On the Frontlines: AI in 'IA'

There are multiple ways internal auditors can leverage ChatGPT in their work, but they also should be cognisant of privacy concerns.

AI, specifically ChatGPT, can revolutionise internal auditing by assisting auditors throughout different stages of their work. ChatGPT is an AI tool developed by OpenAI, based on the GPT-3.5 architecture, and it has the potential to transform the internal audit profession. The blog post, co-written by the author and ChatGPT, exemplifies the collaboration between humans and AI. The post provides examples of how ChatGPT can be utilised in internal audit, while also acknowledging the need to address privacy concerns.

Planning

During the planning phase of an audit, ChatGPT can play a vital role in assisting internal auditors. By analysing extensive amounts of data, ChatGPT can identify patterns and trends that may not be immediately noticeable to human auditors. This saves time and effort for auditors by helping them identify potential risks and areas for improvement. ChatGPT can also aid in the development of audit plans and testing procedures based on the insights it provides.

Additionally, ChatGPT can educate internal auditors about the process being audited and its associated risks. By inputting relevant data, ChatGPT can provide a comprehensive understanding of the process, which is particularly beneficial for auditors who are new to the organisation or unfamiliar with the process.

Moreover, ChatGPT can assist in identifying areas of improvement within the audit process itself. By analysing data inputted by auditors, ChatGPT can suggest ways to enhance the effectiveness and efficiency of audit plans, testing procedures, and reporting methodologies. This helps auditors develop more robust and efficient audit processes.

Testing Phase

During the testing phase of an audit, ChatGPT can assist internal auditors in various ways. It can analyse and interpret data, both financial and non-financial, to identify anomalies, trends, and patterns that may require further investigation. ChatGPT helps auditors determine areas of focus for testing and can even suggest audit procedures based on the analysed data. By leveraging ChatGPT's capabilities, internal auditors can enhance the efficiency and effectiveness of their testing processes.

Reporting

In the reporting phase of an audit, ChatGPT can play a valuable role in aiding internal auditors. It can generate automated reports that are accurate, comprehensive, and timely, streamlining the reporting process. Additionally, ChatGPT can assist auditors in identifying the root causes of issues and offering recommendations for improvement. It can even suggest remedial actions that can be taken to address the identified issues, enhancing the value of the audit findings communicated to stakeholders.

Monitoring

During the monitoring phase of an audit, ChatGPT can support internal auditors in ensuring that management has taken appropriate actions to address the audit findings. It can be utilised to monitor the implementation of recommended actions and identify any additional areas for improvement. ChatGPT can also assist auditors in identifying emerging risks and opportunities that may require further attention. By leveraging ChatGPT in the monitoring phase, internal auditors can enhance their oversight and contribute to ongoing organisational improvement.

On the Frontlines: AI in 'IA'

- **Privacy Concerns**

Privacy is a crucial concern when incorporating ChatGPT into the internal audit process. Internal auditors must be mindful of the privacy risks associated with using ChatGPT and take necessary precautions to mitigate these risks. It is essential to anonymise the data entered into ChatGPT and avoid sharing or storing sensitive information on the platform. Moreover, internal auditors should obtain appropriate consent and authorisation to use the data in ChatGPT. By prioritising privacy measures, auditors can safeguard confidential information and maintain ethical standards in their use of ChatGPT.

- **Treat it as a Tool**

ChatGPT is an impactful AI tool that offers significant benefits to internal auditors throughout the audit process. By utilising ChatGPT, auditors can enhance their efficiency, effectiveness, and overall audit quality. However, it is crucial for auditors to remain mindful of privacy concerns when utilising ChatGPT and take appropriate measures to address those risks. By doing so, auditors can leverage the power of ChatGPT while ensuring the confidentiality and privacy of sensitive data.

What should Internal Auditors do?

IPPF *Standard 1210* – Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

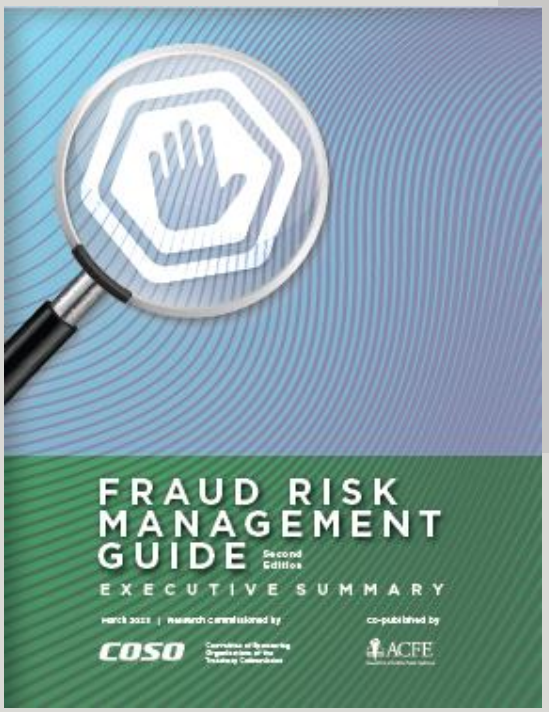
IPPF *Standard* 1220 - Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

Internal auditors are advised to possess the necessary knowledge, skills, and abilities to effectively carry out their responsibilities. This includes staying up to date with developments in their field, understanding relevant laws and regulations, and being proficient in the use of tools and technologies that can enhance their work.

When it comes to leveraging technologies like ChatGPT, internal auditors need to exercise due professional care. This means being cognisant of privacy concerns associated with the use of such technologies and taking appropriate measures to mitigate those risks. It is crucial to ensure that sensitive information is protected, and that proper consent and authorisation are obtained for using data in AI tools.

Reference:

https://internalauditor.theiia.org/en/voices/2023/on-the-frontlines-ai-in-ia/



Fraud Risk Management Guide

The Ever-Present Risk of Fraud and its Costs

All organisations face the risk of fraud, and some may question whether the costs of implementing a Fraud Risk Management Program are justified. However, this guide emphasizes that the benefits outweigh the costs and offers assistance in implementing such a program. Publicised cases of fraud demonstrate the negative impact on reputations, brands, and organisations worldwide. Both large and small frauds can have devastating consequences, including loss of trust, increased scrutiny, reputational damage, and loss of competitive advantage. While it's impossible to eliminate all fraud, effective leaders manage fraud risks like any other risk. The Fraud Risk Management Guide, based on established principles of enterprise risk management, provides organisations with a blueprint to develop a tailored program specific to their needs, regardless of their size or sector.

A Growing Area of Fraud Risk

Organisations dedicated to combating fraud understand the importance of addressing both internal and external fraud risks. Internal fraud risks involve fraud committed by individuals within the organisation, while external fraud risks encompass various evolving schemes perpetrated by external parties, such as ransomware attacks, data breaches, identity theft, and corruption schemes. By focusing on prevention, detection, and deterrence, organisations can effectively safeguard themselves against these internal and external fraud risks.

Fraud Deterrence Now and in the Future

By implementing the principles outlined in this Guide, organisations can significantly increase the chances of preventing or timely detecting fraud, thus establishing a robust fraud deterrence mechanism. COSO's mission is to enhance internal control, risk management, governance, and fraud deterrence to improve organisational performance. The Fraud Risk Management Guide serves as a crucial tool in achieving this mission, specifically in the realm of fraud deterrence. To initiate the discussion on fraud deterrence, the Guide adopts a practical definition of fraud.

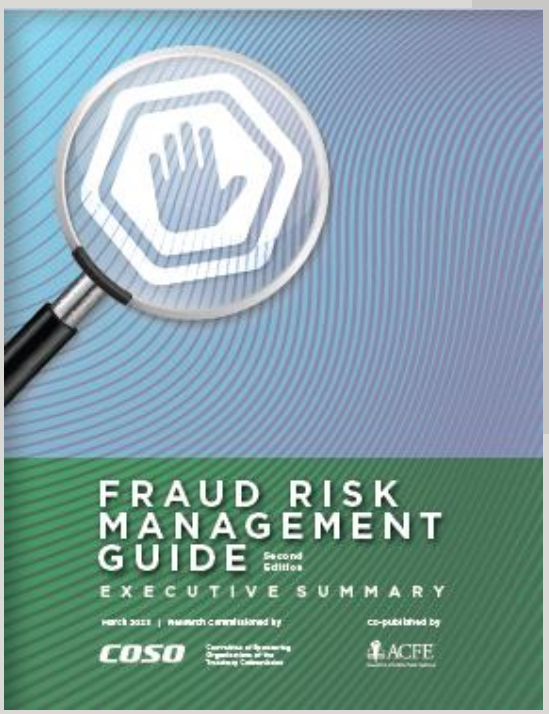
> Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

To effectively deter fraud, organisations should implement robust policies and procedures aimed at preventing and detecting fraudulent activities. By establishing a rigorous Fraud Risk Management Program, organisations can enhance fraud deterrence by creating a strong perception that potential fraud perpetrators will be apprehended and face consequences.

Roles and Responsibilities

The board of directors and top management are responsible for managing fraud risk in an organisation. They need to be well-informed about the organisation's approach to addressing heightened risks, emerging exposures, and stakeholder scrutiny. Understanding the Fraud Risk Management Program, including the identification of fraud risks, preventive measures, detection methods, and the processes for investigating and taking corrective actions, is essential. All personnel within the organisation also play a part in comprehending the impact of fraud and the importance of preventing it. This Guide aims to provide guidance in addressing these complex issues effectively.

Fraud Risk Management Guide



- **How it works?**

This Guide offers practical guidance for implementing a Fraud Risk Management Program, providing principles and focal points for effective fraud risk management. It caters to organisations of various sizes and types, assisting them in establishing their own tailored Fraud Risk Management Programs. The Guide includes examples of essential program components and resources that organisations can utilise to develop their programs efficiently. Recognising that every organisation is unique, it also references other sources of guidance for customising Fraud Risk Management Programs to specific industries, government entities, or not-for-profit organisations. The degree of emphasis placed on fraud risk management will vary based on each organisation's size and circumstances.

- **What's New in the 2023 Fraud Risk Management Guide?**

i) Fraud risk management and deterrence.
ii) Relationships among COSO's two frameworks and fraud risk management.
iii) Expanded information on data analytics.
iv) Internal control and fraud risk management.
v) Assessing the effectiveness of existing control procedures as related to fraud risk.
vi) Changes in the legal and regulatory environment.
vii) Fraud reporting systems or hotlines.
viii) Changes in the external environment and fraud landscape.

- **Fraud Risk Management and the COSO Internal Control Framework**

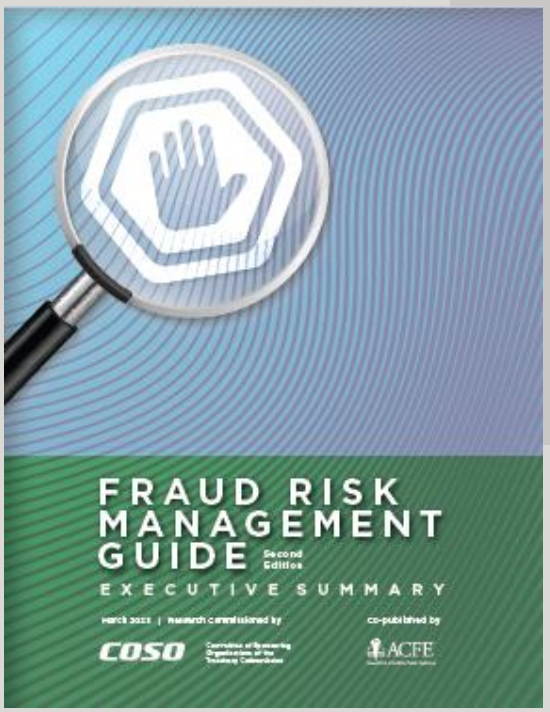
In 2013, COSO revised its Internal Control — Integrated Framework and introduced 17 principles associated with the five internal control components established in 1992. These principles offer guidance in designing and implementing effective systems of internal control and understanding the requirements for such control. According to COSO, for a system of internal control to be effective, all 17 principles must be present, functional, and operating in an integrated manner. This Guide draws on the COSO 2013 IC Framework as a source for discussing various aspects of internal control.

Principle 8, one of the risk assessment component principles, states: The organisation considers the potential for fraud in assessing risks to the achievement of objectives.

This Guide aligns with the COSO 2013 IC Framework and offers support and guidance for organisations in conducting a fraud risk assessment. While its primary focus is on the assessment, the Guide goes beyond that by providing additional guidance on establishing the various components of a comprehensive Fraud Risk Management Program. Therefore, organisations seeking a broader approach to managing fraud risk can find valuable information and guidance within this Guide.

... 4

Fraud Risk Management Guide



- **Summary of Fraud Risk Management Components and Principles**

Fraud risk governance is a crucial element of both corporate governance and the internal control environment. Corporate governance encompasses the responsibilities of the board of directors and management in fulfilling the organisation's objectives, fiduciary duties, reporting obligations, and legal responsibilities to stakeholders. The internal control environment establishes the framework for assessing risks that may hinder the organisation's goal attainment, providing the necessary discipline for managing and mitigating such risks.

Principle 1: Control Environment
Principle 2: Risk Assessment
Principle 3: Control Activities
Principle 4: Information & Communication
Principle 5: Monitoring Activites

What should Internal Auditors do?

IPPF *Standard 2120* - The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

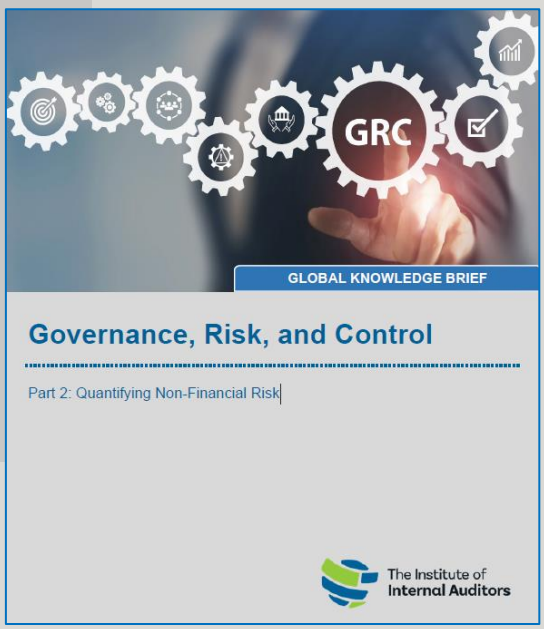
Internal auditors should be well-informed about the organisation's approach to managing fraud risks, including heightened risks, emerging exposures, and stakeholder scrutiny. Understanding the Fraud Risk Management Program, including the identification of fraud risks, preventive measures, detection methods, and investigation processes, is crucial.

In addition, internal auditors should play proactive role in fraud risk governance so that they could contribute to strengthening fraud risk governance and promoting an effective internal control environment within the organisation.

Reference:

https://www.coso.org/Shared%20Documents/COSO-Fraud-Risk-Management-Executive-Summary.pdf

Governance, Risk, and Control



Part 2: Quantifying Non-Financial Risk New COVID-inspired frauds will emerge

Understanding Non-Financial Risks

Non-financial risks arise from the organisation's impact on the world and vice versa. These risks can be challenging to define and measure due to inconsistent definitions. Non-financial risks also exist in financial transactions, where factors like time, effort, and internal controls contribute to the overall risk. Reporting and disclosure of non-financial risks can be unreliable, with concerns about intentional inflation or understatement of sustainability goals (known as greenwashing) due to the lack of globally embraced standards. The absence of consistent standards and the availability of multiple frameworks further complicate companies' determination of which guidelines to follow. The existence of various non-financial measurement and reporting standards adds to the complexity, with different performance measures and target organisations.

Setting the Stage

Organisations often struggle to quantify non-financial risks, which leads to a lack of proactive measures. Financial risks are more straightforward to address as they align with the goal of maximising shareholder wealth.

Non-financial risks, on the other hand, require investments that may not immediately contribute to revenue, making it challenging to secure management buy-in. Another obstacle is the siloed nature of control functions for non-financial risks, with different teams handling diverse risks and employing separate processes and IT systems.

This duplication of effort increases costs and can discourage information gathering and quantification efforts. However, taking preventive measures reduces remediation costs and safeguards the company's brand and relationships. While risk reporting methods may not be sophisticated enough, selecting appropriate indicators can accurately quantify non-financial risks and provide context for management. Proactive identification of potential threats enables organisations to understand and quantify risks. For example, in the food and beverage industry, considering health and safety risks can lead to steps like improving cleanliness to prevent customer illness. Non-financial risks can have greater impacts than financial risks, affecting stakeholder trust and questioning the company's practices. This places significant pressure on organisations to effectively manage non-financial risks.

Working Toward Quantification

Non-financial risks can be assigned numerical values by defining the risks and identifying tangible considerations for measurement. For customer risk, factors such as complaints, losses, declines in new customers, and trends over time can be assessed. When tangible criteria are lacking, risks can be categorised descriptively, such as high, medium, or low levels.

Compliance and regulatory risks can be quantified by determining potential findings from regulators in each risk category. Implementing an organised ratings framework allows for capturing findings on various non-financial risks.

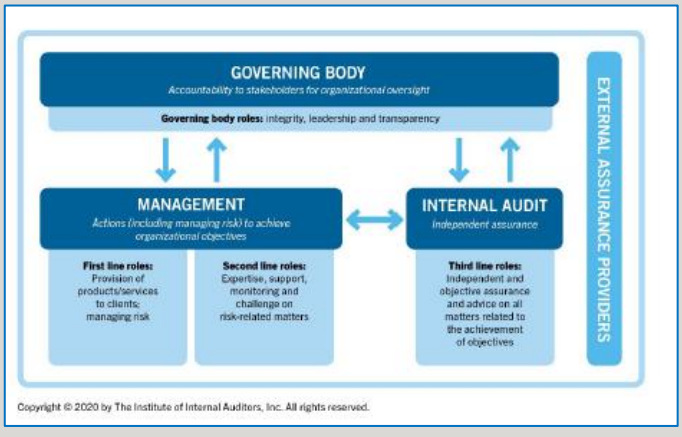
... 6

Governance, Risk, and Control

Internal audit teams can use this framework to rate observations from different teams and assess the impact of risks, facilitating quantification. The United Nations Global Compact and Principles for Responsible Investment Value Driver Model is an example of a framework that helps companies understand and communicate the financial impact of sustainability measures.

- **Remaining Future-focused and Monitoring Controls**

Internal auditors should play a strategic role in addressing non-financial risks and adding value to the organisation. They should go beyond analysing financial risks and take a proactive approach to non-financial risks, following a risk-based approach and considering the future. Internal auditors should focus on identifying and addressing future risks before management is even aware of them, making them one of the more future-oriented departments in the organisation. While internal audit doesn't define the risk categories or definitions used by the organisation, they should challenge non-financial risk policies and ensure their implementation aligns with the overall risk assessment process. Maintaining independence is essential in carrying out these responsibilities.



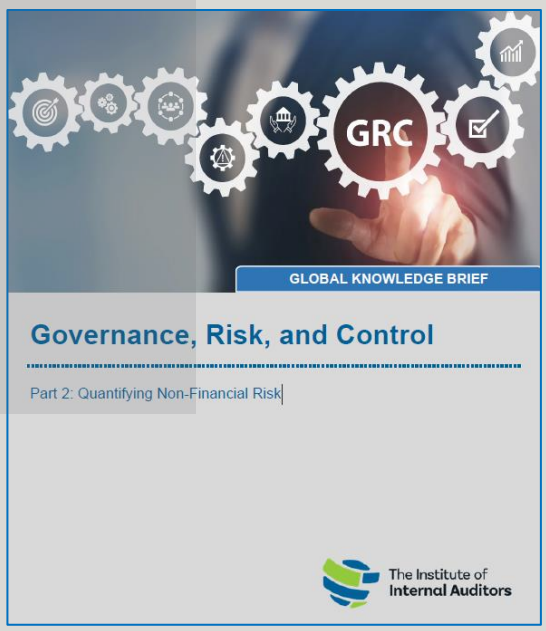
Consultants and internal auditors can follow a similar approach when addressing non-financial risks. They begin by engaging in high-level conversations with organisational leaders to understand their definitions of risk, how they identify risks, and the controls in place.

However, auditors will require new skills, such as facilitating brainstorming sessions and conducting interviews, to effectively identify non-financial risks. Leadership support and investment in training are crucial for auditors to perform this role effectively. Internal auditors can also assess the reliability of existing key performance indicators and metrics and develop new measures specific to non-financial risks. By creating a common language and refining definitions, organisations can enhance communication about non-financial risks among different lines of defense and clarify responsibilities for risk management.

- **Future – facing Responsibilities**

At Khayal's organisation, anyone involved in controls and risk self-assessment must take a detailed risk training course that includes non-financial risk. He also encourages his staff to focus on three key tasks such as stay up to date, keep current on emerging technologies and remain in tune with organisational strategy, mission, and vision.

Governance, Risk, and Control



What Internal Auditors should do?

IPPF Standard 2110 - The internal audit activity must assess and make appropriate recommendations to improve the organisation's governance processes for:

i) Making strategic and operational decisions.
ii) Overseeing risk management and control.
iii) Promoting appropriate ethics and values within the organisation.
iv) Ensuring effective organisational performance management and accountability.
v) Communicating risk and control information to appropriate areas of the organisation.
vi) Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

To assess and make appropriate recommendation, internal auditor should assess the effectiveness of governance frameworks, risk management frameworks, policies, and procedures that address non-financial risks. They have to keep abreast of the latest world, local events, and organisation's latest news to gain a better understanding of incidents that could have an impact on risk now or over the near or long term and propose recommendation or bring forward new perspectives and insights to the organisation.

For example, they can understand from the heads of departments and audit client to learn more about day-to-day operations and where risks may occur. With that understanding, the internal auditor can brainstorm and easily identify the non-financial risks of the organisation.

In addition, they should also evaluate the effectiveness of risk identification methods, risk assessment techniques, and risk mitigation strategies specifically related to non-financial risks.

Based on the assessments, internal auditors able to provide recommendations to management and the board for improving governance processes related to non-financial risks. These recommendations should aim to strengthen risk management frameworks, enhance risk culture, improve reporting and communication, and enhance monitoring mechanisms.

Reference:

https://www.theiia.org/en/content/articles/global-knowledge-brief/2023/may/grc-part-2-quantifying-non-financial-risk/