Internal Audit's Guide to Planning, Managing and Addressing Risks

How to Achieve Efficiency and Effectiveness to Improve Audit Quality
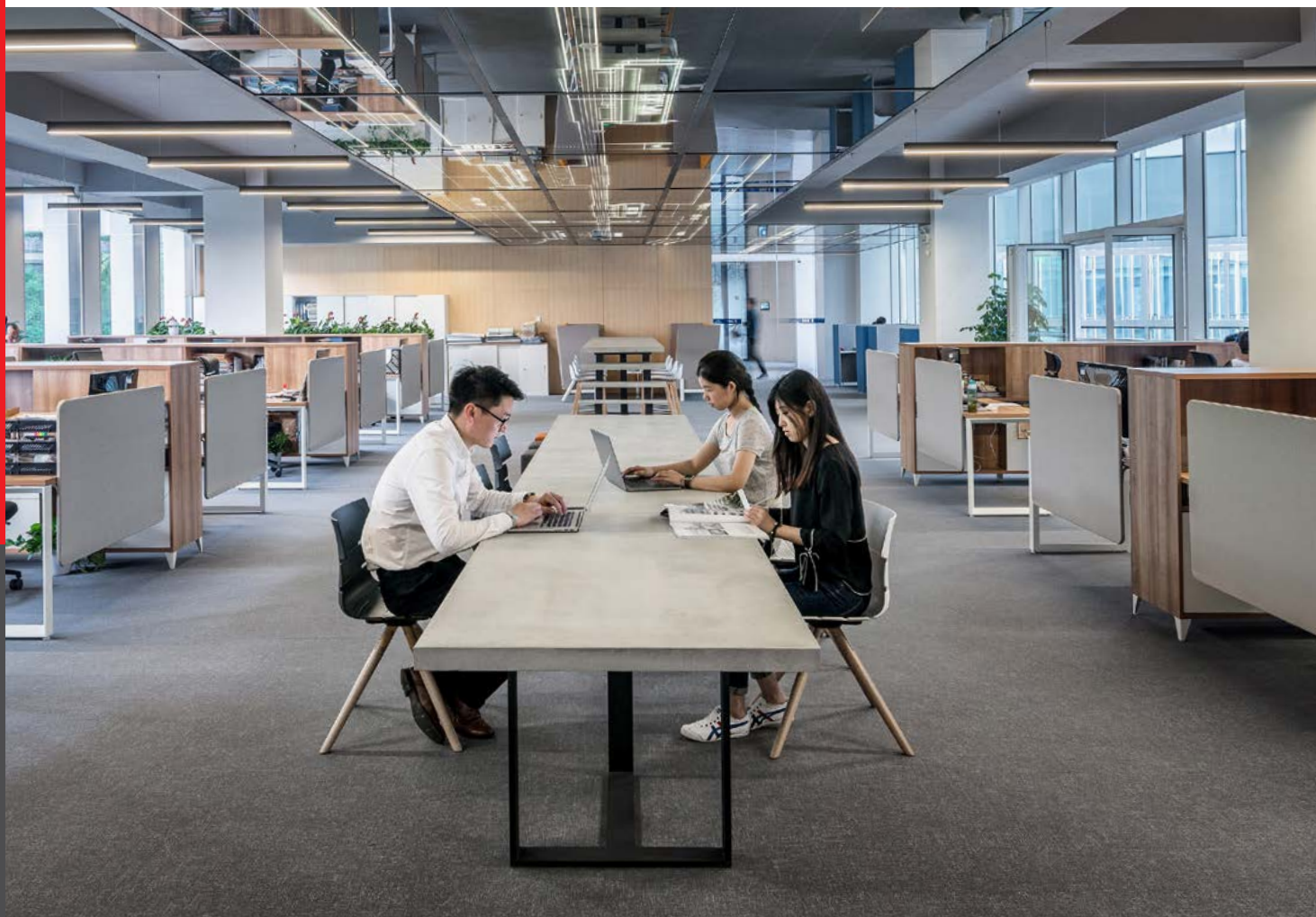
CONTENTS

About MIS Training Institute

MIS Training Institute (MISTI) is the international leader in internal audit, IT audit, and information security training and conferences with offices in Boston, New York, and London. MISTI's expertise draws on experience gained in training more than 200,000 delegates across five continents. Helping internal audit and information security professionals stay at the top of their game has always been at the core of MISTI's mission. To that end, MISTI has developed and focused its vast variety of training courses, events, newsletters, and other informational products on the wide-ranging needs of internal and IT auditors and information security practitioners. MISTI's unparalleled course curriculum covers the most up-to-the-minute topics, provides proven internal audit and security practices, and delivers the information needed to be successful in today's organizations. **www.misti.com**

About Workiva

Workiva is a leading provider of enterprise cloud solutions for data collaboration, reporting, and compliance. More than 3,000 organizations worldwide, including companies of all sizes, government agencies, and educational institutions, trust our cloud platform to improve productivity, connect data, and gain confidence in their data-driven decisions. For more information about Workiva (NYSE:WK), please visit **www.workiva.com.**

Jose Tabuena, Author

Jose Tabuena provides audit and compliance services drawing on Big 4 firm experience and a variety of roles, including compliance auditor, risk manager, corporate counsel and chief compliance officer. He has held major compliance and audit management roles at Kaiser Permanente, Texas Health Resources, Orion Health and Concentra/Humana. He is certified as a fraud examiner in healthcare compliance, as well as an OCEG Fellow.

Author,
Internal Audit's Guide to
Planning, Managing, and
Addressing Risks

Introduction

As time passes and the modern-day enterprise evolves, so does the role of the internal auditor. What was once a function that was perceived as rule enforcers and compliance police is expanding into one that is a trusted advisor within the business. The last several years have introduced an enormous amount of change, but the proliferation of technology within the enterprise is accelerating every aspect; from operations to decision making.

The progressive steps organizations are taking as a result of the digital age present a bevy of benefits, but in turn, create a slew of challenges and risks. Subsequently, the internal audit function has been forced to adapt along the way, assuring key stakeholders in the business that risks have been identified, but above all, addressed and mitigated.

This eBook's focus covers the necessary areas to sharpen as it relates to conducting an audit that's both efficient and effective. Our first article provides a deep dive on internal audit risk assessments, defining what this dynamic and iterative process should look like. But most importantly, it offers tips that allow you to ramp up the means to achieve more dynamic audit planning.

While identifying and managing risks tied to the business fall on management, it's internal audit's responsibility to focus on closing the loop. That's why our second article focuses on the effective audit follow up, in addition to outlining the how and when tied to escalating risks.

Last, our sponsor Workiva ties the cyclical theme together by providing an in-depth look at the four-part approach for audit efficiency and effectiveness. Given the resource and time constraints that internal auditors face, this piece offers a breakdown of how you can leverage existing guidelines to improve your team's performance.

We hope you can take the actionable takeaways we've provided in this eBook and apply them immediately so you can enable positive change within your organization. Change is the one constant we should all expect, and the principles and practices outlined in this eBook are intended to help you adapt and continue to provide value in the business as an internal auditor.

> "While identifying and managing risks tied to the business fall on management, it's internal audit's responsibility to focus on closing the loop."

Planning to Do the Right Audits:
An Effective Internal Audit Risk Assessment

By Jose Tabuena

While the responsibility for identifying and managing risks belongs to management, a key role of internal audit is to provide assurance that those risks are being appropriately addressed and mitigated. For the traditional internal audit function, this has come to mean a yearly review of the various business processes and financial reports coupled with senior management discussions that result in the creation of the annual audit plan, which is then presented and approved by the audit committee.

The Institute of Internal Auditors (IIA) Professional Practices Framework in Performance Standard 2010.A1 states that the "Internal Audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually." Are you confident that your department understands the risks that are critical to the delivery of value and the achievement of corporate objectives? Every organization faces numerous risks that matter individually to managers with whom auditors interact, but are they risks that matter to the organization as a whole? The risks that truly matter are those that need to be addressed in the audit plan.

The basic elements of risk assessments are well-known: information gathering on key risks and the associated likelihood, impact, and controls, gap analysis and design of remediation or mitigation steps. Yet the challenge of regularly identifying and assessing risks on an ongoing basis is no small undertaking.

PRO TIP **Looking to ramp up the process to achieve more dynamic audit planning? Try increasing the frequency of the process and designing a rolling service of assessments and audit planning.**

A DYNAMIC AND ITERATIVE PROCESS

The COSO *Internal Control – Integrated Framework* (2013) provides that a "risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives." (emphasis added). To be effective, internal audit should be aware of and responsive to changes in known risks and additionally the emergence of new ones.

A purpose for the traditional (i.e., annual risk assessment) is to allow internal audit to develop a planning horizon which is understood by stakeholders and, in particular, executive management and the audit committee as a basis for the risks identified. In this process there can also be a push to finalize the internal audit "plan" so that budgets, schedules and staffing can be arranged.

With the emerging concept of "risk velocity"—measuring how fast a risk may affect an organization—is recognition that the typical risk assessment process is one that is not dynamic and iterative nor responsive to change in real time. Change does not occur on an annual basis. The move to a continuous and dynamic audit plan is significant for most internal audit departments.

Some departments are already moving on this path and have had to adjust from a static process focused on listening to management on a seasonal basis to monitoring business objectives and risks that are rapidly changing. Tony Redlinger, internal audit director with IHS Markit, observes the difficulties of the timely capture of risks as "asking the pertinent questions often without the broader knowledge of what the business is getting into, where the technology often advances much faster than the controls."

BEYOND THE TYPICAL INTERNAL AUDIT RISK ASSESSMENT

What approaches can internal audit functions can take to ramp up the process to achieve more dynamic audit planning? One technique is to increase the frequency of the process and design a rolling service of assessments and audit planning. If existing processes can be made more streamlined and efficient, the time trajectory can be intensified to occur more frequently. Potentially, a concerted effort can result in an audit plan being updated every six months instead of annually.

Since the risk identification process ideally is ongoing, management should be encouraged to implement a schedule to periodically review risks, while reserving the ability to accelerate reviews if a company objective changes, or risk factors increase. For example, if management is considering an acquisition in a new jurisdiction, it could require the re-evaluation of risk factors to determine how the decision could impact operations. Such processes can be formally linked into internal audit planning.

Of course, existing sources of risk information should be identified and integrated into internal audit planning. Other assessment processes including Enterprise Risk Management activities, department self-assessments and other function-specific reviews in high-impact areas depending on industry (e.g., environmental hazards, cybersecurity threats, etc.), should connect and feed into internal audit processes.

TECHNOLOGY TOOLS AND REALISM ABOUT SURVEYS

In the typical risk assessment, preparatory materials are provided and participants are asked a series of questions during sessions with audit staff. This process is expected to produce information to guide the allocation of resources and activities within internal audit so as to optimize the match between the company's greatest risks and the corresponding mitigation efforts.

The availability of sophisticated technology tools such as online surveys can seem to make it cheap and easy to gather voluminous data from a larger population, and to conduct statistical analysis of that data. Dr. Hernan Murdock, vice president of the audit division at MISTI, finds surveys and questionnaires to be a technique to collect information. "[Questionnaires] promote risk and control awareness, while encouraging transparency and accountability," he says.

Potentially, this means we can conduct a much larger assessment with the same resources. There is definitely a place for crowdsourcing risk as well as casting a wide net for particular fact patterns of concern, such as use of third-party sales intermediaries or collection of consumer personal data.

Still, more data is not always better data. The essence of a good risk assessment is not popular opinion, mechanically sliced and diced; it is informed opinion and expert judgment applied to the facts. Be careful with gathering far more data than can be followed up on or that can be analyzed meaningfully which can result in human-judgment bottlenecks in the process.

Ordinarily, risk assessments gather information from senior executives and managers, as well as a sample of senior operational personnel in the business units. To the extent that "risk owners" are not in these groups, they are usually sought out, and sometimes manager-level input is also requested. Front-line workers should be considered as well. It's usually those who are in the details on a daily basis that have the best perspectives on risks and low-hanging fruit when it comes to increasing operational efficiency.

How many people, and who, should participate depends on the risks being assessed, the required timeline (scheduling difficulties increase with the number of people required in a meeting), and the methods of inquiry. One-on-one interviews and focus groups can uncover valuable information, but may seem costly compared to surveys, particularly in a large organization. Surveys can reach more people faster, but may yield information of questionable quality. As a sample size grows, survey results will get closer to the true average opinions of the entire population from which the sample is drawn. But the important question is whether the average opinion of a broad employee population about risk actually gives better insights than we can get from a smaller but more carefully selected sample.

> **PRO TIP**
>
> More data is not always better data. Be careful with gathering far more data that can be followed up on or that can be analyzed meaningfully.

> "With surveys, experience suggests that the more questions you require people to answer the less effort and the more guesswork will go into the answers."

Especially with surveys, experience suggests that the more questions you require people to answer—particularly questions not intimately related to their jobs—the less effort and the more guesswork will go into the answers.

Customizing surveys by department, job function, or risk area can be costly. To deal with this dilemma, one precaution is to ensure that the survey is done in a way that allows the data to be sorted and analyzed according to business unit, department, location, etc. This way, filtering the results on the back end might produce much clearer and more consistent information. Further, include a question about the employee's familiarity with each risk area, or to offer some form of a "don't know" option, rather than forcing everyone to assign likelihood and impact values to every risk.

Interviews and focus groups seem to produce better quality information than written surveys, while surveys with a few open-ended questions, or that invite the respondents to explain their conclusions, are usually better than purely numerical ratings. Surveys can still be valuable, but should be viewed as a starting point for analysis. They tell you where to look closer. So be careful before committing a lot of resources to expanding and fine-tuning surveys, and requiring larger and larger groups to answer them.

For most organizations, an expert-driven process will yield the best results at the lowest cost. Subject-matter experts should triage the original inventory of risks to be assessed, vet the questions to be asked, independently review the existing control environment and make the final assessments—after considering everyone's input, but without according survey ratings any special scoring power.

THE RISK OF THE INTERNAL AUDIT RISK ASSESSMENT

Here we are not talking about the risk assessment that drives the audit plan. Rather, this is the risk that the internal audit function itself will not achieve its objectives as a result of the risk assessment. Should you perform this type of quality engagement as well? See IIA's Standards for the Professional Practice of Internal Auditing 2120—Risk Management: "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes."

The internal audit function in this regard should consider risks such as:

- The potential that the audit risk assessment is inaccurate or incomplete leading to an ineffective audit plan
- Audit staffing that is insufficient in terms of quality and capacity to deliver useful results on every engagement
- Changes in business and risk not promptly identified so that the audit plan can be updated
- Audit communications failing to provide information organizational stakeholders need, when they need it
- Governance roles not able to understand audit results and their implications for management of the organization

Anticipating risks with awareness of what could go wrong and then developing preventative responses are management responsibilities. Internal audit assesses whether management has the capability to identify, assess, and address new or changing risks. By performing the right audits identified from a dynamic and iterative process, internal audit is better positioned to provide the insight and advice that management needs.

Effective Audit Follow-Up and Escalating Risks (When Needed)

By Jose Tabuena

You've completed the latest risk assessment exercise and revised the current internal audit plan. Now, in addition to actually executing the audits, the internal audit function must establish and maintain a system to monitor the disposition of results communicated to management. And this includes escalating matters as appropriate when issues have not been adequately addressed.

The Institute of Internal Auditor's Standards for the Professional Practice of Internal Auditing 2500—Monitoring Progress, provides that internal auditors "should establish a follow-up process to ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action." At the conclusion of an audit, findings and proposed recommendations are discussed with management and subsequently management action plans are developed to explain how the agreed recommendations will be implemented.

Competing priorities, budget limitations and other factors may prevent managers from implementing agreed actions within the determined timeline or as previously designed to mitigate the risk. The purpose of follow-up is to ensure that management has implemented the action, and to confirm if identified issues are resolved. In practice, this can be a challenge.

Managers who do not implement agreed-upon actions from internal audit findings expose the organization to further risk. The mutual understanding needs to be clear on the following:

- How outstanding management actions will be tracked

- How resolution will be reported and validated

- What further follow-up action may be needed with high risk areas having more internal audit resource and focus as part of the process

TECHNOLOGY TOOLS

To facilitate the follow-up, generally an internal audit unit maintains a database on the status of outstanding audit comments. This database can track identifying information about each audit report and a close-out letter, along with a summary of each finding, the position responsible for taking corrective action, and the estimated completion date for the corrective action. Effective use of the database can track whether or not a finding has been corrected, what was done to fix the issue and the date the corrective action was completed.

> **"The purpose of follow up is to ensure that management has implemented the action, and to confirm if identified issues are resolved."**

Software applications designed by the organization or purchased from vendors can make follow-ups more efficient and effective. The process enables the ownership of actions to be assigned to managers and enables tracking of action through completion. Automated emails can notify and remind the responsible manager of tasks to be completed and to update the status in the system.

At National Grid, one of the 10 largest utilities in the U.S., the status of open actions is updated monthly and sent to the business unit and executive management, according to Director of Corporate Audit, Gretchen Sutcliffe. Timely and effective closure is an audit metric that is used by National Grid to monitor and manage expectations.

Reminders also prompt the internal auditor to contact the operational owner and other liaisons to monitor for progress. The process can take into account whether to accept management's representation or if further testing is required. All critical and significant actions should be reviewed by internal audit management and subject to being re-opened if there is insufficient evidence to support closure. It is the auditor's responsibility on a systematic basis to flag the time needed to re-test actions as needed.

Organizations may want to consider management performance measures also being tied directly to the timely and effective closure and mitigation of issues. This is often a sensitive topic as auditors don't have the ability to implement corrective action but need to find ways to influence issue resolution. While National Grid does not formally use closure of issues as a performance measure, "we do raise it as a discussion point at executive and audit committee meetings," Sutcliffe says.

Where risk management is embedded, the monitoring of action plans arising from assurance activities may be integrated into wider performance reporting. In this approach, management also takes responsibility for the related reporting, up to and including reporting to the audit committee. The reporting highlights whether recommendations/management actions are pending, in progress or complete in the form of a dashboard for senior management and committee use.

USE A HEAT MAP

The COSO guide, *Enterprise Risk Management—Integrating with Strategy and Performance*, promotes the use of risk matrices and heat maps to focus management on the most important threats, and to support the groundwork for responses to the risks. The map can help the company visualize how risks in one part of the organization can affect operations of another business unit within the organization. Additionally, it helps to clarify the company's relative response to risks. Since there are not unlimited resources to manage risks, the response must be in proportion to the risk. A heat map can help identify where resources are being used disproportionately to the threat implied in a given risk and perhaps justify delay the implementation of audit recommendations.

The actual mapping of risks is fairly easy once the data is gathered and consensus is achieved on scores. Audit teams have used different tools over the years such as Excel spreadsheets, Access databases and commercial software packages. More sophisticated programs and ERM software packages will also be able to produce risk heat maps from existing risk-assessment work without re-entering lots of data.

The feedback and consensus process starts again with the full map in view and adjustments are made to fix outliers, errors, and in consideration of the relevant risk scores. Use the feedback to make adjustments and then create the process for updating the map and ensuring that the information is not stale. Is review of risk data an annual process to coincide with the risk assessment to be completed as part of the audit planning stage? Should it be updated on a quarterly, monthly or more frequent basis? At each iteration the map can also be refined, and more complexity can be added as those in the organization become more familiar and comfortable with using it.

You can also incorporate risk ratings that are generated from the risk assessment into regular monitoring reports. The status of mitigation efforts can be tracked and the impact on the risk rating reported as part of regular audit updates to senior management and the board. This approach can serve to build the risk assessment process into operations as monitoring of the risk level will be dependent on business people reviewing their own operations. Once the map is revised, feedback can be obtained from senior leadership and the board.

> "The actual mapping of risks is fairly easy once the data is gathered and consensus is achieved on scores."

ESCALATION

Finally, there may be times when an issue needs to be further escalated, including to the board. A number of highly publicized incidents have shown the impact for failing to alert the governing body of a significant issue, and to allow for appropriate oversight. Risk functions at Wells Fargo, Volkswagen and Yahoo were roundly criticized for knowledge of warnings of major risks (from internal investigations, calls to the hotline, audits, etc.), but failing to escalate to ensure they were addressed.

Significant matters involving senior management should be reported directly to those charged with governance—typically the audit committee or full board of directors. This includes major risks that have continuing control implications. Conversely, the auditor should consider whether the absence of controls itself is a matter to be reported at the governance level.

The reporting of a significant matter other than to senior management and those charged with governance is ordinarily not part of the internal auditor's responsibilities and may be precluded by legal or ethical obligations of confidentiality. Be aware that AU 240 states there may be a duty to disclose information to outside parties in certain circumstances, such as to comply with legal and regulatory requirements (e.g., SEC rules).

To keep the board appropriately informed, regular board reporting is indispensable. But raising concerns in-between scheduled meetings before issues spiral out of control is also critical and often difficult. This is especially true today with increasing regulatory scrutiny and the rapid spread of information to the public. Failing to promptly communicate a significant issue that later has serious consequences may prove to be career limiting.

Determining the right information and the right time to escalate can help avoid major damage to the company. The best way to do this is to set up rules for escalation ahead of time and build consensus with the board and senior executives.

SETTING ESCALATION THRESHOLDS

In certain situations, it will be obvious that an issue should be escalated to the board. But for other matters, it may not be so clear-cut. Working with legal, compliance and risk management functions, internal audit can help build a framework to help determine whether an issue rises to the level to report to the board.

The framework can be a 2 x 2 matrix starting with the three basic impacts to assess on one axis:

- **Monetary:** What will be the total cost to the organization (percentage of annual revenue)?

- **Operational:** How will the ability to operate be affected?

- **Reputational:** How will the reputation of the organization change amongst customers and the public?

Then set threshold ranges on the next axis to identify the seriousness of the risk with respect to the three types of impact. The level of the range should intensify as you take into consideration the organization's risk appetite and the degree of impact.

Each threshold should be assigned actionable guidelines. For instance, at a level 2 no reporting is needed but the issue requires monitoring. At level 3 there is no immediate action, but the matter is to be raised at the next board meeting. When level 4 is reached, you notify board members you have a working relationship with (audit committee) and ask them to decide if the rest of the board should be notified. At the highest level, you may need to encourage the board to hold an urgent meeting.

Beyond Quality: The Four-Part Approach for Audit Efficiency and Effectiveness

By Ernest Anunciacion

The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing, colloquially known as the "Standards," is a set of core principles and a "framework for performing and promoting internal auditing." As they function as guide rails for the practice, not mandated tactics, the Standards offer best practices on how an auditor should conduct his or her work.

In many professions, the concept of quality is vague and frequently differs from person to person or team to team. However, the IIA and the Standards are articulate about what constitutes quality for the internal audit function, going so far as to establish a Quality Assessment Manual.

Accordingly, any discussion of quality in internal audit—and, subsequently, effectiveness and efficiency—must first begin with a clear understanding of the IIA's existing interpretation of quality, as well as an understanding of the actions that should be taken to promote it.

This paper will detail how internal audit leaders can improve the efficiency and effectiveness of their teams, despite time and resource constraints, using existing guidelines for improving audit quality.

THE IIA AND QUALITY ASSURANCE

As the introduction to the Standards explains, the practice of internal auditing is conducted in diverse legal and cultural environments, spanning organizations "that vary in purpose, size, complexity and structure." While these differences influence the internal audit practice in each environment, conformance with the Standards helps assure the fundamental responsibilities of the role are being met.

Chief audit executives need assurance that their internal audit activity is performing to expectations and that staff members are performing quality work. The only way to meet these expectations is through a comprehensive quality assurance program, which must include ongoing and periodic internal assessments. The Standards agree: section 1300 states that the chief audit executive "must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity."

Additionally, these assessments, according to the Quality Assessment Manual, should not be an afterthought nor an element to be tacked on at the end of the year. Rather, they should be an ideology of constant, iterative growth:

> *"Quality should be built into, not onto, the way the activity conducts its business—through its internal audit methodology, policies and procedures, and human resource practices. Building quality into a process is essential to validate and continuously improve the internal audit activity, demonstrating value as defined by stakeholders."*

With this core tenet in mind—that quality must be approached throughout the process, not just acknowledged at the end—the IIA suggests the following four-part approach to monitoring and improving audit quality.

FOUR STEPS TO AUDIT IMPROVEMENT

1

PLAN ahead by establishing specific objectives, goals or deliverables

2

DO the necessary processes, along with the data collection required for analysis and follow-up in later steps

3

CHECK the actual results, compare them to the expected outcomes, indicate the differences and suggest areas of improvement

4

ACT upon the results provided in the previous step

GOING FURTHER THAN QUALITY

The four steps above give a high-level perspective on the creation of a quality assurance and improvement program for the internal audit function of an organization. With such a set of standards, quality is effectively a baseline expectation.

As a former practitioner for some of the largest companies in the country, I have learned that good work is not enough. Organizations must go further than quality. Improving efficiency and effectiveness throughout the methodology can streamline processes and save money, time and resources.

What, precisely, do "efficiency" and "effectiveness" mean in the context of quality? Loosely defined, effectiveness is the results that come from work, while efficiency is the time and resources that are required to achieve those results. In essence, effectiveness is about doing the correct things, while efficiency is about doing things correctly.

> "High-quality work can be done in the absence of effectiveness and efficiency, but it is ultimately not as beneficial to the company..."

High-quality work can be done in the absence of effectiveness and efficiency, but it is ultimately not as beneficial to the company if it fails to consider the resources used or if the right work is being conducted.

I recall a time when my team was scheduled to conduct a routine travel and expense audit. The testing procedures were fairly standard—however, the company had recently switched expense systems, and we failed to update the appropriate procedures.

All of my staff were allocated to other projects, and the only available team member was a new hire who came from the company's operations with no auditing background. Given the urgency to complete the engagement before the next audit committee meeting, I ended up postponing one of my audits to assist the new associate.

While we were able to complete the audit on time and identify transactions inconsistent with our policies, what should have been a 40-hour engagement required more time for me to coach the new associate. I failed to forecast the schedule appropriately to ensure that the best resources possible were available at that time. Also, I failed to ensure that the testing steps were updated accurately to reflect the new travel and expense system.

In this example, efficiency was sacrificed for quality and effectiveness. While some circumstances are unavoidable, proper planning can afford internal auditors the ability to improve and optimize their work.

To evaluate and find opportunities to improve your team's effectiveness and efficiency, use the aforementioned four-part approach—plan, do, check and act—and take your internal audit processes further than quality.

STEP 1: PLAN FOR ORGANIZATIONAL GROWTH

While the concept of quality is uniform for internal auditors of different varieties and capacities, effectiveness and efficiency can vary from organization to organization. Accordingly, clear definitions for these terms—the expectations for your team—must be established and adopted to plan for growth.

Use these questions as guidance when defining exactly what effectiveness and efficiency mean for you and your team:

- Are we equipped with the up-to-date tools needed to conduct the best work possible?
- Do we have the right resources and skill sets required to deliver our audit plan?
- Are we contributing to organizational improvement? If so, can others see this?
- Have we obtained any validation of our team's quality, such as notification from managers or executives?
- Is feedback effectively distributed to team members, so they know what areas to improve?
- What quantifiable metrics can we associate with these definitions?

While you and your team's definitions of effectiveness and efficiency are crucial, it is also important to gain the approval of key stakeholders involved in internal audit. A major reason that process improvement initiatives fail, according to one Harvard Business Review article is that the people whose work will be directly impacted are often left out of the process.

Accordingly, feedback from stakeholders at the helm of the financial success of your company should also be incorporated. Here are a few stakeholders who should weigh in on your definitions of effectiveness and efficiency:

- Internal stakeholders: Board of directors, audit committee, executives, senior management and department leads

- External stakeholders: Regulators, standard-setters, vendors, customers and external audit teams

STEP 2: DO THE WORK NEEDED TO SET EXPECTATIONS

The second step of this process continues to articulate the definitions of effectiveness and efficiency, and sets expectations for your team.

By this stage, you should have an internal definition of effectiveness and efficiency, and you have tempered that definition in the context of what key internal and external stakeholders need. To better set your organization up for success, make these definitions more actionable and specific through the assignation of qualitative and quantitative metrics.

As described in a Forbes article, Forrester reports 74 percent of firms say they want to be "data-driven," but only 29 percent are actually successful at connecting analytics to action. Actionable insights appear to be the missing link for companies that want to drive business outcomes from their data.

Make these definitions more actionable and specific for your team by assigning qualitative and quantitative metrics for each. To collect qualitative and quantitative metrics, try the following tactics:

- Look back at past performance data to determine quantitative metrics:
  - → How many audits were scheduled?
  - → How many were completed?
  - → How was staff utilized?
  - → What were the budgeted hours as compared to the actual hours?

- Go on a listening tour of departments impacted by your work to determine qualitative metrics:
  - → What do clients think of your team's performance?
  - → What do other internal stakeholders think of your team's performance?
  - → Do they consider you and your team leaders in their role or order-takers?
  - → Would they want to engage in future projects with your team?

One of the things I implemented in the past was a balanced scorecard—a view of metrics and key performance indicators detailing areas of strength and areas for improvement. As part of the audit committee presentations, we presented to the audit committee both the quantitative and qualitative metrics that comprised our key performance indicators. In addition to items such as budget, time, and expenses, we also included metrics that highlighted staff utilization, CPE tracking for active certifications, and net promoter scores from our internal stakeholders. My goal with the balanced scorecard was to be open and honest about our team's performance and back those statements with data-driven results.

With these actionable definitions in hand, the expectations for your team should be crystal clear. It is ultimately up to chief audit executives to hold their teams accountable for efficient and effective—along with quality—work.

STEP 3: CHECK PROGRESS AGAINST SET EXPECTATIONS

To check the quality, effectiveness, and efficiency of your team's work, internal audit leaders should look at individual performance on an ongoing basis—not just an annual one. After all, it is easier and less problematic for leaders to reevaluate individual performance in small increments before it becomes a major issue.

In organizations of all sizes, a traditional once-per-year approach to employee reviews is fading away in favor of more ongoing ones. As a Washington Post article describes, today's employees have come to expect instant feedback in many other areas of their lives, and performance reviews should be the same. Besides, the article states, one report found that two-thirds of employees who receive the highest scores in a typical performance management system are not actually the organization's highest performers.

Chief audit executives should encourage the completion of self-appraisals. A Harvard Business Review article explains that an effective self-appraisal should focus on what you have accomplished and talk about weaknesses carefully, using language with an emphasis on growth and improvement,

> "It is ultimately up to chief audit executives to hold their teams accountable for efficient and effective —along with quality— work."

rather than admonishment. Highlight your team's blind spots that they might not be aware exists.

In short, employees want more frequent and iterative assessments of their work, and internal audit leaders need to step up to deliver this and ensure quality, effectiveness, and efficiency at all stages.

STEP 4: ACT UPON WHAT YOU HAVE LEARNED

By this step, internal audit leaders have an array of tools at their disposal, including:

- Actionable definitions of effectiveness and efficiency for their teams
- Qualitative and quantitative metrics to bolster these definitions
- Information gathered from self- and manager-guided evaluations
- An understanding of how team members have performed along these guidelines

With this information in hand, many opportunities for growth are apparent—simply compare where you want your team members to be against where they are right now. By implementing these fact-based changes into your internal audit processes, leaders set the stage for cyclical organizational and personal improvement.

According to a survey, this type of continuous improvement yields a positive ROI for organizations, helping increase revenue, along with saving time and money—an average annual impact of $6,000. Additionally, these improvements are designed to compound with each cycle.

Just as the approach to monitoring and improving audit quality is ongoing and cyclical—there are always improvements yet to be made—this approach to improving effectiveness and efficiency is fluid as well.

By weaving this four-part process into the fabric of your internal audit methodology, leaders can improve effectiveness and efficiency in their organizations.
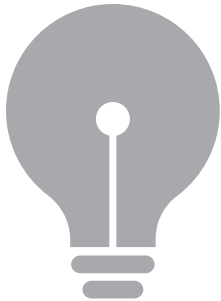
Quality, effectiveness, and efficiency intermingle and collaborate to make a high-performing internal audit function. Years of internal audit experience have taught me that, when improving those three aspects, an often-overlooked tool is technology.

The IIA recognizes the importance of technology's role, as reflected in the Standards. Section 1220 states: "In exercising due professional care, internal auditors must consider use of technology-based audit and other data analysis techniques."

That said, according to the 2017 AuditNet Survey, the majority of internal audit functions only use basic technologies to support their activities. Improving the tools used in internal audit can ultimately improve quality, build more efficient teams, and prove the worth and effectiveness of the function throughout the organization.

Streamline Your Internal Audit Process

Increase transparency, aggregate vital data, and improve collaboration between teams.

Over 3,000 organizations trust Wdesk to optimize financial reporting, ICFR, and compliance processes.

Learn more at **workiva.com/audit**

workiva

MIS Training Institute
153 Cordaville Road, Suite 200
Southborough, MA 01772
(508) 532-3649
www.misti.com

Workiva
2900 University Blvd
Ames, IA 50010
www.workiva.com

eBook brought to you by: **MIS|TI**™ TRAINING INSTITUTE & **workiva**