CASEWARE

COMBAT FRAUD USING AUDIT ANALYTICS

A CaseWare eBook

INTRODUCTION

The ACFE's 2018 Report to the Nations - Global Study on Occupational Fraud and Abuse recently revealed that, globally, the rate of occupational fraud affecting organisations has risen sharply in the last two years, from £4.7bn ($6.3bn) to £5.3bn ($7bn), with a median loss per case now sitting at £99,000. The median loss per case was even more significant for small businesses with <100 employees, sitting at £152,000.

The drive to improve efficiencies and streamline supply chains has led many organisations into unwittingly opening themselves up to both internal and external fraud. By adopting semi-automated IT systems to support their day-to-day business processes, systems that reduce the level of human intervention required (which traditionally acts as a fraud control in and of itself), organisations make themselves more reliant on annual audits and tips to identify fraud after the fact.

It was identified that internal control weaknesses were responsible for nearly half of frauds committed. Conversely, it was found that in every instance where a system of anti-fraud control was utilised, businesses enjoyed faster detection rates and lower resulting losses. Other benefits include:

- Identifying employees vulnerable to fraud
- Organisational controls that help prevent repeat instances of fraud
- Gaining/reinforcing the trust and confidence of stakeholders of the organisation

The largest reductions in losses occurred in those cases where data analytics and surprise audits were involved, with the average detection rates being 56% faster and 52% more losses being recouped.

WHAT ARE THE MOST COMMON TYPES OF FRAUD?

According to the International Standard on Auditing (ISA) 240 the two most relevant types of fraud to the auditor are misstatements arising from both fraudulent financial reporting and misappropriation of assets.

Fraudulent Financial Reporting

Involving intentional misstatements such as omissions of amounts or disclosures in financial statements aimed to deceive financial statement users. Fraudulent financial reporting can be accomplished by:

1. Manipulation, falsification (including forgery), or alteration of accounting records or supporting documentation from which the financial statements are prepared

2. Misrepresentation in, or intentional omission from, the financial statements of events, transactions or other significant information.

3. Intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure.

Fraudulent financial reporting often involves management override of controls that otherwise may appear to be operating effectively. Fraud can be committed by management overriding controls using such techniques as:

- Recording fictitious journal entries, particularly close to the end of an accounting period, to manipulate operating results or achieve other objectives.
- Inappropriately adjusting assumptions and changing judgments used to estimate account balances. For example, changing stock provision calculations.
- Omitting, advancing or delaying recognition in the financial statements of events and transactions that have occurred during the reporting period.
- Concealing, or not disclosing, facts that could affect the amounts recorded in the financial statements.
- Engaging in complex transactions that are structured to misrepresent the financial position or financial performance of the entity.
- Altering records or naming conventions related to significant and unusual transactions.

MISAPPROPRIATION OF ASSETS

Misappropriation of assets involves the theft of an entity's assets and is often perpetrated by employees in relatively small and immaterial amounts. However, it can also involve management who are usually more able to disguise or conceal misappropriations in ways that are difficult to detect.

Misappropriation of assets can be accomplished in a variety of ways including:

- Embezzling receipts at POS – voiding transactions, false returns, unauthorised discounts
- Removing physical assets or intellectual property
- Causing an entity to pay for goods and services not received
- Using an entity's assets for personal use

Misappropriation of assets is often accompanied by false or misleading records or documents in order to conceal the fact that the assets are missing or have been pledged without proper authorisation.

HOW DATA ANALYTICS CAN HELP

Whether you are dealing with employee abuse of company cards, high-value contract fraud and breaches of controls, or simple theft, data analytics can have a significant role to play in early-warning, detection, and monitoring of fraud.

Whilst previously you might have relied upon stratified or random sampling to test the veracity and completeness of your data, such analyses might not be sufficient to fully quantify the potential impact of fraud on your business. Certain fraudulent transactions–especially those being perpetrated by more experienced fraudsters–may well fall outside the boundaries of sample testing and as such not be flagged. It is here that automated and continuous analysis comes into play.

By using your previous experiences of fraud, and your knowledge of common fraud indicators, you can develop a series of standardised fraud analytics tests that can be run against your organisation's business data on a scheduled or ad-hoc basis. Classic examples of fraud that can be easily detected via a reliable data analytics solution, and thus challenged, include:

Journal Entries gaps

Easily identify:

- Missing items, such as P.O. number or invoice dates

Duplicate and fuzzy duplicate detection

Easily identify:

- Sales invoices with duplicate invoice numbers or similar customer data (e.g. name or address)
- Duplicate debtor numbers or names/addresses
- Duplicate payments to suppliers
- Duplicate creditors by looking for names and addresses, bank account details etc.
- Duplicate fixed asset reference/serial numbers
- Stock duplicate parts, item numbers, prices or descriptions

Fuzzy Duplicate detection identifies multiple similar records:

- Data entry (e.g., "Compny" instead of "Company")
- Multiple data conventions for recording information (e.g., "J P Smith" vs. "John Peterson Smith")
- Invoice numbers; 1234 and 1234a etc.

HOW DATA ANALYTICS CAN HELP (CONT.)

Time and Expenses anomalies

Easily identify:

- Unauthorised time or expenses filed outside of normal working days (e.g. weekends or bank holidays)
- Overlapping time sheets filed separately
- Expenses not related to legitimate working activities
- Overtime abuse
- Payments to ghost employees

Reconciliation of separate datasets (e.g. Supplier versus Customer or Supplier versus Own)

Easily identify:

- Supplier entries not included on authorised supplier list
- Customer entries not included on authorised customer list
- Supplier data, for example bank details, that matches employee data
- Instances where expected output does not match previous
- Diversion of payments

P2P analysis

- Cancelled cheques
- Invoices paid without corresponding order
- Unauthorised payments or payments authorised by recipient
- Transactions with unapproved or duplicate suppliers
- Order splitting – identical items purchased simultaneously or within a short period of time that fall under authorisation limits

Manager-level fraudsters are most likely to alter existing evidence to conceal their activities, whilst owner/executive-level fraudsters are more likely to create evidence or delete evidence entirely. 80% of reported concealment included creation of evidence, 80% included alteration of existing evidence, and 43% included destruction of evidence.[1]

1 Association of Certified Fraud Examiners (2018). Report to the Nations 2018 Global Study on Occupational Fraud and Abuse. Report to the Nations. p.15.

THE DATA ANALYSIS POWERHOUSE

Spreadsheets are simply not equipped with many of the core capabilities that auditors require to audit effectively.

If you're looking for a secure, extensive, and efficient way to audit, then CaseWare IDEA Data Analytics is the professional data analysis solution for you. With more than 500,000 users in 130 countries, CaseWare technologies are built upon the foundation of best practices in assessing risk and controls, enabling audit and finance professionals to use real data insights to create remarkable ROI and business improvement opportunities.

To learn more about how IDEA can help you complete your audits quickly and effectively, or to enjoy a free live demonstration of IDEA in action, contact us at sales@caseware.co.uk or +44 (0)1622 355200. You can also visit us at www.CaseWare.co.uk to schedule your free demo.

CaseWare

Sales & Enquiries
UK: **01622 355 200**
IE: **0818 333 981**
contact@caseware.co.uk

Technical Support
UK: **01622 355 250**
IE: **0818 333 980**

www.caseware.co.uk

CaseWare UK Ltd | County Gate 2,
Staceys Street, Maidstone, Kent, ME14 1ST