Inside the internal audit

The true value of the internal auditor

By Carrie Connell and Cayci Branum

Businesses continue to face elevated levels of risk as they not only invest in new technology but also expand their products and services to drive new revenue streams. In addition, the COVID-19 pandemic and an onslaught of accounting and operational challenges is further elevating the risk profile of many organizations.

To respond, the internal audit function is being called on to play an elevated role in risk management, control and governance processes. More than ever, leaders are looking to internal audit for a wider scope of risk assessment and fresh insight on corporate strategy.

In this white paper, we're going to review the internal auditor role, from baseline best practices to evolving expectations.

WIPFLI

Table of contents

The responsibilities of your board and audit committee

Internal audit starts at the very top.

Your board of directors is responsible for creating a risk management culture. The tone at the top is critical, since middle management and staff will take their cues from your senior leadership.

In regulated industries, regulators have made it clear that responsibility ultimately sits with the board. (Specifically, while leadership cannot delegate responsibility for risk management, they can delegate the design, implementation and monitoring of internal controls.)

The same top-down approach should hold true in nonregulated organizations. In strong risk management cultures, leaders communicate buy-in and support around controls and compliance.

So what makes up a strong risk management culture? Organizations with strong risk management cultures demonstrate the following:

- They perform ongoing risk assessments to identify changing risk areas, and they update audit schedules to reflect those risks accordingly.
- They hold company-wide training that incorporates ongoing risk management education.
- They ensure open lines of communication (top down and bottom up) to discuss any deficiencies, opportunities for improvement or corrective actions.
- They hold regular internal audit committee, enterprise risk management and/or board meetings to discuss risk management. This involves active group review and discussion, not simply providing a report in a packet or email.
- They track audit failures to a specific employee, department or product, and they take corrective action and hold additional training to address the issue and ensure understanding.
- They pay ongoing attention to emerging software capabilities to determine whether opportunities to mitigate the risk of human error exist.

The importance of the risk assessment

Every internal audit has a foundation, and that foundation is the risk assessment.

A risk assessment helps identify your organization's existing internal controls and develop the internal audit plan.

This is a high-level look at your organization's risk and should be a living, breathing document that evolves throughout the year with changes to your organization's risk profile. The risk assessment should be approved by your audit committee each year, along with the coming years' audit plan.

At its core, the risk assessment focuses on two elements: inherent risk and residual risk. However, we also recommend your organization evaluate risk direction.

- Inherent risk: The risk assessment identifies management's and the board's perceived level of risk from an inherent perspective. Inherent risk is defined as the risk that an activity poses if no controls or other mitigating factors are in place.
- Residual risk: The next step is to look at the controls in place to mitigate those risks and assign a residual risk. Residual risk is defined as the level of risk remaining in a business process or activity after considering the internal controls and risk management system. The residual risk is what's going to drive the internal audit plan.
- Risk direction: This signifies whether the risk environment for the respective business/audit area is stable, increasing or decreasing. Factors that may impact the direction of risk include regulatory changes, the introduction of new products and services, the competitive landscape, changes to information systems and turnover of key management personnel.

Categorizing areas of risk

One way to approach the risk assessment process is to break out risks by significant business area. Organizations that are new to risk assessments may begin at the department level. But as your risk assessment capabilities mature, you should look deeper into the risks that go along with different products or service lines.

You might have a heavy concentration of your business in a particular area, or you might handle more sensitive information, so it's important to think about those things when doing a risk assessment.

We also recommend the internal audit teams compare risk against their organization's strategic plan. There may be an area in which the organization does little business now, but if you believe you're going to be doing more in that area, you can begin adding it to your internal audit plan — proactively helping to keep your organization prepared.

Scheduling reviews

The results of the risk assessment then drive the plan for how frequently each area is tested. In general, high-risk areas should be reviewed annually, moderate-risk areas audited every other year, and low-risk areas audited every third year. Keep in mind that regulated industries may need to override some risk assessment results to ensure frequency of audits remain in line with regulator expectations.

How internal audit helps you think strategically about risk

The internal audit role continues to evolve. Traditionally, internal audit serves an inspection role, policing financial controls and regulatory compliance.

But the Institute of Internal Auditors is pushing organizations to think beyond mandates to more effectively anticipate and respond to evolving risk scenarios. So, too, are savvy leaders who are looking to derive greater value from the internal audit function.

Given the ever-evolving scope of risk facing businesses today, internal audit has the opportunity to become a value-added business partner. They can do this by playing a larger, more holistic role in helping organizations think strategically about a broader range of potential risks. These risks include:

Macroeconomic risks:

- Geopolitical conditions
- Labor issues
- Interest rates
- Digital transformation

Strategic risks:

- Differentiation, business model stagnation
- Culture issues
- Aging customer base
- Retaining top talent
- Industry M&A trends
- Competition
- Growth plans

Operational risks:

- Cybersecurity
- Supplier scarcity
- Vendor outsourcing
- Talent retention, succession planning
- Performance management
- Business continuity and crisis response

Regulatory risks:

- Environmental, safety and privacy
- Corporate governance
- Tax compliance
- Local, state, national and international

Reputation risks:

- Cybersecurity
- Environmental, social and governance practices
- Leadership conduct
- Social media
- Crisis response

"A mature, modern internal audit function can move beyond assurance issues to play a more proactive role in identifying a wider scope of strategic risks."

Internal audit has the responsibility for helping the board and senior leaders understand risk within the organization. A mature, modern internal audit function can move beyond assurance issues to play a more proactive role in identifying a wider scope of strategic risks — thereby improving business processes and helping the organization maintain a competitive position.

Internal audit's role in cybersecurity

Cybersecurity is a critical focus for organizations. As data breaches make headline news on a regular basis, organizations tend to think about cybersecurity in terms of protecting customer data. And it's true that a loss here comes with very real costs to your business — both in terms of reputational damage and the tactical costs of responding to a breach.

Equally important, however, is the need to protect your financial assets and competitive business intelligence from hackers out to steal from you directly.

A mature internal audit team will have some level of expertise in auditing IT systems and managing risk according to industry best practices and cybersecurity risk frameworks. Organizations with less-developed programs and internal resources can look to outsourcing and co-sourcing arrangements to assess their cyber risk environment.

Areas of focus for a cybersecurity audit include:

1. IT governance

IT governance communicates the rules and responsibilities used to monitor and control cybersecurity. It includes the organization's formal policies and procedures as well as proper board oversight and awareness of their role in the security culture.

2. Security administration

This defines how user access is granted, changed and revoked. Security administration helps ensure that access is set up appropriately based on job responsibilities and is updated as an employee's role changes.

User access should be reviewed at least annually to ensure user access remains appropriate, terminated user accounts have been removed and administrative rights remain appropriate.

3. Logical security

Logical security controls protect computer systems and data from unauthorized access. Logical controls include passwords and multifactor authentication. Here, internal audit can evaluate whether password parameters meet best practices for length, complexity, expiration, history and account lockout rules and whether those parameters are being consistently applied across all applications and the network.

4. Physical security

Physical security restricts access to areas containing sensitive IT systems, including server rooms, data centers, wire rooms, co-location facilities and general business offices. Physical controls can include locks, card access, visitor management procedures, video surveillance and alarms.

5. Operations

Operational security evaluates the effectiveness of your controls (i.e., whether controls are designed properly and functioning as they should). Audit activities here may include ensuring data backups are performed regularly and testing access controls.

6. Change management

Because any change in an IT system could impact company operations, organizations must impose and enforce careful change management procedures. This includes, for example, determining that changes to applications and infrastructure are properly approved, tested and implemented; that backout plans and version controls are in place; and that software systems are adequately supported by the vendor.

How to use internal audit resources effectively

It's the rare business today that can spend unlimited resources on risk management. Internal audit is most effective when its resources align with organizational strategy. That means making sure your organization is focused on its highest areas of risk, as should be identified through the risk assessment process described earlier.

In addition, consider how much of the internal audit area your organization can handle in-house and where outsourcing or co-sourcing would provide greater effectiveness. Considering the range of skills needed to verify controls and maintain compliance, outside support may be more affordable than trying to recruit, train and retain the type of internal specialists an organization needs to maintain a self-sufficient internal audit team.

Recognize that some degree of outsourcing may be necessary to provide your audit committee and the board with adequate assurance in cybersecurity and other key risk areas.

Advantages of outsourcing your internal audit:

- Specialization, access to scarce skills
- Independent perspective, unbiased reporting
- Benchmarking
- Guided coaching for in-house audit team
- Potential for cost savings and greater value versus employee overhead

Potential drawbacks to outsourcing:

- Challenges of defining scope
- Risk of confusion over accountability

When outsourcing or co-sourcing, leadership must be clear about responsibility and accountability. Organizations can outsource risk management tasks but not, ultimately, risk responsibility. Clear communication, formal reporting and approval processes are essential when internal audit functions are outsourced.

What to do with your internal audit findings

Managing the internal audit process requires follow-up and accountability. Inevitably, your internal audit will uncover areas of weakness and ineffective controls that need to be remediated. But how do you make sure those tasks are actually addressed before they crop up again as a repeat finding in the next audit?

For many small and medium-sized organizations, an audit tracking spreadsheet can be a sufficient, effective management tool. This spreadsheet should note the following:

- Date of review
- Person who conducted (internal, regulator, third party, IT audit)
- Date presented to the board of directors or equivalent committee
- Finding/recommendation
- Risk rating
- Management response

For each finding, note the following:

- Finding owner
- Remediation/action plan if applicable
- Remediation/action plan expected completion date
- Explanation if remediation was not completed by the due date

This audit tracking document should be reviewed at each audit committee meeting to ensure the audit committee stays abreast of the status of the audits and is able to effectively question processes and controls. The audit tracking document also serves to keep your team continually engaged in remediation timelines and keep action plans on track. Without an effective process to track the status of audits and the resulting findings and remediation plans, inadequate follow-through may reflect poorly on the internal audit function, and the value of internal audit activities can come into question.

Common pitfalls for internal audit programs

Some of the biggest weaknesses in internal auditing stem from the same few mistakes. Strengthen your program by avoiding these seven common missteps:

1. Stale audits

When pressed for time and attention, many organizations fall into the habit of repeating last year's audit activities without rescoping. It's important to look at how the business changed over the last year (and what changes are imminent) and adjust your audit plan accordingly.

Every year, ask yourself questions like these:

- How has the business changed?
- Does the business plan to add any significant operations (e.g., M&A, new business lines, key initiatives)?
- Is the business subject to any new regulations or standards?
- Are any current conditions hindering our risk management efforts?
- What new methods of attack and theft are emerging?
- Did we perform any audit procedures last year that we no longer need?
- Are we going deep enough to find problems?
- How could our work add more value?

2. Cookie-cutter audits

You can find internal audit checklists and templates online, and these can be great tools for starting an audit conversation in your organization. But they can also lead to a false sense of security and limit real consideration of the risks in your unique environment. Moreover, they can be a poor use of resources, leading your organization to audit too much and/or focus on low-value work. If you want a substantive audit, you have to tailor your process to your distinct risk environment.

3. Repeated findings

This indicates a lack of follow-through and follow-up. Repeat findings can occur for many reasons, such as lack of understanding regarding the scope or complexity of the issue, lack of resources or managers who don't value internal controls. Repeat findings indicate increased risk. Leadership needs to understand and clearly accept that risk, or they need to allocate resources or enforce accountability for change.

4. Siloed risk management

Help your top-line leaders avoid a dangerous case of "audit fatigue" by coordinating internal audit, compliance and risk management activities. One way to do this is to assign a point person to track and coordinate all risk management activity. Set up regular meetings among your internal audit, compliance and assurance functions to share information, align risk priorities and reduce redundancies.

5. Missing out on system capabilities

System access, segregation of duties, signoffs and authorizations — a lot of this can be managed and automated by modern enterprise-wide software. If you're not sure how your software systems can help with internal controls, reach out to a system consultant and find out how to maximize the tools you already have.

6. Ineffective communication

Boards that are provided education on risks are engaged, if it's presented at the appropriate level. The focus must be on business risks and not on reviewing the intricate details of technical exceptions. The better the board understands the issue, the easier it is to build buy-in and secure meaningful participation in the risk management process.

7. Top-down (only) risk management

Senior leadership is ultimately responsible for risk management and should actively set their level of accepted risk tolerance as part of the risk assessment. That said, a key part of internal audit's role is to manage up. If the audit committee is not satisfied with leadership's response to audit findings, they need to be questioning that response and considering whether outside expertise or a different communication approach is warranted to influence leadership and better protect the organization.

"In doing so, the internal audit committee can transform from an 'obligatory' cost center to a value-added role as advisor."

Adding value to your internal audit

Internal audit can be only as effective as leadership and corporate governance allow it to be. And yet managing up allows the audit committee to ensure they are not submitting the organization to undue levels of risk exposure.

The value added by internal audit begins with moving beyond a reporting role to actively oversee risk mitigation.

Internal audit can and should manage timetables and monitor the resolution of internal findings and recommendations. If findings are not addressed and resolved by the appropriate parties, no real change happens — and the internal audit function could ultimately be viewed as irrelevant.

Once the organization is in an established cadence of actively mitigating audit findings, the internal audit committee can go a step further to proactively identify business risks across a broader scope of the organization. In doing so, they can transform from an "obligatory" cost center to a value-added role as advisor.

Wipfli can help you make this transition a reality.

Our experienced auditors work with your internal audit team to:

- Help you identify the areas of highest risk within your organization and build a risk-based internal audit plan that ensures internal audit time and dollars are spent in the areas with the most impact.
- Discuss controls with your process owners, test for compliance with established controls, and provide real-world examples and industry best practices tailored to your organization.
- Save you time and money by supplementing your internal team when necessary to ensure your internal audit plan is completed.

Learn more about the insights you can gain and the risks you can mitigate with internal audit support from Wipfli.

wipfli.com/ia

WIPFLI