INTEGRATING FORENSIC INVESTIGATION TECHNIQUES IN INTERNAL AUDITING

Gerry Schipper
2014 ACFE Asia-Pacific Fraud Conference
16–18 November 2014, Hong Kong

AIA confidential and proprietary information. Not for distribution.
AGENDA

1. Introduction
   - Auditor’s roles and standards

2. How AIA does it? — An Overview
   - Enterprise level
     - Fraud Risk Assessment
     - Audit planning
   - Project level
     - Combining Forensic Techniques in the Audit Process
       - Planning
       - Fieldwork
       - Reporting
       - Real Life Examples
   - Fraud health checks
     - Comparison with integrated auditing
     - Testing approach

3. Challenges

4. Conclusion
INTRODUCTION

- Internal Audit’s Role
- IIA Standards
- 2014 *Report to the Nations*
- AIA Introduction
INTERNAL AUDIT: TRADITIONAL VIEWS

Internal audit and fraud prevention / detection are separate disciplines. Approaches adopted include:

- Internal audit is not integrated, and not required to be, with fraud risk framework.
- Internal Audit takes a reactive approach to fraud.
- Fraud detection/prevention is not a primary objective of internal audit.
- Fraud is not perceived to arise as a result of an internal control failure.
- There should be separate reporting lines.
AIA GROUP – A SNAPSHOT

Leading Pan-Asian Life Insurance Company

- Pure Asian, pure retail, pure life insurer with unique access to Asia’s superior growth markets
  - Leading presence in Asia-Pacific ex-Japan across 17 markets\(^{(1)}\)
  - Top 3 position in 9 markets\(^{(2)}\)
  - Most recognised Asian insurance brand with a 95-year history
  - In-force scale with 28m individual policies and 16m group scheme members

Outstanding Business and Financial Track Record

- Consistent strong financial performance across all metrics since 2010:
  - Value of one year’s new business up 2.2x
  - EV equity up 40%
  - Operating Profit After Tax up 50%
- Balanced and diversified business with broad-based growth

Strong Balance Sheet and Cash Flow

- High quality and prudent balance sheet
- Solvency level of 433%; Low financial leverage of 11.2\(^{(3)}\)\%
- Strong cash and capital generation – US$3.8b free surplus generated in 2013
- Strong capital fungibility – US$5.4b remitted to Group over the last 3 years
Corporate collapses / scandals over the past decades had led to a greater focus on auditor’s responsibilities in fraud detection / prevention:
INCREASED AUDITOR’S RESPONSIBILITY

More regulations and guidelines have imposed greater roles and responsibilities on both internal and external auditors:

For external auditors:

- Statement of Auditing Standards No. 99: Consideration of Fraud In A Financial Statement Audit (‘SAS 99’)
  Requires auditors to concentrate efforts where the financial statements or business processes are susceptible to misstatement as a result of fraudulent acts.

For internal auditors:

- Institute of Internal Auditors’ (‘IIA’) Standard
  Required under both Attribute and Performance Standards
  - IIA standard 1210.A2: Proficiency and Due Professional Care
    • Have level of knowledge that is adequate to understand and respond to fraud risk.
  - IIA standard 1220.A1: Due Professional Care
    • Demonstrate professional responsibility by considering the likelihood of significant errors, fraud or noncompliance.
  - IIA Standard 2060: Reporting to Senior Management and the Board
    • Periodically notify senior management and board of directors on significant risk exposures and control issues, fraud risks in general, governance issues, and etc.
  - IIA Standard 2120.A2: Risk Management
    • Set up an internal audit program that evaluates the potential of fraud occurring and how the organization manages this risk.
  - IIA Standard 2210.A2: Engagement Objectives
    • Consider probability of significant errors, fraud, non compliance and other exposures when developing engagement objectives.
INTERNAL AUDITORS’ INVOLVEMENT IN FRAUD PREVENTION AND DETECTION

For Fraud Detection
- Exposed to key processes throughout the organization and have open lines of communication with the executive board and staff.

- When developing annual audit plan, internal auditors consider the organization's assessment of fraud risk, and periodically may make assessments of management's fraud detection capabilities.

- Internal auditors are experienced in using techniques such as data analytics to evaluate internal controls.

For Fraud Prevention
- Advise management on methods to ensure integrity and involve in communicating or interpreting those methods.

- Help to develop training related to integrity policies and fraud.

- Watch for potential fraud risks, assess the adequacy of related controls, and make recommendations for improvement.
COMMON FRAUD DETECTION METHODS

Internal Audit is the **THIRD** common detection method of occupational fraud.

(Source: ACFE 2014 Report to the Nations on Occupational Fraud and Abuse)
COMMON ANTI-FRAUD CONTROLS

Proactive data analysis & internal audit are two of the **TOP FIVE** controls in reducing the median fraud losses.

![Table: Median Loss Based on Presence of Anti-Fraud Controls](image)

(Source: ACFE 2014 Report to the Nations on Occupational Fraud and Abuse)
INVESTIGATION TEAM

A dedicated investigation unit resides within Internal Audit to:

- Perform fraud investigations (including evidence gathering, ad-hoc forensic accounting investigations, root-cause analysis, and recommend improvement / remedial action).

- Support the assessment of existing controls for fraud prevention and detection / mitigation.

- Conduct anti-fraud training (e-learning or classroom), fraud awareness / alerts / publications, etc.

- Review and evaluate the design and effectiveness of anti-fraud program and related controls.

- Ongoing review of process specific fraud risk controls.

- Provide/suggest internal investigation training as appropriate, to ensure competency.

For a comprehensive investigation practice, Internal Audit has also invested in data analytic and forensic software and recruited forensic talents.
HOW AIA DOES IT? — AN OVERVIEW

AIA’s Group Internal Audit

Enterprise Level
- Audit planning
- Fraud risk assessment

Project Level
- Planning
- Fieldwork
- Reporting

Fraud Health Check
ENTERPRISE LEVEL

- Fraud risk assessment
- Audit planning
FRAUD RISK ASSESSMENT (FRA)

“A process aimed at proactively identifying and addressing an organisation’s vulnerabilities to fraud risk.”
– BBVA Compass’ presentation to IIA (Birmingham Chapter)

Why internal auditors perform FRA?
 Comply with professional standards:
  ➢ SAS 99
  ➢ IIA Standards 1210.A2-1
  ➢ PCAOB Auditing Standard No.8-15

 Identify and prioritise high fraud risk area within the business.

 Address such risks at the planning stage of the annual audit planning, and each audit.
FRAUD RISK ASSESSMENT IN AIA

1. Historical cases assessment
2. Self assessment & Fraud survey
3. High fraud risk areas
4. Annual audit planning
5. Audit plan
6. Address fraud risk
7. Initiate audit project

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, Group ORM conducts a group-wide annual fraud survey that serves 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 address and include the high fraud risks areas identified from annual RCSA and survey.

- Group Internal Audit (GIA) is an advisor in this process.
PROJECT LEVEL

- Planning
- Fieldwork
- Reporting
- Real-Life Examples
APPLICABLE FORENSIC TECHNIQUES

Different forensic techniques could be integrated into audit process.

**Fraud Risk Assessment**
- Identify fraud risk areas
- Assess fraud probability
- Design audit procedures

**Data Analytics**
- Conduct various analysis
- Increase audit coverage
- Continuous auditing

**Background Check**
- Public information
- Social network analysis
- Cold calling

**Site Visit**
- Mystery shopping
- Visit to questionable vendors
- Visit to third party service providers

**Fraud Response Protocol**
- Response to address red flag
- Fraud reporting channel
INTERNAL AUDIT PROCESS

Typical internal audit process: Planning, Fieldwork, and Reporting

① Planning
• Fraud risk assessment
• Data analytics

② Fieldwork
• Data analytics
• Background check
• Site visit

③ Reporting
• Data analytics
• Fraud response protocol
INTERNAL AUDIT PROCESS

Typical internal audit process: Planning, Fieldwork, and Reporting

① Planning
- Fraud risk assessment
- Data analytics

② Fieldwork
- Data analytics
- Background check
- Site visit

③ Reporting
- Data analytics
- Fraud response protocol
PLANNING: FRAUD RISK ASSESSMENT BY ENGAGEMENT TEAM

1. Identify relevant fraud risk factors
2. Identify potential fraud schemes
3. Map existing controls and assess fraud probability
4. Design procedures that consider the fraud risk
5. Input by management
6. Document the FRA
7. Endorse by audit manager
INTERNAL AUDIT PROCESS: FIELDWORK

Typical internal audit process: Planning, Fieldwork, and Reporting

① Planning
- Fraud risk assessment
- Data analytics

② Fieldwork
- Data analytics
- Background check
- Site visits

③ Reporting
- Data analytics
- Fraud response protocol
INTERNAL AUDIT PROCESS: FIELDWORK

Fieldwork

Data Analytics
- Conducts various analyses
- Increase audit coverage
- Continuous auditing

Site Visits
- Mystery shopping
- Visit to “questionable” vendors
- Visit to third-party service providers

Background Check
- Public information
- Social-network analysis
- Cold calling
What is Data Analytics?
‘A process of inspecting, cleaning, transforming and modeling data with the goal of discovering useful information, suggesting conclusions, and supporting decision making.’ - Wikipedia
### Planning/Scoping
- Objectives
- Scope
- Exclusions & Assumptions
- Expected Deliverables
- Selection of Tools and Approach
- Understand environment/data sources
- Data Size and Structure

### Data Request
- Timing of data to be received
- Format of Data
- Minimum Data Attributes to be captured
- Thresholds
- Method of Delivery

### Data Manipulation
- Data Transformation and Conversion
- Normalize or denormalize the data
- Data loading to database
- Data Accuracy, Integrity and Completeness Checks
- Specific Field Validation
- Data Reconciliations

### Identify and Define Analytics Rules
- Business rules
- System rules
- Regulatory requirements
- Fraud /risks indicators

### Conduct Data Analytics
- Develop an understanding of the data
- Apply Analytics Rules to Data (rule based model)
- Programming/scripting
- Data mining/matching
- Research Leads
- Refine Analytics
FIELDWORK: DATA ANALYTICS

Audit Sampling
- Statistical sampling
- Non-statistical sampling

Detailed Analysis
- Identify data gaps
- Observe exceptional trend

Continuous Auditing
- Full population coverage
- Automated process
- Continuous monitoring of red flags, errors, and cost-savings
FIELDWORK: DATA ANALYTICS

Factors to consider in choosing the appropriate DA tools:

- Data Size
- Analysis Type
- Ability to Customise
- Ease of Re-running Analysis

**Choice of DA Tools**

**DA Tools:**
- MS Excel
- MS Access
- IDEA / ACL
- SQL Server
- Oracle
- SAS
DA EXAMPLE

Scope: Account payable expense audit
DA tool: Tableau
DA rule: - Multiple payment records made to each vendor per month
- Average days to pay by vendor

Multiple payment records:

Average days to pay vendors:
DA EXAMPLE

Scope: Expense analysis by city
DA tool: Tableau
Result: Intuitively show the result on the map
FIELDWORK: BACKGROUND CHECK

- ‘A process of looking up and compiling criminal records, commercial records and financial records of an individual or an organization.’ - Wikipedia

- Examples of checks that can be performed:

  - Public records
  - Social-network analysis
  - Internet searches
  - Cold calling
FIELDWORK – SITE VISIT

- Advantages
  - Authenticate event hosted by third parties
  - Verify third parties’ existence
  - Validate the reasonableness of vendors’ price
  - “Seeing is believing”
INTERNAL AUDIT PROCESS: REPORTING

Typical internal audit process: Planning, Fieldwork, and Reporting

① Planning
• Fraud risk assessment
• Data analytics

② Fieldwork
• Data analytics
• Background check
• Site visits

③ Reporting
• Data analytics
• Fraud response protocol
REPORTING: DATA ANALYTICS

➢ Why we need to visualize the data? *A picture is worth a thousand words.*

**Trend analysis:**

**Purchase behavioral analysis:**

**Ratio analysis:**

**Relationship analysis:**
REPORTING: FRAUD RESPONSE PROTOCOL

Integrated Audit

Fraud Response Protocol

Audit project

Red flags found

Escalate case to investigation team

Initiate investigation

Report findings to stakeholders
(Management, Operational Risk Management, and Audit Committee)

Implement disciplinary/ remedial action
**REAL-LIFE EXAMPLES: DISCOVERY OF “SPLIT” PAYMENTS**

- Audit scope: Expense audit
- Observations:
  - Two payments purchased for the similar products/services were made on the same date, paid to the same vendor, and requested by the same employee.
  - However, one payment amount was only a little below the threshold (USD5,000) for price comparison.

<table>
<thead>
<tr>
<th>Ref</th>
<th>Request Date</th>
<th>Requester's Team</th>
<th>Requester</th>
<th>Procurement details</th>
<th>Amount</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11/30/2011</td>
<td>Marketing Development</td>
<td>Peter</td>
<td>IPCI product brochure design</td>
<td>4850</td>
<td>ABC Advertising Company</td>
</tr>
<tr>
<td>2</td>
<td>11/30/2011</td>
<td>Marketing Development</td>
<td>Peter</td>
<td>IPCI product poster design</td>
<td>1001</td>
<td>ABC Advertising Company</td>
</tr>
<tr>
<td>3</td>
<td>11/23/2011</td>
<td>Marketing Development</td>
<td>Peter</td>
<td>LES Sales Board for Branch #2</td>
<td>4980</td>
<td>ABC Advertising Company</td>
</tr>
<tr>
<td>4</td>
<td>11/23/2011</td>
<td>Marketing Development</td>
<td>Peter</td>
<td>LES Sales Board for Branch #5</td>
<td>4975</td>
<td>ABC Advertising Company</td>
</tr>
<tr>
<td>5</td>
<td>11/9/2012</td>
<td>Marketing Development</td>
<td>Peter</td>
<td>Gift for the event - Tablet</td>
<td>4000</td>
<td>XYZ E-commerce Company</td>
</tr>
<tr>
<td>6</td>
<td>11/9/2012</td>
<td>Marketing Development</td>
<td>Peter</td>
<td>Gift for the event - Digital camera</td>
<td>4950</td>
<td>XYZ E-commerce Company</td>
</tr>
</tbody>
</table>

- Same request day
- Same requester
- Purchase for similar product
- Same vendor
REAL-LIFE EXAMPLES: UNRAVELLING OF BID RIGGING SCHEME

- Audit scope: Procurement audit
- Observations:
  - Vendor who always win for every tender in which they participate (e.g., Vendor 1)
  - Vendor who always loses and still keeps participating in tenders (e.g., Vendor 9)
FRAUD HEALTH CHECK

- Comparison with integrated audit and fraud health check
- Typical process
- Typical testing approach
**FRAUD HEALTH CHECK (FHC)**

A process of identifying specific weaknesses through which fraud, or other forms of avoidable loss and compliance breaches, could occur.

### Integrated audits vs. fraud health checks

<table>
<thead>
<tr>
<th>Integrated Audits*</th>
<th>Fraud Health Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify, test, and verify control effectiveness</td>
<td>Focus on authenticity of transaction</td>
</tr>
</tbody>
</table>
| • Findings on control gaps and deficiencies  
  • Identify red flags/anomalies by using forensic investigation techniques | Identify potential fraud and compliance risks embedded in a transaction |
| • Sample selection based on unbiased procedures (sometimes random)  
  • Specific transactions are selected for analysis when anomalies are found | Risk-based sampling methodology (e.g., using keyword searches, trends, and patterns) |

* Internal audits integrated with forensic investigation techniques.
TYPICAL PROCESS ADOPTED IN FHC

**Scoping**
- Identify area(s) where fraud risks could most likely occur.
- Assess potential fraud scenarios (i.e., fraud risk assessment).
- Design testing procedures correspond to potential fraud risks.

**Data gathering & analysis**
- Initiate data and information request.
- Where possible, apply forensic data analysis for identification of high-risk samples.

**Testing**
- Red flag testing to identify anomalies.
- Perform authenticity checks on the anomalies (e.g., site visit, cold calling, internet searches, etc.).

**Reporting**
- Present to management the findings and observations.
- Identify and suggest options for improvement or remediation.
- Depending on severity, report potential fraud to senior management for immediate remediation.
TYPICAL TESTING APPROACH

- **Document examination**
  - Establish genuineness, expose forgery, reveal alterations, additions, or deletions.

- **Identify proof of performance**
  - Did the contractor really perform the service?
  - What is the physical evidence to prove the transaction was really occurred?

- **Obtain market indications**
  - Has this vendor potentially over-charged us?
  - Involve or consult industry expert if necessary.

- **Do not assume but see with your own eyes**
  - Perform site visit to the location where a transaction occurred.
  - Inquiries with the parties involved.
CHALLENGES

- Practical challenges
- How to overcome these?
PRACTICAL CHALLENGES

Resistance to change
• Change the typical auditor’s mindset

Difficulties in applying effective DA
• Incomplete / poor quality data
• Effort required to integrate data from different systems

Investment required
• Expensive DA / forensic software
• Recruit staff with forensic expertise
HOW TO OVERCOME?

- Set the tone from the top by the Chief Audit Head to enforce such integration.

- Establish written guidelines / internal initiatives to drive the change.

- Develop a common data warehouse / enterprise architecture to facilitate data analytics.

- Increase training / hands-on experience for the auditors to apply forensic investigation techniques during audits.

- Show management the value proposition for investment.
CONCLUSION
CONCLUSION

For AIA, by integrating forensic techniques into internal audits, we have found:

- Improved quality audits conducted
- Increased professional skepticism
- Enhanced fraud detection during audits. Year to-date, there is a 13% increase in red flag detection through internal audit findings.
- Reduced incidence of fraud
QUESTIONS?