SAWYER’S
INTERNAL AUDITING

ENHANCING AND PROTECTING ORGANIZATIONAL VALUE

Thank you to the leadership of the following chapters for their sponsorship of Sawyer’s:

IIA-Albany
IIA-Central Kentucky
IIA-Edmonton
IIA-Houston
IIA-Kansas City
IIA-Las Vegas
IIA-Memphis
IIA-Oklahoma City
IIA-Phoenix
IIA-Salt Lake City
IIA-Topeka
IIA-Toronto
IIA-Tulsa
IIA-Vancouver

in honor of their chapter’s 70th anniversary
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>vii</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>xiii</td>
</tr>
<tr>
<td>About the Contributors</td>
<td>xv</td>
</tr>
<tr>
<td>Chapter 1: Developing an Internal Audit Strategy</td>
<td>1</td>
</tr>
<tr>
<td>Chapter 2: Defining Internal Audit Products and Services</td>
<td>27</td>
</tr>
<tr>
<td>Chapter 3: Developing Internal Audit Operations and Capabilities</td>
<td>47</td>
</tr>
<tr>
<td>Chapter 4: Defining the Internal Audit Team and Resourcing Model</td>
<td>63</td>
</tr>
<tr>
<td>Chapter 5: Developing Internal Audit Leaders and Staff</td>
<td>89</td>
</tr>
<tr>
<td>Chapter 6: Building Relationships and Setting Expectations</td>
<td>111</td>
</tr>
<tr>
<td>Chapter 7: Cultivating Business Acumen</td>
<td>133</td>
</tr>
<tr>
<td>Chapter 8: Understanding the Context within Which Internal Audit Operates</td>
<td>155</td>
</tr>
<tr>
<td>Chapter 9: The Internal Audit Mission and Its Risks</td>
<td>181</td>
</tr>
<tr>
<td>Chapter 10: Risk Assessment and Audit Planning</td>
<td>193</td>
</tr>
<tr>
<td>Chapter 11: Planning the Audit Engagement</td>
<td>225</td>
</tr>
<tr>
<td>Chapter 12: Assessing Internal Control</td>
<td>243</td>
</tr>
<tr>
<td>Chapter 13: Internal Audit Communication</td>
<td>273</td>
</tr>
<tr>
<td>Chapter 14: Assembling and Supervising the Internal Audit Team</td>
<td>297</td>
</tr>
<tr>
<td>Chapter 15: Specialty Skill Areas</td>
<td>315</td>
</tr>
<tr>
<td>Chapter 16: Advisory Services</td>
<td>329</td>
</tr>
<tr>
<td>Notes</td>
<td>347</td>
</tr>
<tr>
<td>Glossary</td>
<td>351</td>
</tr>
<tr>
<td>Index</td>
<td>359</td>
</tr>
</tbody>
</table>
CHAPTER 2
Defining Internal Audit Products and Services

As chief audit executives (CAEs) approach a strategic plan, they must step back and consider the value they will be adding upon its successful implementation. Most journeys begin with a clear understanding of the destination. A strategic journey is no different. Once a destination is understood, there must also be a viable path to get there. Similarly, strategic efforts are only helpful if there is a way to reach the defined destination offering additional value that CAEs seek to deliver.

CAEs define their desired strategic destination by defining the gap between the audit products and services of tomorrow and where they are today. This is a strategic position or gap analysis. Closing the gap means changing something about the products or services delivered. This chapter will help CAEs in these efforts by providing:

- A framework for considering internal audit products and services position—this defines thought leadership behind different approaches regarding delivery of internal audit products and services.
- The business perspective for strategic transformation—this is a discussion that centers on the CAEs’ need to challenge the way they look at their internal audit function.
- The architecture within which services and products of the future must be built—this illustrates the foundation of internal audit professional standards.
- A look at outside forces that may impact the role of the internal audit function.

This chapter concludes with ideas for CAEs to consider as they develop details to execute their strategic plans.

The Internal Audit Journey in Products and Services

In *Auditor’s Risk Management Guide: Integrating Auditing and ERM*, author Paul Sobel describes the rough history of internal auditing, which began (before 1941) with a role that focused on internal financial audit. The first internal auditors were the people who made sure that the external financial auditors would not find anything significant in their audit by performing a first review. As internal
Auditors gained stature, the concept of internal control was born, including the idea that necessary actions or appropriate segregation of duties needed to be in place to ensure the right outcome and avoid fraud, errors, or misstatements. As services evolved, internal auditors frequently found themselves in a place to comment on the efficiency or effectiveness of operations, processes, or staff. However, these comments were initially viewed with a suspect eye by management who felt that internal auditors really did not appreciate all of the factors involved in running operations.

In response to management pushback, internal audit professionals reached into the world of risk—and risk-based auditing was born. Risk consideration added an opportunity for internal auditors to tie a situation or threat to its potential impact should it happen. Internal auditors began performing annual risk assessments to guide their work and started reporting the likelihood and impact of findings to management. Importantly, management recognized value in the risk discussion and it led to further exploration and the birth of enterprise risk management (ERM). Sobel argues in his book that since management owns risk, further evolution of internal audit services through risk management-based internal auditing is warranted. In this approach, the internal auditor assumes risk management is (or should ideally be) in place, owned by management, and that the internal audit function’s ideal role is to assess risk management and operations from the top down.¹

Implied in Sobel’s narrative, first published in 2003, is a shift in internal audit services or an opportunity to audit from the top down. Each of the preceding phases of internal audit products and services are best described as “outside-in” approaches or bottom-up root cause analysis efforts. In addition to Sobel’s perspective, other internal audit thought leaders have explored different top-down audit service approaches, all of which can be characterized as “objective-based” internal auditing.

Objective-based internal auditing is a top-down approach that places the business objectives as the central factor in risk assessment. The goals and objectives of the organization are what are at risk. Therefore, understanding how objectives flow down through an organization provides important context for risk management evaluation. Its growth as a concept attempts to reign in risk efforts that may have become silos. Silos are created when risk programs forget that all risk must be placed in context of the strategic or business objective that is “at risk” or impacted. Without such an effort, management is limited on how effectively it can understand/respond and risk assessors may inaccurately value risk.

In both Sobel’s risk management-based and in objective-based audit approaches, the CAE’s value opportunity is to be more of an executive advisor of governance and risk management than a provider of assurance. It does not lessen the need for assurance; rather it means CAEs are capable of providing assurance at a higher level and translating their efforts into the language of organizational management. It notes that assurance information must be translated into executive-level insights. This evolution of internal audit thought leadership regarding internal audit products and services delivered over its history is simplified and illustrated in exhibit 2-1.
This exhibit illustrates how the CAE’s position of influence changes as more value is added. This graphic reflects a typical organizational chart with a person at the top and a few executives reporting directly to them. These executives then have additional individuals reporting to them, and so on down into the organization. These are characterized by the blue person icons.

The red person icons illustrate the first three phases of internal audit service and product evolution discussed previously. The Internal/External Auditor is focused on the output of the financial statements. The Internal Control-Process Auditor works more directly with financial leadership over processes that develop financial and public information. Then the Risk-Based Auditor continues the conversation about risk into more areas of the organization, looking for root causes.
The green person icons illustrate the more modern top-down Risk Management-Based and Objective-Based Auditors. In these efforts the priorities and activities of management, coupled with the business operational context, provide a framework within which to value opportunities for internal audit services and products.

The Internal Audit Products and Services Framework

In exhibit 2-2, this thought leadership concept is displayed in greater detail to provide a framework for discussion. This framework, while detailed, is not absolute, but it can help CAEs who are defining where their internal audit services and products are today and where they want them to be tomorrow.

The first column on the left describes the types of services delivered through each thought leadership phase of the internal audit function. The following columns then connect the resources required, typical products, and the general value they deliver to management and the board. This table necessarily oversimplifies the actual internal audit evolution of products and services. For example, it does not include valuable products and tools in IT, fraud, and data analytics. Yet it does illustrate how significantly different the value proposition of each phase of internal audit is for management and the board. It also challenges CAEs to consider clearly defining the products and services they are delivering and recognize the associated relationship of those choices to the skills of their team and the resources available. It is not enough to correctly define new value-adding products to deliver—they have to be created. New products mean new models or methods and new skills and resources. This is where strategic execution is required. CAEs can plan how these models and methods will be developed, but they cannot forget everything that must go into educating their staff, leveraging technology, and providing enough time for a pilot effort to deliver on planned value. Strategic execution efforts anticipate the change in skills and resources and plan how this will be accomplished. Will it be a simple project management process with a lot of communication? Alternatively, will it require training? Maybe it will result in a need for different staff with capabilities in the desired skill area?

Implied in this evolution of thought is an expectation that each new phase brings new value. Exhibit 2-2 illustrates how the perception of internal audit value to management and the board changes as the types of services and products improve over time. In reality, a typical internal audit function may still be performing services from an earlier era due to tradition, regulation, or stakeholder expectations, even if their aspirations are much higher. Another implication is that all internal audit functions would necessarily start at the earliest point and evolve into the desired performance level. Again, this is not always the case. Internal audit functions should be created at the level that makes sense for their organization, industry, and capabilities. For example, China had not made advancements in telephone land lines at the same pace as other developed countries. However, when cellular phones were created, China did not wait to perfect its land lines. Instead, the country moved forward to get involved in cell phone development and quickly outpaced many other countries in that space. Similarly, there is no need for newly created internal audit functions to perfect outdated ways of providing internal audit products and services. They can learn from the evolution of other internal audit functions and provide products and services that add value today.
CHAPTER 9
The Internal Audit Mission and Its Risks

In 2015, The IIA published a new Mission for Internal Audit: “To enhance and protect organizational value by providing risk-based and objective assurance, advice and insight.” The preceding eight chapters have reviewed how chief audit executives (CAEs) create an internal audit function to accomplish this mission. The next eight chapters discuss, at a high level, how the internal audit function provides services and develops products that deliver against this mission.

Internal audit stakeholders and internal auditors should seek to understand the mission of internal audit and how their internal audit function defines the vision to achieve it. These efforts should align with the organization’s vision for achieving business objectives and strategies. A well-tuned vision for internal audit complements organizational strategies and values, and ultimately helps to protect and enhance organizational value through risk-based and objective assurance, advice, and insight. This chapter introduces the components that comprise service performance and product delivery focused on adding value to the organization and achieving the internal audit mission.

Achieving the internal audit mission comes with its own risks. As business leaders navigate a world that is changing at a pace never experienced before, there is sharper management focus on maintaining and continuously enhancing effective governance, risk management, and control (GRC) arrangements suitable for the changing environment. As management’s world accelerates, so does internal audit’s. The future implies that internal audit does not own the full solution to this growing management need.

Other assurance functions within the organization (second line of defense) and other frameworks (enterprise risk management [ERM] and GRC) conceive of a future where internal audit is only one component of a broad solution that meets board and management needs. If the internal audit function does not respond to these realities, it may be sidelined within its organization and unable to achieve the internal audit mission.

CAEs must be aware of these efforts within and outside the organization and, where beneficial, participate in innovative collaboration. This participation may include risk assessment coordination and information sharing with organizational parties or it may include shared technology to improve board access to risk and issue data. Internal auditors may also find it expedient to rely on the assurance work of other assurance providers rather than perform the work themselves. If it is beneficial to the organization and aligns with the mission of internal audit, these situations should be thoughtfully considered.
Internal Audit Service Delivery

The International Standards for the Professional Practice of Internal Auditing and related guidance provide a specific set of expectations for carrying out services and producing internal audit products. Both the attributes and performance of internal audit are discussed in the Standards. CAEs must determine the frameworks, practices, procedures, and tools to accomplish these expectations. The Standards simply provides principles and a professional baseline, including the internal audit mission, to help internal audit functions optimize the value they bring to organizational GRC.

In this section of the book, important aspects of internal audit services and product development and delivery are reviewed. Chapters 10 through 16 address the core activities performed by internal auditors and the many other value-adding activities and services they provide that expand on the internal audit mission and respond to organizational needs, including:

- Risk assessment and audit planning
- Planning audit engagements
- Assessing internal control
- Audit communication
- Assembling and supervising the internal audit team
- Specialty skills needed in an internal audit function
- Performing advisory services

Risk Assessment

Uncertainty of organizational success is the primary driver of the internal audit risk assessment. For an internal audit function, a risk assessment is a formal activity that happens at least annually if not more frequently. One purpose of the risk assessment is to direct the internal audit effort to areas of the organization where it can add the most value. A risk assessment typically is conducted with research, interviews, surveys, and validation of findings. It historically has created lists of risks rated as high, moderate, or low typically displayed in heat maps or other visual reports. For example, in an interview with the chief operations officer (COO), the internal auditor learned that an important position for plant management was being eliminated due to cost constraints. The individual being let go was responsible for defect monitoring and scheduled maintenance. The COO indicated that these duties would be assumed by others, but the roles had not yet been defined. Upon investigation, the internal auditor identified significant costs related to product rework and production outage. Given the change in management and the high cost of error, the internal auditor places “plant defect management and maintenance” on the risk list to be compared with other risks and ranked.

The output of a risk assessment may serve only internal audit needs for planning or it may be a product by itself delivered to management and the board. With the growth of ERM, internal audit’s efforts for risk assessment may link to ERM data and processes. It is typical to vet the results of a risk assessment with those interviewed to ensure that internal audit is not missing some important component that may increase or reduce the defined risk.
The Audit Plan

The internal audit function must create a risk-based annual or periodic plan reflecting the assurance and advisory services and other activities that the function will deliver. Typically, a risk assessment precedes the development of the audit plan. However, most internal audit functions have several engagements they are required to perform regardless of their level of risk, often as a result of regulatory requirements or management and board expectations. It is common for CAEs to develop a budget of hours for the internal audit function given the period of the plan and then account first for all required audit efforts. Once required audit hours have been accounted for in the plan, the remaining hours are allocated to assurance and advisory services focused on defining and assessing the highest risks from the risk assessment. Because CAEs are responsible for ensuring that plans are risk-based, whenever possible, engagements that are not associated with high risks should be minimized.

Planning an Audit Engagement

An audit engagement provides assurance by focusing on improving GRC. If the engagement is required by regulations, management, or the board, it may not be risk based and may come with specific expectations of what is to be reviewed. However, for all risk-based projects, the planning effort is the most important part of the engagement. At its most fundamental, it is an extension of the risk assessment. It takes the risks that put the engagement on the plan and investigates them further to define a reasonable project scope. For example, when beginning an engagement to assess the “plant defect management and maintenance” risk from the example provided earlier, the internal auditor must follow up with the COO for an update. The COO tells the internal auditor that plan maintenance is now the responsibility of the regional vice president who has assigned a traveling director to visit twice a month to ensure appropriate procedures continue. The COO believes this may be a positive change as the region has a more extensive budget from which to draw. When the internal auditor asks about defect management, the COO notes that the floor manager and the customer service manager have been asked to share this effort. However, the COO notes that rework cost grew by 11 percent last month. In this instance, the internal auditor, following the risk, may write an engagement scope that focuses solely on defect management. The specific activities to be performed are then developed around this scope.

Assessing Internal Control

Internal control is a concept with a long history. When the Committee of Sponsoring Organizations of the Treadway Commission’s (COSO’s) Internal Control – Integrated Framework was introduced in 1992, internal control was largely interpreted to mean the activities that ensure internal financial reporting processes and transactions are accurate and complete.

Today the term is applied more broadly to mean the actions that management and the board take as they seek to improve the ability to achieve strategic objectives. For example, as the internal auditor begins to define the engagement for the plant defect management risk, the expectation is that the
floor manager and the customer services manager have defined processes and oversight activities in place to manage and control defects.

Based on experience with other areas of the plant, the internal auditor creates an initial audit step to define defects oversight, including current defect management objectives, metrics, measures, methods of data gathering, and reporting produced. A second step is created to flowchart or narrate key defect management procedures. These two steps reflect how internal control parallels the expectations of management to oversee and manage operations to optimize objective achievement. However, internal control also applies to nonoperational management actions that help mitigate other risks, including compliance and safety.

In essence, internal control consists of both the activity that promotes operational objective achievement and the activity that mitigates specific types of risk. While risk can be defined as the effect of uncertainty on objectives, in the case of defect management, the objective at risk may be outside the applicable business unit's operational objectives. Reputation, compliance, and other hazard risks must also be considered and controlled.

**Internal Audit Communication**

During an engagement, internal auditors carry out the steps they have defined in their audit program to accomplish the scope of the project. Communication occurs regularly throughout the engagement. As potential internal control concerns are identified, they are documented. During the course of the engagement, these concerns are reviewed by supervisors and further validated by the internal auditor. At the end of the engagement, an audit report is drafted. The audit report is the culmination of the insights the internal audit team wants to communicate to management based on the engagement performed. After discussion and validation, any concerns that reflect an unacceptable level of risk are documented in the report as findings and management provides action plans to remediate them. As management completes the action plans they committed to in the audit report, the internal audit function performs follow-up activities to validate that the actions effectively mitigated the risks.

Individual engagement reports are aggregated together and combined with other information communicating the results of other value-adding internal audit activities into a larger report that is delivered at regular intervals to the audit committee. Audit committees commonly meet three to six times a year and have primary oversight responsibilities for the internal audit function. Internal audit has specific professional obligations to inform the audit committee of their activities and the results.

**Assembling the Internal Audit Team**

To provide high-value assurance and advisory services, internal auditors need a strong understanding of the business. Recipients of assurance and advisory services only find value in the results of the engagement if the internal auditors performing it are knowledgeable about business operations and risks. Internal audit talent management has become a top priority for CAEs as they strive to
align internal auditors’ business acumen with the expectations of these stakeholders. CAEs create internal audit functions that have a mix of skills and expertise represented. Typically, this includes internal auditors who have a variety of certifications (for example, Certified Internal Auditor [CIA], Certified Public Accountant [CPA], Certified Information Systems Auditor [CISA]), and operational and management backgrounds, as well as other industry-specific skills. CAEs have a responsibility to ensure the internal audit engagement teams have the requisite competence to carry out the engagements to which they are assigned. Chapter 7, “Cultivating Business Acumen,” and chapter 14, “Assembling and Supervising the Internal Audit Team,” provide additional details on this topic.

**Specialty Skills**

In addition to business acumen and industry-specific knowledge, the internal audit function needs to employ internal auditors with expertise in relevant, topical areas that is necessary to provide assurance and advisory services that holistically address applicable risks across the organization. While no single individual can embody all of the technical expertise necessary, the internal audit function collectively must include expertise across the spectrum. In addition to the specific internal audit skills represented by the CIA certification, there are three additional areas of technical skill in which internal auditors can become certified that benefit typical organizations:

- Information technology (CISA)
- Fraud and investigation (CFE)
- Financial management and accounting (CPA)

Each of these areas offers professional certification as noted. Historically, most internal auditors were hired into the internal audit function with a finance background. However, the demand for more business acumen has pressured CAEs to hire more creatively, and it is no longer true that all internal auditors have competence in financial areas. Consequently, the internal audit function must recruit for financial experience to be able to adequately assess the financial risks of the organization.

Regardless of the industry in which an organization operates, IT is now part of every process and every operation. As such, most internal auditors are trained in general IT controls and assessment. Yet deeply technical areas, networks, and databases generally require individuals with strong backgrounds in technology.

Additionally, fraud investigation is another area where expertise is needed for the internal audit function to be able to adequately identify and assess potential fraud. Individuals with fraud expertise must be able to effectively interact with other fraud professionals, including law enforcement, chief financial officers (CFOs), and external parties. As CAEs assemble their teams, they typically plan to cover these areas by hiring individuals with applicable certifications, developing skills internally, or hiring consultants as needed to fill experience gaps. Chapter 15, “Specialty Skill Areas,” covers this topic in greater depth.