Getting to strong

Leading Practices for value-enhancing internal audit

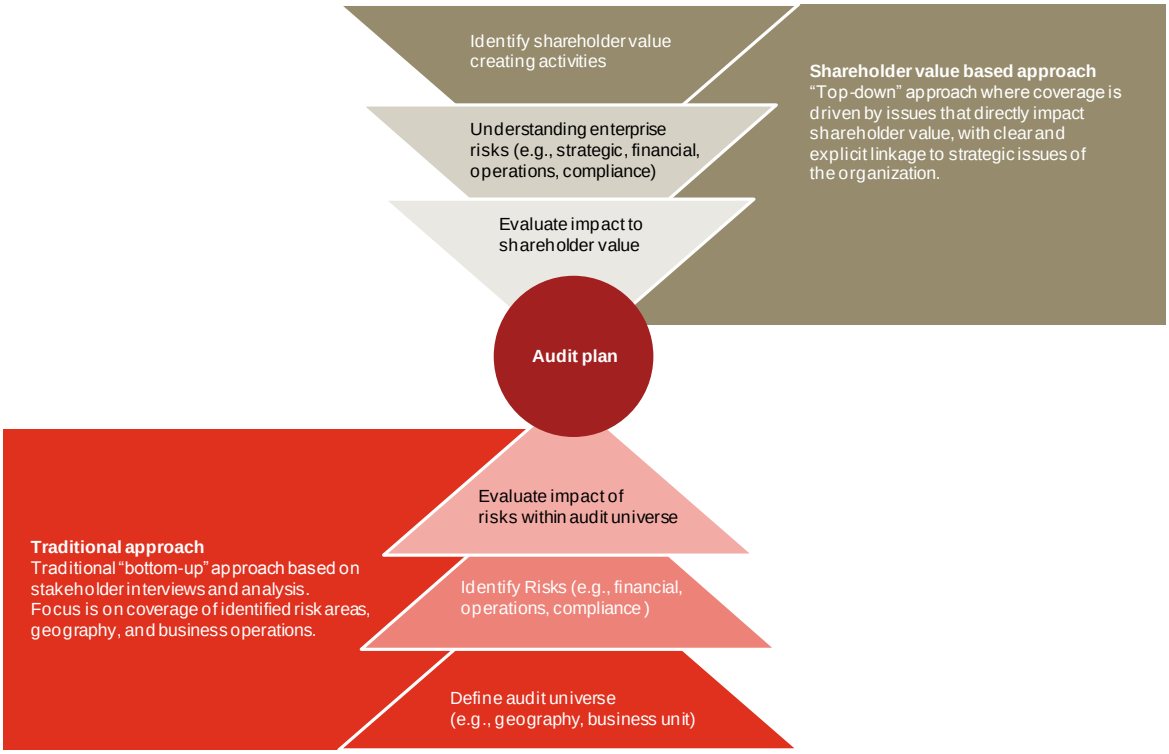
By Richard Reynolds and Abhinav Aggarwal - PricewaterhouseCoopers LLP

Today's unpredictable business climate and challenging regulatory environment is raising the bar for internal audit performance. Obtaining a "Satisfactory" rating in a regulatory examination is no longer viewed as acceptable and regulators have been driving and expecting internal audit to achieve a "Strong" rating. Furthermore, boards and management are expecting internal audit to play a pivotal risk oversight role and be their eyes and ears on the ground. This requires a fundamental shift in the business of internal audit and one that requires internal audit to be more relevant to the board and aligned with management's agenda. Outlined below are suggested areas of focus that can help you flex your internal audit muscle to meet today's demands.

1. Embrace dynamic risk assessment and audit planning

A strong and dynamic risk assessment and audit planning process is the backbone of any well-built internal audit function. A sound risk assessment process informs the audit planning process in a meaningful way by aligning the most significant risks of the organization to the audit plan. Traditionally, organizations have adopted a "bottom-up" approach to risk assessment that begins by defining the audit universe and identifying and evaluating risks to develop the audit plan. However, such an approach may sometimes fail to consider the top enterprise-level risks in the organization, i.e., "miss the forest for the trees."

As organizations reassess their risk assessment process, they should aim to integrate the bottom-up approach with the top-down approach to derive the audit plan, as depicted below.



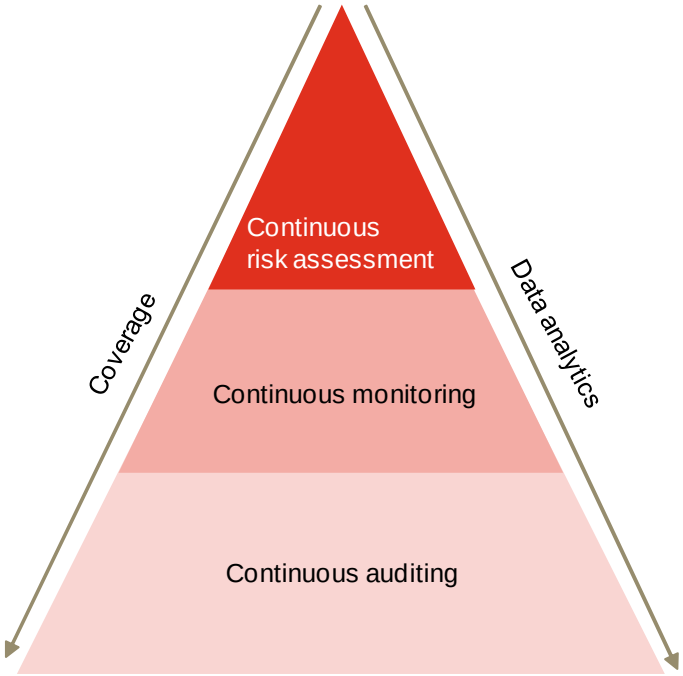
Please see OCC regulatory framework for internal audit for the rating definitions.

Including a top-down approach in your risk assessment and audit planning process can facilitate development of an internal audit plan that focuses on issues that directly affect shareholder value and are clearly linked to strategic organizational factors.

Organizational risks are changing continuously, so the internal audit risk assessment and audit planning process should be dynamic as well. Several organizations have moved away from the traditional annual planning cycle to a semi-annual or quarterly rolling plan to ensure that the most current risks are addressed on a timely basis. While this may not be the best approach for all organizations, in order provide greater value to its stakeholders, internal audit must regularly monitor emerging risks in the organization and make changes to the audit plan to address them. The focus should always be on allocating resources that maximize risk coverage.

2. *Employ continuous monitoring and auditing techniques to identify emerging risks*

The use of continuous monitoring and auditing techniques to identify emerging risks and issues in the organization has been evolving in recent years. The diagram below depicts three elements of continuous monitoring and auditing techniques employed by leading internal audit departments. It is important to note that the level of assurance that internal audit can provide increases as internal audit migrates from continuous risk assessment to continuous monitoring to continuous auditing.



Continuous risk assessment: The purpose of continuous risk assessment is to monitor emerging risks and provide early warning about higher risk activities within the business areas. Internal audit uses the insight and information generated from continuous risk assessment to trigger real-time calibration of the audit plan. The use of data analytics is minimal during continuous risk assessment.

Continuous monitoring: Continuous monitoring requires data-enabled programs to monitor key risk and performance indicators (KRIs and KPIs) in the business units. The focus on data can provide current performance and emerging risk insights, which can then be used to further calibrate the risk assessment and audit plan. Continuous monitoring is an evolution of continuous risk assessment whereby the monitoring

activities are enhanced through the use of data that may or may not be consistent with the qualitative analysis conducted in continuous risk assessment.

Continuous auditing: The final phase of the evolution, continuous auditing, relies heavily on data analytics to detect control deficiencies. Data analytics become an integral part of the audit processes and are used to monitor the risk and control environment and/or identify the potential for additional audit procedures. A high degree assurance can be derived from continuous auditing, whereby repeatable, data-enabled processes are audited through data analytics. The use of analytics can also create greater efficiencies, enabling valuable audit resources to cover other critical business processes.

3. Increase focus on strategic and business risks

Strategic risk is viewed as one of the most significant causes of decreasing shareholder value, far greater than financial, operational, legal, and compliance risks. Incidentally, strategic risk is also the risk category that usually receives the least coverage from internal audit. Although it may be difficult to obtain organizational acceptance for internal audit to directly audit strategic and business risks, risks inherent in the business strategy should be considered for coverage in the audit plan.

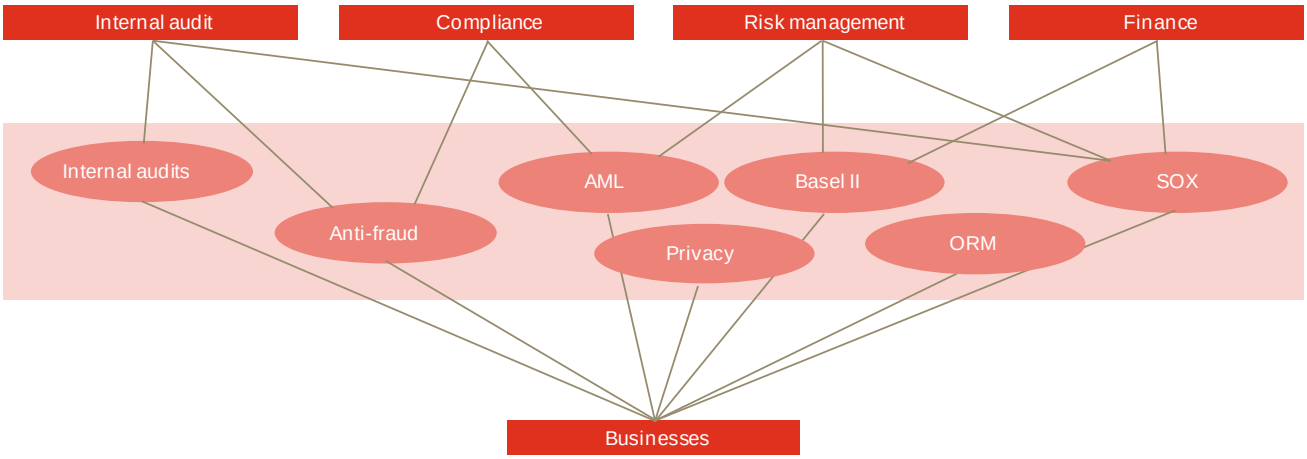
While it is not typically the mandate of internal audit to challenge management on strategy, there are aspects of strategic and business risk that internal audit can and should assess, including the following:

- The risk that the strategy is not well understood
- The risk that business decisions are made that are inconsistent with company strategy
- The risk that the strategy is not achieved because of failure of business processes

Focusing on strategic and business risk is not just a macro- or company-level exercise. Understanding the business objectives and strategies of business units or departments being audited and assessing the alignment of business decisions, risk profile, and risk management infrastructure with those objectives and strategies should be a key step in the execution of individual audits. This knowledge is a key component of moving from a more traditional compliance-based audit approach (i.e., Are you following policy?) versus a true risk-based approach (i.e., Are the policies appropriate given the business objectives, strategies, and risk appetite? And are you following them?).

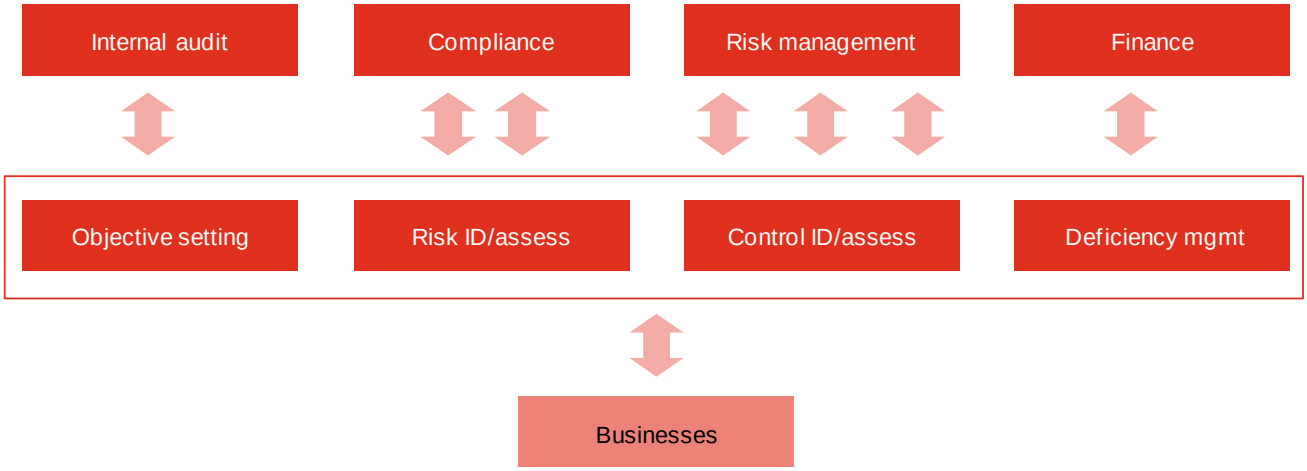
4. Promote better coordination among risk partners

Internal audit's role as the "third line of defense" has long been established and accepted. There have been a number of discussions on its role and effectiveness in auditing the "second line of defense" risk functions, such as the Legal and Compliance functions. However, many organizations are still working to determine the appropriate coordination of the risk management functions and internal audit in ensuring that risks are identified, assessed, managed, and controlled appropriately. As a result, a common occurrence is a coverage overlap (depicted below) between the various risk management and oversight functions and "audit fatigue" by the various business areas that complain about being asked the same questions over and over again.



This lack of coordination can also result in risks and issues falling through the cracks due to the lack of coordination among the various risk management and oversight functions. Normally, in this structure, every risk function reports on its activities individually to the board and management, leaving them confused on the overall state of the organization. Ask yourself: Can the board and management understand what it is they should be concerned with when multiple risk management and oversight functions are providing multiple perspectives? The answer lies in risk convergence.

Risk convergence begins with establishing a common definition of risk in the organization. It is achieved when risk management, compliance, finance, and internal audit work together to identify and assess risks and controls. The diagram below describes the desired risk convergence flow where the risk management and oversight functions use a common risk framework.



As risk convergence takes hold, internal audit can move to risk dashboards and/or theme-based reporting that provides a converged view risk in any business unit/function as well as how those risks are trending over time. This kind of focused reporting will enable the board and management to understand how effectively the business units are managing risks and to identify any areas that need board and management focus.

5. *Identify and resolve skill gaps*

As internal audit functions transform their role and positioning in the organization, the skill sets required to execute this transformed approach will need to adapt accordingly. The 2011 PwC State of the Profession Survey identified the following skill sets as most critical to an internal audit function's long-term success:

Critical skill sets for long-term success*	
1. Knowledge of risk management approaches	69%
2. Specific technology experience	66%
3. Critical thinking and analysis	65%
4. Understanding of organization's strategy and business model	65%
5. Communication	59%
6. Leadership	58%
7. Experience in the business outside of internal audit	55%

*Survey respondents indicating the need for the above capabilities and depth of knowledge will increase over the next three years

Internal audit functions should undertake a formal skills assessment to identify skill gaps and develop a plan to fill the gaps through training and/or talent acquisition. The following is an example framework that can be used to perform a skills assessment. The technical skills and level of proficiency required will vary depending on an individual auditor's role and level in the department.

Core	Technical	Leadership
• Teamwork • Client service focus • Continuous improvement mindset • Ownership and accountability • Flexibility/adaptability • Act as a change agent • Oral communications • Independence and objectivity	• Business acumen • Specialized loan knowledge • General Information technology • Applications/end-user computing • Data analysis • Modeling • Analytical skills • Flowcharts, documentation, and quality review • Knowledge of audit standards	• Sets vision and direction • Develops others and self • Inspires and motivates • Drives execution

Rating scale definitions				
1	2	3	4	5
No experience	Limited awareness	Basic proficiency	Full proficiency	Expert proficiency
Has not had exposure to the stated competency; demonstrates none of the behaviors.	Demonstrates knowledge in some of the behaviors. However, requires close supervision and guidance in applying the behaviors to both routine and non-routine situations or conditions.	Demonstrates knowledge in most of the behaviors. Needs guidance in applying the behaviors to non-routine situations or conditions. Gives some knowledge-based guidance to others.	Demonstrates in-depth specialist knowledge in all of the behaviors. Acts independently in applying and modifying the stated competency and gives guidance and advice to others, often at a high level.	Demonstrates all behaviors at an expert level of proficiency. Acts as one of the highest sources of expertise within the institution or externally and/or is recognized as an expert in the area and called upon to advise on topic.

6. *Improve audit efficiency*

While the bar has been raised for internal audit performance, often the budget has not. As such, many internal audit functions are looking to increase efficiencies. Although chief among these is a drive toward boosting the use of technology, this has been an elusive goal, largely because of a lack of available skills. Other efficiency tactics include moving to a risk-based approach to reduce time spent on lower risk areas, standardizing audit procedures, and performing an end-to-end examination of the audit process.

Organizations should undertake a top-to-bottom review of their internal audit processes in light of the following common failings:

1. Risk assessment is not aligned with drivers of shareholder value
2. Internal audit work is focused on low-value activities and controls, or replicates external audit procedures
3. Financial and human resources devoted to the internal audit function are constrained
4. Use of technology tools is limited and not integrated
5. Audits are planned with overly broad objectives and scope
6. Routine audits do not fully leverage data analysis tools
7. Assignment process and travel requirements create significant process inefficiencies
8. Communications, such as drafting reports, and the assignment of report ratings consume significant resources
9. Recommendations are not impactful
10. Process is weighted toward repetition versus relevance

* * * * *

Today's demanding business and regulatory environment requires an evolution in the way internal audit does its work and interacts with its stakeholders. It's an opportunity for internal audit to up its game and relevance — and get stronger with a top-down approach and a finely tuned internal audit function.

For more information, please contact:

Richard Reynolds, Financial Services Partner Internal Audit Services Risk Assurance – PwC	Richard.Reynolds@us.pwc.com	(646) 471-8559
Abhinav Aggarwal, Financial Services Principal Internal Audit Services Risk Assurance- PwC	Abhinav.Aggarwal@us.pwc.com	(646) 471-0820