

# **Continuous Monitoring of Financial Transactions - Why It's a Priority for Sustainable Compliance**

**April 2006**

*John Van Decker  
Sr. Vice President & Principal Research Fellow  
Robert Frances Group*



120 Post Road West, Suite 201  
Westport, CT 06880  
<http://www.rfgonline.com>

## Forward

---

Since the introduction of the Sarbanes-Oxley Act of 2002 (SOX), there have been countless articles, new product solutions, and seminars focused on compliance and corporate governance in IT and finance bombarding executives. These resources provided important information to those scrambling to understand this new, complex legislation, as well as how to adhere to its stringent requirements. Companies were able to complete their year-one and year-two reporting, but many were concerned that this was an unsustainable effort due to higher-than-expected costs.

What's driving action now? In addition to the usual pressures that companies have always faced to be competitive and profitable and to keep their customers happy, there are growing internal and external demands on financial executives. These stem from analysts, the Board, the CEO, investors, and regulators, who wish to ensure that compliance is sustainable and embedded in business processes. All of these stakeholders are looking for more accurate, frequent, relevant, and transparent financial disclosure. These demands are driven by a renewed appreciation that good governance and compliance *can* contribute significantly to business value.

Most organizations, however, are challenged to develop effective, scalable strategies to respond to the ever-expanding range of regulatory requirements. Many have yet to establish a coordinated approach to enterprise compliance, governance, and risk management, approaching each initiative in a separate organizational 'silo'. These silos limit the ability to achieve integrated compliance, operational efficiencies, or overall improved business performance.

Companies must attempt to satisfy demands for greater financial transparency and corporate accountability in a business environment characterized by numerous challenges, including the following:

- Complex business processes that are not standardized across divisions, functions, or geographies
- Fragmented and inconsistent data sources
- Manual and error-prone financial processes
- Minimal use of automated controls
- Substantial complexity and poor integration in IT architectures

For compliance-related risk management to be effective, senior executives must develop IT and finance strategies that are linked to business performance management (BPM) at the corporate level.

## Burgeoning Regulatory Compliance Mandates

---

Regulatory bodies around the world have instituted a range of compliance mandates that are proving to be costly and burdensome enterprise control requirements. A sample of the regulatory legislation affecting companies that operate or are publicly traded in the U.S. follows. Many other global markets have brought in similar legislation to address the broader considerations of corporate governance, disclosure, privacy, and risk.

- **Basel II:** Capital assessment and reporting standard for global banking
- **Department of Defense (DoD) 5015.2 and UK PRO:** Federal standards of records management
- **Gramm-Leach-Bliley Act (GLBA):** Privacy of financial information
- **Health Insurance Portability and Accountability Act (HIPAA):** Right to carry insurance between jobs; privacy of patient information
- **National Association of Securities Dealers (NASD) 3110:** Written policies and procedures for review of correspondence with the public
- **Securities and Exchange Commission (SEC) Rules 17a-3 and 17a-4:** Requirement for all records related to securities transactions to be maintained for three years

- **SOX:** Fiscal accountability for companies trading on U.S. exchanges
- ***Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (U.S.A. PATRIOT) Act:*** Customer documentation requirements to "know your customer"

In addition to these regulations, auditing standards continue to evolve – most recently with the release of guidance through Auditing Standard Number 2 – and this trend is expected to continue. The only thing certain about compliance is that more regulation will come, and stricter enforcement will continue.

Most companies continue to struggle to determine an appropriate model for corporate governance in an environment of expanding regulations and escalating costs. Ownership of these compliance mandates usually rests with multiple C-level executives throughout the enterprise. Many firms have redirected monies from other mission-critical projects to fund soaring compliance costs, including those to cover substantial professional services and consulting fees to prepare for intensive and costly year-end audits. Compliance impacts business policies, corporate culture, and processes. It can have a material effect on how the investment community views stock prices and valuation. Management must find a means to bridge and connect the multiple compliance efforts across the organization effectively.

### Keeping on Top of SOX Compliance

The most significant compliance mandate for many firms is SOX. Now in its third year of enforcement, SOX compliance has been a major effort for companies – as well as a costly one.

The major flashpoint is Section 404, which requires firms to prove and attest to external auditors and regulators the effectiveness, presence, and rationale of financial controls in business processes that impact enterprise financial management. This challenge is compounded by the fact that there is limited specific guidance on

*how* to comply – within the Act itself, from external auditors, or from the regulatory agencies that interpret and enforce it.

Many firms that have undergone a SOX 404 audit are frustrated by the significant cost and preparation time that it consumed, as well as the meager business value and improvements that it derived. To date, much of compliance spending has been focused on business services to document and set up compliant financial management processes.

According to Financial Executives International (FEI)'s March 2006 survey, companies spent an average of \$3.8M on 2005 SOX Section 404 compliance. While this is down 16.3% from 2004, this is still a very significant overhead cost. The survey shows that the documentation of processes as well as assertion processes are still major issues for firms. To decrease costs, most firms want auditors to have greater reliance on internal audit data and resources but we believe that it will take some time for this to evolve.

During the initial rounds of SOX filings, companies focused on meeting the letter of the law – and on doing what was necessary to satisfy their auditors and regulatory agencies. Now, savvy firms are turning their attention to ways to sustain compliance in a cost-effective manner.

### Looking Beyond Compliance

For most organizations, it is not just SOX compliance that is the issue. Rather, it is developing an effective approach to multiple regulatory compliance mandates, and achieving a return on corporate governance expenditures that can lead to improved business performance and stakeholder value. These cannot be addressed with one-time quick fixes that were hard to avoid in year one and year two of SOX. Instead, compliance needs to be integrated and embedded within business operations – in effect, to become one more key performance indicator (KPI) that is closely managed and measured as a barometer of organizational success.

Perhaps the most vexing issue facing C-level executives is the absence of a clear definition of compliance. There are simply no real targets or benchmarks, or any perceived benefits to "over complying" with SOX or other regulations. This leaves two key questions largely unanswered. First, how much compliance is necessary? And second, how much is too much?

For those with responsibilities for enterprise compliance – executives in finance, internal audit, and IT – it is an issue of where and how to focus attention and resources to deliver on this corporate performance measure. These executives need to consider the following:

- Little practical guidance exists from external auditors and regulators on where to start and what works best
- Many organizations lack depth in their understanding of internal controls, and face a shortage of skilled knowledgeable staff to assist
- Most technology vendors have hopped on the SOX bandwagon, claiming to offer "everything the CFO needs for compliance"

There is no single-source or "silver-bullet" solution. Financial management and audit must select the right combinations of technology, leveraging automated controls within their existing IT infrastructure, and then introducing new enabling technologies to achieve sustainable compliance.

### Evolving Compliance Solutions Market

Since 2002, there has been a stampede of vendors moving to introduce or promote solutions that meet specific aspects of financial compliance management. The market response to these tools has been interesting at best, with many companies adopting a "wait-and-see" approach, electing to delay purchase and implementation. Instead, these organizations worked through year-one and year-two SOX compliance relying on a variety of labor-intensive manual processes, supported by basic

spreadsheet and database management applications.

The compliance technology spectrum includes four main categories of solutions.

- **Audit tools:** Auditors, both internal and external, have long been responsible for identifying organizations' control weaknesses and independently verifying and assessing compliance with business rules and regulatory requirements. Traditionally, audits of the presence and effectiveness of controls have been conducted through periodic point-in-time analyses based on sampling techniques. This frequently involves substantial delays between the time issues are identified (usually long after the transaction has taken place) and when remedial action is taken. Audit solutions provide an important contribution to compliance, and have received increased attention of late, largely due to SOX and related regulatory requirements. Tools that support the audit function in probing for anomalies and risk exposure are those from ACL Services Ltd. and IDEA. In addition, companies can take advantage of working paper packages such as TeamMate from PricewaterhouseCoopers (PwC) to organize audit plans, and general-purpose desktop applications such as Microsoft's Excel and Access.
- **Compliance management:** Another branch of compliance products focuses on tools to document, demonstrate, and facilitate management and auditor assertion of compliance to SOX 404. Initially, some firms used complementary tools provided by their compliance business services providers, such as Deloitte, Protiviti Inc., or PwC, since there were few if any broader solutions on the market. Most of these solutions do not enable effective enterprise collaboration to capture process control assessments and remediation. Emerging products such as those provided by OpenPages, Inc. and Paisley Consulting do; however, provide a compliance, governance, and risk management framework to house and manage enterprise process and documentation controls. Compliance management solutions

are complementary to audit tools and financial transaction monitoring technologies.

- **Financial transaction monitoring:** The primary purpose of these applications is to monitor continuously all transactions, regardless of source, associated with a particular business process, and to highlight those transactions inconsistent with the controls that govern the process. Financial transaction monitoring solutions validate the effectiveness of controls necessary for SOX 404, and can assist management in identifying and reducing errors, fraud, and operational inefficiencies, and thus improving bottom-line performance and business processes. Ideally, these solutions are capable of spanning multiple data sources and application platforms, not just a single enterprise resource planning (ERP) environment, to analyze all relevant financial transactions and provide greater visibility and assurance of controls effectiveness. Three vendor products in this category provide financial transaction monitoring of core business processes, such as the purchase-to-payment cycle, order-to-cash cycle, and financial closing (general ledger). These are ACL's Continuous Controls Monitoring solution, Oversight Systems' Financial Accounting and Reporting solution, and Greenlight Technologies.
- **Security and IT controls:** These solutions are often the first place to which IT management gravitates when attempting to rally around a compliance approach. Many enterprise applications have built-in security capabilities. However, to ensure appropriate segregation of duties (SODs) and change management and version control, as well as to manage user and access privileges, companies are investing in tools for compliance. These types of controls solutions may be embedded in applications to provide "hard" and "soft" stops to anomalies, such as role conflicts, security violations, and unauthorized access to sensitive data. Typically, they are offered through an ERP vendor or one where there is a close partnership. Products are available from SAP (MIC), Oracle (ICM) Applimation, Inc., Approva Corp., LogicalApps, and Virsa Systems (now part of SAP AG), for example.

## Where to Focus First

---

Previously, companies wrestled with defining and documenting controls and establishing a compliance program methodology for dealing with the initial rounds of SOX filings. Now, many organizations are faced with deciding where to begin their automation of controls testing, to achieve more sustainable and cost-effective compliance for the long term.

IT groups often focus on SOD concerns, and advocate adoption of security and IT controls monitoring solutions because they are familiar ground. This is particularly true when solutions are organized around the analysis of controls and potential SOD issues within specific ERP applications. While this approach provides technology support for one aspect of compliance – the ability to demonstrate that IT controls are in place – it does not focus on the integrity of financial transactions. In addition, it does not focus on the governance of the financial management process, which lies at the heart of SOX regulation.

Financial transaction monitoring solutions target this area specifically, providing a more effective way to understand control gaps and weaknesses by analyzing the actual financial transactions for evidence of control failures. In so doing, financial management and business process owners gain insight into their quantified exposure to business risk so action can be taken to improve business performance by addressing operational inefficiencies, detecting fraud, and reducing financial leakage.

Both types of solutions have a place in contributing to a strong and sustainable governance framework and both can help companies get their compliance function on track. However, a financial transaction monitoring approach may be the more prudent choice to consider initially, since it ties in more directly with the Committee of Sponsoring Organizations (COSO) internal controls framework. COSO is the SEC-endorsed standard for enabling compliance

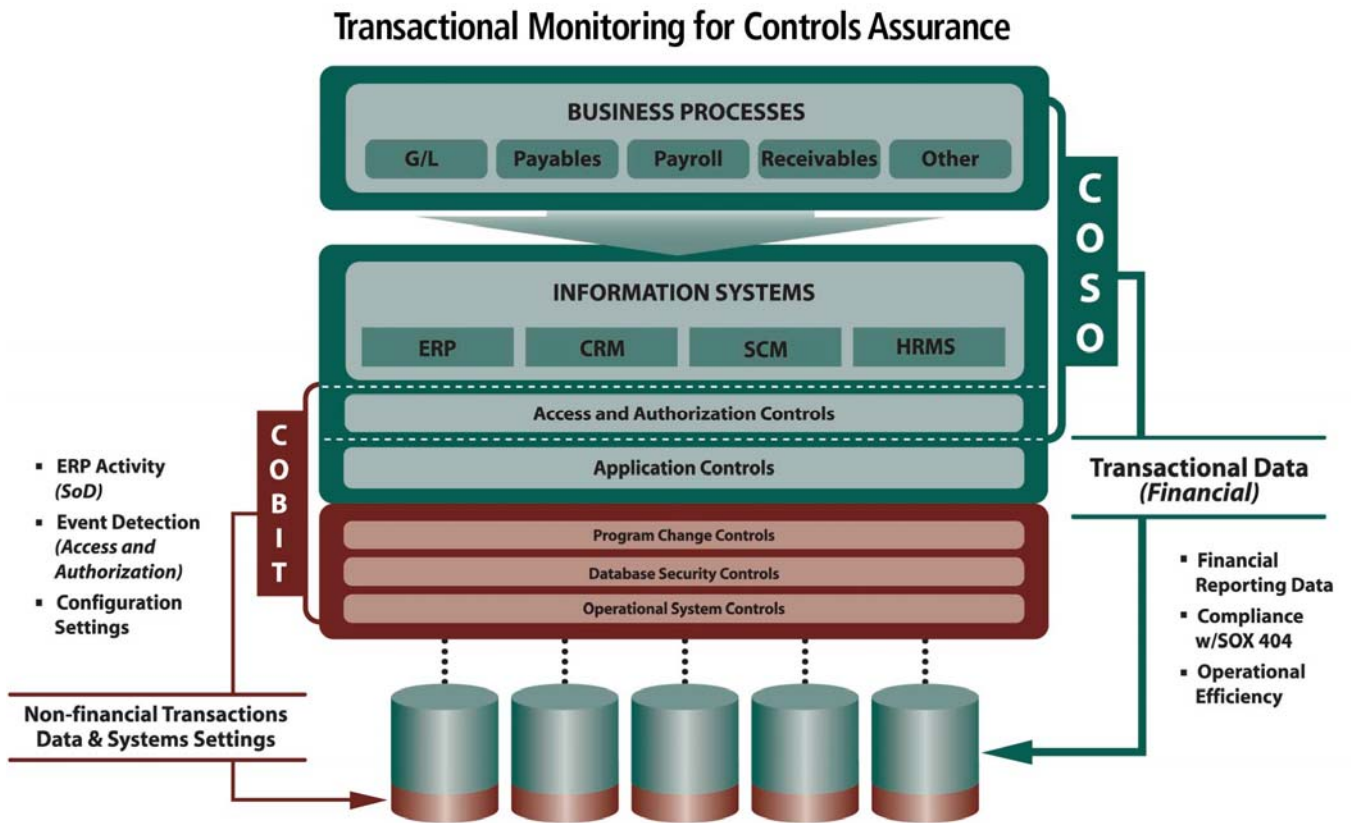
with SOX 404. The security and IT controls monitoring solutions are more closely aligned with the Control Objectives for Information and related Technology (COBIT) framework.

### How COSO and COBIT Frameworks Work Together

COSO and COBIT are governance frameworks frequently referenced as a result of recent regulatory activity.

The COSO Internal Control – Integrated Framework has emerged as the most widely used standard for achieving compliance with SOX 404 when evaluating internal controls over financial reporting. This framework is a blueprint for establishing internal controls that promote the effectiveness and efficiency of operations, minimize risk, help ensure the reliability of financial statements, and support compliance with applicable laws and regulations.

COBIT and the Information Technology Infrastructure Library (ITIL) are IT-specific governance frameworks that enable clear policy development and good practice for IT controls throughout organizations.



Source: Robert Frances Group

With reference to the previous illustration, many of the security and IT controls monitoring solutions concern themselves largely with COBIT compliance, focusing specifically on application controls governing database security, program changes, and system access. These are important elements of an integrated controls environment, and support the broader COSO framework.

However, financial transaction monitoring solutions map directly into the COSO principles by focusing on process-level controls. They examine how financial transaction data is bridged from one system to the next within the context of a complete business process, ultimately rolling up into financial reporting information.

Since most organizations use enterprise systems to collect, process, move, and store financial data, compliance with SOX requires full confidence in those systems. IT departments are more familiar with the COBIT and ITIL models, and may not have invested as much time examining technology solutions that map specifically to COSO.

### **Why Financial Transaction Monitoring and Why Now**

---

Robert Frances Group (RFG) believes financial transaction monitoring initially offers more to an enterprise in terms of ROI. Specifically, it provides:

- **Evidence on which an audit can rely:** Through provision of a complete audit trail of control testing, to validate that key controls are in place and working effectively
- **Extensibility to multiple end-to-end business processes:** With independent testing of controls through financial transaction analysis at the source level, to provide greater assurance of controls effectiveness and transaction integrity across the enterprise
- **Improved fraud detection and reduction of business risk:** Through identification of control gaps and weaknesses that previously

allowed abuse, error, and fraud to slip through undetected

- **Increased operational efficiency and effectiveness:** With opportunities to increase profitability by containing costs, minimizing losses, and enhancing revenue assurance
- **Sustainable compliance:** With ongoing, automated internal controls testing that provides cost-effective support for enterprise-wide compliance programs, replacing manual or spreadsheet controls
- **Timely notification to management of control breakdowns:** An early warning system of business and compliance risk, enabling control weaknesses to be fixed before they are reported externally or materially impact financial results.

The ability to ensure that operational and financial controls are in place and that they are operating effectively lies at the heart of the compliance process. Many firms believe that technology can play an important role in compliance sustainability. It must be understood, however, that it is necessary to weave technology into business processes to ensure enterprise compliance. A SOX compliance and governance solution requires an integrated combination of business processes and technology.

To the pleasant surprise of many though, much of this technology is already in place. Most enterprise applications, including customer relationship management (CRM), enterprise content management (ECM), ERP, and supply chain management (SCM), already play an important role in ensuring that controls are in place, including role-based approval processes and management of SOD conflicts. More recently, firms have been turning to their business intelligence (BI) and business process management (BPM) solutions to understand how these can be leveraged too.

Still, without additional investment in enabling technologies, most firms will not be successful in creating a sustainable model for SOX 404 compliance. Although many firms have moved to an integrated ERP environment, few have the necessary controls-monitoring processes in place to provide assurance of the accuracy and reliability

of financial transactions. This is true both within a single ERP instance *and* across multiple IT platforms (other ERP suites, custom applications, or legacy systems) within enterprise business processes.

Today, organizations can benefit from financial transaction monitoring solutions that go beyond the capabilities of their existing enterprise and BI systems. What is needed are independent solutions that focus on key controls outlined according to COSO principles that provide a fully auditable record of the results of continuous controls testing.

Moreover, lessons learned from corporations that have already undergone initial rounds of compliance with these new regulations highlight why a financial transaction monitoring approach can provide quantifiable benefits. Financial transaction monitoring solutions typically deliver a higher and more immediate ROI than is derived from the traditional IT approaches to controls monitoring. Ultimately, this should provide business process owners, CFOs, and finance departments with information to satisfy external auditors and regulators while enabling tangible business performance improvements.

### **Monitoring Financial Transactions within Business Processes**

---

A number of core enterprise business processes are ideal candidates for a transaction-level approach to financial controls monitoring. The key controls within these often extremely complex processes are seldom tested and analyzed in sufficient depth within discrete applications. Moreover, enterprise processes frequently touch multiple platforms, such as ERP applications, legacy systems, outsourcing arrangements, and processing through shared services. Additionally, within large organizations there is another level of complexity introduced by multiple business units and global operations. A financial transaction monitoring system must be capable of overcoming these barriers, to provide a single, integrated view into the controls health of the organization within core processes.

Some examples of the ways financial transaction monitoring can be applied in automating testing of financial controls include the following:

- **General Ledger (GL):** The journal entry is the primary means of booking financial activity. As such, timely identification of duplicate, missing, restricted, or unauthorized journal entries constitutes critical analysis in the quest to demonstrate internal controls effectiveness. Another area for focus is the adjustment process, typically involving journal entries directly within the GL, but outside the enterprise sub-ledger system. As a result, such adjustments must be validated independently of the internal GL system controls, to ensure that the financial activity is booked correctly to the appropriate accounts. Timing of a variety of journal entries must be carefully managed and actively monitored, including pre and post-close period entries, journal entries to temporary accounts, as well as reversals of journal entries, accruals, and deferred income.
- **Order-to-Cash:** Optimizing the order-to-cash cycle is a strategic priority for most businesses. Monitoring controls in this area should focus first on customer management, including tests to validate that business is only being done with approved customers or in adherence to established credit limit policies. Financial transaction monitoring can identify errors in order entry, inconsistent application of credit limit policies, SOD conflicts around price management and maintenance, goods shipped but not invoiced, and billing errors. The economic benefits of improving controls within the order-to-cash cycle include the ability to reduce days sales outstanding (DSO) and minimize revenue leakage and incorrect billings. In addition, companies can cut administrative efforts and costs, detect and prevent fraud, improve collections processes, and increase customer satisfaction.
- **Purchase-to-Payment:** Organizations have focused on the automation of purchasing, payables, and payments processes to reduce costs and gain operating efficiencies. However, the push to automation (and, in some instances, outsourcing) has a potentially costly downside. Without constant oversight

into transaction-level detail, there is an opportunity for significant financial leakage stemming from duplicate payments, payment errors, and vendor and employee fraud, which could run into millions of dollars of losses each year.

## Developing an Enterprise Approach to Financial Transaction Monitoring

When determining the enterprise approach to financial transaction monitoring, RFG recommends that companies first focus on areas where optimal value can be achieved. Organizations have been frustrated with prior attempts to bring in enterprise applications to deliver on this promise of business improvement – particularly multi-year projects for ERP implementations. However, RFG believes that financial transaction monitoring technology can be a candidate for quick deployment, payback, and demonstrated business value.

IT departments may choose to develop a financial transactions monitoring approach in house, or take advantage of the best practices inherent in an off-the-shelf application. If the organization decides to develop a custom solution using common BI reporting tools along with general-purpose desktop applications there is still a significant investment of time and domain expertise required to ensure a consistent approach to the following:

- Accessing the data for metrics management and analysis from various online and offline processes
- Storing data in a common data mart or database and rationalizing metadata management and data inconsistencies\*
- Identifying, testing, and monitoring key controls within core business processes aligned with the COSO internal controls framework
- Building internal consensus as to what should be managed with metrics

\* Note: An application that is geared for financial transaction monitoring must have

established processes to collect critical data, normalize, and ensure consistency.

This is not a simple exercise, and in many organizations the controls and technology expertise to develop such an application is in short supply. Organizations should, therefore, consider the applicability of packaged financial transaction monitoring solutions that have built-in best practices that include pre-defined analytics for key controls, metrics, and dashboards for display. Moreover, a third-party solution may be the ideal approach rather than piece-meal configurations embedded into native applications.

Ideally, financial transaction monitoring solutions should function like an auditor, providing an independent third-party opinion on the effectiveness of financial processes. The application should provide a reliable trail of evidence for internal and external auditors to verify that testing and monitoring has been conducted, and what remedial action has been taken to strengthen the controls framework.

## Evaluating Financial Transaction Monitoring Vendors

When considering a vendor for financial transaction monitoring, several evaluation criteria must be considered:

- **Best practices and functionality:** Rate the vendor on the basis of the best practices and functionality inherent in its application. Determine if the vendor is leading (or lagging) trends within the technology space, and if its service management meets the needs of the organization.
- **Decentralization and globalization:** As companies attempt to consolidate technology initiatives globally, the vendor's ability to provide global support becomes increasingly important. Even if the company does not require a global solution, a vendor unable to support global requirements will eventually suffer the consequences in a competitive marketplace.

- **Implementation services:** The vendor should be able to provide implementation services for the solution to help effectively configure the product either directly or through a network of authorized partners.
- **Leading technology:** The vendor should maintain a commitment to leading technology, including open source, service-oriented architectures (SOAs), and Web services. In addition, the vendor should be able to integrate with leading BI vendors for extended reporting.
- **Vendor references:** Find out the experiences that existing customers have had with the solution, including the vendor's new release management, responsiveness to issues, and willingness to listen and respond to current and future requirements.
- **Vendor financial viability:** Determine the financial strength and capability of the vendor by reviewing forward-looking statements (if available), as well as analysis and opinions provided by leading IT advisory services and research firms such as RFG. In addition, ascertain the vendor's market share, growth plans, and ability to execute and be aware of vendor consolidation trends in the applications space.

## Summary

---

Effective regulatory compliance is a continuous process. Organizations must manage it as such by acquiring technology that ensures compliance is cost-effective and sustainable and adds value through business performance improvement.

Financial transaction monitoring solutions are an area where companies need to focus. Such solutions automate many of the manual compliance processes, provide immediate visibility into the health of an organization's controls, and identify areas where controls are weak or non-existent. They can also probe the condition of financial processes, identify anomalies that may represent compliance issues, and, perhaps more importantly, flag opportunities for operational and financial performance improvement.

Not only can financial transaction monitoring support a sustainable approach to compliance, it is also a sensible business approach that can help eliminate costly errors that detract from financial performance, such as payment errors or revenue leakage.

In addition, financial transaction monitoring solutions can help organizations identify where to focus additional compliance technology solutions, in particular, on aspects of IT and security controls monitoring, managing controls documentation and remediation, or enabling independent audit assessments and reporting.

Copyright © 2006 Robert Frances Group, Inc. All rights reserved. 120 Post Road West, Suite 201, Westport, CT 06880. Telephone 203/429-8950. Facsimile 203/429-8930 [www.rfgonline.com](http://www.rfgonline.com). This publication and all publications may not be reproduced in any form or by any electronic or mechanical means without prior written permission. The information and materials presented herein represent to the best of our knowledge true and accurate information as of date of publication. It nevertheless is being provided on an "as is" basis. Reprints are available for a nominal fee.