INTEGRATING FORENSIC INVESTIGATION TECHNIQUES INTO INTERNAL AUDITING

The internal auditors’ roles in combating fraud are becoming more profound within an organization. Internal auditors may assume a variety of consulting, assurance, advisory, collaborative, oversight, or even investigative roles within an organization’s fraud risk management process. Integrating the appropriate forensic techniques into the auditing process is crucial in ensuring that these roles are carried out effectively. This session will explore how appropriate investigative techniques can be applied effectively throughout the audit process to fulfill auditors’ fraud combatant role within the organization.

You will learn how to:
- Define the auditor's fraud-related responsibilities and challenges.
- Realize the benefits of applying investigative techniques into auditing.
- Explain the importance of effective fraud risk assessment within the organization and in audit planning.
- Leverage technology (i.e., data analytics) for fraud detection and response.

GERRY SCHIPPER
Group Head of Internal Audit
AIA Co Ltd
Hong Kong

Gerry Schipper is responsible for leading and overseeing the internal audit function across all lines of business for the AIA Group of companies. In that role he manages an internal audit plan that is aligned with appropriate regulatory and risk management requirements. Gerry oversees all internal audits and investigations of employee dishonesty and misconduct within the organization. He has led and conducted high-quality forensic audits and investigations of fraud and abuses, financial misstatement, and regulatory and compliance assessment audits. He also advises senior management and the Group Audit Committee on risk and control issues, and provides recommendations on how to manage and mitigate risks.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, re-published, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
## Overview

- Introduction
  - Auditor’s role and standards
  - AIA introduction
- How AIA does it—an overview
  - Enterprise level
    - Fraud risk assessment
    - Audit planning
  - Project level
    - Combining forensic techniques in the audit process
      * Planning—FRA and DA
      * Testing—DA, background checks, site visits
      * Reporting—DA, fraud response
      * Examples
  - Fraud health checks
    - Comparison with integrated auditing
    - Testing approach
    - Success stories
- Challenges and how to overcome them
- Conclusion

## Introduction

Traditionally, internal auditing and fraud preventions have been separate disciplines in organizations. Views adopted include:

- Internal audit is not integrated with the fraud risk framework.
- A reactive approach to fraud is adopted.
- Fraud detection/prevention is not a primary objective of internal audit.
- Fraud is not perceived to be an internal control failure.

With large corporate collapses and global scandals over the past decade, more regulations and guidelines have been established for auditors to play a greater role in fraud risk management. The Institute of Internal Auditors (IIA) has...
set standards for auditors to concentrate their efforts on the financial statements or business processes that are susceptible to fraudulent acts. This is required under both Attribute and Performance Standards. Applicable IIA standards are set out below.

**IIA Standard 1200: Proficiency and Due Professional Care**

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.”

**IIA Standard 1220: Due Professional Care**

1220.A1: “Internal auditors must exercise due professional care by considering the probability of significant errors, fraud, or noncompliance.

**IIA Standard 2060: Reporting to Senior Management and the Board**

“The chief audit executive must report periodically to senior management and the board on the internal audit activity’s purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.”

**IIA Standard 2120: Risk Management**

2120.A2: “The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.”
**IIA Standard 2210: Engagement Objectives**

2210.A2: “Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.”

Nowadays, internal audit is expected to assume greater responsibilities towards fraud risk management by:

- Managing fraud risk more proactively.
- Considering fraud risk and controls as an objective of internal control activities (fraud perceived to result from potential internal control failures).

This view is also supported by the results in the ACFE’s 2014 Global Fraud Study, highlighting that:

- Internal Audit is the third most common detection method for occupational fraud.
- Proactive data analysis and internal audit are two of the top five controls in reducing the median loss of fraud schemes.

Integrating the appropriate forensic techniques into the auditing process is therefore crucial in ensuring that these roles are carried out effectively. Some of these forensic techniques include adopting fraud risk assessment, data analytics technology, site visits, and background checks.

**Brief Introduction to AIA**

- Largest independent pan-Asian life insurance group.
- Headquartered in Hong Kong and originally founded in 1919 in Shanghai.
- Leading presence in Asia-Pacific (ex-Japan) across 17 markets.
- Outstanding business and strong cash flow.
Balanced and diversified business with broad-based growth offering a range of life insurance, accident, and health insurance and savings plans.

Has a solvency level of 448 percent.

There is a dedicated investigation unit within Internal Audit that:

- Performs fraud investigation (including evidence gathering, ad-hoc forensic accounting investigations, root cause analysis, and recommending improvement/remedial action).
- Supports the assessment of controls for fraud detection/mitigation.
- Conducts anti-fraud training and initiatives in the Group.

For a comprehensive investigation practice, Internal Audit also invested in data analytic and forensic software and recruited forensic professionals.

**Enterprise Level**

**Fraud Risk Assessment**

Why do auditors need to perform fraud risk assessment?

- **SAS 99**—*Consideration of Fraud in a Financial Statement Audit* requires the auditor to assess the risks of material misstatement due to fraud throughout an audit.

- **SAS 99** also requires auditors to approach engagements with professional skepticism, a questioning mind, and an awareness that fraud can occur anywhere and anytime.

- Internal auditors usually have a continual presence in the organization that provides them with a better understanding of the organization and its control systems.
• Auditors can create fraud awareness, enhance the ethical environment, and protect company assets.

The following processes are involved in a fraud risk assessment:
1. Historical cases assessment.
2. Self-assessment and fraud survey.
3. High fraud risks areas.
4. Annual audit planning.
5. Audit plan.
6. Addressing fraud risks.
7. Initiating audit project.

Fraud risk assessment can be split into two levels:
• Enterprise level.
• Project level.

**Audit Planning**

Fraud risk assessment at the enterprise level is conducted annually. It is facilitated by Operational Risk Management (ORM) under the Risk and Control Self-Assessment (RCSA), a group-wide risk management program.

RCSA records the fraud risks identified by management through self-assessments, brainstorming, actual fraud experiences, and control assessments.

In addition, ORM conducts a group-wide annual fraud survey to facilitate the functional heads across the Group to brainstorm and update their assessment of potential fraud risks.

Annual audit planning will be adjusted accordingly to consider and include the high fraud risks areas identified from the annual RCSA and survey.
Project Level
A typical internal audit process can be divided into three main stages:
- Planning.
- Fieldwork.
- Reporting.

We set out below how forensic techniques can be integrated into an internal audit process in these three stages.

During Planning
The planning stage involves:
- Gathering relevant information, such as organizational charts and processes.
- Understanding findings from past audits.
- Gathering information about previous frauds, if any.
- Formulating the audit scope and objectives.
- Conducting fraud risk assessment on the area to be audited.

The following forensic techniques can be applied:
- Fraud risk assessment (project level)
  - Fraud risk assessment aims to consider fraud risks in the assessment of internal control design and determination of audit steps to perform. This process helps auditors to systematically identify where and how fraud may occur, discover what controls are in place to prevent/detect frauds, and consider the audit steps to perform.
- Group Internal Audit has also created a fraud library that includes the following information:
  - Potential fraud risks for areas like underwriting, investment, policy owner services, finance, etc.
  - Historical fraud incidents in AIA Group.
INTEGRATING FORENSIC INVESTIGATION TECHNIQUES INTO INTERNAL AUDITING

This information is made available to the audit team when the audit scope and testing procedures are designed to address potential fraud risks and to test the effectiveness of the relevant anti-fraud controls.

Keys steps involved in integrating the fraud risk assessment into the audit process include:

- Identifying relevant fraud risk factors
  - This involves gathering information about the organization’s business activities to understand fraud risks, review documentation of previous frauds and suspected frauds committed against or on behalf of the organization, evaluate related frauds at similar organizations, and review the organization’s performance measures over the past few years compared with competitors.

- Identifying potential fraud schemes
  - Potential fraud schemes can be identified through brainstorming, management interviews, analytical procedures, and review of previous frauds.

- Mapping existing controls to potential fraud schemes and assess fraud probability
  - This involves identifying existing controls in place to address each fraud risk in order to assess its probability. If there is a control deficiency leading to higher probability of fraud, additional/specific audit procedures may be required.
  - Designing procedures that consider the fraud risk
  - This involves designing the appropriate procedures to detect the potential fraud. Cost and benefits should be considered in selecting the procedures.
INTEGRATING FORENSIC INVESTIGATION TECHNIQUES INTO INTERNAL AUDITING

- Documenting the fraud risk assessment
- The process and results of the fraud risk assessment should be documented.

**During Fieldwork**

This phase allows an auditor to identify risk areas and concerns in the internal controls and procedures before a conclusion is drawn on the fieldwork. To enhance the internal auditing process during fieldwork, the following forensic techniques can be applied.

**DATA ANALYTICS (DA)**

Data analytics is a process of inspecting, cleaning, transforming, and modeling data with the goal of discovering useful information, suggesting conclusions, and supporting decision making. Data analysis has multiple facets and approaches, encompassing diverse techniques under a variety of names, in different business, science, and social science domains.

DA is applied to gain more insight into data from the transaction systems by:

- Performing audit sampling using either statistical (e.g., random and systematic) or non-statistical (e.g., judgmental or discovery) methods.
- Conducting various analysis and statistical functions (e.g., identifying duplicates, gaps, and unusual trends in data).

Various DA tools in the market to facilitate the above tests/analysis include the simple Microsoft Excel spreadsheet, databases (SQL /Oracle), and auditing software (ACL/IDEA). Here are some
factors to consider in determining a suitable DA tool:
- Data size.
- Type of analysis to be performed.
- Ability to program the tool to customize desired audit steps.
- Ability to re-run the analysis easily.

This includes selecting risk-based samples based on internal audit focuses and testing on a sample basis—gaining insight from data in individual transaction systems—to perform its work.

A more robust application of DA would be continuous auditing. This includes performing audits on a continuous basis using automated tools on certain key controls. Benefits of continuous auditing include:
- Increased audit coverage and assurance (the full population can be audited).
- Continuously monitoring policy violations, errors, adverse trends, potential red flags, and even cost-saving opportunities within the business.
- Automating the monitoring process, rather than just relying on periodic audits.

BACKGROUND CHECK
A background check or background investigation is the process of looking up criminal records, commercial records, and financial records of an individual or an organization. This forensic technique allows the gathering of more facts from publicly available information to understand the profile/identity of a vendor company/individual.
(external third party) or employee whose background is potentially suspicious.

Such checks may be obtained from the following sources:
- Public databases, including company registries, litigation check, criminal check.
- Internet searches.
- Social network analysis.
- Telephone enquiry.

Another verification that could be performed includes in-person site visits. Based on the address of a vendor company/individual, a site visit can be performed to confirm the existence of the vendor/individual.

**SITE VISIT**
Such visits are conducted to verify the existence of a third party, authenticate whether an event actually took place, and validate the reasonableness of price quoted by vendors.

**During Reporting**
When fieldwork is completed, it is important to compile, present, and discuss the findings with the client, management, or audit committee.

**DATA ANALYTICS**
Presentation of the audit findings can be enhanced using data visualization or relationship mapping software. Appropriate visualizations (i.e., graphs and charts) can be selected to highlight yet simplify critical findings. As the saying goes: “A picture paints a thousand words.”
FRAUD RESPONSE PROTOCOL
If an audit finding uncovers a potential fraud red flag, a systematic protocol response is established to address the red flag. This includes a preliminary assessment of the red flag by the investigating team to determine whether the red flag warrants further investigation.

Fraud Health Check
Definition
A fraud health check is a proactive process of identifying specific weaknesses through which fraud or other forms of avoidable loss and compliance breaches could occur.

Comparison with Traditional Auditing and Fraud Investigation
In terms of testing procedures, traditional audits emphasize testing controls and verifying control effectiveness, whereas fraud health checks focus on the authenticity of transactions. A fraud investigation is performed to identify suspicious transactions that correspond to certain indicators of fraud. For traditional audits, findings include control gaps and deficiencies. However, fraud health checks focus on identifying potential fraud and compliance risks embedded in a transaction. Fraud investigation concentrates on identifying red flags that might substantiate allegations.

The sampling method varies too. For traditional audits, the sample selection is based on unbiased procedures. For fraud health checks, risk-based sampling methodology (e.g., using keyword searches, trends, and patterns) is leveraged. However, specific transactions are selected for analysis when conducting a fraud investigation.
Typical Process
The typical process of performing fraud health check involves four steps: (1) scoping, (2) data gathering and analysis, (3) testing, and (4) reporting.

First of all, it is essential to identify areas where fraud risks could mostly likely occur, assess potential fraud scenarios, and design testing procedures corresponding to potential fraud risks.

Secondly, for data gathering and analysis, we need to apply forensic data analysis for identification of high risk samples based on the information and data obtained.

Thirdly, conducting red flag testing (for example, site visits, cold calling, Internet searches, etc.) is critical in identifying anomalies.

Lastly, after gathering the evidence, we need to report findings and observations to the management and suggest options for improvement or remediation.

Typical Testing Approach
The testing approach includes:
- Document examination to establish authenticity or expose forgery of the document reviewed.
- Acquiring a proof of performance in order to prove the transaction has really occurred.
- Obtaining market indications to benchmark whether the vendor has overcharged (in some cases, consider consulting an industry expert to assess the reasonableness of the price).
- Not assuming, but seeing with your own eyes (for example, performing site visits at the location where
a transaction occurred or inquiring with the parties involved).

**Challenges**
The benefits of integrating forensic techniques are obvious, but there are some practical challenges that need to be tackled first. Some of these challenges include:

- Significant investment required.
- Expensive investment in data analytics tools and forensic software.
- Recruiting employees with the appropriate forensic expertise.
- Difficulties in applying effective DA due to:
  - Incomplete data or poor data quality.
  - Different systems with different data formats (huge effort is required to standardize and centralize the data population).
- Resistance to change:
  - Auditors may resist changing their mindset to a more forensic investigative approach as they are too used to an audit/checklist mindset.

How can we overcome the above challenges?

- Setting the tone from the top by the chief audit head to enforce such integration.
- Increased training/hands-on experience for the auditors to apply forensic techniques during audits.
- Establish written guidelines/ internal initiatives to drive the change.
- Show management the value proposition for investment.
- Develop a common data warehouse/enterprise architecture to facilitate data analytics.
**Conclusion**

At AIA, by integrating forensic techniques into internal audits, we found better quality audits were conducted and professional skepticism/alertness increased in fraud detection. The results are evident!