

SOLUTION OVERVIEW

RETAIL AND DISTRIBUTION

The Retail and Distribution Business

Effective loss prevention continues to be an essential activity for the Retail Industry. The ongoing evolution of customer purchasing trends, technology and fraudulent activity are major factors. According to The Centre for Retail Research¹ an estimated 58% of all shrinkage is attributable to internal theft and errors in vendor/supplier related activity.

The constantly changing nature of retail shrinkage can only be contested through a greater understanding of the business activities within an organization's internal control environment. Most retailers are already using technology to do in-store analysis and examine point-of-sale (POS) data to identify customer buying patterns for creation of better marketing and sales campaigns to drive revenues. Similar emphasis and focus should be placed on protecting revenues not only in stores but throughout the process lifecycle from stock source to POS. In an industry with razor thin margins, fraud, errors or inefficiencies in any aspect of the business could be the difference between profit and loss.

In a recent KPMG Fraud Survey Report, inadequate oversight and lack of clarity regarding ownership of controls are cited as key factors leading to ineffective fraud prevention. Examples include individuals being temporarily assigned 'super' user rights but are not revoked at the correct time or exception reports going to stakeholders that cannot take action to remediate issues before they become material to the organization.

Retail fraud and abuse schemes can come from varying angles, such as:

- Unusual, Excessive and Unauthorized Discounts
- Segregation of Duties Violations
- Invoicing Errors & Fraud
- Lack of Policy Enforcements
- Vendor/Employee Collusion

These issues are a source of frustration for management in their efforts to gain visibility into their business processes and final revenue recognition. They want to foster an environment that strikes the delicate balance between stringent fraud prevention and an optimal customer experience to maximize revenues amidst ever changing market conditions.

Continuous Monitoring

Continuous monitoring provides an organization with an independent point of observation over their entire business. The technology enables all aspects of any business process to be monitored holistically and removes blind spots associated with monitoring only a single application.

Insight

How internal controls fail to prevent frauds:

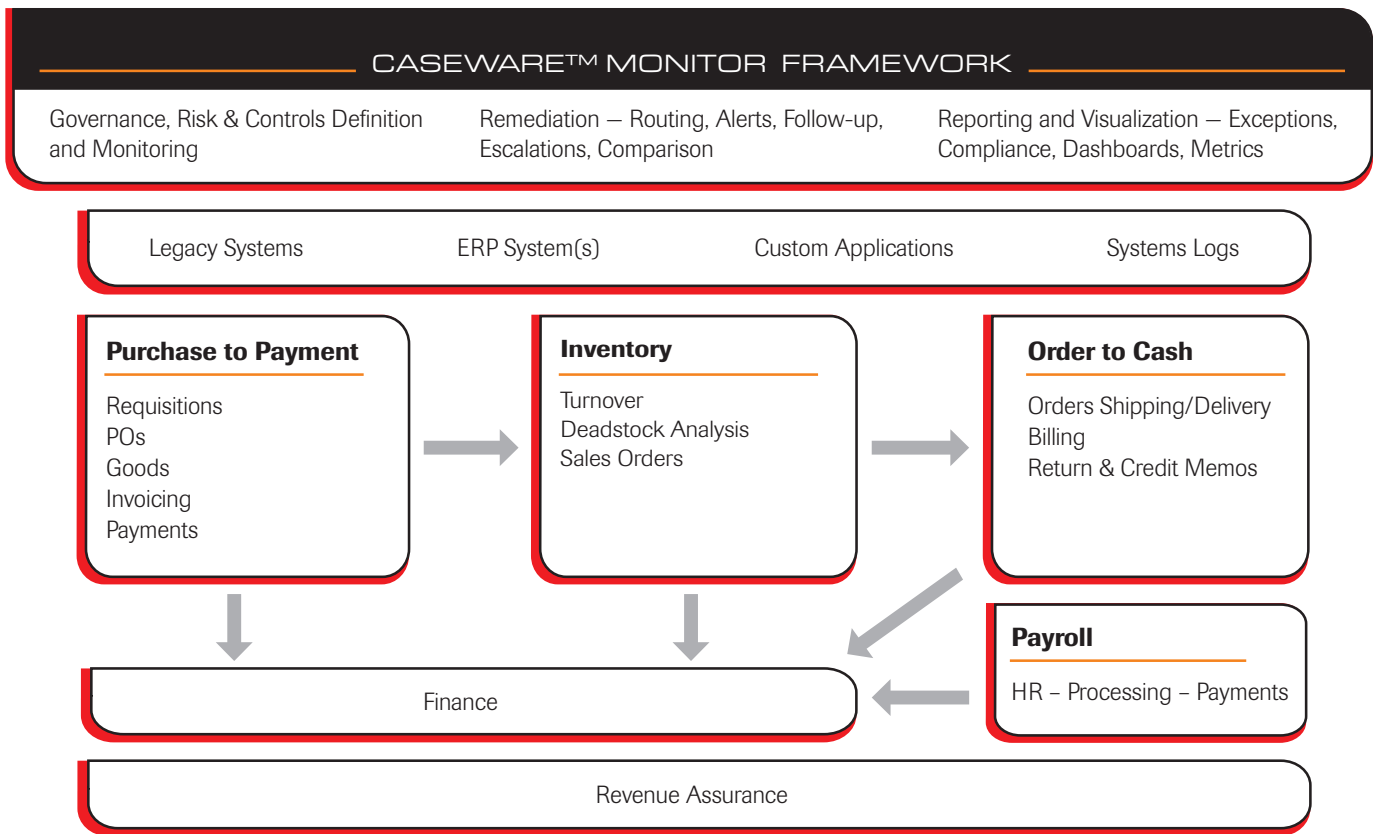
- Lack of clarity in assigning ownership for internal controls
- Controls were not updated in conjunction with changes to the process
- Failure to implement any type of early warning indicators or monitoring activity
- Lack of assessment of the effectiveness of supervisory controls

KPMG India Fraud Survey Report 2010

¹ 2010 Global Retail Theft Barometer

Potential breakdown in internal controls are flagged as they occur, within a framework, ensuring that they are addressed in a timely manner. CaseWare™ Monitor enables all processes to be monitored regardless of the underlying systems, data sources, platforms or locations. Results from these disparate sources are consolidated and presented in CaseWare™ Monitor for use by any authorized users, regardless of location.

Figure 1 – CaseWare™ Monitor for Retail



Through a single portal coupled with built-in workflow and notification, all stakeholders and key decision makers can independently monitor processes across varying businesses and systems. This collaborative framework helps users across multiple departments such as loss prevention, procurement, finance, operations, and audit, to detect and correct errors and abuses before they become detrimental.

All facets of the Retail processes from order fulfilment through to invoicing and billing can be monitored to provide insight into specific issues as well as the overall health of the internal controls. Notifications and workflow management are built into the CaseWare™ Monitor framework ensuring that issues receive proper attention and their resolution managed. Various stakeholders such as Loss Prevention, Operations or Audit can easily identify control breaches, fraud and money leakage, while CaseWare™ Monitor ensures data quality and provides feedback on key performance metrics across any or all business processes.

Workflow and Reporting

When a breach occurs relevant alerts are triggered and a stringent remediation process is followed to ensure that high risk activities are addressed as stipulated by the business process owners. Other key aspects of the solution are the automation of reporting and visualization of the control environment. CaseWare™ Monitor Retail Solution automates key reporting for stakeholders, including statutory and regulatory bodies.

Standard dashboards are included in the framework:

- Trending of results across dates
- Grouping by risk ranking
- Grouping by status (new, pending, overdue, etc.)
- Comparisons across processes and users

SAMPLE OF RETAIL MONITORING REPORTS

Inventory Analysis

Highest/Lowest Turnover

Price Change Impact

Vendor Management

Potential Duplicated Vendors

Vendor – Employee and other Related Parties Matching

Requisitioning

Split Requisitions

Requisition SOD Conflicts

Purchasing

PO vs. Requisition

Purchase Order SOD Conflicts

Receiving

Received vs. Purchased

Receiving SOD Conflicts

Invoicing

Invoice Numbers Sequence Anomalies

Split Invoices

Invoicing SOD Conflicts

Orphaned Invoices

Excessive Credits or Returns

Billing Delays and/or Errors

Payments

Duplicate Payments

Rapid Payment

Payment SOD Conflicts

Order Fulfilment

Discount Overrides

Variations in Unit of Measure

Pending Shortages

SOD Violations

Shipping & Delivery

Shipping Price differs from Billing Price

SOD – Shipments with Invalid Creator

SOD – Shipper same as Invoicer

Customer Checks

Prohibited Customers

Duplicate Customers

Policies Enforcement

List Price vs Order Price

Return Policy Not Enforced

BENEFITS

BUSINESS CHALLENGE

CASEWARE™ MONITOR SOLUTION

STAKEHOLDERS' REQUIREMENTS

Escalating risk and compliance requirements

- Provide enterprise-wide definition and monitoring of controls and assurances that they are effectively implemented across all business processes.

AUTOMATION

Automating control breach detection and remediation

- Detects breaches at the data source.
- Distributes data across the enterprise by user-defined rules via dashboards, e-mail, SMS
- Provides workflow for remediation including automatic detection of resolution of errors
- Allows the user to define controls in multiple business processes with a consolidated view
- Increases efficiency by making analytics repeatable with the ability to adjust tolerances
- Business rules and parameters are customizable and new logic can be built by the organization
- Monitoring can also be applied to business metrics
- Issues are identified as soon as they occur

INTEGRATION

Seamless integration into existing solutions

- No changes required to underlying systems being monitored
- Non-intrusive access to data and cannot amend source data
- User and group security with LDAP support
- Strong encryption
- Distributed service oriented architecture (SOA).

PROCESS OPTIMIZATION

Makes the process more efficient and less costly

- Issues detected on a more timely basis
- Lower recovery costs
- Greater level of automation
- Compliance and other reporting automatically generated
- Knowledge and expertise captured in the control systems and made repeatable



CaseWare RCM Inc.

1420 Blair Place, Suite 400
Ottawa, Ontario, Canada K1J 9L8

Phone: +613 842 7920 ext. 712
Fax: +613 842 9475

Email: rcmsales@caseware.com
www.caseware.com