Emerging Trends in Internal Audit

May 2019
Fasten your seatbelts... Your feature awaits!
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.
In a snapshot

Competing in a rapidly changing world, companies must grapple with emerging challenges seemingly every day: cyber threats, emerging and potentially disruptive technologies, business performance risk and more. In this increasingly complex environment, Internal Audit ("IA") has a crucial role to play to help the organization in managing risks associated with these diverse business trends.

An impactful IA function will stay current with these wide-ranging business issues as they emerge so it can help monitor related risks and their potential effects on the organization. To provide the greatest value, IA must find opportunities to challenge the status quo, to reduce risk, improve controls and identify potential efficiencies across the organization.

Source: KPMG Internal Audit: Top 10 in 2018. Considerations for impactful internal audit departments, KPMG International
In a snapshot

Definition of Internal Auditing

“Internal auditing is an independent, objective activity designed to add value and improve an helps an organization accomplish its objectives by disciplined approach to evaluate and improve the management, control, and governance processes.”
In a snapshot

In the ever-changing risk landscape, IA is evolving from a cycle of reactive audits to predictive and value adding assurance activities. Internal audit must respond to the challenge of managing IA costs while reacting to the challenges posed by the emerging market conditions.

- **Hindsight (Reactive)**
  - Traditionally IA focused on past events.

- **Insight**
  - IA currently focuses on how to mitigate existing risk.

- **Foresight (Progressive)**
  - Future perspective and added value.
    - IA teams will now need to focus on emerging risks and trends to provide added value to an organization.
Traditional IA roles and expectations

- Manage average cost of compliance
- Focus on auditing accounting issues
- Focus on compliance with existing policies and procedures

- Market expansion
- Detection of problems and errors
- Restricted by functional lines

- Considered to be investigators
- Considered reactive as opposed to reactive
- Use of substantive audit approach
- Adversarial relationship with business areas
Current IA demands

Performance of efficient and effective audits
Diverse and dynamic skill sets
Critical thinking and judgment
Rapid identification of opportunities for improvement
Objective perspective
Strong Objective stakeholder communications
Help assessing risk and risk management practices
Embrace new technologies
A command of the use of data and analytics throughout the audit process
Rapid response to changing business conditions
Increase value from traditional business functions with measurable impact
Assessing the current of the Internal Audit Functions

Quick exercise:
Answer yes or no to the following questions to determine which phase your IA function is currently operating in. A ‘YES’ answer is an indication of a progressive IA while a ‘NO’ is an indication of a traditional IA.

Traditional  
Static  

Is your IA function able to identify improvements to the risk and control environment and key business processes or functions?

Progressive  
Dynamic  

Do you employ leading practices in performing your annual risk assessment and identifying the audit universe?

Heavily manual and sample based  

Reactive  

Do you use metrics to measure or improve audit productivity?

Status quo  

Isolated  

Are you employing data and analytics tools for advanced reporting activities?

Do you utilize a formal program or techniques to evaluate the processes within IA?

Heavily manual and sample based  

Are the business proactively asking Internal Audit to come in and conduct audits?

Data and analytics based analysis  

Continuous improvement  

Business partner
How can you maximise the value of Internal Audit?

To ensure value is derived from your Internal Audit function, the following questions should be addressed:

**Internal audit strategy**

**Company strategic objectives**
Is the IA plan aligned to the company’s strategic objectives and initiatives?

**Stakeholder expectations**
What do the stakeholders expect from the IA function?

**IA mission and charter**
Is the IA mission and charter defined and effectively marketed to the business?

**IA road map and talent assessment**
Do we have the right positioning, people and processes to meet our stakeholders needs?
Emerging Areas of Focus
What should IAFs be focusing on in modern day

- Cybersecurity
- Strategic Alignment
- Regulatory Compliance
- Integrated Assurance
- Data Analytics & Continuous Auditing
- Crisis Management and BCP
- Third Party Relationships
- Anti-Bribery/anti-Corruption
- Emerging Technologies
- Culture/Soft Controls
Cyber Security Drivers

In today’s world of constant connectivity, cyber security is a key focal point for many organisations as they require an overall framework for mitigating cyber security threats and an adequate crisis response mandate to provide much needed guidance and direction in the face of adversity. IA should play an active role in:

- Avoiding the costly consequences of data breaches
- Mitigating the risk of business disruption
- Mitigating the risk to employee safety and the organisations profitability
- Averting significant reputational damage
- Protecting security of capital, intellectual property and other privileged organisation information
- Protection from growing sophistication of capabilities and techniques used by hackers
Cyber Security Headlines

Hackers target more than 50,000 people a day with tax refund scam

Cyber crime 'cost UK residents £210 each in the last year'

At least 5 companies in Kenya have been hit by the WannaCry virus attack that has affected over 300,000 users globally amid warnings by tech experts underlining the vulnerability of local firms.

It is expected to get worse as about 80 per cent of the country’s large and small organisations’ back-up systems run on Microsoft Windows, which is the malware’s target.

This is according to IT services and business consulting firm Serlanu, which declined to name the Kenyan firms hit by what tech analysts are describing the largest ransomware attack in history.

“Almost 80 per cent of our servers are based on Windows, we have another almost 16 per cent on unix or the Linux variant and then you have other operating systems ... we are very vulnerable,” Serlanu CEO William Makatiani said Monday.

Banking shortcomings make cyber crime the consumer’s problem

Liberty refused hacking ransom demand

Hackers Demand $770,000 Ransom From Canadian Banks

Cybercrime: FBI Says Ransomware, Extortion Continue to Dominate

An excerpt from the ransom note sent to restaurants owned by Recipe Unlimited on Friday.
Cyber Security – How IA can help

- Provide advisory services to senior management and the board during strategy formulating process on emerging risks and trends.
- IA must critique the assumptions undertaken by senior management and the board in strategy formulation for relevance, practicality and accuracy.
- IA must continuously review the strategy to ensure timely detection of deviations from the intended objectives and action plans.
- IA continuously keep senior management updated on any emerging risks that might affect the implementation of the plan.
- IA must align the annual plans to the strategic initiatives for continuous provision of assurance that the attainment of the SP is still on course.
Strategic Alignment

- With the changes in the business environment in the recent past arising from globalization, a continuous meltdown and uprisings of some economies, significant shifts in technology and energy costs, and the challenges of regulatory compliance, IA should be an active participant in considering impacts to risk and related governance and controls.

- Often, efforts to bring about strategic change can sometimes neglect to revise internal controls to conform to new business models. IA brings a unique perspective to strategic change and should be present and active in key strategic initiatives.

For this reason, IA needs to ensure:

- It aligns to the company’s strategic priorities and remains relevant in light of organizational and other transformational changes
- It is involved in key strategic initiatives of the company, whether through consultation or reviewing progress/outcomes
Strategic Alignment - What is the strategic role of IA?

**It is Insightful**
- IA should provide additional insights such as advise on emerging trends that beyond what may be ordinarily known by the stakeholders

**It leverages on Technology**
- IA must adapt its methodologies to utilize technology in the execution of audits to increase efficiency and provide deeper insights into the business

**It understand the Business Dynamics**
- IA should have a profound understanding of business strategy and operations across all levels of the organization

**It focusses on Creating Value**
- IA activities should not only provide assurance but also deliver advisory services, which can be leveraged to improve business processes, manage strategic risks or gain a competitive advantage
Strategic Alignment - How IA can help

- IA must actively participate in the formulation of the corporate strategies and advise management on emerging risks and factors that might affect successful adoption and implementation of the strategy.

- IA must assess the measures in place by management to identify, measure, report and monitor risks that might affect implementation of the strategy.

- IA must continuously review the implementation of the strategy for timely detection of any deviations from the set objectives and implementation timelines.

- IA must ensure its annual and strategic plans focus more on the strategic objectives and initiatives of the company.
Regulatory Compliance

Drivers in regulatory compliance

- Companies, regardless of industry, are being overwhelmed with new regulatory requirements. These new regulations are putting increased burdens on management and compliance officers and raising the possibility that certain compliance requirements are being missed. For this reason, compliance is aimed at:
  - Ensuring compliance with a dramatically increasing number of regulations, both domestically and abroad
  - Mitigating the increasing costs of complying with this ever-growing number of regulations
  - Developing a strategy to lessen the restraining effects of compliance activities on business operations
  - Ensuring compliance operations are aligned following a merger or acquisition
Regulatory Compliance - Headlines

Five banks fined Sh392m for illegal Sh3.5b NYS transactions

In a statement, CBK said the banks were found to have been in violation of requirements stipulated under Kenya’s anti-money laundering/ combating financing of terrorism laws and regulations.

Safaricom, Airtel and Telkom Kenya fined KSh 311 million for worst services

U.K.’s Tesco Bank Fined $21.4 Million Over Cyberbreach

The Financial Conduct Authority said the cyberattack was ‘largely avoidable’ had the bank been more diligent.

(Reuters) - South Africa’s central bank on Friday fined HSBC's (HSBA.L) local business 15 million rand ($44,927 pounds) for weaknesses in its processes meant to detect money laundering and terrorism financing, and ordered the bank to fix the problems.

UK watchdog fines Tesco £16.4 million for bank cyber failings

WASHINGTON (Reuters) - The U.S. Justice Department has reached a $513 million settlement with U.S. Bancorp (USB.N) over charges that it willfully failed to have an adequate anti-money laundering program, the department said on Thursday.

Dutch bank ING fined $900 million for failing to spot money laundering
Regulatory Compliance and how IA can help

- IA should undertake an inventory of the regulatory bodies and requirements affecting the company
- IA must assess the company’s approach to managing its compliance activities, including integration of the requirements of acquired companies
- IA must evaluate the company’s response to any notable instances of noncompliance
- IA must assess whether compliance training programs offered to employees and other stakeholders are appropriate for role and geography
- IA must provide assurance with regards to the design and operating effectiveness of the organization’s compliance framework
- Ensuring compliance operations are aligned following a merger or acquisition
Data Analysis and Continuous Auditing

In the past few years, data analytics have helped to revolutionize the way in which companies assess and monitor themselves. With data analytics, companies have the ability to review every transaction, which enables more efficient analysis on a greater scale. Additionally, big data techniques enable companies to proactively identify new trends and related risks such as the early detection of social trends that will likely lead to regulatory changes. For this reason, DA and CM is crucial in:

- Enabling real-time, continuous risk management
- Increasing overall efficiency of audits being performed (frequency, scope, etc.)
- Taking a “deeper dive” into key risk areas through analysis of key data
- Enabling early detection of potential fraud, errors, and abuse
Value of data & analytics-enabled internal auditing

Added value

- Deeper insight into the business through data analysis
- Enabling real-time, continuous data monitoring
- Enhanced overall risk assessment capability through early detection and monitoring
- Enhanced visibility to potential exceptions and controls’ overwriting related to corporate reporting and other criteria and metrics monitored by the business
- Increased scope coverage of specific audits
- Adoption of risk-based testing methods instead of traditional sample testing
- Enabling early detection of potential fraud and errors

Increased efficiencies

- Increase the number of audits performed per year
- Decrease the time required to cycle through the audit universe
- Reducing costs associated with auditing and monitoring
Data Analysis and Continuous Auditing

How Internal Auditors can help

- IA must continuously monitor the business on key risks by creating an effective process for gathering, mapping, analyzing and presenting data extracted from a complex variety of information systems

- IA must promote data analytics enabled audit programs designed to verify the underlying data analysis and reporting of risk at the business level

- IA must implement automated auditing focused on root cause analysis and management's responses to risks, including business anomalies and trigger events

- IA must recommend consistent use of analytics, including descriptive, diagnostic, predictive and prescriptive elements
Integrated Assurance

The risk landscape is constantly evolving and board and senior management now expect all assurance functions to work together to provide an integrated view of the organisation’s risk profile and enable the organisation to:

- Respond to rapidly changing risk environment coupled with need for insights to make decisions;
- Streamline risk assessment and assurance activities to gain efficiencies and maximise coverage;
- Allocate limited resources towards highest risk areas;
- Identify critical risks earlier and respond effectively and efficiently; and
- Move away from traditional approaches to providing assurance over risk responses that are often siloed and uncoordinated.

How Internal Auditors can help

- Lead or support coordination of the risk assessment, planning, work execution and reporting across multiple assurance functions, thereby minimizing the footprint on the business.
- IA must develop and execute holistic assurance plans considering enterprise risks, leveraging the various assurance functions across the organization.
- IA should evaluate business implications of emerging trends and their associated risks.
- IA should utilize data and analytics to optimize insights into the emerging risk environment.
- IA should advocate for Continuous Self Assessments (CSA) by management to enhance control consciousness, enable early identification of problems and enhance IA’s audit efficiency.
Many organizations have existing crisis management plans in place. However, with the rapidly evolving business environment, the nature of crises traditionally planned for is evolving. For these reasons organizations require adequate planning covering immediate response, decision-making, recovery, communication and contingency plans for various scenarios which may suddenly arise.

In more recent times there is increased exposure to:

- Cyber security threats due to increasing implementation of digital technology
- Reputational crisis due to digital and social media platforms increasing the speed, nature and impact of information dissemination
- Financial crisis due to market volatility
- Physical crisis, including misconduct in the workplace

How Internal Auditors can help

- IA should conduct an independent review of the entire crisis management system including leaderships readiness for various crisis situations.
- IA should have a sound knowledge of the potential and emerging risks and crises which may impact their organization
- IA should acquire expertise in effective crisis management and business continuity good practices
- IA must critically analyse existing crisis continuity plans and challenge effectiveness
Third Party Relationships

Drivers

To boost productivity and adapt to changing business models, companies are increasingly relying on third parties to carry out vital business functions. However, using third parties opens up companies to new risks and potential service, compliance and other failures that can lead to fines, lawsuits, operational bans and reputational damage.

- Third party relationships are therefore important due to the need to:
  - Monitor increase in associated risks;
  - Evaluate increased staff productivity relative to the third party costs;
  - Enhance revenue while reducing costs;
  - Prevent or timely detecting risk management failures at third party business partners;
  - Improve contract and vendor governance;
  - Enhance revenue and cost reduction; and
  - Create more effective contractual self-reporting processes.

How Internal Auditors can help

- IA must review third-party identification, due-diligence, selection and on-boarding processes and control.
- IA must evaluate contract management processes used by management to track third party relationships.
- IA must monitor regulatory developments related to third-parties.
- IA must assess third-party compliance with company’s information standards.
- IA must develop, implement, and calibrate a continuous monitoring system of self reported data from third party business partners.

What outcomes are we trying to achieve?
The benefits of an effective anti-bribery/anti-corruption (ABAC) compliance program are clear. It is critical to demonstrate that the organization’s program actively identifies potential issues and initiates remediation measures in a timely manner. The program should include support from senior leadership, clear policies, training, monitoring, and oversight.

Policies that spell out prohibited activity, the commitment of executive management, audit clauses in agreements with third parties, and vigilance by compliance personnel can deter bribery and corruption, thereby reducing the risk of costly and disruptive regulatory enforcement activity. An organization can make use of IA activities in:

- Providing insight to stakeholders regarding the effectiveness of existing ABAC compliance activities;
- Identifying emerging regulatory and compliance risk; and
- Preserving the company’s control over its operations in case of potential violation to the regulators.

How Internal Auditors can help

- IA must conduct a gap assessment of the company’s existing anti-bribery and corruption procedures in relation
- IA provide assurance regarding the design and effectiveness of the preventative and detective anti-bribery controls
- IA must assess the strength of end-to-end third-party management, including due diligence and monitoring practices to ABAC
- IA must Evaluate due diligence and post-deal integration practices for managing ABAC risk, including review of acquired third-party relationships
- IA should conduct culture audits to evaluate not only the hard controls, but also the soft controls that influence and provide insight into informal norms and behaviors

What outcomes are we trying to achieve?
$7 BILLION+ IN TOTAL LOSSES

$130,000 MEDIAN LOSS PER CASE

22% OF CASES CAUSED LOSSES OF $1 MILLION+

TIPS are by far the most common initial detection method

TIPS 40%
INTERNAL AUDIT 15%
MANAGEMENT REVIEW 13%

EMPLOYEES provide over half of tips, and nearly 1/3 come from OUTSIDE PARTIES

ORGANIZATIONS WITH HOTLINES detect fraud by tips more often

46% OF CASES DETECTED BY TIP
30% OF CASES DETECTED BY TIP

Median duration of a fraud scheme
16 MONTHS

CORRUPTION was the most common scheme in every global region
## Emerging Technologies

**Drivers**

- Planning the adoption and implementation of cloud computing as an alternative to traditional computing
- Rethinking traditional approaches to DRP and BCP as changes in technology, workforce expectations and unforeseen challenges evolve or are identified
- Considering robotics and other mechanisms which reduce dependence on the human workforce
- Rapidly emerging or disruptive technologies such as fintech and blockchain

Mobile, remote, cloud computing, social media and big data have allowed us unprecedented access, usage and management of information and have completely altered the business landscape. Emerging technologies are bringing information to the fingertips of employees at companies the globe. However, with each new evolution in technology comes risks that companies need to stay on top of to optimize the impact of technology and mitigate concerns over its implementation and use.

### What outcomes are we trying to achieve?

### How Internal Auditors can help

- IA must conduct an assessment of the organization’s existing and emerging technology and the impact of these on the operations of the organization
- IA should evaluate changes in the business model, and related changes in the control environment, that may result from adopted technologies
- IA must review policies and procedures around the management of technology, including governance and controls, data integrity, security and privacy etc.
- IA must evaluate the DRP and BCPs, including approach to testing those plans, in light of the emerging technologies
- IA evaluate and advice the governance and controls required for digital labor, robotics and related initiatives
Cultural Risks/Soft Controls

Drivers

- Heightening regulatory scrutiny and increasing cultural expectations;
- Increasingly global organizations with much more varied cultural norms and practices;
- Increased publicity via social media outlets; and
- Stricter governance, oversight, and accountability expectations.

Cultural risks have caused many incidents of misconduct that have impacted the public’s trust. Culture can be observed, monitored and changed over time to mitigate misconduct and encourage strategic behaviours.

How Internal Auditors can help

- IA must conduct an assessment of the organization’s cultural drivers
- IA must review the alignment of performance measures to strategy and core values to ensure desired behaviors are being incentivized and rewarded
- IA must provide assurance regarding the evolution and alignment of the organization’s culture with compliance activities
- IA must perform systematic root cause analysis on audit findings and other non compliance incidents with specific consideration of soft controls
Cultural Risks/Soft Controls
Parting shot

...For Internal auditors to successfully provide assurance on dynamic operations that change on a day to day basis, there is need to remain abreast with and as current as possible on these changes...

**Source:** Seeking value through Internal Audit, KPMG International
Q & A
Thank You!