

Controls, Compliance and the Role of Continuous Monitoring

Co-written by Patrick Taylor, CEO at Oversight Systems, and Anne Marchetti, former partner at Parson Consulting and author of *Beyond Sarbanes-Oxley Compliance: Effective Enterprise Risk Management* and *The Sarbanes-Oxley Ongoing Compliance Guide*

All public companies are experiencing the significant cost and resource burden of sustaining compliance with Section 404 of the Sarbanes-Oxley Act (SOX) – and many are voicing their complaints. Despite all the criticism directed at the cost of SOX, the SEC and most investors still see its value. In December 2006, however, the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) recognized problems in implementing and enforcing Section 404 of the SOX. Both took specific steps toward providing public companies with relief from certain burdens of compliance with Section 404. In short, this new guidance from the SEC/PCAOB embraces top-down, "risk based" approaches and focuses management's efforts on:

- (1) Evaluating the design of controls to determine whether there is a reasonable possibility that a material misstatement in financial reports will not be prevented or detected in a timely manner.
- (2) Gathering and analyzing evidence about the operation of those controls based on its assessment of the risks associated with them.

Under this guidance, SOX compliance efforts are shifting from controls documentation and user provisioning of financial systems to business process integrity. Finally, we've been given the go-ahead to address risk...with the potential for real business value.

Organizations have spent numerous hours remediating internal control weaknesses. And because they lack the internal resources or skill set to maintain compliance, many companies must continue to rely on external resources to support on-going compliance activities, further increasing cost.

Lack of automation has also contributed to the high cost of compliance. In many organizations a high number of manual controls, as well as a substantial amount of manual testing, still remain.

Organizations, therefore, are faced with a challenge: In the current regulatory environment, management and stakeholders will only accept one result – 100% accuracy and integrity in financial reporting. Non-compliance is not an option. However, companies are struggling to find an efficient, cost-effective method of attaining this goal.

Based on the factors outlined above, the development of a sustainable, long-term compliance plan should focus on minimizing cost, strengthening the control environment, ensuring financial reporting accuracy and adding value to the organization. Continuous monitoring can play a major role in accomplishing these goals.

Continuous Monitoring

Faced with unacceptably high ongoing compliance costs, many organizations are considering technology solutions for continuous monitoring to facilitate the compliance process and minimize cost. Continuous monitoring offers the greatest benefits when applied to automated controls and compliance tasks that were excessively manual and labor intensive in first-year compliance efforts.



Compliance automation, specifically the use of continuous monitoring, has consistently gained momentum in the market as companies look to improve business processes and reduce ongoing compliance costs. Software solutions for automated continuous monitoring can:

- Strengthen the control environment
- Automate risk-based controls
- Eliminate excess control testing required for weaker control environments
- Sustain SOX compliance
- Minimize risk by reporting control breakdowns as they happen
- Deliver a return on investment by improving financial operations

While its benefits can spread across the compliance process, continuous monitoring can be applied to different components of SOX compliance. Specifically, continuous monitoring can:

- Automate previously manual controls
- Inspect the entire process and minimize the number of controls to be tested
- Automate control self assessments and validate process integrity

Controls Automation

The first step to reducing the cost of SOX compliance is to reduce the manual labor required to achieve and sustain compliance. Continuous monitoring provides companies with a means to transform manual process controls and automate them as system controls. When utilized to automate controls, continuous monitoring saves labor costs associated with performing the control and improves the reliability of the control because it no longer relies on perfect human execution.

For example, remote offices with small finance staffs often require periodic manual review of transaction logs to identify errors and investigate transactions that violate the principles of segregation of duties or other company policies. Even large enterprise financial centers may implement a manual control to review transactions above a set threshold. The manual control of transaction log review can be automated with continuous monitoring through the creation of a system control that inspects every transaction for:

- Duplicates
- Matching principles (e.g. purchase order-to-invoice-to-voucher or invoice-to-shipment)
- Appropriate authorization and segregation of duties
- Patterns of abuse, collusion and outright fraud (e.g. ghost vendors or transfer of expenses to capitalized assets)
- Errors in accruals (e.g. unreleased funds in un-vouchered receipts)
- Company-specific and user-defined exceptions

Continuous monitoring automates and applies the manual control process to every transaction. With unwavering vigilance, continuous monitoring strengthens the control environment as it eliminates costs associated with manual reviews.

As an automated control, continuous monitoring can reduce costs associated with control testing. While manual controls require an audit of 30 historical transactions, automated controls only require a binary, positive-negative test with theoretical transactions. Consequently, instead of analyzing a sample of 30 transactions, an effective test can rely on just two transactions.

In one case, a large U.S. utility company applied continuous monitoring as an automated control to its centralized accounts payable function. While the company's Oracle ERP system was configured with strong system controls, the complexity of its vendor management and payables systems still required manual review for all payments above \$5,000. The company devoted three



full-time employees to this manual control, yet still relied on a recovery auditor to find and collect more than \$3 million a year in erroneous payments.

After deploying continuous monitoring as an automated control, the company reassigned two of the employees from performing manual control, and now relies on a single employee to review and correct errors identified by the continuous monitoring control. Rather than only reviewing payments larger than \$5,000, the automated control analyzes every transaction. As a result, all potential payment errors are stopped before they are executed. Subsequent recovery audits proved that the company had nothing to collect from erroneous payments.

Process Monitoring for Risk-Based Controls

While continuous monitoring can automate manual review and replace specific manual controls, it can play an even larger role as end-to-end process monitoring for risk-based controls. Risk-based controls allow companies to eliminate lower-level preventive controls that introduce a burden to productivity. As a result, compliance costs are lowered as companies have fewer controls to test. However, process monitoring ensures process integrity is always achieved.

Early compliance efforts attempted to achieve complete prevention of any and all threats to financial integrity. This ambitious goal proved to be excessively expensive to design, document and maintain. Furthermore, pursuing all of the theoretical risks imposed an unnecessary burden on operations. Many controls introduced new manual steps into a process and required more employee involvement to completely segregate responsibilities, review each step in the process, and sign-off on control execution.

The result could be eerily similar to a unionized shop floor where employees can only perform one specific task and which often requires the creation of a new position and a different employee for every step in the process. Without risk-based controls, this could be SOX's most expensive legacy.

However, end-to-end process monitoring allows companies to replace hundreds of low-level preventive controls with a single automated detective control. Employees are free to conduct their jobs efficiently, and every transaction is tested for policy violations as well as against control objectives. Fewer controls lead to less control testing and reduced compliance costs – without sacrificing financial integrity. Every transaction is inspected from beginning to end, strengthening the overall control environment while reducing the operational burden of overly stringent operational controls.

Segregation of duties is an example of where continuous monitoring can be applied as a risk-based, mitigating control. Most companies function in an environment where financial processes cannot be completed without allowing for some form of segregation of duties (SoD) conflict within user-access rights. For example, a remote office may not have enough qualified employees and/or skill sets to stringently divide ERP functional responsibilities. Other processes demand some managers retain "super user" privileges within a financial system. And still some SoD conflicts present such a low risk that the cost to reconfigure the ERP system to correct the SoD conflict far exceeds the risk.

To address these SoD conflicts, companies have traditionally relied on manual controls such as transaction log review on a monthly or quarterly basis. This manual control adds extra work to the business process because it requires individuals to log activities and review transactions. Auditors do not consider this type of manual control as most reliable because it relies on manual intervention. These areas, therefore, become a major focus during control audits.

Continuous monitoring provides an automated mitigating control that eliminates manual controls and satisfies auditor demands for effective SoD management. Real-time monitoring of financial processes provides fully automated, mitigating controls that effectively manage segregation of duties for both low-risk SoDs and privileged ERP users by:

- Logging all ERP activities into a secure audit log
- Analyzing every new transaction against all previous transactions
- Reporting all transaction-level SoD violations
- Providing a case management framework for resolving every violation

Automate Control Assessments & Monitor Process Integrity

Continuous monitoring that analyzes each step in a financial process provides financial executives with an independent view of process integrity. This transparency can lead to automation of management's assessment of control effectiveness. With a high-level view of financial processes, executives and managers can quickly discover and address risk areas that suffer from patterns of control breakdown. Additionally, executives can confidently sign-off on the effectiveness of controls when continuous monitoring shows processes consistently meet all control objectives.

When applied to automate control assessments, continuous monitoring provides managers with a holistic view of their financial processes. Dashboards and scorecards present a complete picture of process integrity and control effectiveness. Processes and sub-processes can be prioritized for review, testing, and re-engineering based on actual risk from non-compliant transactions.

Continuous monitoring solutions can then integrate with compliance management and controls documentation solutions to provide a complete governance and risk management platform that incorporates real-time data about aggregate results of a financial process. Actual transactions match to the documented control objectives for continuous updates on control effectiveness.

While confidently maintaining SOX 404 compliance between annual control audits, management can use the same process monitoring to improve financial processes. A solution for continuous monitoring can be applied to benchmarking and scorecard financial processes with real-time information. Based on process-specific and user-defined metrics, financial managers can apply continuous monitoring scorecards to perform the following activities:

- Track key performance indicators
- Monitor service level agreements
- Match transactions with control objectives
- Identify real-time leading and lagging indicators

Benefits of Continuous Monitoring

There are a number of benefits that can be derived from both automated controls testing and control automation through continuous monitoring. Primarily, continuous monitoring reduces cost by reducing the control testing effort required for SOX compliance. It inherently strengthens the control environment, and minimizes risk due to the increase in preventive controls and the reduction in manual processing/human intervention. And, quite simply, the elimination of manual activity minimizes risk.

Continuous monitoring applications provide a detailed audit trail as well as automated status reporting. Both of these functions facilitate an efficient external audit through a reduction in the amount of internal and auditor resource time spent on preparation and review of information. In addition, automated control testing and control automation can facilitate overall process improvement, leading to both cost reduction and a focus on more value-added activity.

While many organizations utilize external resources for compliance testing, a reduction in manual testing and an increase in control automation can decrease the use of external resources. The result of these steps is an overall reduction in cost.

Continuous Monitoring Requirements

To reduce compliance costs, strengthen the control environment and improve financial operations, a solution for continuous monitoring must contain several key components. First-generation solutions for continuous monitoring are available, but depend upon manual efforts to load data, run reports and analyze results. False positives are a common problem as they require extra work to investigate and prove that control objectives were met.

A continuous monitoring solution that requires too much manual intervention is bound to be less reliable and not deliver the expected benefits. In contrast, a solution for automated continuous monitoring minimizes false positives and reduces manual requirements for managing the continuous monitoring system.

As a result, automated continuous monitoring provides a lower total cost of ownership and greater return on investment by relying on technologies that power a second generation of continuous monitoring solutions. Specifically, automated continuous monitoring relies on a platform solution that encompasses:

- Data and Transaction Acquisition
- Audit Data Warehouse
- Intelligent Reasoning and Analysis
- Resolution and Process Improvement

Data and Transaction Acquisition

All continuous monitoring solutions operate by first acquiring information and transaction data from financial systems. However, first-generation solutions operate with only one or two systems (mostly SAP or Oracle), and acquire historical data with periodic batch extractions that only “pull” partial data based on “date changed” fields in the database. Because of the impact to ERP performance, these batch extractions must be scheduled on weekends and off-hours to avoid severely impacting operations.

Second-generation solutions for automated continuous monitoring normalize and standardize data across applications to create a universal transaction flow and effectively centralize people, processes, documents, transactions and systems across the organization. Proprietary algorithms produce real-time extractions without impacting or interrupting application performance. And, rather than exclusively relying on direct queries to the database, automated continuous monitoring also incorporates message-based data collection.

Audit Data Warehouse

After collecting data, continuous monitoring solutions must maintain an archived history for analysis – as well as compliance and legal needs. First-generation solutions employ basic data warehousing that emulates the data structure of the financial application.



Second-generation automated continuous monitoring transforms transaction-level data to reflect a real-world view of exact human and business objects (vendors, customers, sales orders, invoices, etc.). Automated continuous monitoring maintains the status of the business objects as they are modified during day-to-day operations. This provides unique visibility into the evolution of transactions, customers, vendors and products within the business framework, offering a basis for detecting acts of concealment, timing issues and other errors or anomalies.

Intelligent Reasoning and Analysis

Transaction and data analysis drive the initial value from continuous monitoring. First-generation solutions begin with custom-built rules that rely on static thresholds and exact duplicates to produce binary, "yes-no" conclusions. Most of this analysis is conducted with single field-level comparisons. Because these first-generation solutions are incapable of identifying trends or errors in multi-step transactions, users can be overwhelmed with false positives.

Second-generation automated continuous monitoring evaluates the unique business flow from every angle to drive intelligent reasoning and ensure precise results. Automated continuous monitoring applies a reasoning engine for unparalleled "common sense" analysis to automatically address a business process without the false alarms and missed opportunities that historically plague current application-monitoring programs. An advanced reasoning engine includes:

- Process-level inspection for out-of-sequence events and collusion
- Objects-oriented analysis with easy customization
- Dynamic, calculated thresholds (standard deviations)
- Risk-based conclusions based on frequency, value and control objectives

Resolution and Process Improvement

Rather than simply relying on basic email alerts and batch reports, a second-generation automated continuous monitoring platform includes the functionality necessary to resolve all identified errors and improve processes. Dashboards deliver corporate-wide trending reports with the ability to click and drill down into specific exceptions. Related exceptions are linked within a case management framework to automatically identify corrections. Finally, real-time reports correlate with performance goals and service level agreements to achieve continuous improvement and process optimization.

Benefits of Risk-Based Controls

After implementing risk-based controls for SOX compliance, companies can expect to see a direct payback from reduced compliance costs and business process efficiency and integrity.

A risk-based approach to internal controls first reduces the un-needed manual work to implement the preventive controls for low-risk or no-risk areas. Second, a risk-based approach focuses testing on areas of greatest risk. This drives real value from compliance and avoids spending absurd amounts of time on low-risk areas.

Risk-based controls can also drive business process efficiency while improving financial integrity. When applied as an automated mitigating control, continuous monitoring inspects every transaction for errors and suspicious behavior to deliver 100 percent compliance without the overhead costs of preventive controls that drag process efficiency.

Companies benefit from these risk-based controls by identifying errors as they happen and increasing the quality of the business processes. And in the end, companies benefit from reduced risk in their financial reporting. Finally, we've accomplished the original goal of SOX without the costly burden.