

---

Oversight<sup>™</sup>  
Systems

**Forensic Auditing:  
Structural Requirements  
for Fraud Monitoring**

## Forensic Auditing: Structural Requirements for Fraud Monitoring

Companies today need a cost-effective and efficient way to identify and resolve potentially fraudulent transactions flowing through their ERP and financial systems. Without automated forensic auditing tools, finding these fraudulent transactions can be nearly impossible, especially if the person committing the fraud knows the criteria a company uses to look for suspicious activity. With time and resource constraints, human auditors can only take a sample of data to analyze, greatly increasing the chances of missing key evidence, whereas an automated 'virtual auditor' can monitor in real-time all of the transactions flowing through a company's ERP and financial systems. Continuous controls monitoring software with strong forensic auditing features serves as such a 'virtual auditor', protecting companies against fraud and misuse.

### Impetus for Fraud Monitoring

Although the prevalence of heart-stopping fraud headlines seemed to spike going into 2009, corporate fraud has been steadily on the rise since 2003 [see Figure 1], in spite of the enactment of the Sarbanes-Oxley Act (SOX) in 2002.

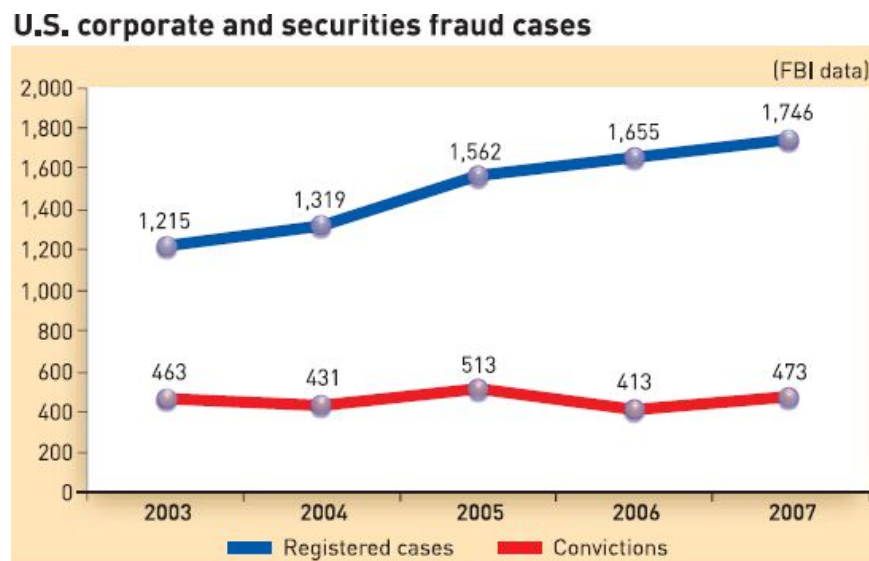


FIGURE 1: Corporate Fraud Task Force Report, 2008

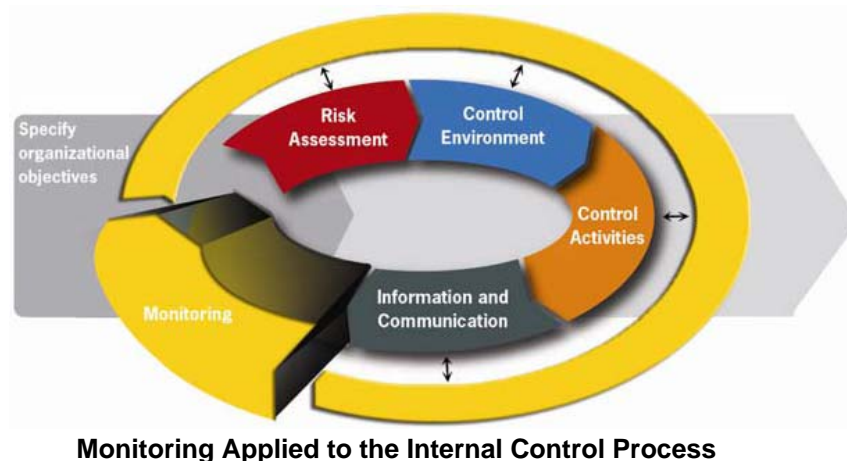
In the face of this escalating fraud, the Public Company Accounting Oversight Board (PCAOB) issued what amounted to an edict to auditors to improve fraud detection in its January 2007 report, *“Observations on Auditors’ Implementation of PCAOB Standard Relating to Auditors’ Responsibility with Respect to Fraud”*. Specifically, they cited management override of controls as an area of risk that should be more proactively addressed by audit firms, and recommended that more forensic techniques be applied in the audit to decrease the risk of fraudulent financial reporting. This is based on the fact that standard audits verify the filings that *represent* management inputs, whereas forensic audits provide fraud detection by verifying the inputs themselves.

In a June 2007 letter that would seem prescient in light of the accounting scandals of late 2008, Gregory J. Jonas, Managing Director of Moody’s Investor Services wrote to the SEC that investors were demanding controls that would be effective in preventing management from “cooking the books”. Jonas wrote, “While much of the commentary about control reporting has been concerned with compliance costs, evidence suggests that important

goals of reporting on controls are not being fully achieved... There appears to be insufficient emphasis on controls that prevent senior management from fraudulently manipulating financial reporting.”

Even the SEC itself formally recognized that Internal Control over Financial Reporting (ICFR) is insufficient to prevent such fraud, and advised public companies to take appropriate action to mitigate the risk. According to SEC Release No. 33-8810 (June 27, 2007), “ICFR also can be circumvented by collusion or improper management override. Because of such limitations, ICFR cannot prevent or detect all misstatements, whether unintentional errors or fraud. However, these inherent limitations are known features of the financial reporting process, therefore, it is possible to design into the process safeguards to reduce, though not eliminate, this risk.” (As we will see, automated forensic auditing constitutes such a safeguard.)

This focus on fraud risk was further supported by the PCAOB in their Auditing Standard No. 5 (AS5), released in May 2007. In contrast to its predecessor, Auditing Standard No. 2, AS5 directs auditors to focus on a top-down, risk-based approach to compliance, and specifically fraud risk in the General Ledger. This includes auditing controls over journal entries, review of period-end adjustments, and flagging of significant or unusual transactions.



**FIGURE 2: COSO Internal Control Framework**  
**SOURCE: COSO Guidance on Monitoring Internal Control Systems**

Early in 2009, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its new Guidance on Monitoring Internal Control Systems. COSO, too, has identified monitoring (one of the five components of effective internal control delineated in COSO's *Internal Control - Integrated Framework* – see Figure 2) as the key component in identifying control failures and management override of controls. According to the Guidance, “When people who are responsible for internal control know their work is subject to oversight through monitoring, they are more likely to perform their duties properly over time.” As such, monitoring is the only effective “cooking control” and a powerful fraud deterrent.

In general, this is well accepted. According to Gartner, “By 2010, auditors will expect regulated organizations to detect fraud by performing transaction monitoring on a continuous basis, and 60% of regulated firms will have such an automated process in place (0.8 probability).” With the recent economic impact of catastrophic corporate fraud, 2010 may seem too late, and indeed, companies who have felt as if they were invulnerable to internal fraud may now be scrambling to close the door *before* the horse leaves the barn.

So the question becomes not *whether* to implement continuous monitoring, but how to ensure that it functions effectively to fight fraud. This is where forensic auditing comes in.

## Structural Requirements for Effective Fraud Monitoring

According to the Hackett Group, even world-class companies on average operate 27 different financial systems per \$1 billion of revenue.<sup>1</sup> In this kind of heterogeneous environment, the key to effective monitoring of transactions is in having a pervasive monitoring architecture – one that is transparent to the various source systems, and unaffected by ongoing consolidations and upgrades. This requires that data from the underlying ERP data models (designed for efficient processing within the ERP system) be transformed into a Business Entity model, designed for analyzing business transactions end-to-end.

The foundation for building this Business Entity model is an Audit Data Warehouse (ADW), a single repository to record transaction data and history. Creation of the ADW leverages heterogeneous data acquisition and mapping, and enables the design of analytics for business process issues, without being limited by source applications. This approach should incorporate key fraud fighting capabilities, such as extraction logging and control totals to ensure the integrity of information within the ADW. The ADW must be highly secure, with independence from the IT infrastructure, and a revision history should be captured to provide evidence of concealment.

The keys to a building and maintaining a flexible and effective ADW include:

- Avoiding software installation on application servers where possible
- Extracting data by precisely-crafted read requests to minimize performance impact on source systems
- Mapping to source systems in XML files for fast implementation and easy maintenance

Continuous monitoring solutions with integrated forensic auditing capabilities will include an ADW component that meets these specifications.

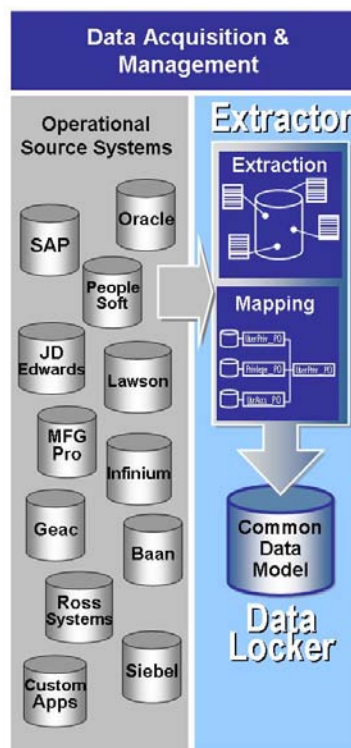


FIGURE 3: ADW Model

### Analyze, Resolve, Document

Once you have accessed your data, there are three keys for effective fraud monitoring: persistent and advanced data analytics; efficient resolution and comprehensive documentation.

<sup>1</sup> "Conflicts Between ERP Systems and Shared Services Can Inhibit Return on Investment" David Hebert and Dr. David Oppenheim. Answerthink, Inc. 2004

## Persistent and Advanced Data Analytics

First-generation continuous monitoring systems used field-level comparisons of data to spot errors. For example, if the order numbers are the same, it could be a duplicate. But finding simple duplicates is easy; many are caught by the financial systems' edit controls, and most financial applications stop identical documents from being entered. Finding the real problems – those that may constitute fraud or misuse – is much harder. In order to do that, you need analytics capable of performing near-human reasoning; seeing documents as a whole. This is how second-generation continuous monitoring systems work, identifying *similarities* overall that are supported by matches at the detail level. For example, the order numbers are similar, the line item details match, and the order dates are close – could be a duplicate order. As such, these systems are able to apply the same analytic techniques as those used by forensic auditors.

### Developing the Fraud Picture

As cited above, General Ledger fraud – “cooking the books” – is a growing problem. The Deloitte Forensic Center reports that one-third of all fraud schemes subject to SEC enforcement involve manipulation of financial statement items. This means that internal controls have failed, and assets, expenses, reserves and/or liabilities have been fraudulently manipulated. So how could the ICFR failure have been revealed, and these actions prevented, by continuous monitoring?

The key is to employ analytics that can detect “unusual” Journal Entries to identify risk. This risk may be revealed by first analyzing a combination of attributes, including:

- Time of day, week and month
- Large dollar adjustments in one transaction or accumulated in many transactions
- Isolated in one account or accumulated across accounts

These attributes are then evaluated according to each user's activity compared to normal vouchering participation, and the timing and frequency of the entries, to identify the “unusual” and flag potential fraud or misuse for investigation.

#### **Advanced Analytics to Detect “Fraud Chains”**

A Fraud Chain consists of sets of debit/credit pairs (General Ledger journal entries) that when connected net out to a fraudulent transaction. The individual pairs appear to be normal transactions. It is only when they are linked that the fraud becomes evident. To make detection even more difficult, the fake debit/credit pairs can be split, so that the “chain” is not obvious. It becomes even more difficult to uncover the fraud when the fraudulent transactions are intermixed with thousands of valid journal entries. It requires a complex algorithm and advanced fraud chain analytics to handle such split transactions, including multiple actors and heterogeneous amounts through multiple intervening accounts, and successfully identify funds flow from source to sink. This kind of forensic analysis is a feature of the Oversight fraud monitoring solution. For more information, visit [www.oversightsystems.com](http://www.oversightsystems.com)

In addition to fraud prevention, other business benefits accrue from continuous monitoring of Journal Entries. Along with any deliberate misuse, unintentional errors are identified – such things as inappropriate end states for accounts, or basic debit/credit typos – that, undetected, could become material reporting errors down the road. Early identification of problems and trends also simplifies the process for closing the books.

Another high-risk area is revenue recognition fraud. Deloitte indicates that this type of fraud scheme accounts for 41 percent of all SEC enforcement actions. These schemes are broken down into:

- Fictitious revenue (35%)
- Swaps, round tripping or barbers (16%)
- Transactions not shipped (12%)
- Contingencies (12%)
- Inappropriate reserves (13%)
- Incomplete delivery (12%)

Identifying fictitious and overstated revenue requires continuous monitoring of transactions to detect anomalies in the revenue recognition details, such as shipments processed against invalid/incomplete sales orders; invoices inconsistent with shipment documents; or intra-divisional transfers booked as sales. It is also important to identify patterns of revenue transactions that could signal abuse, for example, patterns of cross period bookings and returns, or “channel stuffing”.

#### **Analytic Approaches to Forensic Auditing**

As we’ve seen, effective fraud monitoring requires analytics that are capable of defining the “usual” and the “unusual”. An advanced analytics set will combine a number of different approaches to effectively make this evaluation.

*Structural and Knowledge-Based* approaches determine if critical fields are malformed or missing, and identify apparent duplications and second-order anomalies (e.g. Journal Entry compared to sales order).

*Statistical* approaches look for numerical outliers, such as individual postings or gross margin changes; timing and frequency anomalies, such as end of period clusters, or a missing recurring posting; discrete valued outliers – user never posted before; or any combinations of these, such as a large ramp in postings by unusual user.

*Similarity Comparisons* check for things such as similar account numbers – 123456 resembles 1230456 – that are not screened out by the financial systems.

The ability of a continuous controls monitoring solution to apply these approaches in combination is what enables an automated solution to function as a virtual forensic auditor in terms of identifying issues that warrant further human investigation.

#### **Efficient Resolution of Identified Issues**

The advantages of scale gained by automating forensic analytics can be lost without the right tools for the efficient and effective investigation and resolution of the potential issues, or control ‘exceptions’, identified by the software.

There are two primary cost drivers inherent in transaction monitoring: the quantity of exceptions generated by the analytics, and the effort required to deal with each exception.

In terms of quantity, identifying true positives – exceptions that turn out to be actual cases of fraud, misuse or error – is what generates the ROI from your continuous monitoring implementation. You do not want miss any of those. False positives, on the other hand, are an obvious cost, as they require an equivalent investigative effort before it is possible to determine that they do not require corrective action. Repeat positives are a hidden cost, for example, when daily analysis over a 30-day window identifies the same exception (true or false) 30 times.

The required effort per exception involves interpreting the reasons why the transaction was flagged as suspicious; evaluating related information in order to adjudicate the exception; assigning true positives for correction; validating the correction; and documenting the reconciliation.

With the effort involved, it’s easy to see how false positives can choke the continuous monitoring process. The primary key to avoiding false positives is to employ analytics capable of temporal reasoning – viewing transactions in context of their relationships through time to determine usual and unusual transactions. This will enable the solution to recognize whether the recurrence is part of a pattern, for example, a set of payments to a particular vendor occurring approximately every 30 days for a similar amount, versus two similar payments to the same vendor with no historical pattern.

### Integrity Checks vs. Rules

In addition to minimizing false positives, the use of sets of related indicators to determine the integrity of a given transaction, versus traditional rules-based tests, will significantly reduce the amount of effort involved in resolution. For example, the validity of a Journal Entry might be based on the following set of indicators:

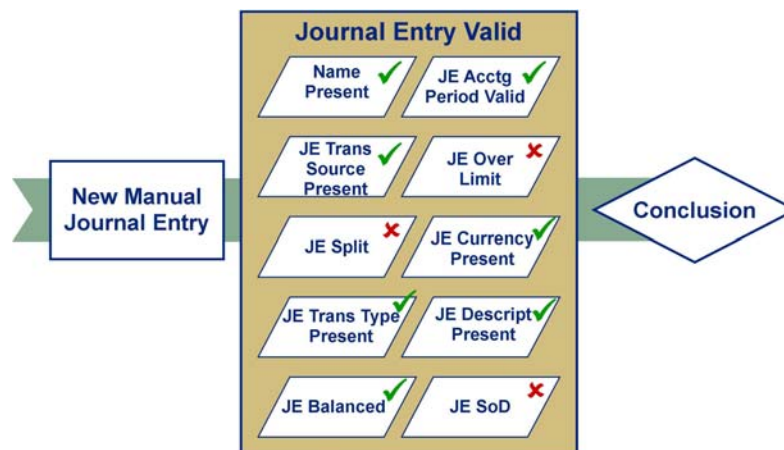


FIGURE 4: Example Integrity Check with Indicators for validating Journal Entry

If three of these indicators were to fail (i.e., JE over limit; JE split; JE Segregation of Duties violation) it would clearly indicate that the Journal Entry was non-compliant – but would that constitute one problem to be investigated, or three? Evaluating the Journal Entry in terms of an overall Integrity Check enables the investigator to assess *at the business transaction level* whether the three failed indicators taken together indeed constitute a potentially fraudulent Journal Entry.

## Prioritizing the Exceptions

Additional efficiency in the resolution process can be gained through the implementation of 'fraud scoring', whereby weightings are applied to each indicator within the Integrity Check. You may have thresholds set to flag the transaction as non-compliant if some specific number of indicators fire. With the addition of weighted averages, using Bayes theorem<sup>2</sup>, you can add an informed confidence rating that refines the conclusion. In the previous example, for instance, you might have set the following weightings for each of the indicators:

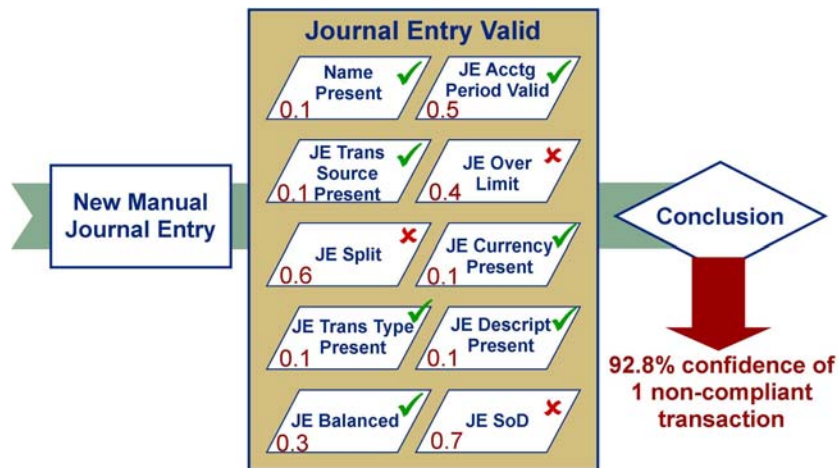


FIGURE 5: Example JE Integrity Check with Weighted Indicators

In this example, the three failed indicators are weighted as follows: JE over limit – 0.4; JE split – 0.6; JE SoD – 0.7. Applying the weighted averages of the failed indicators leads to a conclusion that this transaction is non-compliant, with a confidence level of 92.8%.

With a weighted confidence level, the next step to efficient resolution is calculate the potential financial impact of the exception, and then combine the confidence and dollar-value ratings to come up with a priority ranking that will enable investigators to focus their efforts for the greatest return. For example, a \$1,000 exception with 90% confidence level would be a \$900 priority, but a \$1,000,000 exception with 50% confidence would be a \$500,000 priority.

## Resolution - More than Reports

Another key to efficiency in the resolution process is to automate as much as possible. The typical resolution process revolves around the issuing of reports from a continuous monitoring tool. In this scenario, the investigator reviews the original report of the exception, then must identify and locate related documents, compare data in individual spreadsheets, search a customer database to validate information, pull reports from an ERP System – all the while keeping detailed notes to document the ultimate resolution for external audit.

<sup>2</sup> "Bayes' theorem relates the conditional and marginal probabilities of two random events. It is often used to compute posterior probabilities given observations." - Wikipedia

Truly automated fraud monitoring incorporates case management and compliance workflow tools, presenting exceptions not in static reports, but within an interactive investigative user environment. Features of an efficient forensic investigation workbench include:

- Presenting exceptions in a risk-prioritized list (prioritized as described above)
- Presenting plain-language descriptions of all of the indicators that fired to flag the transaction as a potential exception, for example:

- Journal Entry was created by user JMILLER who has never posted to account 1843 - Accumulated Depreciation
- Journal Entry was created by user JMILLER who has never posted to account 5382 - Depreciation Expense
- Journal Entry is a manual entry
- Manual Journal Entry posted to account 1843 - Accumulated Depreciation that typically has automated or systematic entries

- Offering click-through access to all supporting data, to facilitate investigation

Workflow features integrated within the investigation environment should drive exception resolution through a defined process.

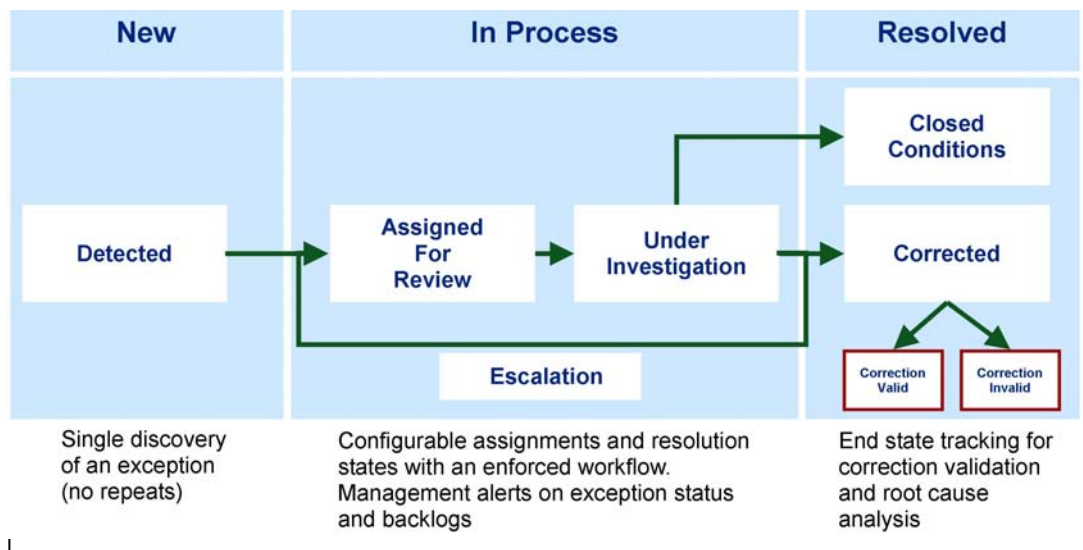


FIGURE 6: Workflow attributes required to drive resolution through defined process

Efficient resolution workflow will ensure that each issue will only need to be resolved one time, and provide for the automatic assignment of exceptions to specific users or roles. The stages and states of the process should be configurable, providing a customizable framework for establishing and enforcing a mandatory resolution process. The efficiency of the process should be easily monitored, with automatically generated alerts for excessive backlogs based on volume, or resolutions that exceed time limits.

Reports on exceptions by error types, person(s) handling and resolution state will help identify any patterns that may indicate further abuse, cover-ups, or collusion within the resolution process itself. In addition, it is important to have correction detection features that validate whether corrective changes were ultimately made in the source system(s).

### Documentation to Prove Compliance – and Lower Audit Costs

All resolution activities should be permanently recorded in a secure journal, for the use of both internal and external audit, and to prove regulatory compliance.

One of the key changes that the PCAOB made with the release of AS5 was to stress reliance on the work of others. Under AS2, auditors could look at reporting data collected by a company, and while it would show them everything they needed to know, they still had to go through the process of pulling together the same report for their own use. Now, under AS5, external auditors are allowed to rely on well-documented results to know where to focus their time and attention, thus reducing costs and duplication of work.

With the AS5 guidance in effect, companies that have a continuous monitoring system in place can show the data already collected and addressed by the solution, eliminating the need for third-party testing. In many cases, companies have found that their external auditors have been able to significantly reduce the effort required to audit those business processes where continuous controls monitoring of transactions has been implemented – especially in cases where the solution automatically generates a comprehensive audit log. This audit log should be a secure, permanent investigative journal that records exception ownership, state changes, and investigator’s notes, and validates that corrections were made within the source applications.

### Hiring a ‘Virtual Forensic Auditor’

Implementing continuous controls monitoring for transactions can be like hiring a team of forensic auditors, if the solution can provide the advanced analytics, resolution and documentation capabilities described above. The right technology will enable companies to cost-effectively and efficiently identify and resolve potential fraud and misuse – even the kind of internal fraud that traditional ICFR cannot prevent. Such a solution will not only facilitate fraud *detection* and resolution, it will serve as a fraud *deterrent*, as well. At the same time, it will lower a company’s costs of regulatory compliance, improve audit performance, and boost shareholder confidence along with the bottom line.

**If you’d like more information about adding the right ‘virtual forensic auditor’ to your team, visit [www.oversightsystems.com](http://www.oversightsystems.com), or call Oversight Systems at 770-984-4600.**