



THE ROLE OF IT MONITORING, ALERTING AND REPORTING
IN
SATISFYING SARBANES-OXLEY REQUIREMENTS

CONTENTS

[Introduction](#)..... 1
 [Section 302](#)..... 2
 [Section 404](#)..... 2
 [Section 409](#)..... 3
[Success Factors](#)..... 4
[What Can TNT Software Solutions Offer?](#) 6
 [How TNT Software Solutions Work](#)..... 6
 [How Do TNT Software Solutions Fill Compliance Needs?](#) 8
 [Added Benefits of TNT Software Solutions](#) 10
[Conclusion](#) 11

For more information, please visit our website at www.TNTSoftware.com or call 360-546-0878.

INTRODUCTION

The sins of a few have forced all of Corporate America to change the way we do business. In response to the corporate malfeasance of Enron, Adelphia, and several others, the United States Congress passed the U.S. Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as the Sarbanes-Oxley Act, named for the authors of the bill.

The Sarbanes-Oxley Act (SOX) requires publicly held companies to:

1. Implement internal controls over financial reporting, operations and assets,
2. Evaluate the strengths and weaknesses of those internal controls in statements included in documents filed with the SEC and,
3. Make regular disclosures about the effectiveness of those controls, and potential fraud or losses that may affect the company's financial standing.

Because most companies' financial reporting and operations rely on information technology, and because many companies' assets take the form of critical data, SOX has significant implications for the IT departments of U.S. publicly held companies.

SOX has numerous components designed to increase corporate transparency, but there are three parts of the law that have particular importance to the IT community: Sections 302, 404 and 409 (and corresponding SEC Rules and Regulations). These sections focus on:

- Internal Control
- Evaluation (governance, measurement and recordkeeping)
- Disclosure

These elements do not stand alone, and must work together as part of the overall compliance process.

So where do we start? What can the IT staff and management do to ensure compliance?

Let's start with better understanding the requirements.

SECTION 302

Section 302 of SOX and the corresponding SEC regulations issued to implement it require corporations to establish internal controls over financial reporting and operations. They require the chief financial officer and chief executive to certify in corporate quarterly and annual reports that they:

- A. are responsible for establishing and maintaining internal controls;
- B. have designed such internal controls to ensure that material information [about the company and its subsidiaries] is made known to such officers by others within those entities.¹

¹ Sarbanes Oxley Act Section 302(A)(4)(a) & (B).

The goal of Section 302 is to force creation of a process ensuring that top management receives truthful information and reports it to the SEC. Establishment and maintenance of such a process assure shareholders that they receive accurate reports and that executives cannot blame subordinates or a breakdown in processes not directly under their control. The SEC regulations implementing SOX define “internal controls” as:

A process designed by, or under the supervision of, the registrant’s principal executive and principal financial officers... to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes... and includes those policies and procedures that:

1. Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant;
2. Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant’s assets that could have a material effect on the financial statements².

To satisfy the first item, companies must adopt policies and procedures to ensure that electronic records of transactions and asset disposition are kept and not later corrupted. This requires document retention policies and technologies that detect changes and can restore records to a previous “known correct state”. This presents a challenge; according to a 2003 survey by the Hackett Group, 47% of the companies surveyed use individual spreadsheets on diverse workstations for planning and budgeting.

To satisfy the second item, security policies and procedures must be implemented to protect the company’s information assets. Such security must prevent access to and distribution of company assets by unauthorized persons. This security should not be limited to financial records. Unauthorized access to information such as customer lists, product development plans and trade secrets could have a serious impact on the company’s value.

In addition, Section 302 requires that the chief financial officer and the chief executive of a company provide quarterly and annual reports that evaluate the effectiveness of their internal controls. They are required to disclose deficiencies and weaknesses in those controls and any fraud, material or not, that involves management or other employees who play a significant role in those internal controls.

Such reports are not possible without IT technologies that detect and audit changes to the systems that support the internal controls. This requirement heightens the need for technologies that monitor software and systems, alert when misuse is detected, and for general monitoring of employees’ use of the company IT systems.

SECTION 404

Section 404 requires that a company evaluate “the effectiveness of the internal control structure and procedures... for financial reporting” in an annual “internal controls report.” Overlaying

² Exchange Act Rules 13a-14(d) and 15d-14(d).

Section 302 requirements requiring a quarterly evaluation of controls, evaluation for Section 404 compliance must take place at least quarterly.

Since testing and validation of security systems on a regular basis is common practice in IT departments, Section 404 compliance is relatively easy. IT must provide a written description of their security processes and systems with accompanying risk analysis and mitigation plans, and a discussion of test strategies.

SECTION 409

Section 409 requires companies to report “on a rapid and current basis” any information about material changes to the company financial condition. This requires companies to immediately report any security breach or vulnerability that may affect the company financial condition or operations.

Again, IT technologies that monitor and alert play an important role in satisfying this requirement.

SUCCESS FACTORS

There are many factors that will indicate the potential for a successful compliance posture. “Sarbanes-Oxley Section 404: 10 threats to Compliance” by Deloitte & Touche LLP poses a number of questions highlighting issues surrounding the IT department that must be considered. Among them are:

Is the IT department highly customized? Custom-built applications and platforms are fertile ground for internal control issues. Inconsistencies that can be introduced through software that is non-standardized, not widely used, nor well-tested have an inherently high risk of errors and may introduce opportunities for unauthorized usage.

Does the IT department have a high turnover rate? Technology specialists tend to gravitate toward best-of-breed, sophisticated, cutting edge IT environments. A high turnover rate might indicate a dated technology whose unreliability could compromise internal control effectiveness.

Is there a large backlog of outstanding program maintenance requests? If IT professionals are having trouble keeping up with program maintenance requests, the systems may be overly complex and tedious to work with, casting doubt on their reliability.

Has the company needed to extensively rework or retrofit an installed ERP system? Badly designed or incompletely activated ERP controls can create significant internal control gaps.

Does the company rely on disparate legacy systems to manage financial reporting? Every time information must be altered for the sake of inter-system compatibility, the risk of introducing errors goes up.

Have formalized, consistent IT standards been established across all areas of the organization? Lack of such standards encourages variability among different areas of the business, increasing complexity and risk.

Are significant manual control activities required to manage the results provided by information systems? If employees feel they cannot rely on company technology, they may use manual processes to compensate for IT weaknesses. This introduces the specter of further inconsistencies and human error.

Do the organization’s IT processes maintain an adequate segregation of duties? Technology makes it easier for one person to do the work of many, but also introduces the risk of concentrating too much responsibility in one person. To satisfy Section 404 requirements, companies must be able to document the existence and enforcement of appropriate segregation of duties in IT in order to support a realistic security plan.

To these factors, we can add:

Does the IT department have the time required for the added burden placed upon them by SOX? Most IT departments are intensely busy with the already demanding day-to-day task of keeping a robust and reliable system available. Where will they find the time to monitor the large, often

multi-tiered systems on which their companies rely? How will they devote the time necessary to respond to security alerts when all of their time is already accounted for in responding to system reliability and performance issues? Clearly, significant participation is required from the IT organization to ensure that internal controls are not only in place, but are effective, as well. The integrity of financial data relies on the integrity of the underlying IT systems. Monitoring and alerting tools might capture huge quantities of data, but the appropriate people and filtering tools might not be in place to enable a timely response to critical incidents.

Is the SOX IT strategy consistent? According to Fred Roth of the MIS Training Institute, “The larger the organization, the more software-based control there should be.” Roth, a 25-year veteran of system development and IT audit and security now delivers training for SOX auditors. He continues, “The more we see manual controls, the more questions we ask – and the more we get nervous about the internal controls being consistently followed. Just having software is not going to ensure compliance, but it gives us an extra level of comfort.”

And finally, is the SOX strategy cost-effective? A SOX compliance strategy may involve significant modification of current manual or paper-based processes. Modifications to those processes for the sake of compliance could introduce operational inefficiencies and increased costs. For each compliance area, a basic cost/benefit analysis should be done. If the only benefit of implementation is compliance, and if modification of processes increases operating costs, then automated solutions could be the best approach.

Understanding what SOX requires and having thoughtful answers for the points raised in this section, we now have a framework for implementing SOX compliance in the IT organization.

WHAT CAN TNT SOFTWARE SOLUTIONS OFFER?

The validity and integrity of information is the goal of Sarbanes-Oxley compliance. To this end, companies must implement processes to adequately protect their networks and critical systems. IT organizations can be overwhelmed by the huge data collection task that they face. They find themselves wrestling with large amounts of disparate data reflecting a massive number of daily events that must be addressed.

HOW TNT SOFTWARE'S SOLUTIONS WORK

With TNT Software solutions (ELM), administrators can monitor Windows systems at scheduled intervals or in real-time. Real-time monitoring uses a Service Agent on the target system, while scheduled monitoring is performed with a Virtual Agent.

The ELM family of solutions meets or exceeds requirements for monitoring today's large-scale implementations. On the front end, ELM monitors hundreds of machines and processes tens of millions of event log entries every day, gathers system performance and diagnostics information, monitors application and server availability, and sends real-time notification when things go wrong. In most implementations, a single ELM server collects, evaluates, and distributes the information as it occurs. This reduces downtime, increases security, increases server and application availability, and escalates the return on investment.

ELM automation of these tasks frees system engineers to manage more systems and to complete other pressing tasks required by today's regulatory and security demands.

On the back end, ELM produces meaningful views of that massive amount of data. Summary views and event views can be generated in seconds to give the System Administrator a bird's eye view of consolidated information, an essential analytical tool in times of crisis. Management reports showing critical performance and security conditions can be generated with the built-in, easy-to-use reporting capability of ELM. Management can have important information regarding the health and status of mission critical systems and applications on a regular basis.

ELM supports multi-tier architecture. An ELM server can forward an Alert, Event, Syslog message, or SNMP trap to another ELM server. This allows tiered system configurations or management of multiple systems in multiple locations, all at a single console. Because all communications between ELM servers is encrypted, ELM servers can be located in a DMZ, enabling real-time monitoring and notification without compromising security.

ELM automates the monitoring of:

- Events
- Performance data
- Services and Processes
- Software Inventory
- Microsoft Exchange Server
- Microsoft SQL Server
- Microsoft Cluster Server

- Internet Information Services
- Internet Services (HTTP/ FTP/SMTP/POP3/PING/ Port)
- WMI
- Log files
- SNMP and Syslog
- Web pages and links

ELM allows IT Managers to customize notification options to reach the responsible administrator or take automated corrective action. Barrage protection prevents event storms from becoming a nuisance.

ELM Advisor is an innovative desktop notification exclusive to TNT Software that informs IT Administrators of changing conditions without disrupting their workflow.

Other notification options are:

- SMTP or MAPI email
- Pager
- MSN Instant Message
- Network pop-up
- Web post
- LED marquee sign
- Audibles
- Command script
- Syslog message
- SNMP OID/trap

ELM Reports automates the configuration of informative reports designed for distribution to IT Managers, Security Auditors, and other IT professionals.

At-a-glance Views display critical data for rapid problem identification and resolution. The IT professional can easily see alerts, events, outages, and software inventory data from each monitored system without leaving the ELM Console.

Filtered Views provide the ability to build views tailored to functional objectives. Administrators can immediately focus on specific sets of event data.

ELM supports Microsoft SQL Server and Microsoft SQL Server 2000 Desktop Engine. **Database Failover** provides fault-tolerant, continuous collection of monitored system information. Filter-based archiving and pruning tools are provided to efficiently manage critical data and storage costs.

HOW DO TNT SOFTWARE SOLUTIONS FILL COMPLIANCE NEEDS?

Let's revisit the requirements for SOX:

- Internal Control
- Evaluation (governance, measurement and recordkeeping)
- Disclosure

TNT Software solutions automate the tasks that must be performed to meet these requirements.

INTERNAL CONTROL:

Critical logs from systems and applications are monitored on a regular basis, without human interaction. Events are collected and displayed at one central console and stored in a central database. ELM integrates with and leverages the world standard Windows security subsystem. This enables administrators to secure both containers and items. Administrators can modify native Windows access control lists (ACLs), and apply the ACLs to any item or items via the ELM Console.

When combined with a customizable snap-in, an administrator can deploy "read-only" instances of an ELM Console to subordinate administrators, help desk staff, managers and other individuals in their organization. Administrators can assign the following permissions:

- Read only
- Read, Write, Delete
- Full Control

ELM also includes support for Windows auditing of access to and modification of ELM Server Objects.

EVALUATION:

Event data is converted to meaningful information and displayed in several ways. Event Views and Summaries, At-A-Glance views, and the ELM Advisor give immediate, on-screen feedback about what is happening on the monitored systems.

ELM Reports mine the data to produce meaningful reports with charting. Reports can be scheduled for routine analysis and can be customized for special circumstances. ELM includes a built-in database engine that provides database support for:

- Microsoft SQL Server/MSDE

ELM stores a variety of information in its database:

- Alerts
- Events generated by ELM Server and Agents
- Software Inventory (Enterprise Manager Only)
- Event Log Records (Enterprise Manager and Log Manager only)
- SNMP Traps (Enterprise Manager and Log Manager only)
- Syslog Messages (Enterprise Manager and Log Manager only)
- Knowledge Base Articles (Enterprise Manager and Log Manager only)
- Performance Data (Enterprise Manager and Performance Manager only)

ELM's robust reporting engine enables administrators to create and schedule reports without requiring any additional software. Reports in ELM use ASP.Net to produce and manage reports. Predefined reports are grouped into categories for easy reference. Reports can be viewed through the ELM Console or a web browser.

All reports are stored in the Reports container in the ELM Console. This container, as well as individual reports, supports the application of Windows Access Control Lists (ACLs). You can secure the entire container, or secure individual reports.

DISCLOSURE:

ELM has the unique ability to alert IT staff in real-time. Any monitored item can be configured to alert when things look suspicious, when systems begin to degrade, when service is interrupted.

Microsoft Windows event logs are designed for consistency and efficiency. Event logging starts automatically at each system boot time. The event logs contain the most important information for diagnosing application and operating system failures, determining the health and status of a system, verifying that system and applications are operating properly, and ensuring system-wide security.

ELM monitors all of the event logs, including application-specific event logs such as the DNS Server log.

TNT Software solutions provide complete compliance coverage for IT organizations.

ADDED BENEFITS OF TNT SOFTWARE SOLUTIONS

The Success Factors listed earlier in this paper carry far-reaching implications for an IT organization. Meeting SOX requirements is, of course, our focus. But let's spend a moment discussing other benefits that satisfaction of the Success Factors can produce:

Time: The automated processes implemented with the installation of a TNT Software solution ease the daily burden borne by IT staff. With event data delivered to a centralized console and alerts configured to send real-time notifications, IT staff is freed to perform other pressing services.

Money: Automated controls over IT processes and policy enhance the flow and security of data. TNT Software solutions are scalable, so can be used enterprise-wide. Piecemeal installations become a thing of the past. Customers have experienced and remarked on the ease of installation and deployment of TNT Software solutions. Down time or fluky behavior becomes a thing of the past. IT staff productivity increases due to realignment of schedules and the confidence of using cutting edge tools.

Peace of mind: Those who have used TNT Software solutions will tell you. They go about their days with significantly less worry about system security and performance. With the added burden introduced by SOX, those using TNT Software are ready for the auditor, confident that their operations and processes will meet with approval.

CONCLUSION

Companies faced with SOX must adopt a compliance process that satisfies the control, evaluation and disclosure requirements of Sections 302, 404 and 409. Because information technology is at the heart of financial reporting and other company operations, IT processes and technologies must be designed to meet these requirements.

Companies adopting a policy that embraces strong IT governance are best prepared to give the chief financial officer and chief executive the tools they need to satisfy the SOX requirement to implement and certify the existence of controls, evaluate the performance of those controls and disclose events having a material effect on the company financial position.

TNT Software's solutions provide that strong governance stance. They allow IT staff to improve and manage system integrity and provide a natural complement to the Windows security framework. By offering real-time monitoring, alerting and reporting, TNT Software solutions improves general IT controls, increasing the efficiency and productivity of the organization and producing the peace of mind that SOX has been satisfied and that the critical systems for business processes are reliably monitored and maintained.