Fraud and Internal Audit

The Institute of
Internal Auditors

Pamela J. Stroebel Powers

2023 Illinois Government Auditing Conference

Objectives

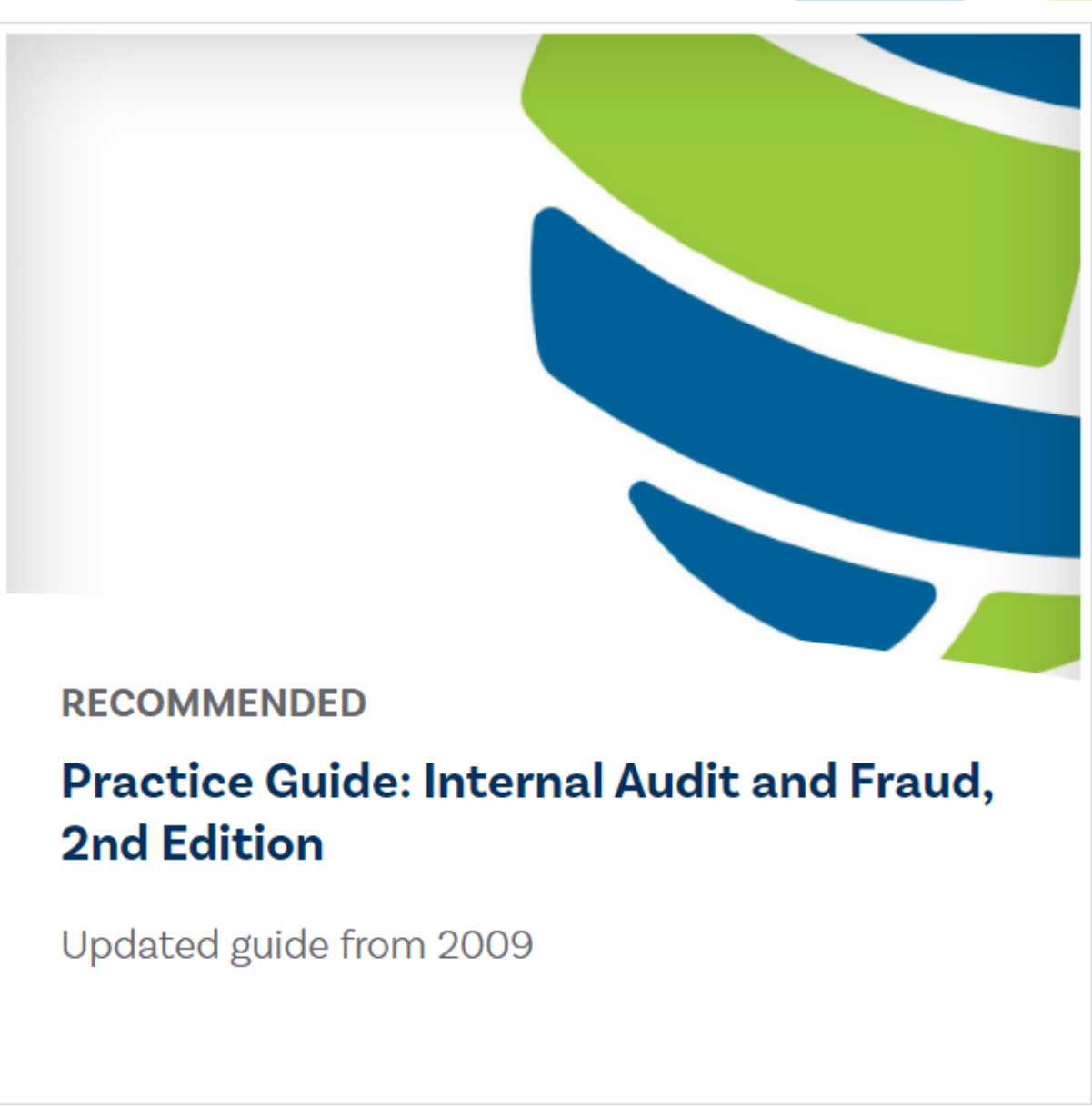
This session will provide an overview of, and insight into, the Institute of Internal Auditor's Practice Guide - *Internal Audit and Fraud: Assessing Fraud Risk Governance and Management at the Organizational Level*. This Practice Guide was recently updated and released in its second version in May of 2022. Specifically, participants can expect to receive insights into:

- Understanding and assessing fraud risk
- Fraud risk roles within each of the Three Lines
- COSO's Fraud Risk Management Framework
- Providing assurance on organization wide fraud risk governance and management
- Where fraud factors appear in the proposed revisions to the *Standards* included within the International Professional Practices Framework and how they compare to the *Standards* in place today

Note: This Practice Guide is scheduled to be updated again to align with the IPPF Evolution and COSO's Recently Released Updated Fraud Risk Management Guide

Practice Guide – Internal Audit and Fraud

https://www.theiia.org/en/standards/what-are-the-standards/recommended-guidance/supplemental-guidance/



Purpose of the Guide

- Increase awareness of fraud.
- Understand how to perform internal audit's role in fraud risk assessment.
- Know what the IPPF says about fraud.
- Know what is needed to achieve internal audit compliance with the *Standards*.

Types of Fraud Considerations

- **Fraud Risk:** When there is the potential for fraud.
- **Fraud Schemes:** When fraud is being planned.
- **Fraud Events:** When fraud has been perpetrated.

Both organizations AND their auditors should be mindful of these!

Understanding and Assessing Fraud Risk

Considerations

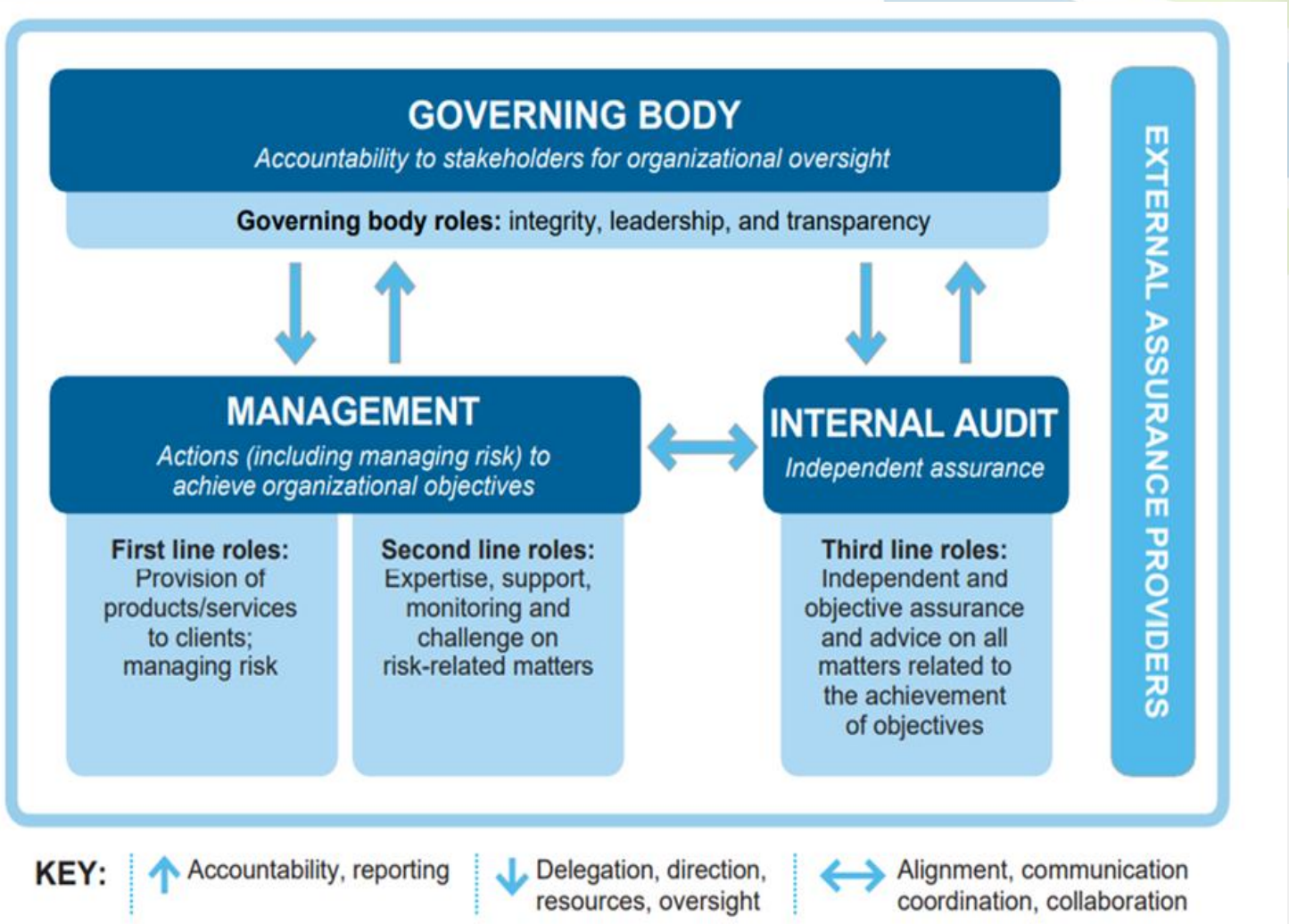
- When it comes to fraud, there is no ‘one size fits all’ approach
- To be effective with fraud assessments, just like any internal audit work, the internal auditor needs to become familiar with the organization
- Management and the Board must identify their fraud risk tolerance

Examples of Fraud Risks

A. Collusion
B. Under or Overreporting
C. Misappropriation of Assets or Data
D. Misrepresentation
E. Falsification of Documentation
F. Destruction of Records

Fraud Risk Roles within the Three Lines

Three Lines Model



Source: The IIA's Three Lines Model: An Update of the Three Lines of Defense, 2020

Board/Audit Committee Roles

- Ultimate responsibility for effective fraud risk governance and promoting an antifraud culture
- Helps set Tone at the Top
- Works with management to set expectations for ethical behavior and sets the appetite for fraud risk
- Ensures an appropriate fraud risk management framework and program are in place
- Monitors and evaluates management's antifraud activities

Management: First and Second Line Roles

- Authorized by the board to apply resources and execute decisions to achieve organizational objectives
- Adopts an appropriate fraud risk management framework and sets antifraud tone
- Primary responsibility for monitoring and controlling processes to prevent, deter, detect and recover from fraud
- Responsible for establishing and maintaining an effective internal control system
- Implements and monitors fraud risk controls

Internal Audit: Third Line Roles

- Provides assurance to the board and management on how effectively the organization assesses and manages its fraud risk.
- Consulting/Advisory roles may include:
  - Providing input to draft policies
  - Providing, assisting or promoting fraud training
  - Contributing to the awareness of fraud risk across the organization
- Supporting fraud investigations

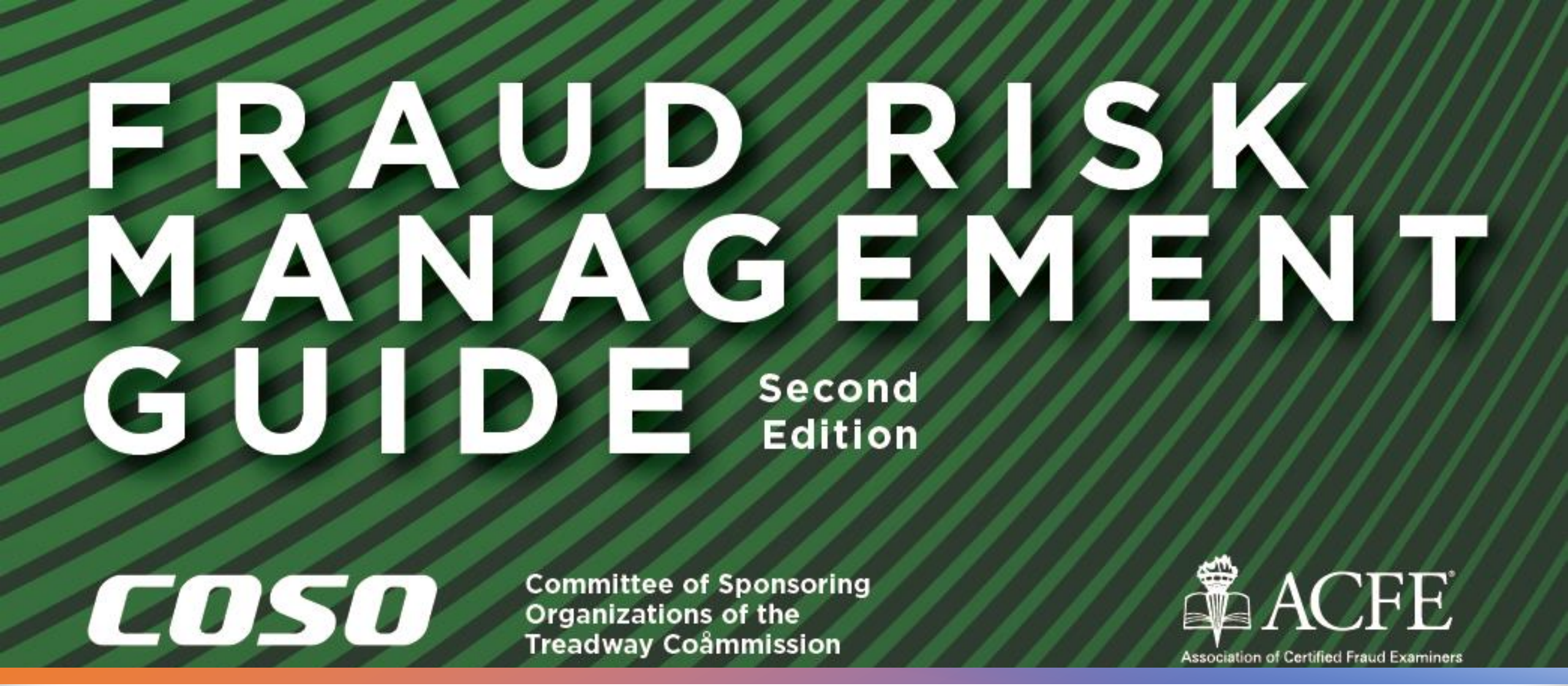
All Employees Have a Responsibility!

- Awareness built through Training
- A ‘see something, say something’ attitude
- Knowledge of the organization’s framework and processes for controlling and reporting potential fraud

Fraud Risk Management Framework

A Framework…

- Includes policies, tools, training and other antifraud controls
- Promotes a commitment at all levels to communicating and enforcing an antifraud culture
- A selected framework should align with the organization's internal control environment and risk management practices
- Assists with:
  - Establishing a fraud risk management program in a methodical way
  - Ensuring consistency in approach and implementation
  - Adequacy of design and implementation effectiveness



Originally Published in 2016 - Newly updated in 2023!

www.coso.org

The Institute of Internal Auditors
Elevating Impact

COSO's 2013 Internal Control Framework

Principle 8, one of the risk assessment component principles, states:

- The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Applying COSO's Internal Control Framework to Fraud

Internal Control Component	Fraud Risk Management Principle	Examples
1. Control Environment	Fraud Risk Governance	Antifraud culture supported by Tone at the Top
2. Risk Assessment	Fraud Risk Assessment	Management self-assessments and periodic third party assessments
3. Control Activities	Fraud Control Activities	Fraud awareness training
4. Information and Communication	Fraud Investigation and Corrective Action	Fraud risk communication strategy, control activity monitoring, and disciplinary action
5. Monitoring	Fraud Risk Management Monitoring Activities	Reports by Internal Audit to the Board/Management and timely attention to resolving weaknesses

Update Themes

- Additional emphasis on DETERRENCE
- Explanation of the relationship to COSO's other guidance: Internal Control and ERM
- Expanded information on data analytics
- Stressing the importance of assessing the effectiveness of existing control procedures as related to fraud risk
- Additional information on the importance of fraud reporting systems
- Addressing changes in the external environment and fraud landscape
- Updated and expanded appendix: Managing the Risk of Fraud, Waste and Abuse in the Government Environment (some appendices containing 'samples' were moved to a ACFE's tools website and more were added!)

Providing Assurance on Organization wide Fraud Risk Governance and Management

Coordination of Assurance Activities

Fraud risk management assurance may be provided through various sources:

- Management
- Second Line Functions (Risk Management)
- External Assurance Providers
- Internal Audit

As emphasized in the 3 Lines Model and required by Standards, the CAE should work to coordinate across assurance providers to avoid duplication.

The Internal Auditors Role

- Should be clearly outlined in the Internal Audit Charter (approved by the Board/Audit Committee)
- Independence and Objectivity must be safeguarded
- Competency must be assessed for certain fraud responsibilities such as investigations
- Internal auditors should not assume responsibility for MANAGING risks

Requirements for Providing Assurance

- Evaluating Structures and Processes for Fraud Risk Governance
- Performing an Organization wide Assessment of Fraud Risks
- Evaluating the Design of the Fraud Risk Management Program
- Communicating Results and Assurance to Senior Management and the Board

Comparing the IPPF Today to the Proposed Standards

IPPF Glossary: Fraud

Old Definition

Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

COSO's Definition

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.

Proposed Definition

Any act characterized by deceit, concealment, or violation of trust perpetrated by individuals or organizations to secure personal or business advantage.

Rationale for Change:

After researching several sources, the decision was made to modify the former IPPF definition to remove "illegal" because not all frauds are illegal. Definition was simplified because "personal or business advantage" seemed to include everything else described.

Standards Comparison

2017 Ref	Standard Language	2023 Ref	Proposed Language
1210. A2	Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.	3.1	**Competency:** For internal auditors, being competent requires possessing and demonstrating knowledge, skills, and abilities relevant to: ..... ● Business functions, such as financial management and information technology, and pervasive risks, such as fraud. *(Considerations for Implementation)*
1220. A1	Probability of significant errors, fraud, or noncompliance.	4.2	**Due Professional Care:** Internal auditors must exercise due professional care by taking into account the nature, circumstances, and requirements of the services to be provided, including: ..... • Probability of significant errors, fraud, noncompliance, and other risks that might affect objectives, operations, or resource (Requirements and Examples of Evidence of Conformance)
2120. A2	The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.	9.5	**Internal Audit Plan:** The internal audit plan must: .... ● Consider coverage of information technology governance, fraud risk, and the effectiveness of the organization's compliance and ethics programs. (Requirements)

Other Places Fraud is Mentioned in the Proposed Standards

- 11.1 Building Relationships and Communicating with Stakeholders – under Considerations for Implementation around obtaining input for emerging issues around risk.

- 11.5 Communicating the Acceptance of Risk - as an example of the types of risks that might exceed the tolerance level.

- 13.2 Engagement Risk Assessment – Fraud is included as one of the types of risk auditors MUST consider. (*Requirements)*

Other Fraud Resources (IIA Partners)

- The IIA is a partner with CAQ, NACD and FEI in the Anti-Fraud Collaboration:
  - https://antifraudcollaboration.org/

- Association of Certified Fraud Examiners:
  - www.acfe.com

Summary

- Standards require specific considerations of fraud but the work is not that different from our regular internal audit work, just with a specific emphasis
- Internal audit has an important role to play with fraud, specific to the third line role
- Internal audit can provide important risk assessment, assurance and advisory services to management and the board related to an organization's fraud risk management governance including adopted framework, as well as the effectiveness of controls
- Internal auditors may need to coordinate and collaborate with other assurance providers related to fraud roles and responsibilities
- The IIA has many resources available to assist internal audit in their role with fraud!

Questions? Contact:

Pam.stroebelpowers@theiia.org OR Guidance@theiia.org

Questions and Answers


Thank You !