CHAPTER 12
Assessing Internal Control

As discussed in chapter 11, "Planning the Audit Engagement," during the planning phase of an assurance engagement, internal auditors perform a high-level risk assessment to develop the audit objectives, scope, and general approach. This then leads to the development of the audit work program and its detailed steps to accomplish the scope and objectives. When developing specific audit work program steps, internal auditors must understand both the risks and controls involved. At this point, the risks are those gathered in the risk assessment process and refined during audit planning efforts. The internal auditors should also have a general basis for defining expected controls given the scope of the engagement.

Defining and Evaluating Internal Control

The Glossary of the IPPF defines Control as "Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved." Based on this general definition, control can be many things that make up daily governance and management.

Exhibit 12-1 illustrates the levels of internal audit maturity and the related products and services provided, as introduced in chapter 2, "Defining Internal Audit Products and Services," and leveraged in chapter 10, "Risk Assessment and Audit Planning," and chapter 11. The comparison is continued here to link the focus of risk and control definitions to the desired level of products and services. This is critical as audit work programs are developed to execute the scope of the engagement.

Developing Audit Programs

When planning an engagement, risks are specifically considered. These risks then drive the scope of the engagement. The risks to be addressed are often inherent in the scope statements and can help internal auditors understand the service or product they are expected to deliver. The following audit scope statements can be compared to exhibit 12-1.

- Example 1: Evaluate regulatory compliance with Federal Acquisition Regulations (FAR).
- Example 2: Evaluate existing efforts to replace admissions technology.
- Example 3: Review management and alignment of claims operations with overall mission.

Exhibit 12-1
Applying Risk and Control Definitions by Type of Engagement

Product/Service Maturity	Type of Services/Products	Risk Definition Focus	Control Definition Focus
Level 5 – Optimized	• Places risk management-based efforts in context of the specific business objectives at risk. • Internal audit is recognized as a key agent of change.	• Risk definition is simplified as the effect of uncertainty on business objectives.	• Control actions align more clearly with processes of strategic action, governance, objective oversight, and operational alignment of people, process, and technology.
Level 4 – Managed	• Evaluation of risk management expectations first in risk assessment and audit program development, focused on strengthening controls from the top down • Internal audit provides overall assurance on governance, risk management, and control (GRC).	• Risk identification and response becomes an assumed responsibility of management. • Risk management culture, training, and processes support this effort.	• Control expands to include expectations of good management practices (good governance) and effective risk responses (risk management) throughout the organization.
Level 3 – Defined	• Assurance services expand on Levels 1 and 2. • Advisory services are provided. • Risk assessments are performed at least annually. • Internal audit engagements are planned and findings are identified by risk likelihood and impact.	• Risk becomes a management perspective on what could go wrong.	• Control definitions are less tangible and more focused on what stops bad things from happening. • Toolsets for control expand, giving credit to many management actions that limit negative event impact.
Level 2 – Repeatable	• Evaluation of financial and important operational process controls	• Risk expands to include ineffective and inefficient processes.	• Controls expand focus to include process documentation. • Common tools for control include process analysis and control identification.
Level 1 – Initial	Internal/external auditor services are provided and focus on: • Financial statement assurance and reviews of documents and transactions for accuracy and compliance • Compliance with external regulations, standards, and requirements • Compliance with internal policies and standards	• Risks are defined by noncompliance with standards and regulations.	• Controls are focused on transactional accuracy and compliance with regulations, policies, and standards. • Common tools for control include policies and training.

In the first example, the implied risk is noncompliance with regulations. The second scope statement covers a much wider set of risks that could go wrong that could boil up to an overall risk of failure in replacing admissions technology. The final example is clearly focused on an oversight or operational governance risk. Based on the definitions outlined in exhibit 12-1, the first example would be a risk at Level 1, the second describes a risk at Level 3, and the final example describes a risk at Level 5. These inherent risks should then drive the level of controls that will be addressed by the overall audit work program.

Identifying the inherent risks within the scope helps internal auditors understand what the audit product will be. With this end in mind, they can then evaluate the level of internal control that must be included in the audit work program. It is important to match the level of expected controls with the focus of the risk. For example, the scope statement in example 3 requires an audit work program that provides assurance that claims operations are aligned with the overall mission. That would not be possible if the audit work program called for evaluating compliance with compliance and regulations. The reverse would also be true if the audit program steps for example 1 focused on evaluating oversight controls for the procurement department when the scope should be to evaluate compliance actions related to FAR requirements. In this case, the audit program would cover a much broader scope and a level of control not related to the specific risks within the scope. To create an effective audit work program, the scope statement must provide a clear indication of the product or service to be delivered and the level of risks and controls to be assessed.

Levels of Internal Controls Assessed

An evaluation of a risk depends largely on the context within which that evaluation happens. For an internal auditor who, by profession, is charged with providing assurance over effective risk management, it becomes particularly important to understand and be able to communicate to management the context for the assurance provided. Exhibit 12-1 provides that context for the levels of internal control evaluated within an engagement.

Level 1

When the definition of the risks to be assessed is focused on accuracy of financial statements and noncompliance with standards and regulations, then the context for controls to be assessed is focused primarily on education of staff and transactional accuracy. The resulting audit product is likely to be policy and tool improvement and training recommendations supported by errors identified. The product produced is assurance over actions that enable compliance.

Level 2

When the definition of risk expands to include a focus on ineffective and inefficient processes, then the context for controls expands to include a focus on process documentation and analysis. The resulting audit product is likely to be assurance over processes that contribute to meeting these

external and internal expectations. Control recommendations in this scenario cover process inefficiency, segregation of duties, and other ineffective outcomes.

Level 3

As the risk definition begins to focus on management's overall perspective of what could go wrong, it becomes more complicated to define the context for internal control evaluation. The first decision is to determine if the scope of the engagement requires assurance or advisory services. The second decision is based on the identification that something is going wrong. If that is unknown, an audit work program that focuses on root cause analysis related to each finding is needed. However, if there are known issues in the audited business area, the audit work program can first evaluate the oversight (governance) of that area, followed by how well the operations (at a high level) are meeting their objectives. Many internal audit functions operate at this risk-based level with efforts sometimes starting at the detailed control level and working up to the root cause. Conversely, there are times when it makes more sense to focus on the controls at the management and operations level and work down to the level where findings are identified. While this approach provides maximum flexibility, it also creates the highest potential for evaluating controls that do not match the risk assumptions in the scope statements of the project.

Level 4

As internal audit efforts improve and management more directly addresses their risk management responsibilities, there is an attempt to start at the top and work down. For example, if an area under review has compliance issues, billing disputes, and delivery concerns, then rather than approach each of these individually, the audit effort would focus first on what management is doing to ensure overall success. Management refers to this as objective-setting and operations oversight. Internal auditors often refer to it as operational governance or management control. The concepts of governance, risk management, and control (GRC) begin to align with management's processes of performance management. What activities does management engage in daily to ensure objective success? Leading governance and management practices become a resource from which internal auditors can draw to evaluate management controls. A gap at this level may cause some of the issues to happen at a lower level. Absence of these top-level controls (risk management) can have a cascading impact on the overall area.

Level 5

As internal audit efforts optimize, the understanding of internal control aligns much more directly with management's perspectives and operational processes. The language of GRC parallels the management processes (objective oversight and operational alignment of people, processes, and technology). The definition of risk becomes "the effect of uncertainty on business objectives," meaning that internal control becomes entirely responsive to the business objective at risk. Internal auditors must be capable of defining strategic and business objectives and evaluating the governance, risk consid-

erations, and controls in place to ensure their success. This level is much different than the other levels in that it does not consider internal control as black and white—something that is or is not there. Rather, it allows for the possibility that operations grow in capability over time and so does the strength of internal control. At this level, internal control is the next important step management can take to strengthen the likelihood of objective success. And internal audit is truly a partner of management in promoting objective success.

At this level, internal auditors must be capable of seeing the organization from the perspective of management. They must be able to define business objectives and apply expectations of good management (sometimes referred to as operational governance) in their internal control considerations.

Adequacy and Effectiveness

As noted in chapter 11, IIA Standard 2130.A1 requires the internal audit function to "evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems."

This is a tall task. As indicated in exhibit 11-1 in chapter 11, specific planning considerations for an audit engagement change based on the expected internal audit product and service maturity. Similarly, there is a maturing of risk and control concepts and tools used to assess their adequacy and effectiveness. See exhibit 12-1.

Internal audit functions cannot just accept an area's policies and procedures without question as the standards they audit against. They must evaluate the design adequacy of those policies, procedures, and other risk management techniques if they plan to move the audit service or product to a higher level of control evaluation and value delivery. Typically, internal auditors find that assessing higher-level controls generates more significant audit findings. For example, testing a well-designed control may result in a 15 percent error rate. That is not good, but it means the control accomplished its purpose 85 percent of the time. A poorly designed control, on the other hand, will never really accomplish its purpose, even with a 0 percent error rate. In fact, if internal auditors detect a design weakness and management agrees, there is usually no need to test whether it is operating as intended.

However, internal auditors may conduct additional work to determine the potential for fraud, misappropriation, financial and nonfinancial losses, as well as actual losses. Internal audit management should coordinate promptly with the investigation team and legal department on any matters

Of Note to Internal Audit Staff

Strong organizational governance is made up of clear operational objectives and measures. Organizational components must have a clear awareness of their specific purposes for operations above and below them. If operational objectives are not linked, it is an indicator that the governance environment is ad hoc and inefficient. When operational objectives are clearly articulated and descend the chain of command efficiently, effectiveness and capability can increase. Strategic objectives are not always operational and are typically achieved by coordinating specific initiatives that may cross many operational areas. As the auditors understand these management realities, they can create realistic expectations of organizational governance.

regarding fraud to comply with corporate policies and investigation protocols. In most cases, a fair amount of time is spent understanding and analyzing the design of the system of internal controls to determine whether it provides adequate control prior to the start of testing for effectiveness. This provides a firm basis for addressing root causes for findings, which can sometimes be the result of poor control design. It will also help internal auditors identify missing controls.

Level 1-3 Internal Control Design

For Levels 1 through 3, internal control design may be a secondary or primary decision based on the risk being assessed relative to the scope of the project. For example, a strictly defined compliance audit engagement may only include a review of transactional compliance controls to define the level of compliance, with no control design evaluation. In practice, at these levels, internal audit functions might choose to evaluate design adequacy at any of several points in an audit engagement. For example:

- Some evaluate design adequacy during a specific phase of the engagement. This approach has the advantage of focusing on what is often the most value-adding part of the evaluation.
- Some evaluate design adequacy during the planning phase.
- Some evaluate design adequacy while performing tests of effectiveness.
- Some evaluate design adequacy at the entity level during audits of locations. For example, if one set of standard operating procedures (SOPs) is used for all branches or plants, their design can be evaluated once at the entity level. In these situations, the internal auditors should also ask about any changes or activities at each location that are not covered by the SOPs and, if significant, assess the related risks and evaluate the design adequacy and operating effectiveness of the risk management techniques. The internal auditors should also ask location management and employees for their opinions about the SOPs, especially where noncompliance is found. Sometimes a procedure that is theoretically sound does not work in practice. Management in charge of designing the procedure or the process owner needs to be made aware of this. In fact, effective communication between process owner and process operators is an important control to ensure sound design adequacy and operating effectiveness of key processes.

Evaluating the design adequacy and operating effectiveness of controls depends entirely on what assurance product the audit engagement is intended to provide. Is it Level 5 assurance over the organization's governance controls or is it Level 1 assurance of compliance expectations? Evaluating the adequacy of control design becomes more and more important the higher the level of internal control assessment implied in the project scope.

Level 4 and 5 Internal Control Design

When assessing Level 4 or 5 internal controls from the top down, the assessment is focused on the organization's governance before operations. However, to assess these areas, it is necessary to first establish control expectations. At these levels, controls are much more clearly defined as what

management does to ensure successful achievement of their objectives. What are leading practices? This is a question relating to the design and development of management control, also referred to as organizational governance practices. At these levels, it is helpful to consider that internal control matures with the development of the organization. Consider the following example.

In a large hospital, the director of patient admissions has seen growth in errors and employee turnover. He is concerned and invites internal audit to evaluate the area. The internal auditor begins by asking the question, what is expected of the director of patient admissions? A list is started:

- The purpose of patient admissions is clearly understood and documented.
- There are measures or metrics that are monitored by the director that define success of the area.
- There are reports that provide accurate and timely data on measures and metrics.
- Reports on measures and metrics are reviewed by the director timely.
- Policies and procedures are used to ensure consistency as much as possible.
- The director intentionally manages the culture to promote productive and positive outcomes.

In effect, the internal auditor is evaluating the design of admissions oversight. If reasonable efforts in these areas are being performed by the director of patient admissions, admission operations are assessed. What would be on the list related to admissions operations?

- People: Are the skills necessary to conduct admission activities present?
- People: Is training an oversight function available for those needing guidance?
- Process: Is there a narrative or flowchart of the overall processes within admissions?
- Technology: Are applications leveraged as possible to enable efficiency and effectiveness within operations?
- Alignment: Are the skills held by people aligned with the complexity of the process and the enablement of technology?

At Level 4 or 5, internal auditors start by evaluating the design of governance and operational controls to determine where, if any, specific control testing must occur.

Detailed Assurance Engagement Risk Assessment

As noted in chapter 11, the high-level risk assessment performed during the planning phase is not a linear process. It requires internal auditors to sort through a wide variety of diverse information to find the key indicators of risk. The detailed risk assessment of the activities that fall within the audit scope is linear. It proceeds step by step through a disciplined analytical process. That process is embodied and most easily understood in an audit tool that many internal audit functions use: the risk and control matrix.

There are almost as many versions of the risk and control matrix as there are internal audit functions that use it. Typically, internal auditors start using one version, find that certain parts of the thought

process it embodies are not working very well, and change it until it embodies a thought process that is intuitive for both the internal auditors and business managers.

For illustrative purposes, **exhibit 12-2** provides an example of a risk and control matrix that is fairly simple and embodies the basic elements of risk analysis.

Exhibit 12-2
Sample Risk and Control Matrix

Objectives	Risks	Impact/ Likelihood	Controls (and Other Risk Management Techniques)	Evaluation of Design Adequacy	Tests of Operating Effectiveness	Final Evaluation

Internal auditors can complete the matrix themselves, but the results will be better if they can engage the responsible manager or supervisor in the analysis. That person knows the business objectives and risks better than the internal auditors do. That person, however, has probably never performed a formal risk assessment unless the organization has strong enterprise risk management (ERM) practices that include assessments at the detailed level. The internal auditor then guides the manager or supervisor through the analysis in a logical and efficient manner.

Identify Objectives

Analysis starts with the business objectives of the audited business area, each of which occupies a row on the matrix. After completing this column, it is good practice to compare these objectives with those of the area to which they report, as applicable, and the organization's strategic objectives. Misalignment of objectives can be a serious issue.

The objectives of the audited business area should be clearly stated to ensure proper identification of the scope. For example, one of the objectives of customer relationships management is to protect privacy of customer data. Privacy refers to "the freedom from intrusion into one's personal matters and personal information." Management needs to identify the universe of customer data; the lifecycle of all the customer data; who handles the data; and when, where, and how they are initiated, processed, stored, and destroyed. If the assurance internal audit wants to provide is on adequate protection over all critical customer data, the scope of the audit engagement needs to cover all of the parties that are involved in using, processing, and storing the data. This may include business partners, third-party service providers, and advertisers, among others.

Identify Risks

The risks to an objective include anything that could prevent it from being achieved. For example, the operational objective "Hire 10 new qualified nurses to replace retiring staff" would have several risks, two of which are external:

- Lack of qualified nurses in the local area
- Competition for available nurses from rival hospitals

Risks can also arise in pursuit of the objective. For example, a private sector CEO has the objective of meeting financial analysts' expectations for financial results each quarter. The pressure to meet those expectations creates a temptation for fraudulent financial reporting, which is certainly a risk.

A good way to include both risks that prevent achievement of an objective and those that arise in pursuit of it—and also a commonsense way to ask a manager to identify risks—is to simply ask "What could go wrong?" This is a Level 3 question. It allows the internal auditor maximum flexibility, but it may result in many risks of different value being compared equally.

Internal auditors do not, of course, rely entirely on what the manager says. They also independently identify risks and will typically think of risks that did not occur to the manager. These will also be included in the analysis.

Risk is everywhere; there are an infinite number of things that could go wrong. Equally important is understanding what must go right. The list of things that must go right is typically substantially smaller and more manageable. In part, this is what internal auditors ask as they look at Level 4 and 5 controls when assessing the adequacy of internal control design discussed earlier. What must management put in place to achieve their objectives? In fact, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) codified this list into 17 principles of effective internal control in its 2013 revised *Internal Control – Integrated Framework* (see **exhibit 12-3**). These principles, when translated into operating philosophy and processes and when operating effectively, can mitigate the portfolio of risks. If the governance structure is strong, management exercises effective oversight and monitoring through operationalizing these principles, which will promote achievement of objectives. Many objectives are interdependent. When management oversight is effective, it has significant impact on the achievement of all the objectives. Similarly, the root causes of all findings identified in an organization can be traced back to weaknesses in the design adequacy and operating effectiveness of management control.

Management oversight is defined by COSO as watchful and responsible care, supervision, and the duty of overseeing the performance of a function or group. These definitions embody the "hard" element of duties and responsibilities and the "soft" element of care, being watchful and alert and performing due diligence. Therefore, effective management oversight depends on having management with the right character, personality, management style, a mature governance and risk management environment, and an enabling corporate culture. Internal auditors can help the organization improve management oversight by focusing their assessment on management control design at Levels 4 and 5, as illustrated in exhibit 12-1. Through the audit process, management can learn about the linkage between performance and management's responsibilities of planning, organizing, directing, controlling, and coordinating; the importance of setting the right objectives and strategies; implementing effective monitoring, decision-making, and execution processes; and hiring the right

Exhibit 12-3[1]
COSO's *Internal Control – Integrated Framework*
Principles of Effective Internal Control

Internal Control Component	Principles
Control environment	1 Demonstrate commitment to integrity and ethical values. 2 Ensure that the board exercises oversight responsibility. 3 Establish structures, reporting lines, authorities, and responsibilities. 4 Demonstrate commitment to a competent workforce. 5 Hold people accountable.
Risk assessment	6 Specify appropriate objectives. 7 Identify and analyze risks. 8 Evaluate fraud risks. 9 Identify and analyze changes that could significantly affect internal controls.
Control activities	10 Select and develop control activities that mitigate risks. 11 Select and develop technology controls. 12 Deploy control activities through policies and procedures.
Information and communication	13 Use relevant, quality information to support the internal control function. 14 Communicate internal control information internally. 15 Communicate internal control information externally.
Monitoring	16 Perform ongoing or periodic evaluations of internal controls (or a combination of the two). 17 Communicate internal control deficiencies.

talents and promoting a growth-oriented, positive corporate culture. By focusing on management controls, internal audit can help all three lines of defense gain capabilities for greater maturity in GRC.

Assess Risk Impact and Likelihood

Each risk must be assessed. Internal auditors should decide how much audit effort to devote to that assessment. The two key factors to assess are the *impact* of the risk event if it occurs and the *likelihood* of it occurring. These are indicated in the third column of exhibit 12-2.

Impact and likelihood can be measured in various ways. For example, financial service companies measure credit risk and market risk with highly sophisticated quantitative methods. They do this because the natures of these risks lend themselves to quantitative analysis and the potential impact justifies the cost. However, for the purposes of assurance engagements, most risks can simply be assessed as high, medium, or low.

It is typically helpful to assess impact and likelihood separately, because doing so helps management decide on the best risk management technique and helps internal auditors decide (a) whether management has selected the best technique and (b) whether to continue with the risk analysis.

Management can respond to risk in any number of ways as outlined in COSO's framework, *Enterprise Risk Management – Integrating with Strategy and Performance.* COSO also gives examples of specific risk management techniques:

- Accept: No action is taken to change the severity of the risk.
- Avoid: Action is taken to remove the risk.
- Pursue: Action is taken that accepts increased risk to achieve improved performance.
- Reduce: Action is taken to reduce the severity of the risk.
- Share: Action is taken to share all or part of the risk.[2]

Internal controls, which reduce the likelihood or impact of risk occurrence, fall under the risk response technique. Internal auditors should not limit themselves to evaluating controls; they should evaluate whatever risk management technique management is using.

Evaluating impact and likelihood separately helps internal auditors evaluate the strength of management controls and determine if the remaining risk is great enough for the internal auditors to devote the time to analyzing it further. Many factors influence the decision on risk assessment and whether internal auditors should pursue continued analysis. Some key points to be taken into consideration are:

- If the risk is minor, internal auditors should not spend time analyzing it further.
- Impact should be given more consideration than likelihood. For example, high impact/low likelihood risks are often ignored because no one thinks they will ever occur. When one does, the impact is catastrophic. However, these risks may be managed by second line of defense functions.
- Unless the impact is so low as to be negligible, low impact/high likelihood risks are sure to be recognized by management and almost certainly managed with cost-effective controls.

Of Note to Internal Audit Staff

Internal auditors have historically focused on risks and risk events. The potential challenge to this perspective is that it does not align with how management thinks. Management thinks of objectives and their achievement. So, what does this mean in assessing an individual risk? It means that management may agree with the internal auditors' impact assessment but is not likely to agree with their consideration of likelihood. To managers, the likelihood of a risk event occurring is mitigated by the quality of their staff and the resilience built into the maturity of their operations, among other factors. They will assume that internal audit's likelihood assessment is missing considerations of these assumptions around how "probable" a risk is of occurring. A savvy internal auditor gives management credit for the strength of their objective oversight, their people, and the resilience or maturity of their operations.

Identify Controls and Other Risk Management Techniques

If a risk is worth analyzing further, the next step is to identify the controls or other techniques used to manage the risk. Risk management techniques other than controls (avoidance, acceptance, pursuit, and risk-sharing techniques like insurance, hedging, or contractual arrangements) are best

discussed with the manager. There are usually few of these techniques, and it is important to understand management's rationale in choosing them.

Level 4 and 5 Internal Controls and Risk Management Techniques

When an audit engagement is performed from the top down and first considers direct objective oversight and operations alignment controls, some assumptions are important:

- The area being audited has clear business objectives, metrics and measures, and progress reporting (governance controls).
- The operations within the area being audited are developed with alignment of people, processes, and technology as a priority (operational controls).
- Governance and operational controls mature with the area and should be aligned with their capabilities.

Risk management efforts in a mature environment typically include specific decision-making processes focused on eliminating bias and quantifying options at a level that risk-taking choices can become clear.

Other Internal Controls and Risk Management Techniques

For audit engagements executing at other levels, there is less context for control. Controls are usually numerous and many operate at a detailed level. The manager is a good source for high-level controls and soft controls, but other sources are often better for more detailed controls (for example, control activities in a transaction-processing system). Also, using other sources for identifying controls does not require the manager's valuable time. Other sources include:

- Written policies
- Procedure manuals
- Process documentation like flowcharts and process narratives
- First-line employees
- Supervisors

In general, controls within governance of an area being audited or alignment of operations inherently are more important as they can have cascading impact on lower-level objectives and controls. However, at the detailed level it is important for the internal auditor to distinguish controls from procedures and key or primary controls (those controls that must operate effectively to reduce the risk to an acceptable level) from secondary controls (controls that help the process run smoothly but are not essential). For example, a process might have a verification control that will detect any errors that occur before the verification is performed. Other controls in the processing stream help to reduce the error rate, but if they fail, the errors will be detected and corrected without significant harm. In this case, the verification is the key control.

Evaluate Design of Controls and Other Risk Management Techniques

When evaluating control systems, it is important to evaluate the key types of relevant controls: management, operational, IT, financial, financial reporting, and compliance. These controls often fulfill multiple objectives. Evaluating them collectively minimizes redundancies and costs of implementing, executing, and monitoring controls. With technological advancements and breakthroughs, technologies are embedded in products, services, and processes. In some cases, procedures are even performed by robots. Internal audit should pay particular attention to IT controls. It is not unusual to see that IT planning, strategies, development, implementation, and monitoring are not fully integrated with businesses and operations because IT can be intimidating. This creates risks of redundancies and gaps in controls. Internal audit can make a significant contribution educating management and employees by bringing these control disciplines together to show how they complement and support each other. Improved understanding of IT controls reduces their fear of IT.

When controls are identified by a manager or through documents, it is good practice to verify them with the employees who perform the controls. This is best done by a walk-through in which the employees explain and show the internal auditor step by step how they and the system perform the tasks. The auditor sees if the controls are present. If they are not, there are a few likely reasons:

- Management oversight is not as consistent or mature as implied. (Control Design)
- Operations are misaligned at some level of people, process, or technology. The procedure, designed by people who do not do the work, is theoretically sound, but it does not work well in the real world (or it worked well when it was designed, but the environment has changed and the procedure has not been updated). (Control Design)
- An employee is not following proper procedure. (Control Failure)
- The system is not operating as designed. (Control Failure)
- The IT controls have not been designed or implemented. (Control Design)

Walk-throughs serve a dual purpose. They are tests of effectiveness (whether the control is operating as designed), which is addressed later in this chapter. They are also an important part of the design evaluation phase for two reasons:

- The internal auditor needs to document the actual state of controls.
- If the control does not work well in the real world, the weakness is in design, not execution.

Evaluating design is highly judgmental, yet it can also be simplified, particularly at Levels 4 and 5. At these levels, control design from the top down is driven by governance and operational expectations of management. In many ways, this also is the risk management expectation. Leading practices from the business can help define these expectations. For lower-level objectives, it is basically a matter of asking what could still go wrong, assuming the risk management technique is applied effectively, and whether this is an acceptable risk.

Theoretically, management is the owner of the subject of the topic (for example, business activities, operations, and functions) and responsible for implementing controls to keep risk within their own risk appetite. In reality, most organizations' risk management and control knowledge and practices are not at the desired Level 4 or Level 5 and their management does not have training in effective risk management and controls. Responsibilities for controls are not well defined and shared among a group of process operators. Internal auditors have a responsibility to use their professional judgment and knowledge of risk and control to form their own opinion regarding whether a risk is acceptable or not and confirm their opinion with management. Usually, when an internal auditor believes the risk is not acceptable, business unit management will agree to correct the situation. Sometimes management will say it accepts the risk. When this happens, the internal auditor's responsibility is to see that risks are accepted in accordance with senior management's risk appetite or addressed by management at the appropriate level of authority. Internal auditors should report these findings, the root causes, and corrective actions taken by the business unit or management with appropriate responsibilities.

The identification of risk accepted by management may be observed through an assurance or advisory engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. When the chief audit executive (CAE) concludes that management has accepted a level of risk that may be unacceptable to the organization, Standard 2600 – Communicating the Acceptance of Risks specifies that he or she must discuss the matter with senior management. If the CAE determines that the matter has not been resolved, he or she must communicate the matter to the board.

Secondary controls should be included in the design evaluation, but usually for process efficiency only. Are the secondary controls needed? Perhaps they were in the past, but other changes in the process have made them superfluous. Or maybe the manager and staff are so risk-averse they refuse to accept even a minor risk and are wasting resources. In such cases, internal auditors should recommend discontinuing the controls.

The evaluation of controls and other risk management techniques is recorded in the fifth column of exhibit 12-2, labeled Evaluation of Design Adequacy. Internal audit functions that use a matrix like this usually have one conclusion for each risk, indicating whether the set of techniques to manage this risk brings the residual risk to an acceptable level. This conclusion can be as simple as yes/no, or there can be an explanation. If a design weakness exists, there would be a cross-reference to another workpaper where the finding is fully developed for discussion with management.

The sixth column, Tests of Operating Effectiveness, could serve as the audit work program for the testing phase. More often it would have cross-references to that program because there is too much information in the audit work program to contain in this column. There would be a cross-reference for testing of each key control and a note like "secondary" or "pass" for controls that will not be tested. The last column, Final Evaluation, is completed after the effectiveness testing is completed.

As stated above, there are many variations of the risk and control matrix. Exhibit 12-2 illustrates the key steps in the detailed risk assessment; another matrix or other audit tools might work better for a given internal audit function.

Tools for Documenting and Evaluating Control Design

As indicated in its definition, internal auditing brings "a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." The systematic and disciplined tools most commonly used by internal auditors to document and evaluate the design of control processes are the risk and control matrix and the flowchart. These tools are typically complemented by narratives when more detailed descriptions are needed.

Risk and Control Matrix

As has been discussed, many internal audit functions use a matrix as their central audit tool because it embodies the analytical process that drives the entire engagement. Some accomplish the same thing without the matrix format because their planning workpapers have a section heading for each objective, followed by section headings for the risks to that objective (including the assessment), controls and other risk management techniques, and so forth. This can be thought of as another version of a risk and control matrix, so it accomplishes the same thing.

Risk and control matrices can be applied at any level. Some internal audit functions use one to develop their periodic audit plan. For small assurance engagements, a single matrix may be all that is needed. Or, there can be a nonlinear, high-level risk assessment to determine audit objectives and scope and several matrices for the detailed risk assessment of activities that fall within the scope.

Some organizations have strong ERM processes through which every area of the business develops its own risk and control matrix. In these organizations, internal auditors start from management's risk assessment but perform their own independent risk assessment, just as they did at the entity level during planning. One of the positive outcomes could be to help management improve their risk and control matrices.

Internal audit functions that use a risk and control matrix as their central audit tool usually supplement it with other tools. This is partly because including all the information in a series of narrow columns would be cumbersome. It is also because some of the information is better documented and analyzed with other tools.

Flowcharts

Most business areas process transactions or information, or they have other linear processing streams (for example, the hiring process proceeds step by step). Each time the process moves from one step to the next (for example, when information or a transaction moves from one person, document, or

Exhibit 12-4
Sample Flowchart

Narrative	Op. No.	
VERTICAL FLOWCHART Ordering and Receiving		Central Purch. Dept. (Purchasing Clerk)
Report received from Central Computer Department. Report reviewed, order quantity changed if necessary. EOQ (economic order quantity) criteria must be changed to stop item from reappearing on report.	1	**Stock Requirement Report**
P.O. typed in five copies; number recorded on stock requirement report; estimated receiving date confirmed with supplier and entered on P.O.	2	**Purchase Order 5**
Purchase orders reviewed by supervisor; P.O. and stock requirement report initialed as evidence of approval.	3	
Stock requirement report filed according to date report.	4	**Stock Requirement Report**
Copies of purchase orders distributed: 1 to Supplier 2 to Buyer 3 to Warehouse/Receiving 4 to Accounts Payable 5 to Purchasing Files	5	**Purchase Order** 1, 2, 3, 4, 5
		Warehouse Receiving Dept. (Receiver)
Goods and packing slip received on receiving dock.	6	**Packing Slip** With goods
Receiving copy of P.O. pulled from file to serve as receiving memo; goods refused if no P.O.	7	**Purchase Order 3**

system to the next), there is an opportunity for error. These are often called control points because controls should be applied to ensure that errors do not occur and information and transactions remain intact.

Flowcharts (also called *process maps*) show the process flow visually, which highlights the control points and therefore helps internal auditors identify missing controls and assess whether existing controls are adequate. **Exhibit 12-4** shows an example of a simple flowchart.

The flowchart is an effective internal audit tool for two reasons. Most people can understand a process flow more quickly when it is shown visually than they can when reading process narratives. And the discipline built into the flowchart (highlighting the control points) helps the internal auditor evaluate the design of controls.

The flowchart, though, is a limited audit tool. It only applies where there is a linear process flow and there are many risks that are not part of a linear process (for example, unethical behavior or loss of business to competitors). Internal audit functions that use flowcharting as their primary audit tool are likely to miss some of the most critical business risks.

Flowcharts are best used as subsidiary to the risk and control matrix. That is, the internal auditors first perform a detailed risk assessment and document it in a risk and control matrix or equivalent format. Many, but not all, of the risks will be managed by controls within linear processing systems. In exhibit 12-2, the Controls (and Other Risk Management Techniques) column for those risks should contain a cross-reference to a flowchart as applicable.

Narrative

Narratives are free-form compositions that are useful for things that require an explanation too lengthy to fit within the confines of the disciplined tools like risk and control matrices and flowcharts. Narratives are usually written up on separate workpapers and cross-referenced to the related matrix or flowchart.

Control Concepts and Principles

Perhaps the most important thing for internal auditors to realize about controls is that they have no value in themselves. They are only tools to reduce risk. Their value lies in the amount of risk reduction they achieve, and a lack of controls is acceptable if the risk is reduced to an acceptable level in some other way.

Some of the most commonly used concepts of control are:

- **Preventive or detective.** A preventive control stops an undesirable event from occurring. Some examples of preventive controls are required authorizations, segregation of duties, and password protection. A detective control uncovers the event after the fact so corrective action

can be taken. Some examples of detective controls are reconciliations and exception reports. Preventive controls are generally preferred to detective controls because it is better to do the thing right in the first place than to detect and correct errors. At the same time, detective controls may be required if the preventive controls in place can fail or are cost prohibitive.

- **Directive.** A directive control causes or encourages a desirable event to occur. Examples are guidelines, training programs, and incentive compensation plans. Also included in this category are soft controls like tone at the top.
- **Compensating.** A compensating control reduces the risk to an acceptable level when a preferred control fails or is not cost-effective. For example, close supervisory review can compensate when a staff is too small to adequately segregate duties.
- **Manual or automated.** Manual controls require a human being to act, and there is always the risk of human error or intentional nonperformance. Automated controls are built into the computer system and are therefore more reliable. For example, an automated reconciliation is more reliable than a manual reconciliation.
- **Entity-level, activity-level, or transaction-level.** Entity-level controls operate for the organization as a whole. Examples are human resource policies, entity-level reconciliations for financial reporting, and the soft controls like tone at the top that influence the control environment. Activity-level controls operate for the entire activity (business area, process, or program) that is the subject of an assurance engagement. Examples include review of cost center reports, inventory counts, and the soft controls that influence the mini-control environment within the activity, which may or may not be consistent with that of the organization as a whole. Transaction-level controls operate within a transaction-processing system. Examples are authorizations, segregation of duties, and exception reports.

IT controls share many of the same attributes as those discussed above, but they have unique features as well. These are discussed in chapter 15, "Specialty Skill Areas."

Testing Determinations

When to test and when not to test? Many factors unique to each audit project enter into this decision, but some general principles apply in most cases.

As a general rule, key or primary controls (those controls that must operate effectively to reduce a significant risk to an acceptable level) must be tested. If a key control is not operating effectively, there can be no assurance that the related objective will be achieved. Secondary controls (controls that help the process run smoothly but are not essential) do not usually have to be tested. However, there might be reasons to test a particular secondary control. For example, process efficiency might suffer significantly if a secondary control is not performed consistently and correctly. The loss of efficiency might pose enough of a risk to other important objectives that justify the use of audit resources to test the control.

If internal auditors identify a significant design weakness, there is usually no need to test the control. Even if it is operating as intended, the control will not reduce the risk to an acceptable level. There are, however, two situations in which further audit work is required:

- A manager might ask, or the internal auditors might wonder, if there have been any losses. In this case, the control itself will not be tested, but the internal auditors should do further work to determine whether losses have occurred and, if so, the extent of the losses.
- A manager might not agree that there is a design weakness or might say that the risk is trivial. In these cases, the internal auditors should do more work to quantify, or at least clarify, the risk. How to do this will vary from case to case.

For risk management techniques other than controls (those that fit into the risk responses of avoid, accept, pursue, share, or reduce in ways other than controls), the decision on whether to test will be similar. For example, earlier in the chapter an example was discussed regarding sharing the risk in a portfolio of securities by hedging against interest rate changes. If the internal auditors conclude and management agrees that either the analytical technique used to select hedge instruments or the monitoring of their performance is flawed, the internal auditors have a reportable finding and might not need to test. However, if the potential losses are substantial, the internal auditors might also need to do their own calculations to determine whether the hedge instruments are performing as expected and whether there are any unrecorded gains or losses. If the analysis and monitoring techniques are well designed, internal auditors might test a sample to see if the analytical technique is applied correctly and consistently and the monitoring performed as designed.

Types of Audit Evidence

There are four types of audit evidence:

- **Testimonial evidence** is what people tell the internal auditor. It is considered the weakest form of evidence, but some testimonial evidence is stronger than others. For example, the person who performs a task can provide stronger evidence of how the task is actually performed than a supervisor who may only know how it *should* be performed. On the other hand, the person who performs the task has incentive to tell the internal auditor the task is performed correctly even if that is not always the case. For this reason, auditors in information-gathering interviews should usually ask open-ended questions that do not include or imply the control the auditor wants to validate (for example, "How are these transactions processed?" not "How are these transactions authorized?" or "How are duties segregated in processing these transactions?").

  As a general rule, people who are independent of the activities being reviewed—if they are knowledgeable—-provide more reliable testimonial evidence than do people involved in the activities. Also, testimonial evidence from two or more people is stronger than testimonial evidence from one person.

- **Documentary evidence** is contained in documents. This is the second strongest type of evidence, but it may not be as strong as it appears. It is important to consider the source of the document. A memo written by a person is not much stronger than testimonial evidence. It proves the person said what the memo says, but it does not prove that it is true. Records produced by IT systems are the most common form of evidence used by internal auditors. They are as reliable as the organization and IT system that produced them, but they may be fraudulent, the IT system may have programming errors, erroneous data may have been input into the system, or the data in the system could have been changed.

  Documents from sources external to the organization are much stronger evidence than internal documents. For example, confirmations of accounts receivable owed to the organization and returned directly to the internal auditors are almost as strong as physical evidence. Documents from external sources sent to the organization are usually stronger than internal documents but not as strong as those sent directly to the internal auditors. For example, an employee of an organization committing a fraud might create an invoice that appears to come from a nonexistent vendor.

- **Physical evidence** is evidence internal auditors see with their own eyes. For example, they may perform an inventory count, pick a sample of securities and find them in a vault, or see that toxic chemicals are leaking from a barrel. This is considered the strongest form of evidence, but it is important for internal auditors to consider what the evidence proves and what it does not prove. For example, if an inventory of vehicles is kept in a lot after work hours, the auditor can count the vehicles. This proves whether the number of vehicles in the lot matches the inventory records, but it does not prove that they are the same vehicles. Someone might have stolen a new vehicle and left their old vehicle in the lot. To prove they are the same vehicles, the auditor would need to inspect the vehicle identification number on each vehicle and match it to the inventory records.

  When internal auditors find physical evidence of a deficiency, they know it exists, but they may have to prove it to others. Their statement that it exists is testimonial evidence—the weakest type—to others. Having two or more internal auditors see the same thing strengthens the evidence. Having management of the audited area see it strengthens it further. If the deficiency is something like an unsafe condition, a photograph is very strong evidence.

- **Analytical evidence** is obtained by comparing, computing, or otherwise analyzing data. For example, internal auditors can review budget-to-actual comparisons or compute financial ratios. More examples are discussed in the section on analytical review. Analytical evidence—assuming the data analyzed is accurate—proves that certain relationships among data exist. This fact usually has to be investigated further to determine why the relationships exist.

Standards of Audit Information

IIA Standard 2310 - Identifying Information and its interpretation state that audit information (which includes audit evidence) must have the following four qualities to meet the engagement's objectives:

- **Sufficient** information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor.
- **Reliable** information is the best attainable information through the use of appropriate engagement techniques.
- **Relevant** information supports engagement issues and recommendations and is consistent with the objectives for the engagement.
- **Useful** information helps the organization meet its goals.

In terms of audit evidence, the relative strength of the types of audit evidence in the preceding section is predicated primarily on its sufficiency and reliability—is there enough reliable evidence to prove the point? But there is also the question of what point is being proven—is the evidence relevant? An example of evidence that is not relevant is when an internal auditor performs an inventory count, traces the information through the supporting ledgers to the financial statements, and concludes that controls over inventory are adequate and effective. The evidence supports a conclusion that inventory is fairly stated, but in this example, the internal auditor did not review inventory controls and cannot make any statement about them.

Manual Testing Methods

Internal auditors use a variety of testing methods to find the evidence that leads to their conclusions on effectiveness. The decision on which method(s) to use depends on a number of factors, a few of which are:

- **The objective of the test.** For example, to prove the existence of a fixed asset, the best test is to physically examine the asset. To determine the operating effectiveness of a procedure, the internal auditor might test a sample of transactions and determine whether the procedure was followed in each case. To verify the accuracy of information in a report, the auditor might vouch the information to supporting documents.
- **The underlying risk.** A control mitigating a major risk merits more assurance and therefore requires methods that generate stronger audit evidence.
- **The resources required by the method.** Internal auditing must be cost-effective. Testing methods that generate stronger audit evidence often require more time and other resources. If the underlying risk does not justify the expenditure, less resource-intensive methods should be used.

Some of the testing methods frequently used by internal auditors follow:

- **Interviews** are the most commonly used technique for planning, evaluating the design of controls, and conducting root cause analyses. Because interviews only provide testimonial evidence, what internal auditors learn in interviews usually must be corroborated with stronger evidence before it can be used to support conclusions.

- **Surveys** are an efficient way of gathering testimonial evidence from a large or geographically dispersed sample of people.
- **Internal control questionnaires (ICQs)** are efficient tools for determining whether specified control procedures are in place. There are several ways to use an ICQ. Internal auditors can use it as an interview guide and record management's answers, send it during the planning stage of an engagement to be completed, or use it to record the test result of the procedures and their conclusions.
- **Observation** as an audit test means simply watching something being done. What internal auditors see with their own eyes is stronger evidence than what someone tells them. However, what the auditors see may not be the actual procedures. If the employees know that the auditors are watching, they may perform the expected procedures.
- **Inspection** means seeing things with the internal auditors' own eyes. When auditors inspect a physical asset and verify the ownership, they have the strongest evidence that the asset exists.
- **Confirmations** are sent to independent third parties asking them to verify the accuracy of information. Positive confirmations ask for a response regarding whether the information is accurate or not. They provide stronger evidence than negative confirmations, which ask for a response only if the information is not accurate. Blank confirmations, which ask the third party to fill in a blank line with the information requested and return them to the internal auditors, provide the strongest evidence.
- **Tracing** is taking information from one document, record, or asset *forward* to compare to a document or record that was prepared later.
- **Vouching** is taking information from one document or record *backward* to compare to an asset, document, or record that was prepared earlier.
- **Reperformance** means independently performing a control to see if the result matches the audited business area's.
- **Analytical procedures** involve comparing information received from the business with expectations for that information obtained from an independent source, identifying variances, and investigating the cause of significant variances. The analytical procedures available to the internal auditor, especially one who uses audit software, are almost limitless. A few of the more commonly used analytical procedures are:
  - **Comparing expected to actual results:** Using budgets, forecasts, economic information, or similar sources. Large positive or negative variances should be investigated.
  - **Trend analysis:** Comparing information from one period with the same information from the prior period. Unexpected variances should be investigated.
  - **Comparing with independent causal or related factors:** For example, comparing salary expense to number of employees, or changes in interest expense to changes in daily outstanding debt.
  - **Reasonableness tests:** Comparing information to the internal auditor's general knowledge of the organization or industry, rather than to another specific piece of information.

- **Benchmarking:** Comparing performance information with similar information from another source. In *external* benchmarking, the source is another organization or the industry (for example, comparing delinquency rates with industry averages). In *internal* benchmarking, the source is other units of the organization (for example, comparing employee turnover in the audited area with turnover in the organization as a whole).
- **Ratio analysis:** Calculating financial or nonfinancial ratios.
- **Regression analysis:** A statistical technique used to establish the relationship of a dependent variable to one or more independent variables.

As this section indicates, there are a great variety of manual testing techniques available to internal auditors. Deciding which test(s) to perform depends on what is being tested and the amount of risk involved. When selecting and performing audit tests, and when drawing conclusions, internal auditors must always ask themselves what the test proves and what it does not prove.

Sampling

When testing transactions, internal auditors need to decide how many transactions to test and how to select the transactions. Internal auditors could test just one transaction. Doing so would only prove that this one transaction was correct. No conclusion could be drawn about the population as a whole. At the other extreme, auditors could test every transaction. With a small population of high-risk transactions, this might be appropriate, but this is rarely the case. As a general rule, internal auditors want to determine whether controls are consistently operating as designed, with an acceptable level of exceptions. For this purpose, a sample of transactions is sufficient.

Sampling is a complex subject, most of which is beyond the scope of this book. This chapter presents the basics—what every internal auditor needs to know and is likely to use.

The basic question to answer in selecting a sampling method and sample size is how representative of the entire population the sample needs to be. Some of the basic sampling methods and techniques follow:

- **Statistical sampling** allows the auditor to define with precision how representative the sample will be. Internal auditors first define a desired confidence level. For example, a 95 percent confidence level means that there will be no more than a 5 percent probability that the conclusion will not represent the entire population (this probability is also called *sampling risk*). The auditor also defines an expected error rate and an acceptable error rate in the population. The auditor then enters these variables into statistical sampling tables or software, which calculates the sample size needed. After selecting the sample randomly and testing the sample, the auditor can state the conclusion in terms of being 95 percent confident that the error rate in the population, for example, is less than or equal to 6.3 percent.
- **A random sample** means that every item in the population has an equal chance of being selected. Two common methods of selecting a random sample are using a random number

generator (if the items in the population are numbered, like bank checks) and using systematic selection (picking every n^{th} item, starting with an arbitrary number). Statistical samples must be selected randomly. Nonstatistical samples can be selected randomly or judgmentally.

- **A judgmental sample** is selected using the internal auditor's judgment in some way. Doing this biases the results, so the results will be less representative of the population. However, there are often good reasons to select samples judgmentally, as discussed below.

Statistical sampling produces more persuasive audit evidence, but it is also more time-consuming and, therefore, costly. Most internal audit functions do not routinely use statistical sampling techniques because they are not needed to meet their audit objectives. In most engagements, the goal of testing is to determine whether controls are consistently operating as designed and identify opportunities for improvement where they exist. For this purpose, a judgmental sample of 20 to 30 items is usually sufficient. If there are no exceptions, it is reasonable to conclude that controls are consistently operating as designed. If there are exceptions, the auditor investigates the cause. If the cause is a control weakness, the testing has served its purpose. If the cause is not a weakness in controls and the risk created by the exceptions is minor, the exceptions are considered isolated and not pursued further.

One common judgmental sampling approach is to include some large or unusual items in the sample. Selecting large items allows the internal auditor to cover more risk. Selecting unusual items makes it more likely that the auditor will find errors. If no more than an acceptable number of errors is found, the auditor's positive conclusion about the control is actually stronger than it would be with a nonstatistical random sample. If an unacceptable number of errors is found, the auditor cannot conclude that the error rate in the population is unacceptable. Instead, the auditor investigates why these errors occurred. They might be symptoms of an underlying control weakness.

Another common judgmental sampling approach is to stratify the sample in certain ways to make it more representative. For example, if a purchasing department has 10 buyers, the internal auditors might select two or three purchases made by each buyer. If testing covers a one-year period, the auditors might select the same number of items from each month. This would be appropriate for substantive financial audit work. Alternatively, they might select more items from recent months because they are more concerned with how controls are operating in the present and will likely operate in the future than how they operated in the past. This would be more appropriate for operational audit work.

Many factors are involved in determining the best nonstatistical sampling technique, and it is more an art than a science. However, once a sample is selected, internal auditors must be sure they do not draw false conclusions by treating the results of their testing as more representative than they really are. And when they find errors or exceptions, they must investigate the cause.

Computer-Assisted Audit Techniques (CAATs)

In recent years, the demands on internal auditors have been increasing. Systems are becoming more complex. Internal auditors are expected not only to understand the complexity of these systems but also to become more efficient at accomplishing the tasks assigned to them. The computer-assisted

audit technique or tool (CAAT) is an automated audit technique that can help auditors automate some of their work so they can test large populations of data efficiently. Generalized audit software (GAS) is one of the more common CAATs. ACL, IDEA, Easytrieve, and SAS are some examples of GAS products.

CAATs are being deployed by internal auditors in many situations, including computerized anti-fraud audit procedures, imbedded internal controls within IT systems, and those engagements where a large quantity of data needs to be analyzed. CAATs can improve the quality of engagements by analyzing the entire population of data as opposed to a sample of data. By using CAATs, auditors can automate routine audit tasks, freeing up time to think more analytically.

Data analysis using CAATs creates the option of continuous auditing, changing the audit paradigm by allowing ongoing testing of 100 percent of transactions compared to the periodic reviews of a sample of transactions. Continuous auditing is a method of testing controls more frequently. The recent advances in IT and data analytics are the main reason that continuous auditing has become a reality. Internal auditors must consider continuous auditing techniques as an integral part of their entire audit plan.

Continuous monitoring, on the other hand, involves automated processes implemented by management to ensure that policies and business processes are operating effectively. Many of the techniques deployed by management for continuous monitoring are similar to the ones deployed by IT or data analytics auditors for continuous auditing. Here is another opportunity to share audit techniques and tools with management. Some internal audit functions even develop and implement the data analytics techniques and tools within its function and transfer them to the first or second line functions to operate. These initiatives help the organization to improve the effectiveness and efficiency of its risk management and control practices.

By deploying an integrated approach of continuous monitoring and auditing and sharing these practices with management, organizations can significantly reduce the instances of error, risk, and fraud. The return on investment of deploying an integrated approach shows rapid positive results.

Documentation of Audit Workpapers

Workpapers document all aspects of the engagement, from planning to communicating results. Workpaper format, content, and organization will vary depending on the nature of the engagement. CAEs should establish workpaper policies and implement a workpaper system for the various types of engagements performed, with enough flexibility built into the policies to allow for adapting to each engagement's needs.

The Necessity for Workpaper Documentation

Internal auditors sometimes get frustrated with the amount of time they have to spend documenting their work. Thorough documentation is necessary, however, because:

- Internal audit work can be challenged. For example, a defensive manager might not want to believe that certain exceptions exist. Internal auditors' insisting that they saw the exceptions is not very persuasive. If the workpapers include copies of the documents with the exceptions, or have clear instructions on where to find the exceptions, the auditors can show them to the manager.
- While supervision should be exercised throughout the audit, workpaper review is a critical control for the internal audit function. Audit supervisors need to know what work was done and how it was done in enough detail to evaluate the quality of the work and give any necessary guidance to the auditors who did the work. Workpapers should be prepared promptly to enable supervisors to conduct timely review. Review is timely when internal auditors have sufficient time to provide satisfactory responses to the supervisor's questions and take any necessary corrective actions without delaying the engagement.
- If the engagement is performed again in future years, the workpapers can be a road map that helps the future auditors perform the engagement effectively and efficiently.
- External parties, such as the external auditors and regulators, may need to review the workpapers to determine the basis for placing reliance on internal audit work.
- Regulators and external parties may need to review the workpapers to evaluate the quality and effectiveness of internal audit as the organization's third line of defense.
- In cases of fraud and other investigations, internal or external parties may need to review workpapers to understand the status of controls over time, the root causes, and other contributing factors to these incidents.

Guidelines for Preparing Workpapers

In general, internal auditors should keep workpapers understandable, relevant, economical, reasonably complete, simple, and logically arranged. More specifically:

Keep workpapers understandable. Anyone reading the workpapers should be able to determine what the internal auditors set out to do, what they did, what they found, what they concluded, and what they decided not to do.

Keep workpapers relevant. Workpapers should be restricted to matters that are relevant and material; they should be directly related to the audit objectives. Records that may be interesting but not directly relevant should be eliminated. Having a clear statement of purpose on each workpaper helps assure relevance.

Keep workpapers economical. Internal auditors should not try to answer every conceivable question that can be raised. This is particularly true when tests indicate satisfactory conditions.

Internal auditors should cover as many tests as feasible on one workpaper, using the same sample for a number of tests. Where possible, internal auditors should incorporate copies of business area records in the workpapers and use tick marks to indicate the audit steps completed.

Keep workpapers reasonably complete. Workpapers should leave nothing incomplete. No questions asked should go unanswered. If a space has been left for a cross-reference, it should be completed. If a question is raised, it should be answered—or the reason for not answering it should be provided.

Keep the writing simple. Workpapers should be readily understandable to an uninitiated reviewer. Jargon and technical terms should be avoided or explained. The final test of a set of good workpapers is whether another internal auditor, who was not involved with the assignment, could step into the audit engagement midstream, understand what was done, and proceed with the engagement without wasted effort.

Use a logical workpaper arrangement. Workpapers should be arranged in the same sequence as the audit program to facilitate cross-referencing. Each distinct subject should be included in a separate segment of the workpapers.

For each segment of the engagement, the internal auditor should provide general information, such as the objective of the operation being audited, and background information, like the organization structure and performance data. For each audit segment, the auditor should spell out the detailed purposes of the segment, including and, where necessary, expanding on the related matters set out in the audit work program.

Also, internal auditors should explain the scope of work performed on each workpaper: what was covered and what was not covered. If the work includes testing a sample, the scope should include the sample size and selection methods used. The source of all business area information used should be clearly identified.

Following the statements of purpose and scope, internal auditors record their tests and issues. These should be restricted to the facts—the good as well as the bad. After the facts are recorded, the auditors will draw their conclusions from what they found. These conclusions, in the aggregate, will support the auditors' opinion on the audit engagement overall. Deficiency findings are usually summarized briefly in the workpaper's conclusion section and cross-referenced to an audit finding workpaper (discussed below) where they are fully developed.

Each workpaper should generally contain:

- **A descriptive heading.** The heading should identify the activity audited, indicate the nature of the data contained in the workpaper, and show the date or period of the audit.
- **A reference to the audit engagement.** This identifies the reference number of the engagement.
- **Tick marks and other symbols.** Tick marks and other symbols should be small and neatly placed, useful but unobtrusive, and explained in a tick-mark legend in the workpaper.

- **The date of preparation and signature or initials of the auditor and reviewer.** The date should indicate when the workpaper was completed. The signature or initials (manual or electronic) should appear on each workpaper.
- **The reference number of the workpapers.** Workpapers should be referenced as they are prepared and kept in logical groupings.
- **Sources of data.** Sources of the information in the workpaper should be clearly identified.

An independent reviewer should be able to trace information from one workpaper to another easily. To that end, workpapers should be cross-referenced to other workpapers and to the audit program. Effective cross-referencing often reduces the need to duplicate data.

Workpaper files should contain a table of contents. There should also be a system that identifies all the files for audit engagements performed in a given year or other period. These files collectively hold the assessment and conclusion of internal controls tested across the organization for a specific period. Ultimately, this is the information supporting the CAE's opinion on the overall system of internal control.

Types of Workpapers

A typical engagement has many different types of workpapers that vary by engagement. The following list includes some of the more commonly used types of workpapers:

- Planning documents and audit programs
- Narratives of interviews and meetings. These may include emails or memos confirming what was discussed with business area management.
- Organization charts, policy and procedure statements, and job descriptions
- Risk and control matrices, flowcharts, procedural narratives, checklists, control questionnaires, or other descriptions of processes and controls
- Copies of important contracts and agreements
- Copies of source documents, such as purchase orders and invoices
- Copies of records received from the business, such as trial balances and exception reports
- Letters of confirmation and representation
- Photographs, diagrams, and other graphic displays
- Tests and analyses of transactions
- Results of analytical review procedures
- Summaries of conclusions at the end of each workpaper segment
- Audit finding workpapers
- Audit reports and management replies
- Relevant audit correspondence
- Job administration documents, such as time budgets and resource allocation worksheets
- Permanent or carry-forward files that contain information of continuing importance

Electronic Workpapers

Most internal audit functions create and retain their workpapers in electronic form, scanning copies of hard-copy documents for inclusion when necessary. Some do this with common word processing, spreadsheet, and database software; others use software packages designed specifically for internal auditing. When implementing a workpaper software package, the internal audit function should comply with IT policies and procedures. Some internal audit functions use paper and pencil for some or all of their workpapers. The principles, guidelines, and examples in this chapter apply to workpapers prepared in any of these formats.

Regardless of the format used, every workpaper must be reviewed by the CAE or designee and retained for a period of time prescribed by the CAE. Workpapers should be classified and safeguarded in accordance with internal audit's and the organization's Information Classification Policy.

Workpapers related to litigations in process should be designated as "Litigation Hold" in accordance with instructions from the legal department. These workpapers should be retained; they cannot be destroyed until authorized by legal. Internal audit needs to maintain the software required to access and read the workpapers kept within the retention period.

The Value of Assessing Internal Control

Organizations rely on the internal audit function to independently assess how well the systems of internal control have been designed and are operating to mitigate risks threatening achievement of their objectives. When internal auditors take a measured approach like the one described in this chapter, they can confidently report to the board and management on the state of the organization's systems of internal control. This helps management calibrate their systems and enhance internal control where gaps were identified and discontinue internal control activities where areas are found to be over controlled. Ultimately, senior management wants to be able to achieve their strategic objectives in the most effective and efficient way possible. The internal audit function can achieve its purpose, embodied in the Definition of Internal Auditing, by delivering assurance that management is on the right track and providing recommendations to help improve the effectiveness of risk management, control, and governance processes.