IIA Malaysia e-techline
March 2019 Issue 02/19

INTEGRATING FRAUD TESTING INTO YOUR AUDIT PROGRAM: A GUIDE FOR CHIEF AUDITORS

There are four fundamental approaches to integrating fraud detection into the audit program.

1. **Prepare a Fraud Risk Assessment.**

Adopt a methodology for writing fraud risk statements. The fraud risk statement should provide clear guidance on how the fraud scheme lives and breathes in the core business systems. Use the fraud brainstorming session to discuss how to detect the frauds detailed in the fraud risk statements. The fraud risk statement provides a focal point for the conversation, generating much more meaningful discourse than a general discussion of fraud. Discuss the natural vulnerabilities associated with your internal controls.

2. **Perform Internal Control Testing and be Alert to Red Flags.**

Identify actual red flags on documents, data, and internal controls that link to a fraud risk statement and document them in the audit program. Discuss the concept of the sophistication of fraud concealment and consider how it impacts the audit program.

3. **Integrate a Fraud Test into the Control Testing.**

Design a fraud test that targets the fraud risk statement. The fraud test rules: (1) If the scheme involves a false entity, design an audit step that suggests the entity is false; (2) If the entity is real, than design an audit step that targets the fraud action statement. The intent of the audit step is not to prove fraud but rather to prove the need for a fraud investigation.

4. **Create a Fraud Program.**

Allocate the resources to build a fraud data analytics program for your core business systems. To accomplish this, you must do more than just buy the software. You must also improve your fraud risk assessment and understand the difference between a control test and a fraud test.

What CAE should do?

It is time for the auditing profession to become the number one reason for fraud detection. Our profession has the talent to detect fraud; what we need now are the tools designed to detect the fraud risk statements lurking in our core business systems.

Integrating fraud into our audit program requires a different way of thinking about our audit process. Here offer the following goals for senior audit management:

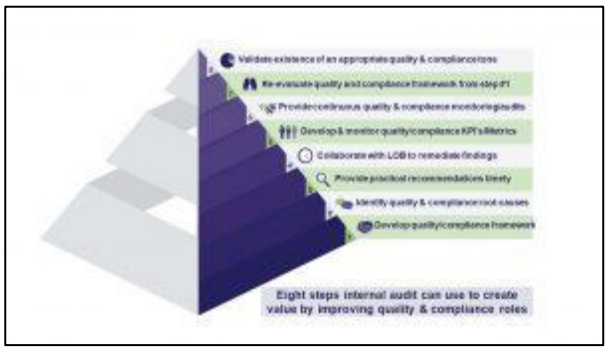
- Recognise fraud auditing as a technical skill.
- Adopt a methodology designed for fraud detection.
- Aggressively invest in building fraud data analytics.

Educate your audit committee and management on the difference between control testing and fraud testing.

Reference:
https://misti.com/internal-audit-insights/integrating-fraud-testing-into-your-audit-program-a-guide-for-the-chief-auditor

HOW INTERNAL AUDIT CAN BOOST QUALITY AND COMPLIANCE

There are eight primary steps internal audit teams can apply throughout an organisation in collaboration with other stakeholders to create and sustain value by improving quality and compliance. They include:



1. Evaluate quality and compliance effectiveness efforts using a framework

The emphasis here is on the specific framework used by an internal audit function to validate that business lines are meeting their respective quality and compliance expectations efficiently and effectively. It is important to ensure any framework adopted—whether it is Lean, Six Sigma, Total Quality Management (TQM), or others—must address issues unique to each operation and how each function contributes to the enterprise-wide quality and compliance success. Addressing quality and compliance efforts in silos without alignment to enterprise-wide objectives is not an efficient approach.

2. Identify root causes of quality and compliance problems

A generic internal audit approach to quality and compliance reviews without hands-on experience and expertise to apply issues unique to that operation will frustrate business unit managers. Such an approach will often result in an inability for internal audit to identify and communicate root-cause of issues from Step #1. Instead, internal audit will spend more time addressing symptoms.

3. Provide cost-efficient recommendations to address quality and compliance problems quickly

Internal audit must demonstrate a level of expertise needed to gain trust, challenge the status quo, and provide practical, cost-effective recommendations that can be implemented by each function to address quality and compliance issues in a timely manner. Obviously, quality doesn't exist in a vacuum and quality improvement decisions must be made with regard to pre-determined price points, time-to-market targets, and other factors that achieve enterprise-wide objectives. This is important for internal audit to gain trust from the stakeholders.

Technology also plays a big role in the assessment and achievement of quality and compliance, and internal audit must keep up on the systems and software that can influence quality. As organisations move towards improving efficiencies through technology and automation, the quality and compliance requirements becomes increasingly important. Configuration and programming errors, or the lack of adopting a new technology, can present significant risks and potential financial loss. Internal audit can and should play a role in the assessment and implementation of new technology that can impact quality and compliance.

4. Collaborate with to remediate findings and implement recommendations

Once trust is earned, and stakeholders see value in the work performed to improve enterprise-wide quality and compliance initiatives, collaboration to remediate findings and implement sustainable recommendations is the logical next step.

Internal audit must collaborate with LOB leaders without compromising independence. The significant cost incurred by the Wells Fargo fiasco serves as a good example to challenge the status quo on internal audit independence expectations and increase the level of support to address potentially significant quality and compliance violations quickly. To increase sales by cross-selling products and services, Wells Fargo failed to identify quality and internal audit compliance issues as employees opened accounts

... 2

services, Wells Fargo failed to identify quality and internal compliance issues as employees opened accounts without customer permission, resulting in negative publicity that began in 2016 and will require several years for the bank to resolve.

Efforts from internal audit to support remediation of findings should also include education and training to LOB managers, stakeholders, and executives on standards, laws, and regulations. Training should be tracked, attested to, documented, and refreshed periodically.

5. Develop quality and compliance Key Performance Indicators ("KPI") and metrics

Internal audit can collaborate with each line of business Point of Contacts (POC's) to identify quality and compliance issues unique to each operation and create KPI's and metrics that align each LOB function to the enterprise-wide objectives to avoid performing tasks in silos.

6. Provide continuous quality and compliance monitoring and auditing

The quality and compliance requirements for many organisations are not static. The dynamic nature of quality and compliance operations means a static once-a-year internal audit review of key LOB effectiveness will not achieve intended effects. Performing continuous quality and compliance monitoring and auditing could identify issues missed during previous reviews and provide the organisation enough time to implement corrective actions, and, if needed, self-report to minimise impact of any potential regulatory fines and reputational damage.

7. Re-evaluate the quality and compliance assessment framework

A good reason to make changes to the internal audit framework is if existing quality and compliance violations are not remediated quickly, or new significant issues are not identified.

We could anticipate Wells Fargo made significant changes on how their internal audit function performed quality and compliance effectiveness reviews after the negative publicity that began in 2016. Such changes were significantly late as the bank suffered substantial losses from regulatory fines and reputational damage.

8. Validate existence of an appropriate quality and compliance tone

Internal audit must perform reviews to validate existence of an appropriate quality and compliance tone and reporting structure to executives and board committees. Is quality and compliance baked into the culture of the organisation? Without this, any organisation remains vulnerable to quality lapses and even excessive regulatory fines and reputational damage.

What internal auditors should do?

Internal auditors should perform all 8 points highlighted in order to boost quality and compliance.

Reference:
https://internalaudit360.com/how-internal-audit-can-boost-quality-and-compliance/

CYBERSECURITY AND REGULATORY CHANGES IN 2019

The developing cybersecurity regulatory landscape is continuing to gain momentum as the number of industries impacted increases.

What are some expected challenges for information security professionals?

1) The Infancy of Cybersecurity Regulations

As with any new law that has not yet been enforced by a regulator, there is much uncertainty as to which elements of these cybersecurity laws regulators will prioritise. Even industries which have already been subject to cybersecurity regulations cannot expect the exact same experience with new regulators. Until precedent is set with a series of publicly known enforcement actions and fines, audit and security professionals will need to use their judgment on where to focus on compliance efforts, especially if meeting all regulatory requirements is not achievable by the effective date.

2) Going from No Law to Strict Law

Although there are many information security ("infosec") professionals who work for organisations that have been subject to cybersecurity regulations, there are many who have not had this experience. The challenge for the latter will be implementing cybersecurity controls that were not previously required, while also learning to efficiently and effectively demonstrate compliance to regulators.

3) Educating the Executive Committee

Although keeping the executive committee educated and informed has been a task for infosec and audit department for years, new regulations will raise new questions. Regulatory compliance has been and will continue to be an increased focus area for organisations, especially because of the risk of large fines for non-compliance as demonstrated by organisations. Infosec professionals will need to thoroughly understand the top requirements of new cybersecurity regulations and be able to give executives comfort that these are being met.

Why are cybersecurity regulations increasing?

1) Protection of Personally Identifiable Information

The increasing frequency of news headlines about companies whose insufficient cybersecurity controls have allowed unauthorised party access to customers' personally identifiable information has not gone unnoticed by consumers or lawmakers. The public's interest for better protection of their personally identifiable information was actually one of the many drivers of enforcement for cybersecurity regulations.

2) Confidentiality of Company Proprietary Information

Manufacturing companies spend large amounts of money on research in development to create and enhance their products. If a company is maliciously infiltrated and product design secrets are stolen, this gives the ability for others in possession of the stolen information to manufacture the same product but at a cheaper price, inevitably resulting in lost business for the company that was hacked. This type of event is also especially concerning for defense contractors who contribute to national security, as other countries can gain warfare advantage when they possess this type of knowledge.

3) Stability of Economies

Traditionally financial institutions have been the targets of hackers searching for financial gain. When a company would once suffer a direct financial loss from a successful hacking attempt, hackers are now searching for other confidential information in order to maliciously manipulate a market, which could have a larger downstream impact on an economy as a whole.

What internal auditors should do?

Both internal auditors and security professionals will need to keep an eye on how 2019's cybersecurity regulatory changes unfold, both those that are currently known, and those to come.

Reference:

https://misti.com/internal-audit-insights/cybersecurity-and-regulatory-changes-in-2019

5 INTERNAL AUDITOR RESOLUTIONS FOR 2019

Richard Chamber's had shared Top 5 Resolutions for 2019. This year's list of resolutions reflects the rapid and almost continuous change that the profession is experiencing. Now, the internal auditors must be aware, attuned, agile, innovative, courageous, and committed.

1. **Keep Your Head Out of the Sand and Take On Difficult Risks**

Stakeholders are demanding more of us. New, technology-driven risks are requiring us to be agile and innovative. That same deluge of technology also offers us new tools — from robotics process automation to artificial intelligence — that require us to quickly adopt and acquire new skills.

We have an obligation to our organisations, to our professional Standards, and to ourselves to be ever vigilant for new and emerging risks, step up to the challenge, and deliver unassailable, independent assurance services.

2. **If You See Something, Say Something**

We must be willing to step up and speak courageously when we see behavior that's potentially harmful or creates risks, even when involving top executives. In addition, if we notice internal audit colleagues taking shortcuts that could undermine the accuracy or credibility of an internal audit, we should not hesitate to say something. I plan to expand further on this theme in an upcoming blog.

3. **Sharpen Your Technology Tools**

Richard's believe there is little room for debate that technology is one of the primary drivers of risk. Cybersecurity and data protection consistently rank at the top of risk profiles from our stakeholders, and the pace of technology-driven change shows no signs of slowing. That's why internal auditors must become fluent in technology. We must recognise and address the risks that technology presents in our organisations and embrace technology in serving our organisations. No practitioner can afford not to.

4. Expect the Unexpected

Internal auditors must be agile and prepared to pivot quickly when the unforeseen occurs. This correlates with the resolution on speaking out. While emerging and atypical risks are not generally part of internal audit's scope of work, it does not release us from our obligation to speak out on emerging or atypical risks.

5. Be Mindful that You Remain Aligned

It has become cliché to say stakeholders don't like surprises and that internal auditors should know what keeps management and the board up at night. While clichés, they do remind us about the importance of being aligned with the needs and expectations of our stakeholders – particularly board members.

What internal auditors should do?

1. To leverage audit committee relationships to make certain internal audit remains aligned with the board's view on risks.

2. To work with executive management to get a clear understanding of strategic and operational priorities and align internal audit's efforts to support those priorities.

3. To respond to changing demands in IT, data analytics, artificial intelligence, and other areas by investing in the improvement, expansion, and alignment of our skills to meet the needs of the organisation.

4. To examine how changing demands and pressures to perform align with conformance to IIA *Standards*.
To align our work effort to deliver on internal audit's mission to provide service that enhances and protects organisational value.

Reference:
https://iaonline.theiia.org/blogs/chambers/2019/Pages/5-Internal-Auditor-Resolutions-for-2019.aspx

AUDITING THE SUPPLY CHAIN IN 2019: WHAT TO KNOW AND WHY

Supply chain audits present an opportunity for internal audit teams to look at the supply chain organisation and make sure they are doing things to control costs and mitigate risk factors.

A first step is identifying supply chain risks. We have broken down some of the common ones below:

1. Working with Vendors and Third Parties

A supply chain audit should check that the organisation is working with vendors that offer quality work at competitive prices and that it complies with relevant regulations.

2. Contract Management

Once an organisation's vendors have been vetted and contracts are in place, the focus shifts to contract management. This often requires gaining clarity over which department usually, purchasing or the business unit is responsible for managing the contracts and monitoring vendor performance. Audit's main concern is that ownership is clearly determined.

3. Data Protection and Cybersecurity

With many companies linking electronically to their vendors, the risks of software supply chain attacks increase, says Bernie Donachie, managing director and leader of the global supply chain practice with Protiviti. To test this, auditors can review what data is accessible and who has access to it.

4. Geopolitical Risks

Geopolitical conflicts can disrupt trade routes, while changes in trade agreements and tariff schedules can increase costs, or even force companies to identify alternate sources of supply. Internal audit can consider ways to mitigate these risks. For instance, has the business unit identified other suppliers in case an issue arises with a country or its currency?

5. Challenges of Auditing Supply Chains

There is the number of processes, from purchasing to warehousing and contract management, contained within a supply chain. Due to time and resource constraints, audits often focus on one segment, which makes it challenging to get a holistic view. Moreover, because the processes are interrelated, identifying the root cause of a problem can require continual digging.

6. Approaching a Supply Chain Audit

Supply chain audits can require visiting vendors, factories, and warehouses to, for instance, physically check the inventory and to make sure the business actually exists.

Because these risks can impact departments throughout an organisation, such as legal and human resources, a cross-functional team usually is also required to identify, prioritise, and decide how to mitigate them.

What internal auditors should do?

Auditors need to be well versed in current affairs, macro-economic trends, and trade agreements, among other subjects.

In addition, given the growing complexity of many supply chains, their audits are likely to increase in both scope and number.

As strong supply chain auditors, they need to understand the business and the environment in which it operates and can work with individuals across the organisation who can help identify supply chain risks and develop response plans.

Reference:
https://misti.com/internal-audit-insights/auditing-the-supply-chain-in-2019-what-to-know-and-why

NEW IMPLEMENTATION GUIDANCE FOR THE CODE OF ETHICS

The IIA has released new guidance for implementing its Code of Ethics. Each of the four Code of Ethics principles -- Integrity, Objectivity, Confidentiality, and Competency -- is accompanied by specific rules of conduct. Four Implementation Guides explain what internal auditors need to know to implement each principle and rule of conduct, and how to show conformance as part of a quality assurance and improvement program.

Access now via https://na.theiia.org/standards-guidance/recommended-guidance/Pages/Practice-Advisories.aspx

... 6

PRACTICE GUIDE: ASSESSING THE RISK MANAGEMENT PROCESS

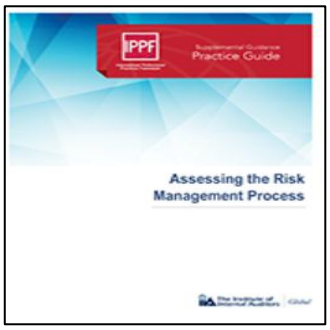
Risk management activities and initiatives are required and expected by regulators, rating agencies, and stakeholders in major industries around the world. However, risk management is driven by more than regulations and external forces; organisations of any type and size could benefit from implementing a risk management process to help increase entity value, achieve operational and strategic objectives, and safeguard stakeholders.

This guide will aid the internal audit activity in developing approaches to review and assess the effectiveness of an organisation's risk management processes and strategies, regardless of the activity's size, maturity level, or resource level.

It also discusses how internal audit may influence the positive side of risk, providing insights to senior management and the board on how organisations can discover and embrace potential missed opportunities.

This guidance will enable internal auditors to:

1) Understand the need to perform audit engagements of risk management activities.
2) Understand the key components of an effective risk management process.
3) Develop an approach taking into account the business environment, the level of maturity and regulatory environments.
4) Collect the necessary information to determine the scope of the audit engagement of risk management activities.
5) Evaluate the effectiveness of risk management processes.
6) Contribute to the improvement of risk management processes.

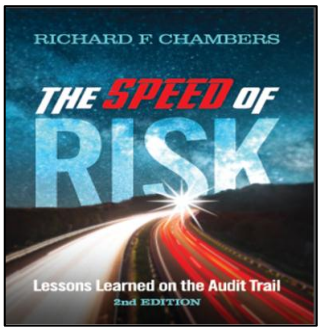


Reference:
https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Assessing-the-Risk-Management-Process-Practice-Guide.aspx

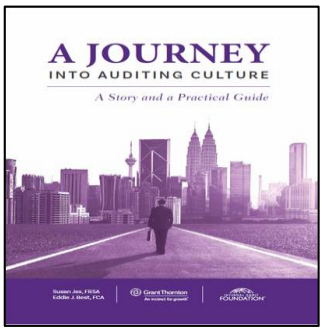
BOOK'S REVIEW

NEW RELEASE! **PRE-ORDER NOW**!!!

1) **The Speed of Risk: Lessons Learned on the Audit Trail, 2nd Edition**



2) **A Journey into Auditing Culture**



Reference:
https://www.iiam.com.my/wp-content/uploads/2017/08/Book-Order-Form.pdf