CaseWare Analytics

Solution Overview

Segregation of Duties Overview

Segregation of Duties

The main elements required for fraud are motivation and opportunity. Accordingly, the best opportunity a company can offer a fraudster is weak or nonexistent Segregation of Duties (SoD). SoD is a critical internal control aimed at limiting opportunities for abuse by a single person, such as requiring two signatures on a check or separating the creation and approval of sensitive transactions.

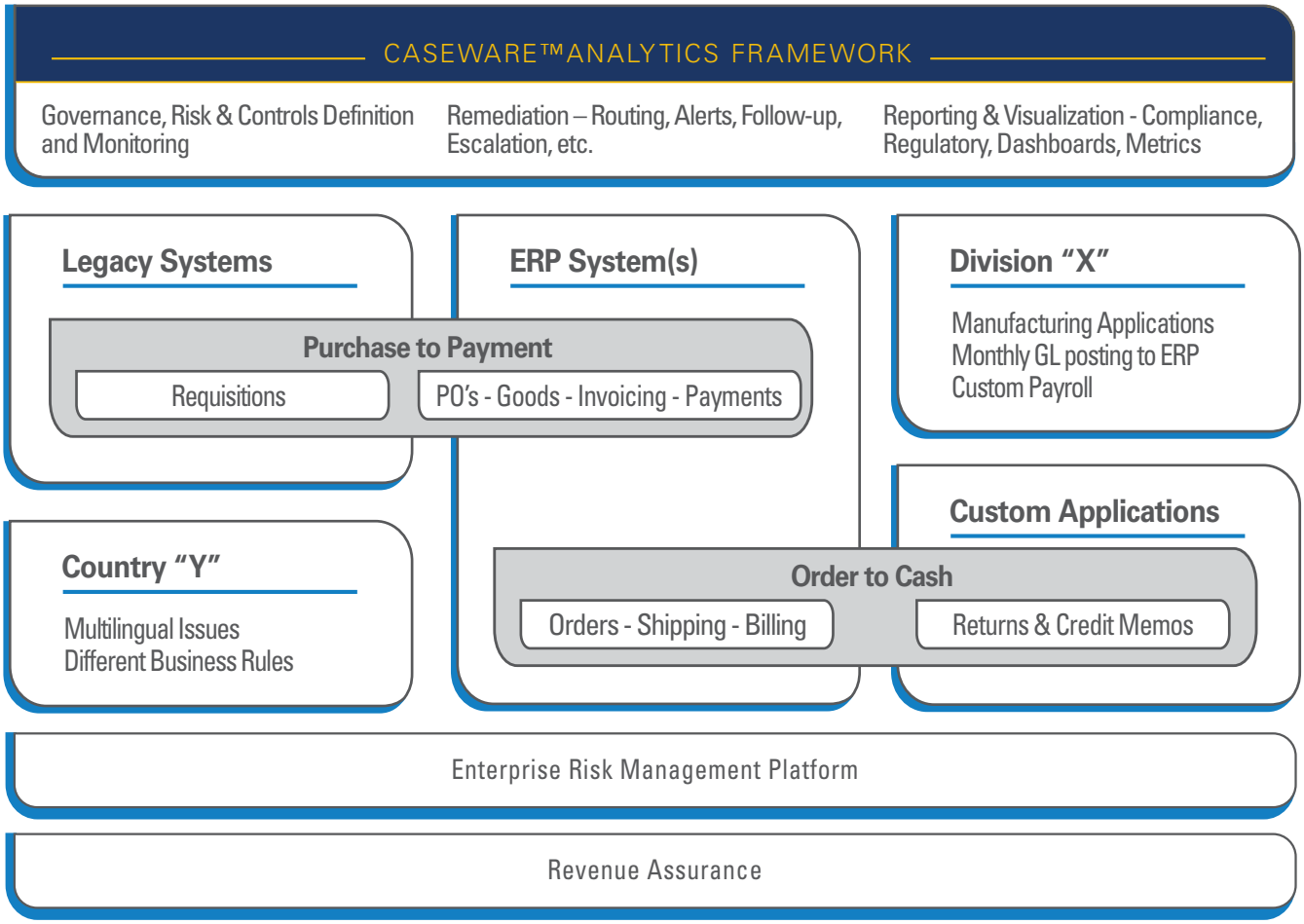
In today's automated business processes, SoD is enforced through business applications and ERPs, making breakdowns in these controls difficult to detect. SoD conflicts caused by insufficient staffing create the physical inability to properly segregate duties, and are worsened by poor or missing controls, such as the segregation of authorization and approval, or budgeting and actual reconciliation.

In one case, a major hi-tech corporation discovered a fraud that had been going on for over seven years. Employees who were checked and validated within the ERP system had additional privileges in other legacy systems within the same business process. The fraud cost the company over $18M, resulting in restatement of their earnings. This case highlights the fact that even with mature ERP systems, issues can inadvertently arise that lead to SoD violations. For example, elevated permissions are given to someone covering for a vacationing employee or an employee inherits elevated privileges from another security group. These types of SoD issues are not caught using the ERP's application controls.

CaseWare™ Analytics SoD Monitoring

CaseWare Analytics enables a holistic approach to monitoring segregation of duties, giving a bird's eye view of all applications. This ensures that user authorizations are properly compartmentalized regardless of the business application, and as a secondary benefit, provides assurance that interfaces between different systems and business operations are working correctly. The CaseWare Analytics platform is an open framework and not application specific, so it can easily adapt to business process changes. Notifications and workflow management are built into the platform, ensuring that issues receive proper attention and their resolutions can be managed.

Figure 1 - CaseWare™ SoD Platform



Solution Benefits

360° View

Within a common portal, all stakeholders can examine SoD holistically across the enterprise, allowing for greater transparency and fraud prevention.

Reduce SoD Risk

Automated monitoring of SoD controls immediately recognizes violations and sends notifications to relevant personnel to ensure that the organization is not negatively impacted.

CaseWare Analytics Capabilities

24/7 Automated Analysis

Ongoing and automated analysis of all data within ERP and custom applications to detect SoD breaches.

Supports Existing Systems

Support any business process on any system and data from any source, without additional infrastructure and integrates easily with any system:

- ERPs such as SAP®, Oracle®, Microsoft Dynamics, etc.
- Data analysis scripting tools such as IDEA®, ACL™ and Arbutus™

Workflow for Managing All Violations

- Identification of Potential Issues i.e. Excessive Management Overrides
- Immediate issue notification via email, sms or dashboard
- Tracking & status updates of resolutions

Segregation of Duties Analytics

Application Controls	❍ Evaluate transactional data against control settings ❍ Identify where custom transactions or programs may be inadvertently bypassing standard system controls ❍ Compare application control settings to control tables to identify potential changes ❍ Identify excessive use of system override
Change Controls	❍ Identify program changes not appearing on change control logs ❍ Compare key program or file size, timestamps, and other characteristics to a control table to identify instances where a change has occurred ❍ Evaluate emergency change frequency by user, application, department, etc.

Segregation of Duties Analytics (continued)

Application & System Security	❍ Extract security rules and independently verify SoD ❍ On potential SoD issues are identified, determine whether rights were exploited ❍ Examine the user IDs associated with specific transactions to determine whether SoD violations have occurred (e.g. initiator = approver) ❍ Identify where users with the same role have different access rights ❍ Highlight users with powerful profiles / responsibilities ❍ Identify user profile / responsibility changes made immediate prior to or shortly after an audit ❍ Identify concurrent logins of the same ID ❍ Look for patterns of failed access attempts to key users (CEO, CFO, Payroll, etc.)
Data Quality	❍ Analyze master data for missing information ❍ Identify inconsistencies in data input ❍ Detect duplicate records ❍ Assess data for suspicious or erroneous entries (e.g., description fields with less than 2 characters input) ❍ Stratify quality metrics by employee to identify training opportunities ❍ Identify outdated or unused information

469 King Street West, 2nd Floor
Toronto, Ontario M5V 1K4
1-800-265-4332 Ext: 2803
sales@caseware-idea.com
www.casewareanalytics.com