CliftonLarsonAllen

The Role of Internal Audit in Risk Governance

How Organizations Are Positioning the Internal Audit Function to Support Their Approach to Risk Management

Risk management has evolved to become risk governance. Learn how to get the most value out of the internal audit function.

Executive summary

Risk is inherent in running any business — understanding those risks, and knowing how much risk to take, is often the difference between reward or failure. The last few years have sharply intensified the focus of organizations on understanding their desired and actual risk profile and how they manage those risks. During this time, it has become clear that basic risk management alone may not be enough. The concept of "risk management" is evolving into a more fully developed, integrated concept of *risk governance,* in which the board of directors, senior management, and the business units of an organization all have distinctly defined roles in the overall approach to enterprise risk management (ERM).

One of the critical components of a robust risk management program is an internal audit function that has a well-defined charter, supports the identification and evaluation of risk, and carefully allocates its resources to give the highest value to the organization. In many organizations the internal audit function has evolved into a function that works with existing risk management functions to complement the overall approach to risk. There is no one "best" way to operate an internal audit function; the charter and its execution must be tailored to each organization. In turn, the organization must carefully consider how it staffs the function; determine if it has the right talent and resource levels to identify and evaluate financial, operational, IT, compliance, and regulatory risk; and do all of this in the context of our challenging financial times. In addition, the execution strategy must evolve as the organization and its risk profile change over time.

From risk management to risk governance

Since the economic downturn began in 2008, times have been difficult for businesses — even for those that have done well. Many of the "rules of the road" have changed, and we now hear talk of a "new normal," implying that the rules have changed permanently, or at least for the foreseeable future. Business leaders are working hard to understand their environment and their customers, and learning how they must adapt in order to sustain themselves and flourish. In addition, the nature of businesses has changed at an increasing pace to adapt to the global nature of commerce and the speed of innovation made possible by information technology.

The upheaval in the business environment has led many to conclude that organizations did not effectively manage their existing risks, and may not be equipped to identify and appropriately respond to emerging risks. As a result, business leadership, government, and academic organizations are calling for a more robust approach to risk management.

The shift toward enhanced risk governance

In response to the changing business environment, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has called on organizations and their boards to strengthen risk oversight, and to explicitly discuss oversight capabilities as part of their governance processes. The National Association of Corporate Directors convened a Blue Ribbon Commission on Risk Oversight, and issued a report in October 2009 focusing on the board's role in risk oversight. These initiatives have resulted in a new emphasis on "risk governance," which involves directors and management assessing and improving their processes for overseeing the organization's framework of risk management activities.

There is no one "best" way to operate an internal audit function; the charter and its execution must be tailored to each organization.

An opposing force

At the same time, pressures to reduce costs and meet profitability targets have constrained resources and prevented many organizations from fully implementing a robust risk governance structure. As the risk governance process is applied for each area of an organization, that part must be re-examined. Roles must be refined based on the tasks assigned and the resources available to optimize risk governance and business results.

Internal audit as part of risk governance

An organization's risk governance system includes both people and processes. While the system of internal control is a basic part of the risk management system, it must be coupled with other monitoring and reporting systems to create an effective risk governance system. The internal audit function is one of these systems, and plays a critical role in risk governance.

Scaled to fit the needs of the organization, internal audit can range from a relatively small compliance-based function, to a full-scale risk identification, assessment, monitoring, and reporting operation. Understanding how internal audit is designed and operated is a key part of the overall design of the risk governance program.

Internal audit — character and design

Organizations have instituted internal audit departments for different reasons. In larger organizations, internal audit may serve as the primary owner of the risk management function, or partner with an existing ERM program, and consider all categories of risk in addition to the traditional financial and compliance risks. This role may

involve assisting with compliance functions, consulting with departments to identify emerging trends, providing benchmarking information, and improving operations. In smaller organizations, internal audit may be focused on fewer categories of risks, perhaps focusing primarily on financial or compliance. It is then scaled up or down based on the perception of those key risks. Big or small, organizations should consider what they need when defining the charter for internal audit.

Evolution of internal audit

The prevailing character of internal audit has evolved over the years. When it was first instituted, internal audit was more focused on compliance and the prevention of fraud. Over time, a number of internal audit organizations changed their focus to regulatory compliance, IT, and operational auditing, driving process improvements and cost savings.

In the late 1990s and early 2000s, many internal audit organizations were organized around regulatory requirements, and some were based on organization type. For example, certain financial institutions are required by law to have an internal audit department. In other cases, broad regulatory overhauls spawned changes, in much the same way as the *Sarbanes Oxley Act* did in 2002. Due to the intense pressure on public companies to comply with this regulation, many internal audit staffs became almost exclusively focused on this effort. As implementation has progressed, this emphasis is diminishing, and the compliance effort is being pushed out to other parts of the risk management system, allowing the internal audit department to reposition itself and its role. As businesses have evolved and adopted new business models and technologies, some have focused internal audit efforts in these new areas.

Today, almost all organizations face challenges in information technology, business continuity, digital security, and knowing how internal controls are integrated into information systems. Others have significantly increased the amount of commerce transacted over the web, and the amount of digital information that is shared with customers and between all parts of their supply chain. Failure to understand and manage the risks in these areas could result in technology failures that are crippling, if not fatal. In addition, privacy and security expectations have been elevated due to regulations and consumer demand. New skill sets are required to manage these areas and the demand for these skills is increasing. As organizations design their risk governance process, they should ask if the current internal audit approach, staffing, and skills — as well as the existing focus on operating, financial, IT, regulatory, or other risks — are appropriate in today's complex, global environment, or if they need to be updated.

Gaining value from internal audit

Proper management of risk can help public, private, nonprofit, or governmental entities build stakeholder value. Internal audit can help drive value in several ways. As such, more organizations are turning to the ERM process.

COSO has defined ERM as:

" . . . a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

ERM enables leaders to take a holistic view of risks, their uncertainties, and their associated magnitude and likelihood, and design an appropriate operational response. This, then, enhances the capacity to build value. Internal audit can then help facilitate the ERM process. Since internal auditors will generally have an in-depth knowledge of the organization and the discipline to identify, evaluate, and report on risks and their consequences, the function can also be a key participant in identifying risks, evaluating the related controls, and monitoring risk mitigation activities.

Another way internal audit can drive value is to allocate resources to areas of higher risk or higher potential returns on investment, helping ensure that key areas are being properly managed. However, allocating resources to areas traditionally identified as high risk may not be where the most value can be derived if organizations have outstanding controls and monitoring is already in place in these areas. A strong internal audit effort in emerging risk areas, or where there is not adequate staffing or systems, may drive more value by providing management with feedback in these areas. This would allow timely mitigation so that emerging problems do not become major crisis, and help provide a road map to address identified issues. New lines of business, operations in new geographic areas, new regulations, and other changes are all opportunities to refocus internal audit resources.

Case Study #1: Crisis management

A multimillion-dollar subsidiary of a global distribution and logistics provider had grown significantly in the United States through expanded service agreements. When an inventory recording and usage issue was discovered, the company found itself in urgent need of an on-site team to assess the issue, understand the magnitude of the process improvements needed, and make recommendations on how the issues could be fixed.

Within four days, the internal audit provider assembled and dispatched a team to the location. The team worked with management personnel to assess and report on the issues. The project led to the implementation of recommended procedures to more accurately record and track inventory usage. The distributor continued working with the audit provider on specific projects and time-urgent issues as an alternative to a full-time, in-house internal audit department.

Risk governance and internal audit

Today's internal audit function plays a key role in an overall risk governance structure by facilitating the identification and evaluation of risk, coordinating ERM activities, providing consolidated risk reporting, and evaluating risk management processes. Internal audit often has the best overall view of risk in an organization and may even develop the overall risk management strategy for board approval. Giving assurance on the risk management process, and that risks are being correctly evaluated is a key benefit of linking your internal audit and risk governance functions.

Case Study #2: Outsourcing saves and strengthens

An $800 million community bank was required by regulation to have an internal audit function. The bank hired a single internal auditor, who encountered issues with training, motivation, personal growth, technical expertise in information technology, and independence.

By outsourcing its internal audit function, the bank was able to bring in professionals to evaluate the risks, and develop an audit plan to address these threats. The new resources were experienced with assessing risks, completing audits, and working with executive and board-level personnel, which saved time. Once the risk assessment was complete, audit programs were developed and the work was performed by people with experience in the areas reviewed. For example, a human resources professional was used for the HR area. This strategy resulted in significantly more meaningful recommendations for the organization.

Communication protocols for success

Well-defined communication protocols between internal audit, management, and the board are critical. The knowledge that internal audit has about the organization (and changes in its risk profile) must be relayed to management in time to be actionable. A good communication plan includes:

- An audit charter with well-defined roles and responsibilities that is reported and reviewed at least annually with management and the board
- An internal audit plan that identifies risks and allocates

Top 10 Questions to Ask Your Organization About the Internal Audit Role in Risk Governance	
1.	Does the organization understand the key risks (financial, IT, operational, regulatory, contractual) it faces? Has organizational performance been impacted by a key risk that was not anticipated?
2.	Does the internal audit plan focus resources on the identified risks? Does it identify emerging risks and reallocate resources accordingly?
3.	Does the internal audit department have specialized skills and resources to audit new technologies, complex areas, emerging industry trends, or new business and product lines?
4.	Is there a better way to staff the internal audit department in light of budget constraints?
5.	Does the internal audit department have the tools and technologies it needs to be successful?
6.	Does the internal audit department understand the information technology risks the organization is facing? Have information systems been reviewed to see that internal controls are in place?
7.	Do management and the board get sufficient communication regarding risk? Is there a standardized reporting process that is repeatable and sustainable?
8.	Is there a common understanding in the organization regarding levels of acceptable risk, and when risks should be escalated to a higher level?
9.	Are red flags occurring in business operations that need additional attention?
10.	Have findings from prior internal audits been corrected and incorporated into the risk governance process?

resources linked to those risks, and is reviewed at least annually with management and the board
- A quarterly update on internal audit activity with key findings (more frequently if needed)
- Quarterly communication on key findings, with reports on open findings included until the issue is corrected
- Escalation protocols that detail the communication plan with management and the board when an unexpected event occurs
- Periodic independent communication with the audit committee and/or board

With this level of communication in place, internal audit can provide input to management and the board to support strategy development, resource allocation, and operational execution that enhances the performance of the organization.

Sourcing of internal audit

Internal audit functions can be sourced in a variety of ways. Some of the most common are:

- Employee-based model — All members of the internal audit department are employees of the organization.
- Co-sourced model — The chief audit executive and members of the internal audit department are employees, but contractors are used for specific projects, industry or technical situations, or geographic locations.
- Outsourced model — An employee performs the chief audit executive role, but all other resources are contracted to an outside firm(s).

The trend behind outsourcing

There are four common reasons that organizations contract the internal audit function. One is the need for specialized skills to effectively audit some portions of their organization. This is especially true in areas that are seasonal, technically complex, industry specialized, automated, and/or dependent on IT internal controls. Hiring and retaining specialized personnel, providing a career path, and keeping up with training needs are difficult, especially for small organizations. An outside audit provider allows access to these skills for only the time needed, and generally at a more reasonable cost than trying to maintain them in-house.

A second reason organizations look to outside help is for specialized audit tools, which can lead to more effective and efficient audits. Developing these tools in-house may be cost-prohibitive. This is often seen in the privacy and security areas of focus.

A third reason is that in selected situations, it may be perceived that outside professionals bring a special degree

With this level of communication in place, internal audit can provide input to management and the board to support strategy development, resource allocation, and operational execution that enhances the performance of the organization.

of independence or expertise that adds credibility to the findings of the internal audit activity.

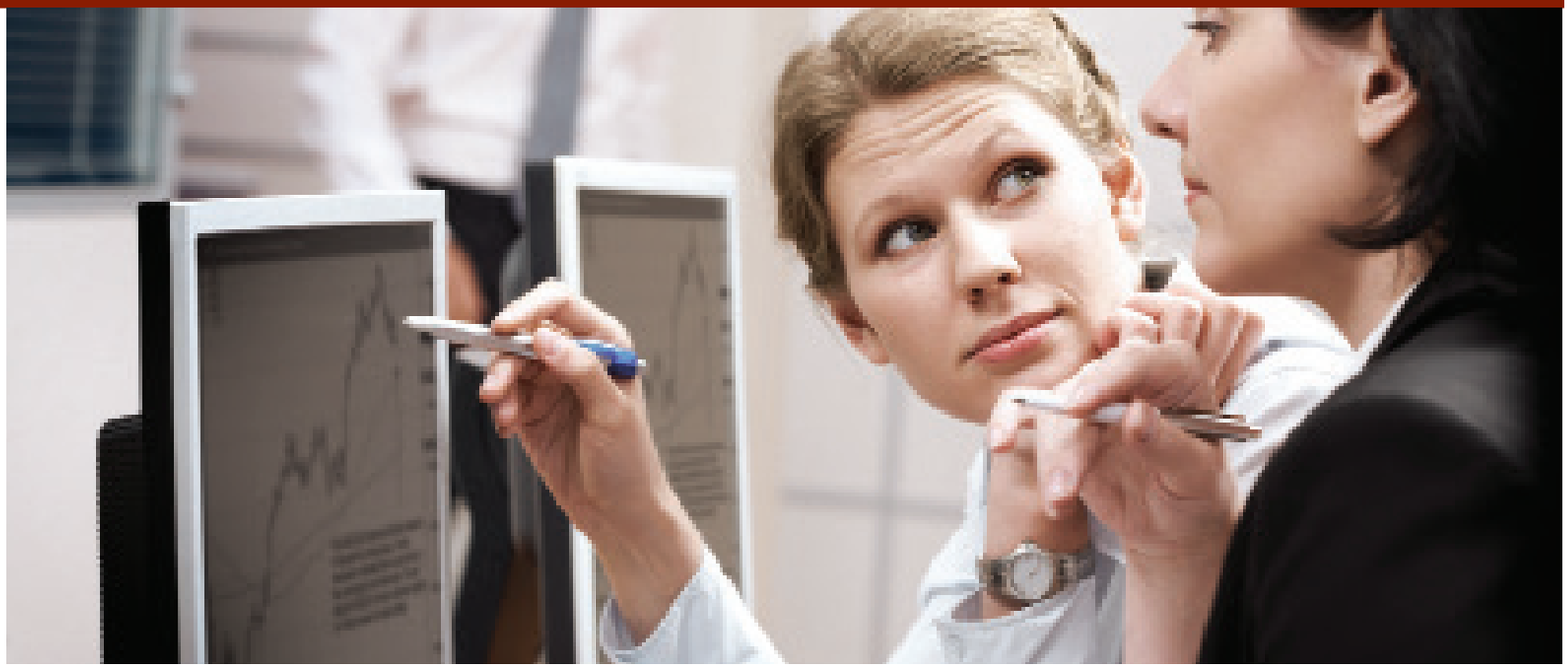
Finally, the ability to expand and contract the staff almost “at will” allows organizations to use outsourcing or co-sourcing to help manage their budgets. In today’s economy, outsourcing or co-sourcing may allow an organization to maintain an audit function while simultaneously reducing costs until the economic outlook improves.

Case Study #3: A hybrid approach

A $3 billion credit union was required to have an internal audit function. There had once been an audit manager, but now just one senior auditor was on staff. The senior auditor was very effective at completing the audit work, but did not have the experience to manage beyond the project needs and report to the audit committee.

By co-sourcing the management of its internal audit function, the credit union was able to reap a number of benefits. The co-source firm provided the management expertise to develop an effective audit plan, present the plan to the audit committee for approval, and communicate the appropriate level of information. The approved plan was completed by the internal staff and supplemented with external resources. The external resources provided:

- Expertise in selected areas
- Assistance with completion of larger projects and special work needs



- Management skills to effectively manage the performance metrics and charter requirements
- Required testing of procedures and controls
- Significant value to the organization

When the credit union later merged with another similar-sized credit union, it was able to obtain the resources from the co-source provider to assist in the transition and maintenance of an effective audit function at both locations.

Conclusions

Risk is inherent in the nature of doing business, and businesses grow and thrive by fully understanding their risks and assuming acceptable levels of those risks. But it is the effective identification, assessment, management, monitoring, and reporting of such risks that allows a business to know what their response should be to a given risk. Organizations are incorporating lessons learned in recent years into formal risk governance processes. By sizing and resourcing the internal audit function to fit its needs, and focusing its resources as part of an overall approach to enhanced risk governance, an organization can maximize its ability to leverage risks that will create value and effectively manage risks that can decrease value.

About CliftonLarsonAllen

CliftonLarsonAllen is one of the nation's top 10 certified public accounting and consulting firms. Structured to provide clients with highly specialized industry insight, the firm delivers assurance, tax, and advisory capabilities. CliftonLarsonAllen offers unprecedented emphasis on serving privately held businesses and their owners, as well as nonprofits and governmental entities. The firm has a staff of more than 3,600 professionals, operating from more than 90 offices across the country. For more information about CliftonLarsonAllen, visit cliftonlarsonallen.com.

NEXIA INTERNATIONAL

An independent member of Nexia International