



Continuous in Action

John Scrivener
Technical PreSales Manager
Toronto, Canada



The Flavours of Continuous

SymSure Monitoring Framework





Case Study - Continuous Auditing

- **Company 'X' is a restaurant chain**
 - ▶ Fortune 1000, over \$2B in sales
 - ▶ Over ten (10) thousand restaurants worldwide

- **Management mandates that GL entries are to be analysed**
 - ▶ GL Entries posted outside of working hours (9am – 5pm)
 - ▶ Weekend and holiday postings
 - ▶ Sensitive GL Accounts (Hedging, etc)
 - ▶ Postings over threshold
 - Frequency,, cumulative amounts

- **Exceptions are to be distributed and reviewed quarterly**
 - ▶ Summary reports to be generated and sent to management





Continuous Auditing – Old Technology

- **Audit prepares the first GL report**
 - ▶ Extracted from SAP, the number of GL records for the quarter far exceed the Excel 64k record limit
 - ‘Stratification’ spreadsheets are developed to compensate
 - \$0 > \$25k > \$100k > \$500k > \$1m > \$10m >
 - Five (5) spreadsheets are developed, each containing multiple levels of stratification
 - Spreadsheets are (continuously!) generated according to a schedule
- **Over 150 people can post GL entries**
 - Each person receives all five reports via email and reviews them, looking for their own entries
 - They then annotate their entries and send back the spreadsheets
- ***The auditor is now responsible for managing and aggregating 750 spreadsheets every quarter***





Continuous Auditing – New Technology

- **The five reports are recombined back into one (1) report with all of the GL entries**
- **A distribution list is created using the userid on each of the GL records**
- **The master distribution list is imported into the SymSure workflow engine**
 - ▶ Facilitates GL entry distribution and subsequent email alerting
- **The report is imported into SymSure and scheduled to run quarterly**
- **Elapsed time: 3 Days**
 - ▶ Software Installation & Configuration: ½ Day
 - ▶ Data Sourcing & Scripting: 1 Day
 - ▶ Integration with SymSure including workflow: ½ Day
 - ▶ Summary & Statistical Reporting: 1 Day
- **Day 4 & 5: User Testing & Final Presentation**





Net Benefits / Metrics

- **Users are only notified when they have exceptions to review**
- **They only get those entries that belong to them**
- **The quality of the reviews increased**
- **Overdue exceptions are automatically escalated back to Internal Audit**
- **Quarter end GL reporting is now automated**
- **Other manual IA tasks are now automated**
- **IA is now in control**





Lessons Learned

- **Rethink the ‘Continuous’ in Continuous Auditing**
 - ▶ The only continuous aspect of Excel is the amount of work generated
- **Manual reviews don’t work with automated systems**
 - ▶ This was only the first GL test to be implemented
- **Match the technology to the task**
 - ▶ If you need workflow, get the proper tools
- **When starting, identify onerous manual tasks to automate**
 - ▶ Manual SOX Tests are a good place to start
- **Find a specific problem and establish a hard ROI/baseline before any Pilot**
 - ▶ Labour costs in this case were significant, both for IA and the users





Case Study - Continuous Controls Monitoring

- **Company 'Y' is a large, diverse and dynamic corporate entity**
 - ▶ Publically traded, widely held
 - ▶ Over \$5B in Revenue

- **Operations span multiple lines of business:**
 - ▶ Financial, insurance, electronic remittance
 - ▶ Hardware retailing
 - ▶ Food processing & distribution industries

- **Highly Decentralized**
 - ▶ Over 50 subsidiaries and associated companies located in the United States, England and the Americas
 - ▶ Server infrastructure is also decentralized
 - ▶ Many legacy and custom systems





Pressing Governance Issues

- **Outside Auditor's report reveals serious IT deficiencies**
 - ▶ No monitoring of Windows Server Security Logs
 - ▶ User access privileges need to be reviewed regularly
 - ▶ Sensitive data is not monitored for unauthorized changes
 - ▶ Access to sensitive/incompatible SAP functions are not monitored
 - ▶ SoD controls need to be in place within SAP
 - ▶ SoD controls are needed between SAP, legacy systems & servers
- **Management mandates an enterprise-wide solution and final business case to be delivered within three (3) months**





Windows Server Tests

- ▶ Consistent access by a user outside of regular working hours
- ▶ Excessive failed attempts to access a specified user account
- ▶ Excessive failed attempts by a user to access functions to which they do not have access
- ▶ Access to a user account when the owner is no longer employed by the company
- ▶ Unauthorized creation of new user accounts





SAP Tests

- ▶ Unauthorized alteration of existing user rights
- ▶ Determination of unused SAP accounts based on a threshold
- ▶ Show all users with access to key/sensitive SAP functions
- ▶ Show all changes to key SAP tables - Customer & Vendor Masters
- ▶ Find all users with access to multiple SAP/custom sales applications



Net Benefits / Metrics

- **The business units were able to review and document exceptions while IT kept control of the final closure of the issues**
 - ▶ Audit has 'informational' access to all tests and transactions

- **The Test Results raised interesting issues:**
 - ▶ One user had 2,900 windows authentication events in one day
 - ▶ One SAP business process manager hadn't accessed the system in over 130 days
 - ▶ Another SAP buyer hadn't accessed the system for over 30 days
 - ▶ One user account was still being accessed after the employee left the company
 - ▶ Many users had access to sensitive SAP transactions

- **Security Log testing is run every two (2) hours**
 - ▶ Control breaches and alerts sent immediately to the business via email and SMS
 - ▶ Security Log reporting is run weekly and monthly for trending over time

- **Implementation completed in one (1) week**
 - ▶ *One ad-hoc test was requested during the pilot presentation and implemented live*





Lessons Learned

- **Controls that span across systems are very powerful**
 - ▶ Virtual Preventative Controls & Policies
- **Windows Security Logs aren't as complex as you think**
- **Audit has a lot to offer IT/IS**
 - ▶ Data quality tests, system introspection & improvements
- **Automate very specific & painful control points first**
 - ▶ User acceptance is not about the tests – it's about the pain
 - i.e. Finding a buyer who didn't use SAP for 30 days was ... 'dramatic'
- **Ask the External Auditors what controls to monitor**
 - ▶ Automate their periodic tests; give them remote access to the results
 - You will get more value for your auditing dollars





Current Trends

- **Over 50% of SymSure installations are now championed by the business**
 - ▶ Audit comes to the table with their own slate of tests
 - ▶ The relationship between audit and business is much more cooperative now
- **In mature GRC environments, active monitoring is a requirement**
 - ▶ SymSure feeds results directly back to GRC
- **IT/IS needs Continuous Monitoring as much as anyone**
 - ▶ This also helps to establish a bridge between Audit & IT
- **More and more interest in accessing monitoring devices**
 - ▶ Network analyzers, firewalls, data collection appliances (i.e. Logs)
- **Companies begin by moving existing tests, reports & metrics**
 - ▶ Test automation i.e. SOX is popular
- **Most SymSure customers have multiple installations**
 - ▶ In completely unrelated areas of the business





Monitoring Futures

- **Continuous Monitoring is embedded:**
 - ▶ Within GRC / ERM
 - ▶ Within Business Process Management software
- **Monitoring is embedded in business applications**
 - ▶ No separate dashboard
 - ▶ Continuous monitoring is 'operationalized'
 - ▶ Creates a sense-and-respond approach to business
- **Monitoring is Just in Time / Real Time**
 - ▶ Precludes hosted solutions
- **Exceptions and Conditions will be Actionable**
 - ▶ Monitors will perform corrective actions
- **Predictive Analytics will be Integrated into Monitoring**
- **Symsure will be on your SmartPhone**





Conclusion

- **In many organizations, ‘Continuous’ is evolutionary**
 - ▶ Simple Continuous Auditing tests can morph into a continuous monitoring platform
- **Monitoring can be used almost anywhere**
 - ▶ Reports, tests, controls & metrics are all possible
- **Small solutions with high value make believers**
 - ▶ It’s about the business pain, not the number of tests
- **Monitoring enables cooperative environments**
- **Organizations always benefit from monitoring**
 - ▶ Average savings for a monitored business process: 3% - 6%





Questions & Answers

