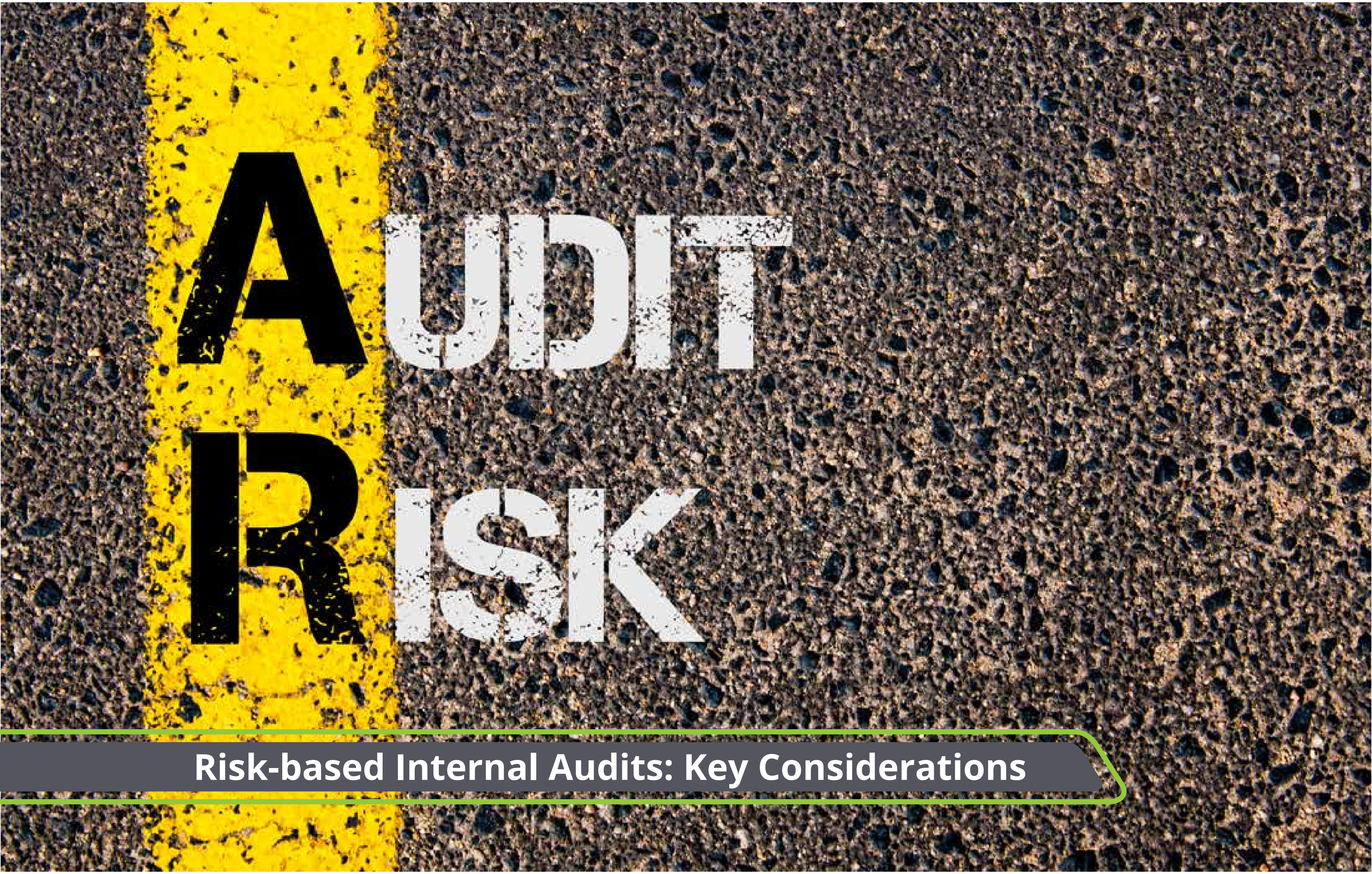
MetricStream
PERFORM WITH INTEGRITY



Risk-based Internal Audits: Key Considerations

In a 2018 MetricStream Research survey, internal auditors reported that one of their top three priorities is to strengthen risk awareness i.e. provide more timely insights on risks. While risk identification is ultimately a management responsibility, internal auditors play a pivotal supporting role by using their evaluations of organizational processes and controls to highlight critical risks that could hinder the achievement of business objectives, while also providing assurance that both existing and emerging risks are properly controlled and monitored.

To achieve these objectives, a continuous, risk-based audit program is essential. It enables auditors to proactively identify potential risks, fraud, errors, and areas of improvement. It also ensures that audit engagements and resources are efficiently prioritized.

Here are a few key points to consider while conducting risk-based internal audits[1]:

Understand the Business, Its Objectives, and Risks

Unlike a checklist-based audit which evaluates compliance with a specific set of requirements, a risk-based audit has a broader scope, and requires an understanding of organizational strategies, goals, and objectives. Auditors must have a thorough knowledge of the business, including its strengths, weaknesses, and challenges, so that they can plan their audits to focus on the most critical risk areas.

A good place to start is by identifying key business objectives and associated risks. Based on that, audit engagements can be prioritized and scheduled to provide insights on where controls are adequate with respect to those risks, and where they are not. Risks across the organization must be considered, be it legal, compliance, IT, or technology risks. Auditors must dig deep enough to identify the most significant business risk or risk category that could impede a project's ability to meet its objectives. They must also check that stakeholders are incorporating risks into decision-making and strategic planning processes.

Another important area to evaluate is the company's readiness to deal with the unexpected. Auditors need to determine if there are well-defined steps or controls in place to manage potentially significant changes that could impact the overall internal control system. For instance, what happens when management identifies a deficiency in their own processes? How do they address it, what actions do they take, and whom do they inform? Posing these kinds of questions helps auditors determine how prepared the organization is for change.

Takeaway: Identify the most significant drivers of the business and use those as parameters for measurement within a risk-based audit.

[1] Based on a MetricStream hosted webinar - **Is your Organization Ready for RBIA?** Featuring Lynn Fountain, GRC Consultant, Trainer, Author, and Former Chief Audit Executive along with Nisha Sharma, Senior Manager, MetricStream

Get Management Involved

While designing a risk-based auditing and monitoring program, internal auditors would do well to work closely with senior leadership and management teams to align business strategy, risks, and issues with the audit mission. Regular opportunities for dialogue and communication allow internal auditors to utilize management's assistance in conducting a true "risk assessment" of various business areas, while also understanding risk tolerance and thresholds.

Emerging risks should be identified in a collaborative manner with management teams. In fact, senior leadership must participate in and agree on high-risk priorities for the audit plan. Given that they are ultimately the "owners" of risk, they are likely to have already identified emerging risks that could threaten the organization. Transparency and ongoing communication are key in ensuring that audits are optimally designed to focus on the most important risks.

More than 20% of the respondents polled in a December 2018 MetricStream webinar reported "lack of management support" as one of the key challenges in a risk-based internal audit.

Takeaway: Ensure that the internal audit function has a "seat at the table" to gain timely insights on strategies. They must be involved in the communication chain on emerging risks across the organization.

Determine Management's Risk Tolerance and Appetite

Risk appetite or acceptable risk is the amount of risk exposure that a business is willing to accept. Stakeholders must set risk thresholds to identify when and where controls need to be implemented. This process is essential in distinguishing between those controls that are "nice to have" and those that are necessary to protect business functions.

For auditors, the first step is to identify and understand the risk management policies in place, as well as the risk appetite at the organizational and individual process levels. Next, determine the risk tolerance of the management and board, and use them as a starting point for independent risk assessments.

This approach of leveraging true risk appetites and tolerance levels adds credibility to the process of audit issue management. When auditors understand management's "tolerance," they can better identify a control gap that is about to breach the tolerance threshold, and flag it as a critical issue for reporting.

Takeaway: Understanding management's risk appetite helps you focus on the key issues to report, while also supporting risk-informed decisions.

Assess Risk Impact and Likelihood

Once the key risks have been identified, they need to be assessed to determine their likelihood and impact on the organization, as well as management's ability to mitigate these risks. Internal audits should assess the effectiveness of defined processes and determine whether or not management is appropriately addressing the most significant risks. The results can then be used in the audit planning activity as well.

Every organization will have a different attitude to risks. Therefore, risk assessment parameters should be defined based on each organization's own unique needs. However, there are a few universal practices to keep in mind:

1. Define risk impact using both quantitative and qualitative methods, while taking into consideration the factors that affect the organization the most (e.g. regulations, shareholder and community expectations).

2. When defining risk likelihood, clearly establish the overall range of values or level of categories. Try to use more levels, if possible, and describe them qualitatively. Include any or all values that could possibly be encountered, so that situations can be differentiated easily.

3. Ensure that assessments include all aspects of risk for a specific business area. Examine critical points in the process to ensure that they have relevant and effective controls in place.

4. Make sure that control tests are designed to adequately cover probable concerns. Ensure that testing processes are well documented with supporting documents or evidence. Enable exceptions to be validated if needed.

5. Be prepared to present and verify all conclusions, audit findings, reports, and corrective action plans to the management.

Takeaway: First, identify the categories that will be used to measure risk (e.g. reputational issues, health and safety issues). Then, put "words" to the categories.

In a Nutshell

Internal auditors, by virtue of their understanding of risks and controls across the enterprise, are well-positioned to not only help organizations enhance operational efficiency and compliance, but also drive better business performance. Through risk-based internal audits, they can be the strategic advisers that the business needs them to be by delivering timelier, deeper insights on risks, as well as advice on how to respond to issues. Armed with these insights, stakeholders can take proactive steps to catalyze business growth in a way that is true to their risk appetite, values, and integrity.