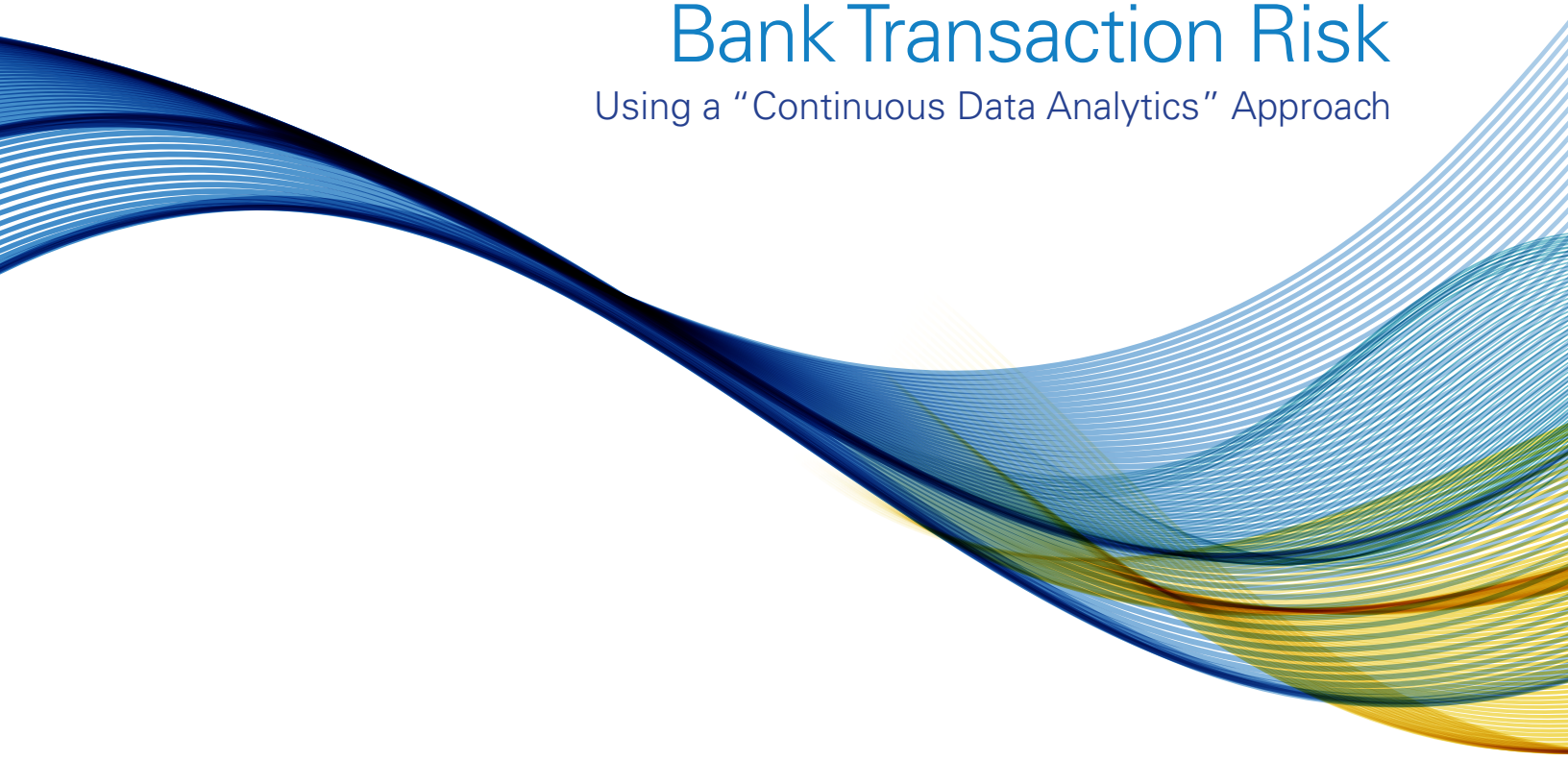
CaseWare Analytics

# Best Practices for Managing Bank Transaction Risk

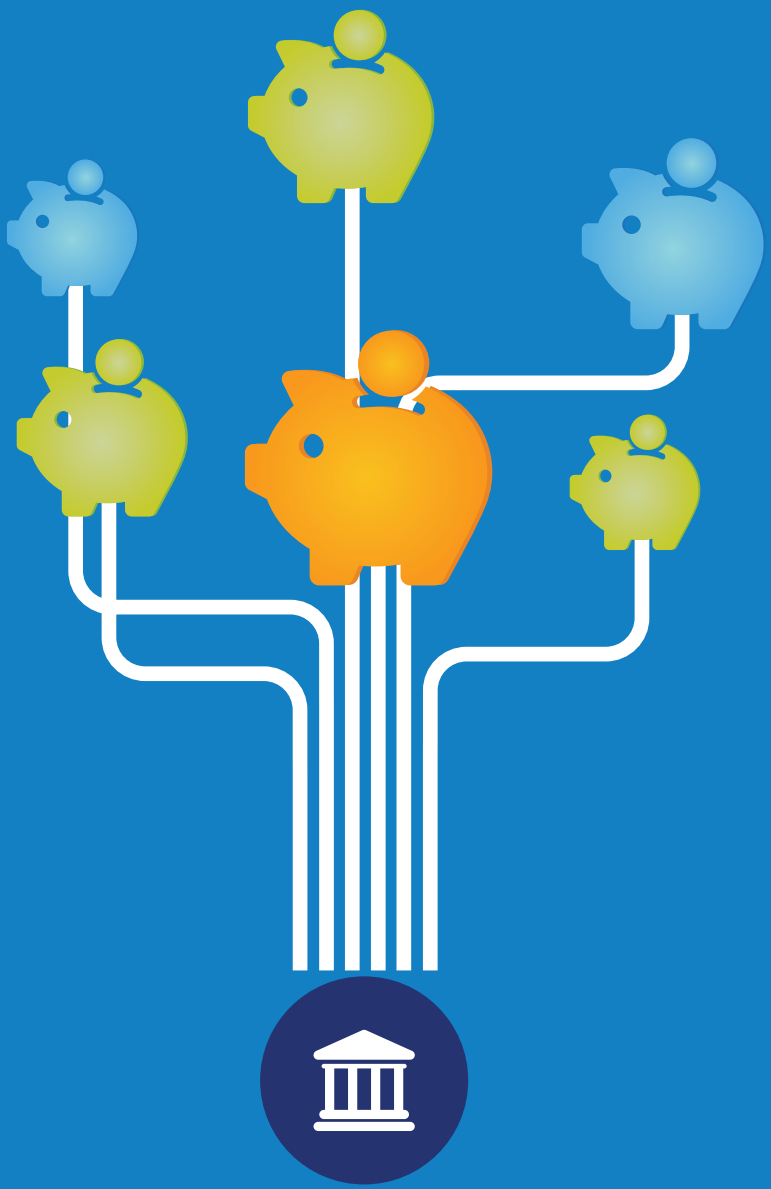
## Using a "Continuous Data Analytics" Approach



**Co-authored by:**
Focus Technology Group

# Contents





## Introduction

Every bank's prospective earnings and capital are exposed to a constant stream of transaction risk. There is **inside transaction risk** that may involve fraud schemes, control overrides and errors & omissions, as well as **outside transaction risk** such as check and debit card fraud, EFT fraud, account takeover and information theft. No bank is immune for all processes have weaknesses that can be exploited.

To protect themselves, most banks have implemented specific anti-fraud prevention and detection measures. These measures include employee screening, audits, fraud training, physical cash counts, etc. However, most risk professionals know that even with these specific controls in place, significant transaction risk may still be present at the bank. Therefore, the next step to protect earnings and capital is to ask the following questions:

- Is our transaction risk management program documented with responsibilities formally assigned?
- How have we validated the effectiveness of our transaction risk management program?
- Can we make our transaction risk management program more cost-effective?

If your answer to any of these questions is there is room for improvement then you should consider implementing a more focused technology driven risk management approach.

## The Approach

A technology driven risk management approach can enhance a bank's insight into its own transaction risk. This will provide the user the ability to identify risk events that may have slipped through a bank's control systems. Banks that use this proactive approach reduce losses and risk by making more informed and timely decisions.

In today's complex banking transaction environment, it is imperative for banks to use data analytics to manage their transaction risk. Data analytics testing should be linked to a risk assessment designed to identify red flags (e.g. transactions, data, trends, etc.) associated with fraud schemes, errors & omissions, internal control performance, etc. Consideration should be given to performing data analytics over the higher risk activities using continuous auditing or continuous monitoring on a more frequent basis. This allows banks to find the existence of risk events and control breakdowns to stem financial losses and other adverse events quickly before they become significant.

This approach results in a more effective and efficient use of resources, yielding more substantial results.

Next we will examine how to apply and integrate these processes (risk assessments, data analytics and continuous auditing/monitoring) into a transaction risk management program.

## Risk Assessment

Implementing an effective transaction risk management program is the by-product of performing a risk assessment. Understanding where transaction risks are hurting the bank most, or are likely to hurt the bank, provides a good starting point for where to focus risk management efforts. For example, if the risk focus is fraud, the bank is subject to specific types of fraud schemes, such as loan fraud, account takeover fraud, debit card fraud, ACH fraud or wire fraud. Therefore, the bank may want to select those fraud types as a starting point.

The transaction risks that can be addressed through a risk assessment include:

- Internal and external fraud
- Policy and procedural non-compliance
- Errors & omissions
- Money laundering

Banks can design their risk assessment to meet specific needs and assess risks within multiple contexts such as: the enterprise; a business process; or class of accounts. A formal risk assessment looks at the inherent risk (significance and likelihood) and evaluates the controls over that risk. In a fraud risk assessment the persons/positions that can actually perpetrate the fraud, inside and outside of the bank, must also be considered. The resulting risk, after factoring in controls and separation of duties considerations, is called the residual risk. It is this that must be addressed. The bank can elect to accept the current level of risk or take the necessary steps to mitigate it.

A thorough risk assessment will identify the **red flags** which are reliable indicators of any risks that may be present. The red flags can be aligned with specific data analysis tests.

## Risk Data Analytics

Using Computer Assisted Audit Tools (CAATs) and data analysis to support transaction risk management efforts allows banks to set-up comprehensive coverage and increases the likelihood of detecting risk events, using fewer resources.

A bank that has performed a risk assessment will be able to design and align specific data analysis tests to the areas of greatest risk. For example, data analysis tests can be designed to detect the existence of the red flags of Account Takeover Fraud identified during the fraud risk assessment.

Some banks may prefer to jump directly into performing data analytics to identify areas of risk prior to performing an assessment. This gives the advantage of providing an immediate "real-time" view of how the risk area is operating, in addition to identifying risk events.

Data analytics tests should be constructed well enough to identify the exceptions/red flags common to the risk area under review. They must provide enough information for the user to understand what the potential impact could be. In the banking environment, data analytics tests should link and analyze data from varied sources within banking systems, such as customer, account, transaction, parameter and maintenance files. Tests can be expanded or reduced based on results and can continue to be redefined to improve results. The goal is to develop repeatable and sustainable tests.

Ultimately, all data analytics tests performed should align with a risk assessment. Aligning each data analysis test with the red flags identified in the risk assessment validates the purpose for the test. When there are changes to the risk areas, those changes in the risk levels will then prompt a review of the data analysis test so that it continues to reflect the current level of risk.

Once the analytics tests are executed, the results will enable banks to accomplish three things:

- Identify actual risk events
- Evaluate the effectiveness of controls
- Determine the level of risk that is occurring

## Continuous Monitoring & Auditing

Continuously performing certain data analytics tests for auditing or monitoring purposes on a regular schedule should be considered by every bank. A continuous approach requires less effort and allows for expanded coverage without adding resources. For example, a bank's internal auditors annually review the controls and test transactions on dormant accounts. Currently, monitoring activity to dormant accounts on a day-to-day basis is the responsibility of the Operations Group. However, the fraud risk assessment shows that 90% of the bank's employees have system access that allows them to change dormant account codes so that any financial activity to those accounts may not appear on the Operations Group's dormant accounts activity reports. Therefore, as a compensating control, a data analysis test can be developed to identify suspicious changes to dormant account codes. The data analysis tests can be run on a weekly basis and monitored by the Operations Group Fraud Unit, - which does not have system access. In this environment, any fraudulent attempts will be identified in a timely manner and now this high risk area is under better control.

Additionally, continuous monitoring and auditing can provide a snapshot of the bank's current state. This is important as the evolving nature of risks can render certain high-value controls ineffective even over a short period of time. This means the risk assessments themselves need to be monitored to make sure they are current.

Continuous monitoring and auditing lend themselves well to showing trends which can reveal issues that isolated data cannot.

## Summary

Board-, management-, customer- and regulatory expectations for bank transaction risk management have never been greater nor the stakes higher in today's competitive bank environment. Reducing transaction risk in an effective and efficient manner protects each bank's bottom line by reducing losses, penalties and operational costs. Now is the time for banks to transition to a more risk-focused and continuous approach to manage transaction risk that leverages technology.

## About Us

Founded in 1988, CaseWare is an industry leader in providing technology solutions for finance and accounting, governance, and risk and audit professionals. With over 400,000 users in 130 countries and 16 languages, CaseWare products deliver tremendous value across industries and continents

CaseWare Analytics
469 King Street W. Suite 200
Toronto, ON, M5V 1K4
1-800-265-4332 Ext: 2803
www.casewareanalytics.com