutes and activity lists and maintain­ing an adequate internal reporting system to the relevant higher and lower ranking management levels. Internal Audit must also ensure that all processes for which management is directly accountable are compliant with the policies of the organiza­tion as well as with external requirements (e.g., legal and financial regulations).

Management audits are characterized by specific challenges. They depend on the corporate culture of the organization and thus the role and importance of man­agement per se, as well as on the personalities of the managers to be audited and the auditors themselves. Due to the required sensitivity, a management audit should be conducted by experienced internal auditors. Ideally, internal auditors who have worked in a management function may be best suited to perform these audits. Other reasons why management audits conducted at the request of the Board pres­ent a special challenge for Internal Audit can be summarized as follows:

* Management audits conducted at the request of the Board may be interpreted as a sign of mistrust in management. This may lead to irritation especially if the company’s position is healthy on the whole and at first glance there do not seem to be any specific reasons for an audit. This may have a company-political im­pact, damaging the relationship of trust between the Board and management. It may be very helpful, even before an audit, if the Board of Directors maintains a clear information policy with regard to audits.
* Managers fear that serious negative findings made by Internal Audit may cause them to lose standing with Internal Audit, the Board of Directors, and perhaps even colleagues and their own employees. For fear of negative consequences, managers may refuse to cooperate or make the auditors’ work more difficult. This makes it hard to arrive at objective audit findings, damaging the working relationship between management and Internal Audit and hampering coopera­tion. In some cultural groups, negative audit findings are interpreted as indi­vidual failings at a purely personal level. This may irreparably damage the man-

**Existing Quality Problems**

**Manager Personality**

**Conflict with Activities of Other Departments**

**Confidential Information**

**Summary**

agers’ standing and reputation, especially with regard to their own line managers. This area in particular is where Internal Audit faces the challenge of presenting the results as impartially as possible, supported by examples.

* If managers already have problems regarding the quality of their work, negative audit reports may further weaken their standing in the company. If that is the case, it is difficult to give the person concerned an objective view of the audit. Internal Audit should then act as a consulting partner and convince managers that, by eliminating the weak points identified by the audit, they may also im­prove their performance with regard to other success factors.
* Managers may generally regard their work as confidential and may be reluctant to share their working practices with others. In such cases, Internal Audit must take a sensitive approach so that it can examine the facts on the basis of a per­sonal relationship of trust.
* Management audits may cause problems if they clash with the activities of other departments, such as employee surveys carried out by Human Resources. How­ever, such activities have a different focus and are based on a completely differ­ent method. Whereas the investigations of Internal Audit normally focus on management processes and the associated internal controls and risks, evalua­tions carried out by other departments are aimed at establishing the personal suitability of each manager. It is important to make this distinction dear and to demonstrate this fact on the basis of the audit findings. For this reason, manage­ment audits should internally also be referred to as management process au­dits.
* Finally, management may be resistant to the audit because being audited re­quires the manager to reveal information, which may lead to a serious moral conflict for managers. That is, management must decide what information can be given to Internal Audit, and what must be kept confidential. Of course Inter­nal Audit is also required to keep information secret and confidential, but there is a large pool of confidential data that is difficult to deal with in this context. In addition to personal information, this may involve strategic and company-po­litical information or budgeted sales and profit figures.

Within the context of a management audit, Internal Audit should focus on pro­cesses, the associated internal controls and specific individual risks, and how man­agement deals with these risks. Depending on the degree of personal trust, each management audit will develop its own momentum to some extent, which should be handled in such a way that the audit objectives can still be met.

**HINTS AND TIPS •**

• Auditors must familiarize themselves thoroughly with the manager s personal­ity, taking into account any problems from the past.

* Because management audits require sensitivity, the work program should be reviewed by an impartial member of Internal Audit before the commencement of the audit.
* Characteristics typically associated with managers (lack of time, etc.) must not prevent Internal Audit from conducting its audit.
* The sensitivity of management’s data must be considered.

**LINKS AND REFERENCES**

* ANDERSON, U. AND A. DAHLE. 2006. Implementing the Professional Practices Frame­work. 2nd ed. Altamonte Springs, EL: The Institute of Internal Auditors.
* INSTITUTE OF INTERNAL AUDITORS. 2000. The International Standards for the Professional Practice of Internal Auditing. Altamonte Springs, FL: The Institute of Internal Auditors.
* INSTITUTE OF INTERNAL AUDITORS. 2001. Practice Advisory 2120-A1-1: Assess­ing and Reporting on Control Processes. Altamonte Springs, FL: The Institute of Internal Auditors.

. SAWYER, L„ M. DITTENHOFER, AND J. SCHEINER. 2003. Sawyer’s Internal Audit­ing. 5th ed. Altamonte Springs, FL: The Institute of Internal Auditors.

1. Operational Audit

**KEY POINTS •••**

* Operational audits can address issues relating to both organizational and work- flow structures. They can affect almost all business units.
* Operational audits may examine traditional, corporate-wide, and project-re­lated processes.
* The audit normally comprises several audit steps, which deal with all issues of process design, internal controls, risk cover, and any relevant financial accounts.
* In addition to the actual processes, the controls set up in the company must be examined and verified with suitable tests.

**Audits of Core Business Processes**

Operational audits include audits along the entire value chain of a company, or specific parts of it. Under the materiality principle, however, a careful selection should be made of the core business processes to be audited and the affected busi­ness units. Responsibilities and processes that either are of lesser importance or not exposed to risks that threaten the existence of the company or its business success are included in Internal Audit’s annual audit plan according to their risk profile.

An initial analysis identifies the following organizational units as common ob­jects of operational audits:

**Main Objects**

**of the Operational Audit**

* specific business units (e.g., development, sales, consulting) and their core func­tions and central tasks,
* central corporate divisions (e.g., Corporate Financial Reporting, Corporate Management Accounting),
* local subsidiaries,
* associates that fall within the remit of Internal Audit due to a majority interest or other legal agreements (in the case of minority interests), and
* other investment relationships (e.g., venture capital participations, joint ven­tures, etc.).

The main function of an operational audit is to improve the organization and work- flows of the company. In this regard, a systematic audit focuses on analyzing the organizational structure, as well as individual processes or transactions. The main objective is to ensure that all the organizational solutions of the company are com­pliant with relevant rules and regulations.

**Objectives**

**Processes versus Discrete Items**

**Internal Control Audit**

**Other Objects of the Operational Audit**

**Recording of Processes and Controls**

The process-oriented approach focuses on entire processes and organizational units rather than on individual circumstances and transactions. The intention is that this kind of audit should identify underlying risks and their interdependencies and thus pinpoint ways in which the information gained can be used to improve the security, efficiency, and reliability of internal processes. In the above organizational units, Internal Audit therefore examines all business, organizational, and legal issues, responsibilities, authorizations, and procedures, the controls assigned, and the risks to be covered.

Audits of internal controls associated with processes have taken on greater im­portance now, because SOX requires the CEO and the CFO of companies listed on U.S. stock exchanges to verify, in writing, the existence and effectiveness of key in­ternal controls as part of its reporting to the SEC (see Section D, Chapter 14).

In addition to the audit objects mentioned above, there are other areas on which operational audits focus. These areas have strong interrelations between audit ob­jects and process steps. Some main areas are:

* global units (e.g., initiatives, departments),
* person-specific issues (e.g., incentive scheme, pension scheme),
* reviews of external and internal projects with regard to project management, contracts, and project content,
* the entire risk management process, and
* information management between established organizational units and proj­ects/initiatives.

An important prerequisite for efficient operational audits is that Internal Audit document all processes, including controls. This is done at the beginning of the fieldwork for process documentation purposes (see Section C, Chapter 8 and Sec­tion D, Chapter 14). In addition to describing each process step, the controls that

the company has established for each process are documented, focusing mainly on the following questions:

* What controls exist in the company at the moment?
* Who is responsible for the controls?
* How are the controls documented?
* Are the controls sufficient to cover material risks?

There are several types of controls that organizations may use, including manual, organizational, automated or programmed controls (see also Section C, Chapter 8). Examples of organizational and manual controls include the segregation of duties, dual control, signature rules, and IT system authorizations. Automated and pro­grammed controls, on the other hand, include consistency and plausibility checks.

As part of the audit, Internal Audit performs an analysis of the business pro­cesses to identify and highlight their strategic importance, the risks, and controls with a focus on the overall objectives and strategy of the organization as well as in the context of the relevant business risks. In the first instance, the documented pro­cess steps required to meet the objectives are analyzed. Here, Internal Audit uses interviews, documents, and guidelines to examine and assess whether the content and purpose of each process make sense. In addition, Internal Audit must establish whether the design of the process is logical, sensible, and effective, whether its structure is clear, and whether it ensures that the intended objective is met.

At this stage, the existing and any missing process controls are identified and examined for correct and full implementation. In particular, the audit must estab­lish whether the controls are adequate, sensible, and sufficient for the process con­cerned, as well as demonstrate and ensure that they function as intended. Under the requirements of SOX, the issue of responsibility for the controls and documenting them is of particular importance.

Another step of the operational audit is to examine to what extent the controls identified cover the established or additional process risks so that they can be mon­itored. Each possible process risk should be monitored and mitigated by at least one corresponding process control. This may lead to additional controls or the develop­ment of controls related to other process steps.

SOX requires another process analysis step: The adequacy and effectiveness of the controls that have an immediate effect on the accounting figures must also be tested. That is, controls must be established that ensure that financial reporting fairly represents the financial condition of the company.

In addition to process analysis, other types of fieldwork are necessary to test process application. In the first instance, discussions should be held to determine whether the employees observe all the guidelines and instructions, whether the flow of information is guaranteed, and the process is practiced as designed. These interviews will demonstrate to what extent the employees are familiar with the pro­cesses.

**Possible Controls**

**Analysis of Business Processes**

**Content of a Control Assessment**

**Process Control**

**Link with Accounting**

**Staff Interviews**

Moreover, examination of documents such as guidelines, contracts, extracts from the commercial register, powers of attorney, etc. should be included in the audit. Thus, an operational audit covers more than testing the internal controls only.

**Document Testing**

**Process Documentation**

**Process and Control Tests**

**Operational Audits and Other Audit Areas**

All process steps, including the internal controls, must be documented fully and in detail. SOX requires that this process documentation (for those processes that affect financial reporting) must be available and up to date at all times. This can be achieved by using a suitable IT tool.

The actual testing of each process and the associated internal controls is another focus of audit work. Various methods can be used. With the help of appropriate sampling procedures, samples of processes are drawn and then tested with regard to the existence and compliance of controls. An alternative method is what is known as the walk-through, where the auditor personally traces a specific transaction or economic event step-by-step through parts of the process or the process as a whole, including all controls. The advantage of this method is that the approach considers all aspects of the process. In practice, a combination of both test methods will ulti­mately be suitable for conducting the actual audits (see the practical examples in Section C).

Operational audits may be performed as a separate audit engagement, but it is important to note that they may also be performed in conjunction with an audit of another audit field (e.g., fraud or financial audit). For example, financial audits gen­erally require operational audits to verify and document the validity of the financial data analyzed.

**HINTS AND TIPS •**

* At the start of an audit, the auditor should ask the process owner to explain the process by means of a walk-through.
* Analyze the documentation available for the process carefully. Aim and purpose of the whole process must be clear.
* The auditor should conduct interviews to get the employees’ opinion of the pro­cess to be examined. Confidential meetings to discuss suggestions or requests made by the employees involved in the process may be a good way to obtain valuable information.

**LINKS AND REFERENCES**

* ANDERSON, U. AND A. DAHLE. 2006. Implementing the Professional Practices Frame­work. 2nd ed. Altamonte Springs, FL: The Institute of Internal Auditors.
* INSTITUTE OF INTERNAL AUDITORS. 2000. The International Standards for the Professional Practice of Internal Auditing. Altamonte Springs, FL: The Institute of Internal Auditors.

• INSTITUTE OF INTERNAL AUDITORS. 2001. Practice Advisory 2120-A1-1: Assess­ing and Reporting on Control Processes. Altamonte Springs, FL: The Institute of Internal Auditors.

. SAWYER, L„ M. DITTENHOFER, AND J. SCHEINER. 2003. Sawyers Internal Audit­ing. 5th ed. Altamonte Springs, FL: The Institute of Internal Auditors.

1. Financial Audit

**KEY POINTS •••**

* When performing financial audits, auditors examine both accounting and fi­nancial data.
* During an audit, auditors can either examine the financial statements as a whole, or analyze individual accounts and items.
* During financial audits, all applicable legal, tax, and accounting standards must be observed.

Financial audits are generally defined as an independent evaluation of past account- Definition

big data for the purposes of assessing whether this data is appropriate, compliant, and reliable, of protecting the assets of the company, and of expressing an opinion on the effectiveness of the internal control system. As part of a financial audit, In­ternal Audit examines areas such as the financial accounts of the company, the pay­roll system, asset management, and the annual financial statements. There are two options in this regard:

* Accounts and financial data can be tested as a whole, based on an analysis of the financial statements, or
* individual accounts and items can be examined specifically using qualified sam­ples.

If the financial data is to be examined as a whole, it is advisable to analyze the finan- Analysis of the Financial

cial statements first. To this end, the data from the balance sheet and income state- Statements ment to be audited should be compared with the corresponding figures of the pre­vious period and analyzed for any unusual items or discrepancies. In addition to period comparisons, object-related comparisons can also be performed, (e.g., local subsidiaries of similar size and with comparable business activities). The compari­son can be made either by using absolute figures or by calculating certain key ratios (e.g., certain accounting ratios like debt/equity ratio, profit ratio, cash flows etc.).

Next, the ratios should be compared with external figures, such as corresponding ratios at peer organizations. This may help auditors identify unusual items among the selected variables from the balance sheet and income statement. Depending on what they have observed, auditors must decide whether these comparisons should

be continued for each case down to the individual account level, in order to estab­lish the underlying causes of any changes or variances. To evaluate the need for more detailed examinations, permissible ranges for variances must be defined. If a variance exceeds the defined threshold, the audit must continue down to individual accounts. Importantly, thresholds should be set in accordance with the materiality principle so that the audit remains manageable. That is, only material findings should be followed by a more detailed examination.

At a minimum, financial audits should include examination of the following accounts: Noncurrent assets, inventories, receivables, cash and cash equivalents, provisions, liabilities, prepaid expenses, and deferred income from the balance sheet; revenue and certain expenses, such as personnel and travel expenses, train­ing costs, and other expenses from the income statement.

**Items to Be Audited**

**Problem of Revenue Recognition**

**Items /Accounts**

**General Rules and Regulations**

In global software companies such as SAP, audits of license agreements and con­sulting contracts are particularly important to ensure that revenue is recognized correctly (see Section C, Chapters 5.2, 5.3 and 9). This often entails complex pro­cesses and controls that involve various departments (such as finance, development, product support, training, etc.). Audits focusing on revenue recognition should in­clude the following topics:

* Software license agreements, taking into account issues such as pricing, mainte­nance, special agreements, legal issues, and accounting policies.
* Any type of consulting contract (for example, fixed-price, or time-and-material projects), taking into consideration legal issues, including accounting policies and the possibilities of individual project reviews.

If the examination of accounting and financial data focuses on a targeted analysis of selected accounts and items, the method described for analyzing the financial state­ments can be used initially. However, the variance limits should be defined more narrowly and accurately so that absolute and relative variances can be detected. Often, specific key variables may be useful (e.g. days overdue, or the discount and credit note ratio). If appropriate, each account is compared and analyzed in turn. Especially in global audits, the careful selection of appropriate subsets or supersets may produce important information (e.g., a summary of balances outstanding from the 50 most important customers). Careful and deliberate evaluation of individual accounts and items should detect the transaction(s) that may be the cause of any inconsistencies identified. However, the principle of materiality can and must be observed in such instances. This means that time and resources for auditing indi­vidual transactions are limited and the materiality and efficiency principles must again be applied.

The accounting function is governed by national and international accounting standards and laws. Companies, such as SAP, that are listed on the U.S. Stock Ex­changes must also comply with US-GAAP and the requirements of the SEC. Such companies must undergo financial statement audits performed by independent ex­ternal audit firms to comply with SEC regulations. In addition to these general stan-

dards, companies often have to observe sector-specific regulations and their inter­nal accounting guidelines.

**HINTS ANDTIPS •**

* Ahead of a financial audit, auditors should try to identify items that could be critical in the balance sheet and income statement.
* The company’s annual report is another document on which Internal Audit can base a preliminary assessment.
* Auditors should look at the documentation of findings from previous audits.

**LINKS AND REFERENCES \***

* ANDERSON, U. AND A. DAHLE. 2006. Implementing the Professional Practices Frame­work. 2nd ed. Altamonte Springs, FL: The Institute of Internal Auditors.
* INSTITUTE OF INTERNAL AUDITORS. 2000. The International Standards for the Professional Practice of Internal Auditing. Altamonte Springs, FL: The Institute of Internal Auditors.
* INSTITUTE OF INTERNAL AUDITORS. 2001. Practice Advisory 2120-A1-1: Assess­ing and Reporting on Control Processes. Altamonte Springs, FL: The Institute of Internal Auditors.
* INSTITUTE OF INTERNAL AUDITORS. 2001. Practice Advisory 2120-A1-3: The Inter­nal Auditor’s Role in Quarterly Financial Reporting, Disclosures, and Management Certifi­cations. Altamonte Springs, FL: The Institute of Internal Auditors.
* INSTITUTE OF INTERNAL AUDITORS. 2001. Practice Advisory 2120-A1-4: Audit­ing the Financial Reporting Process. Altamonte Springs, FL: The Institute of Internal Auditors.

. SAWYER, L„ M. DITTENHOFER, AND J. SCHEINER. 2003. Sawyer’s Internal Audit­ing. 5th ed. Altamonte Springs, FL: The Institute of Internal Auditors.

1. IT Audit

**KEY POINTS •••**

* The aim of IT audits conducted by Internal Audit is to test relevant system struc­tures and processes for their compliance with applicable policies, guidelines, and standards.
* This audit field covers all process-related issues, ranging from planning and or­ganization, information, and support (including project management) to access authorization, and data and anti-virus protection.
* During the audit, it is important to integrate all relevant (internal and external) guidelines and written documentation.
* The structure of the IT processes should be examined in terms of their over­all integration into the entire business process. The main focus in this regard should be on the interaction of organizational and automated controls.
* IT audits can have an internal as well as an external focus.
* The expertise required for IT audits has led to the creation of a separate auditor profile.

Information technology is an integral part of all companies. The information made available through the use of IT must meet the requirements of business processes so that business goals can be achieved. A thorough audit of relevant IT-related matters is therefore an essential part of the work performed by Internal Audit. Because IT is such an extensive area, it has established itself as a separate audit field. The follow­ing are the main audit objectives in the area of information technology:

**Positioning**

**The Changing Face of IT**

**Factual Basis IT Audits**

**IT Governance Focus Areas**

* Controls must be in place to ensure that all IT processes (internal and external) include the necessary data processing functions and meet the relevant security standards at the time the system is deployed. Internal Audit should check to ensure that these IT processes operate as designed.
* In addition, these IT processes have to comply with the latest corporate-wide policies, guidelines, and standards as well as legal obligations.

Like no other aspect of business, information technology is subject to constant change and ongoing development. The innovations in this area are reaching ever greater dimensions. For this reason, Internal Audit faces the permanent challenge of adapting to changes in the technical and software environment as quickly as pos­sible.

A large number of external guidelines and internal rules form an important basis for IT audits. The COBIT® (Control Objectives for Information and related Technology) framework is particularly useful in an organization with a strong in­formation technology environment. The COBIT® framework was issued and is maintained by the Information Systems Audit and Control Association (ISACA). COBIT® supplements COSO and SOX by focusing on the governance of IT re­sources and processes.

COBIT® is especially helpful because it provides a framework and supporting tool set that bridges control requirements, technical aspects and business risks. The IT governance focus areas in COBIT® reflect the central points of the IT audit dis­cussed later in this chapter.

* Strategic alignment emphasizes aligning IT strategy and operations with the organization’s strategy and operations.
* Value delivery ensures that IT delivers the desired benefits.
* Resource management is concerned with the optimal investment in and man­agement of IT resources.
* Risk management includes the transparency of significant IT risks and IT’s awareness of the organization’s risk exposure.
* Performance measurement tracks and monitors IT’s role in strategy implemen­tation, resource usage and process performance.

IT governance may be separated into the responsibility domains of plan, build, run, and monitor. The COBIT® framework labels them Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate, and identifies the pro­cesses and activities within each of the domains accompanied by several control objectives.

**Responsibility Domains**

**Legal Requirements and Internal Guidelines**

* Plan and Organize - Provides direction to solution and service delivery. Typical audit questions include:
* Are the business strategy and IT strategy aligned?
* Is the organization achieving optimum use of IT resources?
* Are IT risks understood and managed?
* Is the quality of IT appropriate for business needs?
* Acquire and Implement - Provides the solutions to be turned into services. Typical audit questions include:
* Are new projects likely to deliver solutions that meet business needs?
* Are new projects delivered on time and within budget?
* Are changes made without upsetting business operations?
* Deliver and Support - Is concerned with the actual delivery of required services and support for those services. Typical audit questions include:
* Are IT services being delivered in line with business processes?
* Are IT resources optimized?
* Is the workforce able to use the IT systems productively and safely?
* Are adequate confidentiality, integrity, and availability controls in place for information security?
* Monitor and Evaluate - All IT processes should be regularly assessed for quality and compliance with both internal and external control requirements. Typical audit questions include:
* Is IT’s performance measured to detect problems in a timely manner?
* Are internal controls effective and efficient?
* Can IT performance be linked back to business goal?
* Are adequate confidentiality, integrity, and availability controls in place for information security?

In addition to the guidelines of the COBIT® framework, legal requirements that recognize the growing concern for privacy must be observed. The Financial Mod­ernization Act of 1999 (also known as the Graham-Leach-Bliley Act) requires fi­nancial institutions to adhere to a set of privacy requirements on consumers’ per­sonal financial data. The Health Insurance Portability and Accountability Act (HIPAA) introduced privacy and security rules covering personal healthcare re­cords. Internationally, legal requirements such as the German Data Protection Act and rules about the security of user-specific data must be observed. Company-spe-

cific internal guidelines and work instructions on technical application-based data

handling must also be complied with.

When preparing for and conducting IT audits, Internal Audit has to focus on

**Central Points of the IT Audit**

the following issues:

* Strategic IT planning: This issue includes aspects of a corporate-wide standard­ized IT strategy, IT-based support of company activities, monitoring the IT market for new developments, and questions relating to the implementability of feasibility studies and system analysis. A critical aspect of strategic IT planning is the alignment of IT goals with business goals.
* Risk management for the IT process: Risks must be identified and their poten­tial impact estimated. The actions taken to minimize risk must be analyzed.
* IT-related infrastructure: This area deals with auditing relevant aspects of physi­cal security, logical access authorizations, and data backup and archiving sys­tems.
* Organization of the IT function: This area primarily looks at aspects of organi­zational structure and process organization in the information technology func­tion, as well as the distribution of central and decentralized IT tasks, operational IT planning, and the entire change management process. This also includes the resource management of IT assets and performance measurement of the IT function.
* Operational IT processes: Internal Audit has to verify whether the information technology assures the continuity of business processes. The audit may cover all steps, from planning to operational implementation, of the IT process and its subprocesses, including all backup and alternative procedures.
* IT applications: This area looks at the entire development, maintenance, and change process during the in-house creation of software, including all testing and release procedures. At the same time it checks that the software versions used are up to date.
* IT project management: Under this aspect, the overall project framework is tested, including issues of project organization, project planning, and the run­ning of the project, including risk management and financial project control.
* Usage of IT applications: this aspect focuses on examining relevant authoriza­tions, system settings, internal controls and reconciliations, as well as reporting and documentation functions.
* Communication security: This area is a significant aspect of all data commu­nication with external parties and therefore an important object in the work of Internal Audit. It includes auditing the use of anti-virus software and firewalls to protect information technology from outside attacks.
* Data protection functions: Audits of this aspect examine whether all privacy re­quirements relating to comprehensive data protection are met, including tracing all sensitive data in the system and logging access right changes, access protec­tion, and all aspects of consistent data maintenance.

The items listed above primarily involve the elements traditionally associated with operational audits. In general, process structures, risks, and internal controls should be examined from an IT perspective as well. This means that inherent technical, organizational, and in some cases even financial-reporting and legal aspects inter­act as part of the processes.

IT audits are conducted on the basis of an extensive IT system environment. In this regard, we differentiate between the following processes:

**IT Audit as Operational Audit**

**Alignment with the System**

**Security-Relevant Levels**

**Internal Controls In the IT Audit**

**Internal and External Focus of the IT Audit**

* purely organizational processes,
* a combination of organizational and IT processes, and
* purely IT processes, i.e. those that run only within the system.

When these process types are reflected in the structure of a modern IT landscape, the following security-relevant levels can be distinguished:

* The pure hardware level is characterized by logistical security matters. Here the audit should focus on the extent to which appropriate equipment and build­ings security is in place, for example access control, emergency plans, anti-terror measures, and protection from force majeure. This also includes the technical aspects of the entire maintenance program and data archiving.
* The operating system level relates to audits in the whole area of system technol­ogy, the user concept, failure control, and the relevant authorizations, including access to special operating software functions, such as data backups.
* The application software level also comprises audits of authorization control, system settings, workflows, the structure, nature, and frequency of certain data, figures, and documents, as well as the change service and system archiving. This level also covers interfaces with internal and external systems.
* User guidance and the user interface are also part of an IT audit, because the main parameters of a computer have to be examined, e.g., specific settings or access paths to data sources or internet sites. In some countries (e.g. Germany), however, this requires the employee’s explicit permission or a court order if the circumstances are suspicious.

Examining all these levels in sequence will ensure that a complete IT audit is con­ducted.

Internal controls exist both outside of and within the system processes. Here it is important to take the individual steps in a consistent sequence, i.e., the controls must fit together and must be mapped logically and without conflict. The possibili­ties the system offers for logging individual process steps provide an important basis in IT audits for meeting evidence and documentation requirements. Since the area of information technology has different escalation levels, resulting in different con­sequences for audit findings, the risks and internal controls have to be particularly closely linked with the relevant process chains. For this reason, risk-based auditing is a core element of the corporate-wide audit approach, especially in the area of IT.

IT audits can have both an internal and an external focus. Internally, the audit focuses on system-internal business processes. Externally, audits often examine the

data of business partners, such as customers and suppliers, but also data communi­cation by e-mail and internet. The examination includes measures to protect the IT system from technical manipulation attempts and virus protection, as well as pos­sible access rights for third parties. Especially internally, Internal Audit has to make sure that the legal and system-related requirements of the technology vendor are respected. In doing so, the responsibilities of individual employees for the whole or part of a process have to be clarified and checked. Any additional internal factors that could have a negative impact on the process also constitute an object of an IT audit conducted by Internal Audit.

Due to the expertise that IT audits require, a specific IT auditor profile should be developed. IT auditors must have sufficient know-how to cover the whole area. For this reason, it is essential to conduct adequate training measures for Internal Audit employees.

**Auditor Profile**

Global  
audit model

Documents

|  |  |  |
| --- | --- | --- |
| iual Work  plan program | Working  papers | Reports |
| \ / w | | |
| • Programs | • Programs | • Programs |
| • IT tools | • IT tools | • IT tools |
| • SAP applications | • SAP applications | • SAP applications |

Regional Internal Audit structure (working level)

Reports

Central

archiving

structure/

database

Annual  
audit plan

Work

programs

Working

papers

f Virus ^ protection

Internet

Archiving

f Data ^ protection

Access

rights

Regional

reporting

Fig. 19 Audits of the Global IT Environment

Particularly in IT audits, cooperation with the external auditors is very important, because they have to form an opinion on the reliability and effectiveness of the in­ternal controls. Here, Internal Audit can use the information gathered during its IT audit to resolve relevant issues in advance. The findings may thus contribute to a reduction in the extent of the external audit. Particularly for IT audits in global companies, there are further aspects to take note of regarding a central or decen­tralized organization.

**HINTS ANDTIPS •**

**Cooperation with the External Auditors**

* Auditors should clarify special requirements with regard to access authoriza­tions before the audit.
* Auditors should pay attention to particular weak points in the IT organization and take any unusual items into account when deliberating their findings.

**LINKS AND REFERENCES**

. CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS. 2004. Privacy Com­pliance, A Guide for Organizations & Assurance Practitioners. Toronto: The Canadian In­stitute of Chartered Accountants.

* INSTITUTE OF INTERNAL AUDITORS. 2005. Global Technology Audit Guide 1: Infor­mation Technology Controls. Altamonte Springs, FL: The Institute of Internal Auditors.
* IT GOVERNANCE INSTITUTE. 2007. COBIT 4.1. Rolling Meadows, IL: IT Gover­nance Institute.
* OLIPHANT, A. 2004. Auditing IT Infrastructures. Mission Viejo, CA: Pleier Corporation.

1. Fraud Audit

**KEY POINTS •••**

* Most cases of fraud have a short- or long-term financial impact that is more or less directly measurable.
* Generally, the term fraud refers to any kind of attack on a company or its em­ployees.
* Internal Audit must respond to fraud with a self-contained, consistent process model.
* Internal Audit’s approach to fraud requires taking preventive measures and in­vestigating suspected or actual cases of fraud.
* The requirements profile for fraud auditors is very broad. In addition to techni­cal knowledge, an interest in forensic audits is recommended.
* During fraud audits, communication with other internal and external parties is

very important and must be carefully executed.

Internationally, there is an increasing trend to refer to all activities driven by crimi­nal intent as “fraud.” Examples include attacks on buildings and institutions, viola­tions of data protection laws, damage to the reputation of the company or an em­ployee, corruption, infringement of intellectual property rights, damage to property, trading of confidential information, or non-compliance of financial reporting.

**Definition**

Fraud audits may focus on fraud prevention or on investigating possible cases of fraud and include the following scenarios (for details, see Section D, Chapter 13).

**Audit Focus**

* Fraud prevention:
* detection of suspected organizational and process weaknesses, and
* exact identification of known weaknesses.
* Fraud investigation:
* investigation of anonymous accusations with or without proof or evidence,
* investigation of specific information on committed fraud without proof or evidence or naming a suspect, and
* investigation of proven fraud, where proof exists and/or the suspect is known, but guilt has not yet been established beyond doubt.

In the context of fraud audits, it is of special importance to establish whether and to what extent an incident has led to directly measurable, or indirectly related, finan­cial consequences for the company. Fraud that can be measured in financial terms must be communicated to the relevant bodies directly and immediately because of the potential impact on financial reporting and the rules of the (international) fi­nancial markets. However, fraud that does not have any financial impact must not be overlooked or trivialized, because it may entail damage to the company’s reputa­tion, environmental damage, staff resignations, product and service defects, and the associated loss of confidence.

**Consequences of Fraud**

In order to categorize possible fraud incidents quickly and reliably and to re­spond with appropriate action, it is advisable to set up a system that centrally col­lates all the information and initiates targeted actions. In order to achieve a maxi­mum of security, a control body of this kind should ideally exist outside of Internal Audit, e.g., within the company’s legal department. The activities of such a body include the compilation of specific guidelines, the treatment of each incident by forwarding and monitoring it, and a periodic reporting system that keeps detailed information regarding all ongoing and closed cases. In addition, cooperation with other bodies that deal with similar issues should be organized. It may also be ben­eficial to establish an anti-fraud/anti-corruption program within the organization. An important part of such a program would be a fraud emergency plan, which contains all necessary steps for handling fraud-related matters in a professional, timely, and appropriate manner.

**Company-Internal Control Body**

Internal Audit’s activities in this context comprise much more than merely re­sponding to cases of fraud. The ultimate objective is to protect the company from attacks of this nature. For this reason, Internal Audit must strive to prevent fraud, or at least facilitate early detection. The preventive exclusion of possible misuse in­volves both identifying potential sources of fraud in general and testing the effec­tiveness of controls already implemented. Cash flows and any other sensitive area where embezzlement is a direct possibility deserve particular attention. These areas must be analyzed and adequate controls must be established.

Internal Audit’s process model must be set up accordingly (see Section B, Chap­ter 7.2). Internal and external communication must be initiated and maintained, and a reporting system should be implemented also with regard to the special re­quirements on documents that may be used in a court of law. Ultimately, evidence has to be provided to demonstrate that external requirements, such as those im­posed on Internal Audit by SOX, are optimally met.

For investigating fraud, each audit involves an individual procedure with regard to the audit steps to be taken, the audit content, the involvement of third parties, reports, and the necessary follow-up activities. To obtain usable audit results in the shortest possible time, fraud audits normally employ the full range of audit proce­dures available, from a comprehensive process approach, including Scope and work program, through special, targeted ad-hoc audits. In this process, the body of evi­dence must be kept as clear-cut as possible.

In addition to technical expertise, auditors need a certain intuition for irregu­larities combined with a healthy dose of skepticism and an ability to put themselves into the position of other people. Fraud auditors can come from different technical areas of a company. Ideally, they will at least have basic audit experience in other audit fields, such as operational or financial audits. Fraud audits, however, increas­ingly also require generalists who can uncover and assess links from both a techni­cal perspective and with an eye for possible criminal motives. Since fraud audits are mostly conducted under time pressure, knowledge and experience in the area to be audited are of great benefit.

In order to increase the efficiency of the work performed by Internal Audit in this very critical audit field, a separate Scope, a separate Audit Roadmap with spe­cific components, and a ranking list of possible audit segments based on past expe­rience should be set up for fraud in line with the risk potential involved.

Relations with other internal and external parties are very important for fraud audits. First and foremost, this includes the legal department, Corporate Security, and Human Resources. The Audit Committee and the compliance officer should also be involved in these processes. Cooperation with the external auditors also must be arranged. Disclosure of incidents of fraud is becoming an increasingly im­portant reporting element for all companies.

The whole area of fraud audits is a very complex and sensitive audit field for Internal Audit. For this reason, there is no single correct way of dealing with fraud

**Preventive Audits**

**Alignment of the Process Model**

**Audit Execution**

**Requirements Profile for Auditors**

**Efficiency of Internal Audit**

**Involvement of Other Parties**

**Possible Treatment**

within the company. The procedure must be determined for each individual case. The following diagram shows possible solutions and the interdependencies that ex­ist in Internal Audit’s treatment of fraud.

Fraud audit with cooperation

Person(s)

responsible identified

Person(s)  
responsible  
cannot be identified

Refer to

|  |  |  |  |
| --- | --- | --- | --- |
| Obligation?  1 | ► public authorities  in charge | Board  decides not to take action | |
| 1 |  | 1 | ' /A, |
|  | | | |

**'repeated'**

**offence**

Fig. 20 Possible Treatment of Fraud by Internal Audit

The police and the district attorney could no doubt also be important external par­ties in this context. Generally, fraud investigations are aimed at identifying un­known perpetrators. If Internal Audit cannot identify them, in consultation with company management and the company’s legal department, they may refer the matter to the police and/or the district attorney. This also applies if the investigation has been successful, i.e., Internal Audit has identified the perpetrators and laid a charge against them.

**Police and District Attorney**

**HINTS ANDTIPS •**

* Cases of suspected fraud must get priority treatment in day-to-day auditing, because it is often very important to act quickly.
* Prevent rumors or hasty reactions at any stage in the fraud audit.
* Ensure that the auditors have the necessary documents to hand, because they may be asked to give evidence in a legal dispute.

**LINKS AND REFERENCES**

* ANDERSON, U. AND A. DAHLE. 2006. Implementing the Professional Practices Frame­work. 2nd ed. Altamonte Springs, FL: The Institute of Internal Auditors.
* INSTITUTE OF INTERNAL AUDITORS. 2001. Practice Advisory 1210.A2-2: Auditor’s Responsibilities Relating to Fraud Investigation, Reporting Resolution and Communication. Altamonte Springs, FL: The Institute of Internal Auditors.
* INSTITUTE OF INTERNAL AUDITORS. 2001. Practice Advisory 1210.A2-1: Auditor’s Responsibilities Relating to Fraud Risk Assessment, Prevention and Detection. Altamonte Springs, FL: The Institute of Internal Auditors.

. SAWYER, L., M. DITTENHOFER, AND J. SCHEINER. 2003. Sawyer’s Internal Audit­ing. 5th ed. Altamonte Springs, FL: The Institute of Internal Auditors.

1. Business Audit

**KEY POINTS •••**

* Today, relationships with external parties (such as partners or critical vendors) expose organizations to risk and therefore require Internal Audit’s attention.
* The Board or management may engage Internal Audit in audits of these external relationships for a variety of reasons, including de-escalation, legal claims, etc.
* Internal Audit may perform full-fledged audits of these relationships or pro­jects, known as business audits. Alternatively, Internal Audit may perform busi­ness reviews, which are less rigorous and require less fieldwork.
* The objectives of business audits or business reviews are generally to ensure compliance with legal, regulatory and contractual requirements and to evaluate risk related to external relationships.
* Internal Audit should seek input from all interested parties to develop a shared responsibility for the success of the relationship and/or project.

For many years, Internal Audit work has focused on auditing internal processes and

**Internal and External Perspective**

organizational units to investigate how effectively departments and their employees

interact with each other and their customers as the main determinant of organiza-

tional success. While this still applies today, the perspective has shifted somewhat. The increasing reliance upon supply and service chains, both within a company and across different organizations, business sectors and countries, has significantly con­tributed to broadening the range of factors that determine an organizations success. This trend is set to continue. Ultimately, the network of suppliers, customers, part­ners, and financial interests as well as relations with public institutions, organiza­tions and governmental bodies has a significant influence on the internal processes of a company and therefore should be in the forefront of Internal Audit’s focus. This means that Internal Audit’s main audit areas are determined by both internal and external concerns.

**Increasing Importance**

**Interest in Up-To-Date Information**

**De-Escalation**

**Legal Requirements**

**Project-Specific Analysis**

The importance of audits related to external concerns will continue to increase as organizations’ reliance on external partners grows. Management or the Board of Directors may engage Internal Audit to examine these relationships or projects for a variety of reasons:

* To effectively manage a relationship or project with outside parties it is impera­tive that the organization examine current and on-going information. Any sig­nificant financial or operational disruptions at any of these organizations may cause (in some cases incalculable) damage to the company’s reputation and its market. Damages to an organization’s reputation are very difficult to control and are often hard to reverse.
* Often when organizations engage in projects with outside companies there is a risk of escalation of commitment (i.e., making irrational decisions to justify pre­vious choices). That is, because the organization has entered into the relation­ship there is a desire to make it work - at all costs. Escalation of commitment often occurs when the project or relationship is not as effective or productive as originally expected and the organization increases the resources dedicated to it in an attempt to improve the likelihood of success. De-escalation activities are designed to counter-act any escalation of commitment tendencies that may ex­ist. The aim of the de-escalation approach is to return to a stable situation inter­nally and to show those involved new ways of reaching their targets.
* When an organization partners with other companies it is exposed to increased compliance and regulatory risk because it is also responsible for ensuring that its partner also complies with all applicable legal and regulatory requirements. If a partner fails to comply with applicable requirements, the organization may be liable for damages and subject to sanctions or penalties. Therefore, Internal Au­dit must carefully examine the relationships and activities of the organizations’ partners in a timely manner to ensure legal and regulatory compliance.
* Rather than focusing on the specific partner, Internal Audit may also examine a project in which the organization has engaged with its partner. Internal auditors may focus on project-specific issues, such as delays, excess costs, and non per­formance of services by the contract partner, or significant product or service defects.

For all of the above reasons, the Board may request that Internal Audit conduct a special audit of business objects, also referred to as a business audit or business re­view. The question as to whether to conduct an audit or a review is usually asked in connection with the extent of the fieldwork that has to be performed. When per­forming a business audit, Internal Audit examines the entire audit environment in depth using the Audit Roadmap. Alternatively, a business review focuses on record­ing and analyzing specific key aspects of the relationship or project during limited fieldwork. That is, during a business audit the auditor performs all the individual audit steps, including the necessary documentation. However, during a review, the auditor draws conclusions on the basis of readily available information. Usually, business reviews produce results faster, although the results must be analyzed from the perspective of a review. The advantage of a review over an audit is that it is sooner possible to make the first statements and implement measures. Overall, the results of a business audit include findings and recommendations, whereas a busi­ness review only concludes with procedural proposals (for more information, see Section A, Chapter 7.2.3). The rest of this chapter deals with business audits in more detail. In addition to the Board, other parties, (e.g., the legal or contracts depart­ment of a company, the sales or consulting officer responsible, other service and support units of the company, and Risk Management) may request an independent audit of the organization’s external relationships and projects by Internal Audit.

A business audit is defined as a preventive audit measure conducted in line with the de-escalation strategy. Its main purpose is to ensure that processes, methods, and guidelines are compliant and working as intended. At the same time, the risks related to the project or partner are examined and, if necessary, appropriate de-es­calation measures are proposed. Objectives and content of a business audit must be defined exactly. The audit may focus on legal, contractual, or organizational mat­ters.

**Business Audit versus Business Review**

**Features of a Business Audit**

The results of a business audit are prepared and presented in a slightly different manner than are those for a traditional audit. Because of the dynamic nature of the business processes it is necessary to explain interim results and perspectives in a timely manner to management and the employees involved. This means that, apart from the traditional report formats used by Internal Audit, additional memos (see Section B, Chapter 5.3.1) or presentations (see Section B, Chapter 5.3.2) may be needed. This may be of specific importance if the parties concerned need to con­sider possible actions or costs. However, it is a challenge to communicate interim results, without revealing important findings too early.

**Preparing and Presenting the Results**

When examining relationships and projects with external parties, it may be nec­essary to conduct audit activities outside one’s own business premises. In this re­gard, it is necessary to clarify in advance to what extent this is legally possible. Often a “right to audit” clause is included in the contract between the organization and its partner. If such a procedure deserves support, Internal Audit contacts the partner in order to agree the objective and the required action. Generally, relationships with

**Audits Outside the Company**

external parties are more productive if the parties are able to cooperate and coordi­nate such audits without conflict.

**HINTS AND TIPS •**

* For a business audit, auditors should enlist support from other specialist depart­ments and corporate communications.
* During a business audit, auditors should examine all the existing documents for the process, including e-mails.
* During a business audit, auditors must keep themselves informed on an opera­tional level as well as on a strategic level with the latest information from the Board of Directors.

**LINKS AND REFERENCES**

• ANDERSON S.W. AND K. L. SEDATOLE. 2003. Management Accounting for the Extended Enterprise: Performance Management for Strategic Alliances and Networked Partners. In A. BHIMINI (ED.). 2003. Management accounting in the digital economy. London: Oxford Press.

. ANDERSON, S.W., M. H. CHRIST AND K. L. SEDATOLE. 2006. Managing Strategic Alliance Risk: Survey Evidence of Control Practices in Collaborative Inter-Organizational Settings. IIA Research Foundation, <http://www.theiia.org/research/research-reports/> downloadable-resear ch-reports/?i=237 (accessed May 31,2007).

1. Audit Approaches

**KEY POINTS •••**

* The risk-based audit approach allows Internal Audit to target its work at areas of critical business risk.
* The audit risk consists of inherent risk, control risk, and detection risk.
* Four audit methods are used under the risk-based audit approach. These meth­ods can be used flexibly in the course of the audit, in response to interim audit results: General risk analysis, analytical fieldwork, system and process based fieldwork, and substantive testing.
* As part of the risk-based audit approach and within the audit methods that its application entails, other audit approaches can be used during audit work, either individually or in combination.
* The system-based audit approach is used to test the effectiveness of the controls and safeguards that have been put in place.
* The objective of the transaction-based audit approach is primarily to detect

transaction errors. This normally means that Internal Audit must use an inves­tigative method.

* The compliance-based audit approach is centered on testing the compliance of any audit object, in relation to meeting a specific requirement.
* The objective of the results-based audit approach is to arrive at a quantified comparison of the audit object’s current condition with the relevant criteria, for example legal standards or business guidelines.
* The risk-based audit approach is a key concept that provides a framework for the other audit approaches. The audit objects that are selected and the specific audit activities to be conducted are determined within the framework of the risk-based audit approach. The selection is therefore guided by the risk attached to the audit object and its materiality.

In principle, an audit approach is a method for developing a certain procedure for Risk-Based Audit

an audit, i.e., for formulating the audit strategy. In response to modern corporate Approach

structures, the aim of the risk-based audit approach is to allow Internal Audit to tailor its audit work to the areas of business risk. Internal Audit’s universality claim of representing permanent control in all areas is giving way to greater focus on au­dit objects with a high risk potential.

The following diagram shows that audit risk has two components, error risk and Audit Risk

detection risk. Error risk breaks down further into inherent risk and control risk.

Audit risk

Detection risk

Error risk

Inherent risk

Control risk

Fig. 21 Audit Risk Components

Inherent risk is the risk that is intrinsic to a process and results from the audit ob- Inherent Risk ject’s susceptibility to errors. It comprises macroeconomic, sector- and company- specific factors (e.g., the economic situation, organizational structure, or the com­pany’s legal environment, as well as factors specific to the audit object). Factors specific to the audit object include the complexity of work processes in business

units and departments and the time pressure to which they are subject. To assess the inherent risk, auditors must have comprehensive knowledge of the company and its environment and use interviews and observations or analyze documents in order to obtain information on workloads, work quality, and techniques in the emit being audited.

Control risk represents the danger that the implemented internal control system does not detect or prevent all relevant errors. There may be two reasons for this: Either, the controls are triggered only after a time delay, which means that any er­rors are identified too late, or certain aspects are not checked because the internal controls are not effective all the time or there are gaps in their coverage.

**Control Risk**

**Detection Risk**

**Audit Risk as the Product of its Components**

**Tolerable Detection Risk Levels**

**Risk Analysis**

**Analytical Audit Procedures**

**System Audit and Substantive Testing**

Detection risk is the other main component of audit risk. It quantifies the pos­sibility that in spite of detailed tests, the auditors do not detect material errors, for example because they have selected an insufficient number of samples or inappro­priate audit methods. Unlike the other components, auditors can therefore directly influence detection risk by selecting the type and extent of fieldwork.

For reasons of efficiency, only material risks are included in the audit planning. Since the three components of audit risk can offset or reinforce each other, audit risk is determined by multiplying its components:

Audit risk = inherent risk x control risk x detection risk.

Once the overall audit risk acceptable for the audit has been defined and the inherent and control risks have been determined, the tolerable detection risk can be set. Auditors must keep within this risk level by conducting appropriate fieldwork. It is, however, impractical to work out the exact level of risk mathematically, so that general risk categories (low, medium, high) are used in practice.

From a risk perspective, four approaches for risk analysis are used as part of the risk-based audit approach:

* general risk analysis,
* analytical audit procedures,
* systems and process based fieldwork,
* substantive testing.

In risk analysis, the areas of business risk are determined and the relevant risks are identified in the overall context of audit risk. The audit objects are determined and the audit is planned on the basis of the results of the risk analysis.

Analytical audit procedures (see Section C, Chapter 3.1) are used to generally assess the risks at process level. The procedures consist of analyzing individual fig­ures and ratios or groups of figures and ratios. They are intended to allow auditors to get an overview of the reliability of the risk management and internal control systems. Analytical audit procedures also help provide a global overview of the pro­cesses and controls of the unit being audited and identify any interdependencies. The audit content is divided into audit areas on the basis of this knowledge.

Detailed system fieldwork helps test the reliability and effectiveness of the inter­nal controls. It is also used to assess the main process risks. These tests are based on a comparison between the applicable standards or company-internal rules and the

actual process or situation in the units being audited. Substantive testing is a de­tailed review of individual material causes of risk or of a specific process.

By combining the above four audit methods in the indicated sequence, the audi- Flexible Combination tors can conduct an audit efficiently with the specified degree of reliability and op- of Methods

timize it with regard to the time and effort it involves. During this process, the reli­ability of the individual audit statements increases continually from general risk analysis through substantive testing. A significant attribute of the risk-based audit approach is that the combinations of methods can, and have to, be flexibly adapted during the audit in line with interim audit results, i.e., Internal Audit’s activities are scaled down or expanded while the audit is being conducted.

As part of the risk-based audit approach and within the audit methods that its Other Audit Approaches application entails, the auditors can use other audit approaches during their audit work, either individually or in combination. The diagram below shows how the dif­ferent audit approaches interact, and the text that follows explains the approaches and the interaction between them.



Fig. 22 Embeddedness of Audit Approaches in the Risk-Based Audit Approach

The system-based audit approach should be used to test the effectiveness of the controls and safeguards. The main objective of the system-based audit approach is to give the managers with overall responsibility for corporate monitoring an as­surance regarding the control systems used. Any actual or possible weaknesses in

the system should be detected and eliminated. The system-based audit approach is generally also based on the risk analysis performed on the company and its pro­cesses and procedures.

Audits that follow a system-based approach are similar to process audits and focus on control mechanisms. Although this approach is also intended to detect errors, it focuses on systematic errors during process or transaction handling, not on specific one-time errors. This means that the system-based audit approach is less retrospective and should also be able to produce forward-looking audit results.

**Characteristics of the System-Based Audit Approach**

**Application of the System-Based Audit Approach**

**Objective of the Transaction-Based Audit Approach**

**Characteristics of the Transaction-Based Audit Approach**

**Application of the Transaction-Based Audit Approach**

**Objective of the Compliance-Based Audit Approach**

**Characteristics of the Compliance-Based Audit Approach**

**Application of the Compliance-Based Audit Approach**

Because of its systematic way of dealing with transactions within the company, which requires them to be comprehensively analyzed, the system-based approach is particularly well suited to audit matters related to or impacting on the following topics: Reliability and integrity of accounting, securing of assets, efficiency of trans­actions, and compliance with legal rules and requirements.

The objective of the transaction-based audit approach is primarily to uncover transaction errors. In line with this objective, the transaction-based approach often means that Internal Audit has to use an investigative procedure.

Audits that follow the transaction-based approach are best suited to fieldwork such as sample tests and full audits of individual business transactions within the company. They assess whether the relevant processes are performed correctly and the transaction has been handled and recognized properly. Under this audit ap­proach, the controls integrated in the corporate processes are only of secondary importance, because these audits analyze not the general process as a whole, but focus on a specific manifestation. As such, the audit procedure used under the transaction-based approach focuses on the past or present, but can rarely arrive at forward-looking audit results.

Because the focus of audit activities under the transaction-based approach is on a specific transaction, it is best suited to investigating suspected fraud, helping with issues relating to the assessment of management decisions, or supporting customer projects or similar consulting tasks.

The compliance-based audit approach is centered on testing the compliance of an audit object. Consequently, the audit object is tested to determine whether or not it meets a specific requirement set to establish compliance. Such requirements may include legal standards or company-internal conduct rules, policies, and guidelines. Audits that test whether certain controls or individual control elements are in place are also feasible.

Audit objects may include internal monitoring systems as well as specific pro­cesses, process steps, and work results. Note that the compliance-based audit ap­proach leads to an audit statement in the form of a yes-no decision. If the audit object is found to be compliant with the relevant benchmark, this results in a posi­tive audit outcome. However, if the audit finds the audit object to deviate from the relevant benchmark, it is documented as non-compliant. The finding does not comment on the extent of the variance, i.e., the error is not rated.

Since it focuses on following rules exactly or the existence of specified controls or process steps, the compliance-based audit approach is best suited for assessing

compliance with legal standards or compliance regulations, assuring the quality of the process structures, or testing whether project targets are achieved as planned.

The objective of the results-based audit approach is to arrive at a quantified comparison of the audit objects current condition with relevant criteria, which again include legal standards or company-internal guidelines. This approach is not only about establishing whether or not the audit object meets the benchmark. If any non-compliance with the requirement is found, it should be quantified as far as possible. This applies to both errors in specific procedures and the impact of any control weaknesses that have been identified.

When the results-based audit approach is applied, audit results are expressed as a quantitative measure, not a yes-no decision. The non-compliances that have been identified can be expressed either as percentages or relative values, or as monetary amounts. If the consequences in the form of a direct percentage or monetary amount cannot be specified, the auditors may alternatively rate the error qualita­tively according to its seriousness. Sample testing is particularly suitable for use under the results-based audit approach, not least because of the flexibility of the variables. The results-based approach is also useful where the audit statement is not to be limited to simply confirming compliance, but where the positive aspects are to be quantified. This approach could be used for projects, for example, where the auditors want to report not only the general fact that the objectives have been met, but also that the project was implemented faster and with greater success than planned.

Since the results-based audit approach focuses on measuring and assessing the variance from the relevant requirements, it is best suited to testing control mecha­nisms and quality assurance systems. In these types of audit, it is not only important to identify the existence of errors, but also to establish whether they are material and what effect they have. The results-based audit approach is also useful as part of internal consulting activities and for auditing customer projects.

In principle, the audit objectives of Internal Audit determine which audit ap­proach is selected. The choice in turn affects the specific audit activities that Inter­nal Audit conducts. Firstly, it is important to clarify whether it is conducting a com­prehensive audit of a whole area or only examining certain key issues. If the audit objective is comprehensive, for example, testing the effectiveness of the intended control mechanisms, a system-based approach is advisable. For more specific issues or substantive tests on single transactions or similar, the transaction-based audit approach is more appropriate.

But the system and transaction based audit approaches are not mutually exclu­sive and can be used in combination with each other. In particular, the auditors can use the transaction-based approach for additional testing under the system-based approach. The reverse procedure, i.e., using the system-based approach as an addi­tion to the transaction-based approach, is normally more difficult and will only rarely be considered a feasible way of achieving the audit objectives. In practice, compliance-based and results-based approaches can also be used in combination, for example to test for the existence of control mechanisms, while at the same time

**Objective of the Results- Based Audit Approach**

**Characteristics of the Results-Based Audit Approach**

**Application**

**of the Results-Based**

**Audit Approach**

**Choice**

**of the Appropriate Audit Approach**

**Combination of Audit Approaches**

arriving at quantitative statements about whether the intended procedures are fully and appropriately complied with.

It is also possible to combine the compliance-based audit approach with both the system-based and the transaction-based approach. A combination of the com­pliance-based with the system-based approach is particularly useful when testing whether control mechanisms or certain process steps exist within process struc­tures. The compliance-based and transaction-based audit approaches can be com­bined, for example when auditing compliance with specific standards, where a positive or negative audit result without quantification is sufficient. However, if the auditors need to quantify the audit result in a transaction-based audit, they should combine this approach with the results-based approach. When assessing control mechanisms or requirements relating to procedures, it is sensible to combine the system-based and results-based approaches. In such cases, the auditors are testing not only the general effectiveness, but also the materiality of variances from stated requirements.

**Other Possible Combinations**

**Risk-Based Audit Approach as a Framework**

**Use in IT and Fraud Audits**

**Use in Internal Consulting and Business Audits**

**Use in Management Audits**

**Use in Operational and Financial Audits**

The risk-based audit approach is a key concept that provides a framework for the other audit approaches: The audit objects are selected and the specific audit activities are determined within the framework of the risk-based audit approach. The selection is therefore guided by the risk attached to the audit object and its materiality. Within the individual steps or audit methods of the risk-based audit approach, the auditors should fall back on other audit approaches that allow them to add specific audit content in the appropriate place within the specified frame­work. It will depend on the case in question whether the auditors should use the pure forms or combinations of audit approaches. This decision is taken in line with the audit objective on the basis of the specific requirements and circumstances.

On this basis, it is also possible to create links between the tasks of Internal Au­dit and the applicable audit approaches. For the more topical tasks, the assignments are relatively clear. For an IT audit, the system-based approach with results-based elements will normally be best. But a fraud audit will almost invariably use the transaction-based approach in combination with the compliance-based approach, unless it investigates the general effectiveness of a preventive system.

In the area of internal consulting, customer projects will tend to be addressed by the transaction-based audit approach, but consulting projects for process improve­ments will probably require a system-based approach. The same applies to business audits. In most cases, the results-based approach will be more prevalent than the compliance-based approach in these areas, because the quantitative impact of audit findings is very important in internal consulting.

When examining the organizational structure, management audits may use the system-based audit approach, but otherwise the transaction-based approach will be more common. In this audit field, a results focus should commonly outweigh a pure compliance assessment.

Since in both operational and financial audits the focus is on processes and busi­ness transactions, system-based audit approaches are the preferred choice. In both fields, transaction-based approaches will only be used in individual cases to con-

firm the results. The adequacy of a compliance-based or results-based approach depends on the audit object in hand, although the results-based approach will probably be used more often.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Audit field  Audit  approach | | Manage­  ment | Operational | Financial | IT | Fraud | Business |
| Risk-based | | X | X | X | X | X | X |
|  | System-  based | X | X | X | X | X | X |
|  |  |  |  |  |  |  |  |
| <D  M  to  -O  A  .S2 | Transaction-  based | X | X | X | X | X | X |
|  | Compliance-  based | X | X | X | X | X | X |
|  | Results-  based | X | X | X | X | X | X |
| X  X | = important = less important | |  |  |  |  |  |

Fig. 23 Relations between Audit Fields and the Audit Approaches to be Used

The above diagram explains the relations between audit fields and the audit ap­proaches to be used. For the assignment of possible audit approaches to the task areas, the risk-based audit approach once again functions as a framework. On the basis of risk considerations, decisions are taken about the content of audit objects, which can belong to one main task or to several activities of an audit field. Once the audit objects have been specified and the basic audit strategy has been defined, the audit approach can be chosen.

**Assignment by Risk Orientation**

**HINTS ANDTIPS •**

* Auditors should always keep risk-based procedures in mind and act accord­ingly.
* Risk aspects are also very important when choosing appropriate audit ap­proaches, and it may therefore make sense to consult with risk management.
* Auditors should thoroughly analyze the impending audit request in order to align their method with one or more suitable audit approaches.
* Even after the audit has started, auditors should regularly consider using differ­ent or additional audit approaches or audit methods in their work.

**LINKS AND REFERENCES**

* KEITH, J. 2005. Killing the Spider. Internal Auditor (April 2005): 25-27.
* MESSIER, W. F. 2003. Auditing and Assurance Services: A Systematic Approach. 3rd ed. Boston, MA: McGraw-Hill.
* RITTENBERG, L. E. AND B. J. SCHWEIGER. 2005. Auditing: Concepts for a Changing Environment. 5th ed. Boston, MA: Thompson.

. SAWYER, L„ M. DITTENHOFER AND J. SCHEINER. 2003. Sawyer’s Internal Audit- ing. 5th ed. Altamonte Springs, FL: The Institute of Internal Auditors.

* SEARS, B. 2002. Internal Auditing Manual. New York, NY: Warren, Gorham & Lamont.

1. Audit Categories

**KEY POINTS •••**

* The audit categories include local, regional, and global audits.
* Local audits focus on local units and processes. They are conducted by the de­centralized units of Internal Audit, taking local circumstances into account.
* Audits of topics that are relevant for the whole region are called regional audits. These include audits of a topic performed centrally for the whole region, or on a decentralized basis at different locations in the region.
* Global audits always involve horizontal process chains that affect either differ­ent organizational units or the same organizational entity as a global function in different regions and countries.
* All audit standards that have been developed apply without exception to the different audit categories. Deviations from the standards are only al­lowed in justified exceptional circumstances. The reasons for such deviations must be documented and permission must be obtained from the Audit Man­ager.

**Assignment of Audit Categories to Audit Topics**

**Multiple Assignments**

**Definition of Local Audits**

Three audit categories are differentiated at SAP: Local, regional, and global audits. All audit topics can be assigned to these audit categories. In practice, some audits, e.g., of financial or process topics, are primarily conducted locally, but audits of strategic topics, such as management processes or risk management, are more often audited regionally or globally.

However, the links between audit fields and audit categories are not always clear-cut, and multiple assignments are possible. A financial audit can be conducted locally in an operating unit, but it is also feasible to conduct it on a global level throughout the company.

Local audits are all audit activities that exclusively cover audit content at a local level, e.g., processes and objects that relate to only one country or those that are to be examined from a local perspective, even though they are globally significant for

the entire company. In addition to local subsidiaries, the audit objects of local au­dits can include joint projects, partnerships, and joint ventures.

SAP’s Internal Audit is organized in several regional teams with a high degree of autonomy (see Section A, Chapter 4.3). A core task of these regional audit units is to implement the audit standards developed in the various audit categories. Local audits of entities in the area represent a virtually autonomous audit category for regional teams. This gives the audit teams a high degree of responsibility. Regional team members are mainly recruited from among the employees of the region, en­suring that the regionally or locally specific expertise remains within the unit re­sponsible for the region.

Typical local audits include process and accounting audits, as well as audits of compliance with corporate law (e.g., register entries and articles of partnership). In addition, local audits also examine specific local processes and approval proce­dures, taking locally relevant legal circumstances into account. This includes audits of local IT processes and IT equipment, as well as specific investigations into al­leged or suspected fraud. Ultimately, many elements of the wide field of audit topics may become locally relevant.

Under normal circumstances, standard audits will be the type most commonly conducted from a local perspective, i.e., audits that could happen in similar ways at different locations. Special audits with a specific topic focus occur more rarely, if at all, because such unique topics are often encountered only once in the company and are therefore normally not conducted in decentralized units but rather on a global level, e.g. audits of the corporate treasury department (for details on audit typology, see Section A, Chapter 6.5).

Local audits always follow the Audit Roadmap, from planning and preparation through execution, reporting, and follow-up (see Section B). In addition, the whole quality assurance framework must be complied with. Local audits are shaped by the combined influence of centrally specified standard processes and contents on the one hand and their decentralized adaptation and application on the other. Central standards must be applied to the audit to the extent possible, but despite standard­ization specific local features must be considered.

Especially in smaller regions, it is important to exchange as much information as possible prior to an audit, because this allows the auditors to identify audit focus areas in a timely manner. This applies to both internal and external contacts, e.g. the local external auditors. Local cultural aspects must also be considered.

Local audits are listed in the regional execution plan (see Section B, Chapter 2.2), which must be based on the overall regional capacity for all audits and the available resources to avoid schedules that are too ambitious. Sometimes, however, especially if capacity suddenly becomes unavailable or specialist knowledge is re­quired, there may be additional demand for auditor capacity. In such circumstances, the regional teams should get ad-hoc support from colleagues of other regions. Even when a local audit is conducted by a mixed team, the audit remains local and fully under the responsibility of the regional audit organization concerned, i.e. the regional team and the regional Audit Manager.

**Regional Teams at SAP**

**Subject of Local Audits**

**Standard Audits versus Special Audits**

**Position of Local Audits within the Process Model**

**Information Exchange with Other Parties**

**Mixed Teams**

Due to their responsibility for conducting audits in their regions, Audit Manag­ers are also responsible for prioritizing and scheduling each audit. All administra­tive processes, such as the audit announcement and the distribution of reports, are also performed regionally on the basis of the applicable distribution lists. This af­fects the managers of the unit being audited at local level in particular.

**Tasks**

**of the Audit Manager**

**Definition of Regional Audits**

**Local versus Regional Audits**

**Value**

**of the Audit Results**

**Global Challenges for Internal Audit**

**Subject of Global Audits**

**Centrally Standardized Audits**

Regional audits focus either on regional matters, e.g. regional management of business partner relations, or on processes centrally organized through shared ser­vices centers, e.g., standardized purchasing. This means that under a regional audit, a specific topic is examined in various different locations, either simultaneously or one directly after the other. The audit organization must make sure in each instance that the audits are conducted uniformly and local preferences cannot influence or distort the audit results.

The comments on local audits with regard to complying with audit standards and putting the audit team together also apply to regional audits. However, there is a major difference in the way the regional nature of the audit impacts the manage­ment of the unit mainly affected by the audit. In the case of regional audits, higher- level (regional) management is responsible for enabling the audit on the one hand and for implementing the audit results on the other. This means that, unlike for lo­cal audits, this management level must always be involved in the main phases of the audit itself and the opening and closing meetings.

Another significant difference is that the results of regional audits may have greater importance for the company than those of local audits. For this reason, it is possible that, in the search for company-wide solutions, critical results of a regional audit will more readily be brought to the Board of Directors’ attention because the objective is to release rules and guidelines at senior management level to help har­monization across regional boundaries.

International corporate audit departments can and must also face global audit topics (see Section C, Chapter 7). Different audit topics can be identified as chal­lenges for Internal Audit on a global level. They are related to different methods that can or have to be used according to the underlying determinants.

A global audit of one topic may occur at locations in different regions under one organization with overall functional responsibility. Examples include the global es­calation department, the global processing of patents to safeguard intellectual prop­erty, or a global purchasing organization. Ultimately, they always involve horizontal process chains that either affect different organizational units or the same organiza­tional unit in different regions and countries. A global audit area may also be a topic whose specific contents are defined by a central unit, which implements and coor­dinates them in the different countries and regions. Examples include global risk management and globally standardized internal controls, particularly in response to SOX. Global structures of this kind may also be found in development or sales organizations, which are therefore also possible subjects of Internal Audit’s work.

From Internal Audit’s perspective, it may be sensible to centrally standardize certain topics thus transforming them into global topics for the time of the audit

engagement. To ensure that for these topics, audit content, procedures, and exper­tise are optimized, such audit objects are easier to enforce and coordinate from In­ternal Audit’s point of view if they are managed under the same technical responsi­bility. The audits in question include primarily management and fraud audits, but also audits of IT processes and information networks. A special feature of these types of audits is that the topics under review are often sensitive and may have a global impact on the entire company.

Global audits are seen as a single unit for the whole duration of the audit pro­cess. This means that the totality of an audit cannot be broken up, even if it covers areas that differ in terms of content (central functions and decentralized units). In a global audit, the audit topic therefore clearly dominates the regions and forms the focal point of all audit procedures. The whole organization and process of an audit must fall in line with the global topic. The only relevant outcome is a complete and globally coordinated audit result, because only this result will permit the auditors to arrive at findings, recommendations, and conclusions that are appropriate from a global perspective. This means in turn that the audit content must be defined on a global level, not with a local or regional focus.

Global audits primarily deal with operational business units that are under uni­form global management and therefore have globally standardized processes. The reporting lines to the global level must be clearly defined in this context. Units that are managed on a decentralized basis, yet follow global processes have clear local or regional reporting lines.

Global audits must be treated as a whole not only with regard to content, but also in terms of method in order to ensure audit success. This is why the work pro­gram, the working papers, and the reports must always cover all areas of a global audit. Individual parts cannot receive independent treatment, even if they involve different countries or organizational units. Each stage of the quality assurance sys­tem should also incorporate the results of all audited units simultaneously. The pro­cedure can only be consistent and deliver a globally cohesive audit result if all audit steps are coordinated across all involved auditors and synchronized with regard to content.

Global audits require the auditors involved to communicate and cooperate across continents and time zones and therefore place great demand on the audit lead. Global cooperation also requires that all team members keep to the work pro­gram (in terms of timing and organization) and deliver partial results when they are due in order to support the audit lead in conducting a successful audit.

What makes global audits challenging is the potential conflict between what has been centrally specified and what can be implemented regionally. In such cases, the right balance has to be found in order to get an acceptable audit result. The nature of different global audit scenarios also requires different ways of conducting the audit. In some audits, for example, the central functions will be examined first, fol­lowed by corresponding audits in the regions, which are conducted simultaneously or successively. It may be sensible to audit different decentralized units simultane-

**Thematic Unity**

**Reporting Lines**

**Standard Method**

**Global**

**Cooperation**

**Different Audit Procedures**

**Global Audits and the Audit Roadmap**

**Planning Phase**

**Audit Preparation**

**Audit Execution**

**Reporting**

ously so that you can use the mutual exchange of information as a basis for the next steps. Alternatively it may be considered to conclude the audit of one decentralized unit first so that the lessons learned can be applied to improving the audit proce­dure for further units. The audit lead and Internal Audit management have to de­cide on a case-by-case basis which procedure is best.

On the whole, global audits also follow the Audit Roadmap (see Section B), i.e., the audit steps to be taken are integrated into the relevant phases of the process model, although there are some special points to consider when auditing globally which will be discussed in the following paragraphs.

The planning phase of global audits normally takes longer, because they involve significantly more coordination in selecting the team members and assigning the tasks within the team. Other points to clarify include the entire infrastructure, the organization of meetings, and how information will be exchanged and require­ments documented. In addition, global audits may entail a need to inform the vari­ous global units of the audit object more comprehensively about the objective and purpose of the audit than in regional or local audits. The auditors must check whether the relevant Scope (see Section A, Chapter 5.3) completely covers the global aspects and update it if necessary.

When preparing the work program, the auditors may find that global audits (more often than local audits) require additional technical expertise, e.g., in the form of guest auditors or expert advisors (see Section D, Chapter 10). The schedule to be compiled has to take into account that, due to the great physical distances, meetings and the documentation of working steps are particularly difficult to orga­nize in global audits.

Global audits do not have any specific requirements in terms of audit execution, but linguistic and cultural needs must be taken into account when creating the working papers and during the closing meeting.

During the reporting phase, the audit lead must ensure that all parts of the re­port are completed on time and are consistent with each other. The amount of work this requires in global audits should not be underestimated. The responsibilities must be defined carefully and clearly to support and to facilitate the subsequent implementation of the audit results.

**HINTS AND TIPS •**

* All involved parties must be aware of the characteristics of the audit category in question.
* Communicate audit-specific information with local and cultural circumstances in mind, using informal channels if appropriate.
* The global audit lead must make sure that the virtual network between all team members is functional.

**LINKS AND REFERENCES**

. SAWYER, L„ M. DITTENHOFER AND J. SCHEINER. 2003. Sawyer’s Internal Audit­ing. 5th ed. Altamonte Springs, EL: The Institute of Internal Auditors.

• SEARS, B. 2002. Internal Auditing Manual. New York, NY: Warren, Gorham & Lamont.

1. Audit Types

**KEY POINTS •••**

* The audit type is an important determinant of the audit method.
* We can differentiate between standard, special, and ad-hoc audits.
* Each audit type has its own objectives, content, and individual procedures, al­though it is based on the Audit Roadmap.
* Standard audits most closely follow the Audit Roadmap. They can be planned almost in their entirety and can therefore be performed as often as necessary and at relatively short notice.
* Special audits usually deal with audit objects that occur only once within the company. They also contain many elements of the Audit Roadmap, but they have a larger number of individual elements than standard audits.
* Ad-hoc audits are the most individually structured audits focusing on special topics, or person-specific one-time audits. They are often commissioned by company management. Although they follow the Audit Roadmap in principle, their very individual nature often requires specific steps, fieldwork, and docu­ments during each phase.
* An ad-hoc audit may also readily lead to additional standard or special audits.

The audit type is another important determinant of the audit method. It refers to Audit Type and the differentiation of audits by purpose, content, as well as organization and execu- Characteristics tion. Three types can be distinguished: standard audit, special audit, and ad-hoc audit. Assignment of an audit to a type results in specific characteristics for the au­dit that affect each stage of the Audit Roadmap, from the way the audit is planned, the existence of a Scope and work program, the form and timing of audit execution, through the various reporting forms and the follow-up procedure.

Standard audits investigate objects that have multiple occurrences in the com- Standard Audits pany, so that the topic of the audit comes up repeatedly. This means that the audit can be standardized, i.e., its content and procedure can be applied to any number of similar audit objects. Examples include individual departments in subsidiaries, such as Accounting or Purchasing. But similar processes such as payroll and travel or other expenses can also be specified for standard audits. They are also useful in areas where guidelines, rules, and process standards are to be harmonized. Stan­dard audits are often conducted locally.

Standard audits have certain characteristics in terms of the Audit Roadmap (see Section B):

* As part of annual audit planning, they are normally subject to risk assessment and are included in the annual audit plan, if appropriate (see Section B, Chapter 2.2 and Section D, Chapter 3). The audit is announced (see Section B, Chapter 3.1) and the team compiled (see Section B, Chapter 2.4) in line with clear proce­dures. A Scope, which describes the audit content, exists for standard audits.

**Characteristics of Standard Audits in the Audit Roadmap**

**Execution of Standard Audits**

**Special Audits**

**Characteristics of Special Audits in the Roadmap**

* The work program is compiled on the basis of the content of the existing Scope, which means that it can be used for similar audits.
* Certain standard fieldwork activities can also be defined for the audit execution stage, e.g., sample test procedures, interview techniques, or questionnaires.
* All standard reports, from implementation report through Board summary, must be used for reporting under standard audits (see Section B, Chapter 5). One of the reasons for this requirement is that the results of standard audits must be documented and communicated according to fixed rules to ensure compliance with the audit process in the Audit Roadmap. Any individual adaptation at this stage should therefore be reserved for special justified circumstances.
* The same applies to the different phases of the follow-up. For optimization pur­poses, it is important that the measures and recommendations made by Internal Audit are rigorously implemented, which is why systematic follow-ups are es­sential.

Standard audits are conducted according to clear rules and following standardized steps. For this reason, they are well suited for less experienced auditors to gain ex­perience, in some cases even as audit leads. Standard audits can also serve as a basis for the other audit types, especially special audits.

The topic of a special audit usually occurs only once in the entire organization. Examples include special development departments that develop add-ons with or without a link to a customer project. Like standard audits, special audits are also subject to the whole annual planning process. Special audits are mostly conducted on a global or at least on a regional basis, because their topics are often too specific to be present at local level. They often require specific technical knowledge and special preparation, which must be considered when composing the audit team, because the auditors’ technical knowledge and interests can make a key contribu­tion to the success of the audit.

Special audits require different treatment under the Audit Roadmap (see Sec­tion B) than standard audits, at least in part:

* Although they are included in the annual audit plan, they need longer prepara­tion times when they are added to the execution plan. This applies particularly to creating the Scope, a process which should be supported by company-inter­nal or external experts if possible. Sufficient time for building up knowledge among Internal Audit employees is also necessary.
* When the audit is conducted, it may become necessary to use special audit ac­tivities or techniques. Such a decision has to be taken on a case-by-case basis.

Pre-structured question catalogs may be helpful. It is important to document work results in the working papers and to disclose references accurately when using additional documents (e.g., contracts, statutes, external guidelines).

* Similar to standard audits, auditors have to ensure that the reports are in line with reporting requirements. The implementation report in particular should be as detailed as possible so that the findings and recommendations can be communicated to all concerned in a comprehensible and clear format. Internal Audit’s recommendations are especially important in this regard, because there are no or few comparisons with similar constellations.
* The same applies to follow-ups, where the progress of implementation measures has to be closely monitored.

Special audits should be conducted preferably by experienced auditors. In addition, Execution

it may be necessary to use internal or external experts as guest auditors. Since for Special Audits

special audits fieldwork activities cannot be planned ahead to the same extend as

for standard audits, adjustments to the work program may be required during audit

execution. Alternative fieldwork activities must be documented in the respective

working papers accurately and completely including the reasons for choosing the

specific approach.

Audit

**Ad-hoc**

audit

**according to plan**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Standard | Special | One-time | Special | ■ Standard ! |
| audit | audit | audit | audit | ; audit i |
|  |  |  | '£ | 4 |
|  |  |  |  |  |

Fig. 24 Audit Types

Ad-hoc audits, i.e. audits conducted at short notice, require that resources can im- Ad-hoc Audits mediately be dedicated to issues and tasks that are part of Internal Audits remit.

Examples include sudden problems in day-to-day business operations, in special projects, or with external business relations, or the need to respond to open or anonymous allegations or suspicions of fraud. The content of ad-hoc audits can

therefore be very varied. It is also possible that standard or special audits turn into ad-hoc audits if circumstances require immediate action. But those are the excep­tion. Normally, ad-hoc audits are one-time audits of special topics or relating to a particular person, especially in connection with allegations or suspicions.

In relation to the phases of the Audit Roadmap, ad-hoc audits have the follow­ing special characteristics:

**Characteristics of Ad-hoc Audits in the Audit Roadmap**

* Since it is impossible to plan either the content or the number of ad-hoc au­dits during a year, the amount of time required in the past is the only basis on which an adequate buffer can be built into the annual audit plan. Experience has shown that around 30% to 40% of annual audit capacity should be reserved for ad-hoc audits. Since their timing is uncertain, any ad-hoc audit will lead to an adjustment to the ongoing execution planning. If the ad-hoc audit is to be based on a Scope, this Scope is often created in stages during audit preparation or sometimes even while the audit is being conducted. Especially when one-time audits relate to a person, it is virtually impossible to define a Scope. In order not to waste time before the audit, but still preserve the knowledge and experience gained for similar cases in the future, internal auditors should document the main audit content after the audit, in the form of a Scope if appropriate.
* Preparations for an ad-hoc audit should always include the creation of a work program (even if it is rudimentary) so that the process model can be applied to the audit as fully as possible, in spite of time constraints and mandated con­tent. When one-time audits are investigations on persons, the audit is not an­nounced; in all other cases, a confidential meeting with the main person respon­sible should be held to discuss the ad-hoc audit announcement beforehand.
* The conduct of ad-hoc audits is very individual and depends on the content to be covered. Even so, standard auditing methods and working papers should be used as far as possible. If special partners such as the police or the district attor­ney’s office need to get involved, the reasons must be documented. In some cases the auditors have to find out whether evidence must be provided to be used in a court of law. Content and objectives may change in the course of an audit: For example, ad-hoc audits may lead to standard audits, either to be conducted immediately or to be added to the planning schedule. Direct escalation and/or information channels between Internal Audit management and the parties re­sponsible, particularly the Board of Directors, are important for ad-hoc audits.
* Some parts of the reporting system follow different rules than that of the other two audit types. Because of its specific content, it may be useful to dedicate a separate column of the special audit report to more detailed information on au­dit content. Detailed information for a follow-up audit is not necessary, or only to a limited extent, because the release of the findings of ad-hoc audits directly triggers the necessary action, or management initiates a targeted response that does not normally interfere with processes.
* For this reason, ad-hoc audit follow-up can be varied, ranging from a full fol­low-up to no follow-up at all. In the case of one-time audits, it is often sufficient

A | 6 | **6.6**

if the audit lead and the manager responsible briefly coordinate their response. Irrespective of the procedure used, Internal Audit must always document when a recommended measure has been completed.

Much of the content and organization of ad-hoc audits cannot be planned ahead and often has to be scheduled, prepared, and started at short notice. It is also impor­tant to note who is making the request. In principle, anyone can make an audit re­quest, but requests from the Board, higher management levels, the legal depart­ment, and internal auditors get special priority, particularly if fraud is suspected. Suspected fraud and requests from the Board are given the highest priority. In some cases, however, an initial analysis of the tasks may show that the request does not fall within Internal Audit’s remit, but should rather be dealt with by entities such as the management responsible, the compliance officer, Human Resources, or the le­gal department (see Section A, Chapter 5.8).

**Execution of Ad-hoc Audits**

**HINTS ANDTIPS •**

* In special audits, it will help the auditors if they can rely on specialist support and discuss the Scope with people who have the necessary knowledge.
* In ad-hoc audits, auditors must gain a clear understanding of the audit content by discussing the audit objectives and content with the requesting party or the person responsible in Internal Audit.
* Even during the audit, it may be expedient to report to the Board of Directors, if the content is time-critical or a response from the people responsible is needed.

**LINKS AND REFERENCES**

* SAWYER, L„ M. DITTENHOFER AND J. SCHEINER. 2003. Sawyer’s Internal Audit­ing. 5th ed. Altamonte Springs, FL: The Institute of Internal Auditors.
* SEARS, B. 2002. Internal Auditing Manual. New York, NY: Warren, Gorham 8c Lamont.

1. Audit Cycle

**KEY POINTS •••**

* The audit cycle is an important formal determinant of the audit method.
* The different statuses (basic audit, status check, and follow-up) are intended to ensure that the audit process is conducted in full, including a check of whether the implementation measures performed have been effective.
* The audit cycle affects the audit types in different ways. It has a major influence on standard and special audits, but ad-hoc audits tend to be more individual in nature.

In addition to the formal determinants already described, the audit cycle is another important factor necessary for defining the audit method. The audit cycle has three stages (also known as statuses): Basic audit, status check, and follow-up. The aim of the multi-stage process is to get away from only looking at the audit process, and to include a check of whether the recommended improvement and implementation measures have been effective. Each audit has to rim through the full audit cycle, although the importance of each stage may vary, depending on the case in question. In some cases, the follow-up audit and the ensuing phases are optional (see Section B, Chapter 6.1).

**Three-Phase Process**

**Basic Audit**

**Link between Basic Audit and Audit Type**

**Status Check**

**Execution of Status Checks**

**Link between Status Check and Audit Type**

A basic audit is performed in accordance with planning, the Scopes, and the work program, and the specifications in the audit request, if applicable. It runs through all the phases of the Audit Roadmap and produces findings and recom­mendations to eliminate any weaknesses identified. The audit results are presented to the auditees and their managers at a closing meeting, and a draft report is for­warded to the parties involved for additional comment. Consultation with the area being audited is intended to create mutual understanding and a shared basis for the subsequent steps. On average, it takes 30 days to conduct a basic audit.

Although the calculated average completion times are often correct for standard audits, basic audits conducted as part of special audits, especially global ones, often take up to seven weeks. In ad-hoc audits, the duration of the basic audit may be up to two weeks shorter than for standard audits, including reporting. Basic audits are the foundation for the audit cycle, especially for scheduled audits.

At least six months should elapse between the basic audit and the next step of the audit cycle, the status check. In case of an escalation process, this timeframe may be reduced. For the status check, Internal Audit asks the persons responsible for the audited area to compile a status update that gives their view of how imple­mentation is progressing. During the status check, senior management evaluates the degree of implementation for each finding and asks the auditees to verify the status on the basis of the implementation report. Problems with the implementa­tion of recommendations can be discussed and recommendations can be adjusted or, in exceptional circumstances, even waived. Internal Audit does not perform ex­plicit fieldwork at this stage. A comprehensive, fully documented check of imple­mentation measures is reserved for the actual follow-up audit.

Status checks are inserted into the annual audit plan without a separate risk as­sessment. They are a type of preliminary test intended to find out whether and how Internal Audit’s recommendations from the basic audit are being implemented. The basic time required for a status check averages two days.

The status check is required for all audit types. In standard and special audits, it is used as originally intended, but in ad-hoc audits it may be applied as a final check for the measures that have been implemented, because under this audit type, rec­ommendations often lead to an immediate requirement for action, and implemen­tation merely has to be confirmed.

A | 6 | **6.6**

Follow-up audits are also included in the audit plan without a separate risk as­sessment (for details, see Section B, Chapter 6). They should take place approxi­mately six to twelve months after the status check. If an audit is in an escalation process, it may be sensible to perform the follow-up within a shorter timeframe. The follow-up audit is based on the results of the status check. Unlike the status check, a follow-up audit involves fieldwork by Internal Audit because the effective­ness of the implementation measures performed has to be verified beyond doubt. The implementation report of the basic audit constitutes the work program for the follow-up audit. Internal Audit prepares working papers to be used as audit evi­dence. If implementation is found to be insufficient, this fact must be documented and additional audit findings may have to be added.

A follow-up audit may give rise to new, additional audit topics, either planned or unplanned. In such cases, the findings of the additional audit work are docu­mented in a new audit report with a separate status.

Again, follow-ups should be conducted by the same audit team as the basic audit (or at least by the same audit lead). The design of the follow-up envisages two fol­low-ups in case there were reasons that made it impossible (or very difficult) to test implementation during the first follow-up (e.g., non-availability of the employees concerned). A second follow-up can also be scheduled if the first follow-up pro­duces unsatisfactory results, i.e. if the identified weaknesses from the basic audit have not been satisfactorily remediated. The second follow-up audit is scheduled approximately six months after the first one. This means that the maximum dura­tion of an audit cycle is approximately 24 months. A follow-up takes around 16 days on average, including all necessary fieldwork.

Follow-ups are normally conducted in the context of standard and special au­dits. In the case of ad-hoc audits, they only make sense if conducted shortly after the basic audit if at all. The following diagram shows each audit type in relation to the extent of its cycle.

**Follow-up**

**Additional Audit Topics**

**Execution of Follow-ups**

**Link between Follow-up Audit and Audit Type**

**Standard audit**

**Special audit**

**Ad-hoc audit**

Fig. 25 Extent of the Cycle of each Audit Type

In connection with the audit cycle, the problem often arises that, since organization and workflow structures in modern (especially global) companies change rapidly, some audited units, e.g., departments or processes, only exist for a limited time. This means that often there is only one audit cycle of Internal Audit that relates to a clearly defined unit requiring the same audit treatment. In such cases, subsequent, separate audit cycles for the audited unit are linked up.

**HINTS AND TIPS •**

**Change in the Organization and Workflow Structures**

* To prepare for a basic audit, auditors should obtain documents from earlier au­dit cycles of the same audit object.
* Auditors should ensure that the responsibilities and deadlines for implementing measures are clearly defined.
* The audited unit should record all its implementation measures by providing clear evidence, documents, and examples for inclusion in the working papers.
* Auditors should document any deviations from the agreed measures and in­clude reasons.

**LINKS AND REFERENCES**

. SAWYER, L„ M. DITTENHOFER AND J. SCHEINER. 2003. Sawyers Internal Audit­ing. 5th ed. Altamonte Springs, FL: The Institute of Internal Auditors.

• SEARS, B. 2002. Internal Auditing Manual. New York, NY; Warren, Gorham & Lamont.

1. Cost/Benefit Analysis

**KEY POINTS •••**

* While the cost of an internal audit is easily quantifiable, measuring its benefits is less straightforward since internal audit findings may have both direct and indirect effects.
* The relevant benefits of internal audits often manifest themselves on several lev­els and may not be immediately visible.
* Cost savings are easier to allocate directly than other benefits.
* By establishing a correlation between the potential benefits and the costs in­curred by the internal audit department, an approximation of the profitability can be obtained.

It can be very important to measure the efficiency of internal audit work. It involves examining the ratio of costs incurred by Internal Audit during the course of a spe­cific audit, or the cost of the entire internal audit department, compared with the actual benefits achieved for the company as a whole, (e.g. through cost savings, re-

**Efficiency Measurement**

duced risk exposure, etc.). The following criteria can be used to analyze each audit with regard to the benefits it delivers in the short, medium, and long term (for de­tails on cost management of Internal Audit see Section D, Chapter 8):

* cost-related benefits (reducing, avoiding, or limiting costs), and
* monetary and non-monetary benefits (increased sales, improved operating profits, motivation, reputation).

Generally, the cost impact of an audit can be seen in the short to medium term. Costs normally respond linearly and usually correlate very clearly and closely with their drivers. They can be quantified, for example on the basis of effective payments made, although direct perception declines as the time between implementing the recommendation and the time of payment increases. In addition, imputed costs can be used as part of the analysis. Normally, imputed costs increase the impact of audit findings in areas more prone to inducing costs, because ineffective internal controls also lead to costs and expenses that could otherwise have been avoided.

**Impact on Costs**

While the costs related to internal audits and the resulting recommendations are relatively straightforward to determine, the benefits are much more difficult to quantify. First, the benefits often continue over long periods of time. Secondly, it is often difficult to measure benefits and attribute them directly to the processes that have brought them about. Benefits are frequently abstract and the interdependen­cies between cause and effect are often obscure. A complicating factor is that the effects of qualitative and quantitative benefits sometimes overlap and can thus ei­ther reinforce or detract from each other. The more general the benefit analysis, the more difficult it will be to reliably assign indicators that map and explain the causal relationship between an audit activity and its findings on the one hand and the perceptible benefits on the other.

**Benefits**

Before it is possible to quantify any benefits, representative benchmarks must be defined for each audit field (e.g., throughput times, purchasing terms and condi­tions, contribution margins), applying either direct or indirect measures. Quite possibly, audit recommendations will lead to tangible benefits, such as an improved working atmosphere, greater motivation, or error reduction, which will in turn en­hance each employee’s understanding of values. There may also be a change in the way effects are perceived externally. An improved position in the marketplace, eas­ier access to finance, and a different public perception, for example, if negative fac­tors are eliminated quickly and with determination and their recurrence is pre­vented by implementing adequate measures. It is important to recognize that there may be both short-term cost savings and longer-term benefits gained from Internal Audits and the implementation of the resulting control recommendations. Both benefits should be considered when performing a cost/benefit analysis, even though they may overlap sometimes.

**Deriving of Benefits**

Including quantifiable benefits in the analysis brings up the most difficult aspect of measuring Internal Audit’s efficiency. The main purpose of examining these ben­efits is to establish a causal link between an audit finding and increased benefit

**Quantifiable Benefits**

A | 6 | **6.7**

values for a business unit or the company as a whole. A key challenge in this regard is to extrapolate the quantified benefit created by eliminating a process weakness, thus making it visible.

**Organizational and Time Delays**

**Anonymous Cost-Benefit Relationship**

**Standard Cost/Benefit Analysis**

With regard to the implementation of audit results organizational effort and time delays should not be ignored. Since each audit field has different content, each must be considered in detail. In business audits (see Section A, Chapter 6.2.7), for example, linear correlations between audit result and increased profits can be estab­lished, because there is a direct link between the audit object and the success driver.

Often, the benefit derived from internal audits is unclear, without a direct link to the measurable benefit-related units. Therefore, equivalents must be established by using auxiliary variables to quantify the cost impact and the benefits related to the audit findings.

To define a standard cost/benefit analysis for each audit field, Internal Audit must define and categorize separate benchmarks (see Section D, Chapter 8 for more on Internal Audit cost management and Section D, Chapter 7 for benchmarking). Thus, Internal Audit is integrated into the business control and decision processes, which results in interdependencies with other disciplines, such as capital invest­ment appraisal, management accounting, and planning.

**HINTS AND TIPS •**

* When preparing for an audit, auditors should investigate whether there are ex­pectations about the audit’s efficiency.
* Auditors should discuss the cost savings and benefit potential for each audit with the audit lead or Audit Manager.

**LINKS AND REFERENCES \***

* ANDERSON, U. AND A. DAHLE. 2006. Implementing the Professional Practices Frame­work. 2nd ed. Altamonte Springs, FL: The Institute of Internal Auditors.

. SAWYER, L„ M. DITTENHOFER, AND J. SCHEINER. 2003. Sawyer’s Internal Audit­ing. 5th ed. Altamonte Springs, FL: The Institute of Internal Auditors.

* SEARS, B. 2002. Internal Auditing Manual. New York, NY: Warren, Gorham & Lamont.