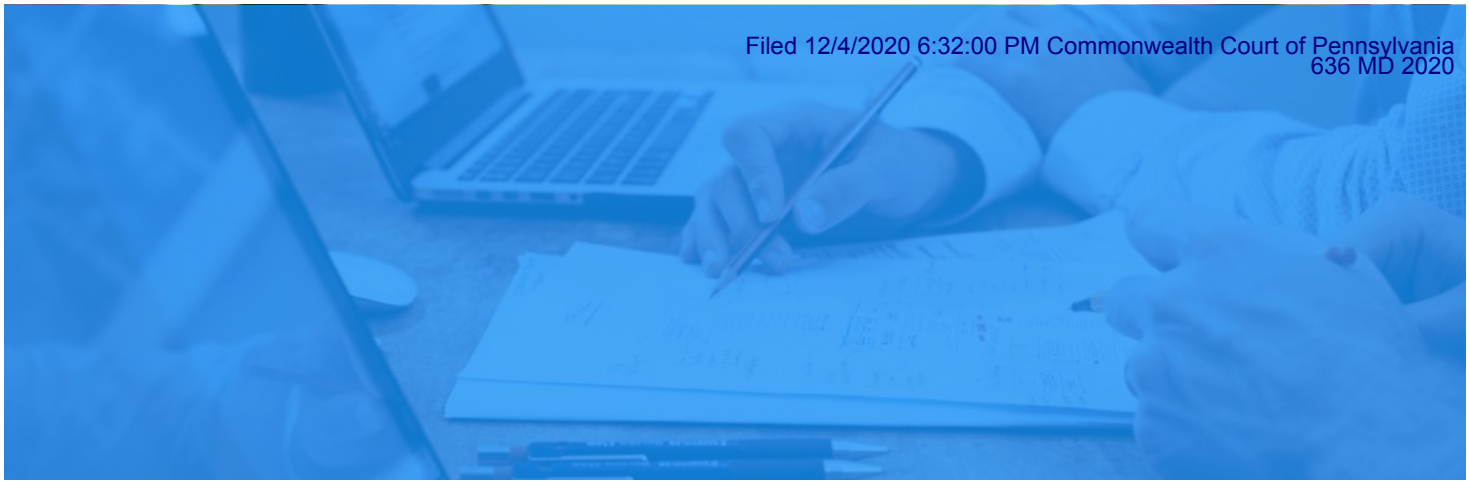

BLACKSTRATUS SOLUTIONS BRIEF

SOX RELOADED:

Essential Practices for Successful Compliance

BLACKSTRATUS™

WHAT SOX IS

The Sarbanes-Oxley Act of 2002 (more commonly known as SOX) is legislation passed by the US Congress to protect shareholders and the American public from fraudulent accounting practices as well as simple errors in the enterprise. As part of its mandate, it was also expected to ensure the accuracy of corporate disclosures. In June of 2003, the Securities and Exchange Commission (SEC) implemented Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) that required corporations not only include assessments of the controls they used to manage their financial reporting, but to also provide an auditor's report on that assessment. Both of which were required as mandatory inclusions to their annual reports.

SOX was intended to improve corporate governance and accountability. It allowed oversight of not only a corporation's financial controls and reporting, but also how it managed its information systems and electronic records. The controls were put in place to help rebuild investor confidence in corporate reporting standards that had been tainted by several accounting scandals in the early 2000s. So while many agreed that the increased oversight was needed, no one was prepared for the costs.

SOX COMPLIANCE IS EXPENSIVE

Based on a survey conducted by Protiviti in 2015, 58% of large corporations spent more on SOX audit fees than in previous year. The research also showed that more than half of large corporations surveyed spent more than $1 million on audit fees associated with SOX compliance, with 25% spending more than $2M. This is an average of $1M spent on SOX for every $1B in revenues. Most of this spending is for increased manpower – internal auditors and accountants – to document, test, and certify internal controls.

REGULATORY RELIEF?

The U.S. SEC and the Public Company Accounting Oversight Board (PCAOB) encourage auditors to consider a risk-based approach in evaluating the internal controls over financial reporting of public companies. They want auditors to focus on matters most important to internal controls that pose higher risk of fraud or material error. Similarly, auditors are being encouraged to consider and use the work of other auditors. As more auditors adopt this risk-based approach and consider the work of others, audits will be more scalable for the smaller and less complex companies. If properly put into practice, this new focus of auditing for SOX compliance is expected to make SOX more manageable, reduce the associated cost, and enhance its effectiveness in ensuring adequacy of controls and integrity of financial reporting.

PROACTIVE SECURITY IS THE LYNCH PIN

A proactive approach to security is the lynch pin to ensuring SOX compliance. Monitoring access to sensitive corporate and customer data is an essential element of an effective SOX compliance and risk management strategy. Companies need to ensure that threats to critical data do not go undetected and when incidents do occur, that they are quickly remediated and documented for internal and external audits.

WE OFFER A BETTER ALTERNATIVE

This paper explores how security information management (SIM) solutions offer a cost effective alternative for proactive risk management across your network, applications, databases, and user activities, while enabling SOX compliance as a result of these actions. Properly implemented, a best-practices SIM solution provides organizations reliable, end-to-end security monitoring and incident management processes surrounding financial applications and data, and the IT systems that support them. SIM can enable companies to meet Section 404 objectives through incident resolution management, data collection and retention, accountability, and reporting. By deploying an effective SIM solution, companies are equipped with a full range of tools that support SOX compliance objectives.

THE SOX CHALLENGE CONTINUES: MAINTAINING ACCUATE AND RELIABLE FINANCIAL REPORTING

SOX mandates all public companies to document, evaluate, monitor, and report on internal controls for financial reporting. It also requires disclosure of controls and procedures that include IT controls. Where SOX or the implementation of PCAOB standards do not define or are not clear on specific issues, auditors will rely on industry accepted best practices that are defined by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. The SEC makes specific reference to the COSO Internal Control Framework. PCAOB has also indicated a preference to COSO as a suitable framework. The objectives of the COSO framework include:

- Preventing fraud.
- Improving efficiency and profitability.
- Developing accurate financial reporting.
- Complying with applicable laws and rules.

COSO has identified the essential components of effective internal controls to include risk assessment, control environment and activities, information and communication, and monitoring. COSO clearly summarized the post-SOX environment when it stated, “The increasing power and sophistication of computers and computer-based information systems may contribute even more to the changing nature of fraudulent financial reporting. The last decade has seen the decentralization and the proliferation of computers and information systems into almost every part of the company. This development has enabled management to make decisions more quickly and on the basis of more timely and accurate information. Yet by doing what they do best –

placing vast quantities of data within easy reach, computers multiply the potential for misusing or manipulating information, increasing the risk of fraudulent financial reporting. Using computer technology effectively to prevent, detect, and deter fraudulent financial reporting is a challenge that requires foresight, judgment, and cooperation among computer specialists, management, and internal auditors.

SECURITY INFORMATION MANAGEMENT: ENABLES IT CONTROL OBJECTIVE FOR SOX

For a public company to maintain the accuracy and reliability of financial reporting required by SOX, its IT teams must have:

- Clear visibility into the network.
- Complete oversight and control of logical access to the network, applications, databases, and sensitive data.
- An effective incident resolution management protocol that allows it to respond rapidly to material events within 24 to 48 hours.
- Access to historical data for audit and forensic activities.

A comprehensive and specific approach to managing the IT controls associated with Section 404 of SOX can begin by leveraging a SIM solution – one that enables real-time monitoring and on-demand trend reporting. But technology alone is not the answer. Tools supplement a comprehensive security program that integrates existing assets – people, processes, and policies – that function within the operating environment. By implementing effective, comprehensive SIM policies and procedures for establishing accountability and consistent data collection, retention, and reporting practices, organizations can successfully demonstrate that IT controls support a sound internal control framework that meet Section 404 requirements. A high-performing organization that executes a proactive SIM strategy will establish six key practices from the top-down and bottom-up to:

1. Clearly define the control environment – Identify the systems, services, devices, data, and personnel associated with financial data and reporting. When selecting controls for the organization, it will help to ensure that such controls support business processes.

2. Strictly control access – Not only protect the data, but the systems, services, and devices within the organization. The organization must be able to demonstrate that it knows which employees, contractors, and partners have physical and logical access to the network, devices, applications, and data for specific and authorized business purposes, and that unauthorized access attempts – both physical and logical – can be identified and mitigated.

3. Validate security controls – Regularly monitor the environment for performance and effectiveness of the controls in place. Establish baseline activity, study trend line analysis, and ensure that unusual activity can be quickly identified and corrected as necessary.

4. Document all corrective action – Demonstrate that the proper steps were taken to correct systems and adjust policy if a noncompliant situation is identified.

5. Study the results of testing and reporting – Continuously manage and oversee the environment through reporting and testing, while providing documented evidence of due diligence to auditors.

6. Retain data according to local jurisdictional requirements – Preserve near-term and long-term data in its purest form for audit, forensics, and evidentiary presentation.

DATA COLLECTION AND RETENTION IS PARAMOUNT

The success of each organization's SIM solution is dependent upon its ability to collect sufficient data from across the network and applications. Each organization should take reasonable steps to ensure that sufficient data is collected to identify and respond to security incidents and to monitor and enforce policies and service level agreements. Appropriate data collection controls enable network and security personnel to review and analyze early warnings of potential system failures, unauthorized access attempts and security violations, provide support for personnel actions, and aid in reconstructing compromised systems. Automated data collection and retention allows many indicators of security and performance across the network and critical applications to be tracked on a continuous basis – as opposed to a periodic review – helping to create a proactive risk management process for:

- Identifying:
  - Policy violations
  - Anomalous behavior
  - Unauthorized configuration and other conditions that increase the risk of intrusion or other security events
- Real-time collection and historical data retention to quickly and accurately identify, classify, escalate, report, and guide responses to security events or weaknesses
- Incident remediation
- Audit trails
- Forensics support

THE ROLE OF SECURITY INFORMATION MANAGEMENT

The BlackStratus Solution: A Holistic Approach to SOX Compliance

BlackStratus security and compliance platform enables an efficient, comprehensive strategy for examining the adequacy and effectiveness of information security policies, procedures, and practices. BlackStratus delivers a robust security information management system with a variety of tools to help organizations:

- Collect and retain security event data from across the network.
- Identify, track, analyze, and remediate incidents.
- Implement an integrated incident resolution management work flow with embedded knowledge to resolve security incidents.

BLACKSTRATUS SOLUTIONS

BlackStratus security and compliance platform automates the collection and correlation of the immense volumes of data created through customer-defined policies and procedures. This high-performance SIM platform also provides periodic assessments of the risk and degree of harm that could result from unauthorized access, modifications, or destruction to data and information systems that support operations and organizational assets, a fundamental principle behind Section 404. More specifically, the BlackStratus platform provides organizations a core-to-perimeter set of tools and technologies that support Section 404 requirements, including:

- **Device, database and application monitoring –** Centralized application and device monitoring enables the collection, correlation, analysis, reporting, and retention of audit events from disparate security and network technologies. The BlackStratus platform monitors web and database applications, security and network devices, servers, and desktops to identify threats at the network perimeter, as well as malicious and erroneous inside activity. By monitoring and consolidating security activity on all systems, databases, and devices, and by leveraging a highly intuitive security and compliance reporting system, organizations can protect the integrity of enterprise data – especially from the increasing prevalence of insider threats.

- **Incident resolution management –** By integrating incidence response processes with existing enterprise workflow systems, the BlackStratus platform enables an accelerated incidence response through a best practice, collaborative approach. Companies need to continuously reduce risk exposure through timely and effective incident response, even when faced with vast amounts of security data including countless false positives. Using a clearly defined, repeatable, documented security information workflow, organizations can ensure quick and accurate handling of security incidents and prove diligence in SOX audits.

- **Compliance dashboards –** BlackStratus' customizable dashboards provide real-time monitoring and a holistic view of the company's security posture at a given point in time, and allows security staff to quickly measure threat levels against high value assets – including those most critical to achieving regulatory compliance.

- **Embedded knowledge base –** The BlackStratus knowledge base delivers guidance in analyzing, documenting, and reporting on security issues, including newly discovered vulnerabilities, malware, and vendor-specific vulnerability data. Security operators and analysts can obtain a continual flow of relevant and actionable information to pinpoint attacks and provide containment and remediation steps to network and configuration managers. Security teams can get highly specific response guidance in the event of a reoccurrence because the knowledge base can be updated with organization-specific data, such as information about a previous incident.

- **Security operations performance measurement –** SOX compliance is driving the need for metrics-based security management. BlackStratus gives organizations the tools to measure the performance of security operations, to better understand risk, and to quantify the success of SOX compliance initiatives. BlackStratus automates key compliance metrics – from vulnerability metrics to high-level risk metrics by providing reports that focus on vulnerability, threat, and incident response for all SOX related assets.

- **Risk assessment –** BlackStratus delivers a continuous, comprehensive picture of risk through a suite of risk assessment tools, techniques, and reports that capture real-time and historical risk information – pinpointing threats and vulnerabilities at the network and user activity level. An array of risk assessment reports provide the necessary details behind each SOX related asset and its associated risk, enabling security teams to pinpoint and prioritize threats. Real-time insight into the risk baseline is delivered through a suite of operational and management reports that are available from a customizable dashboard.

- **Strong correlation of system-wide security events –** BlackStratus' correlation technologies go beyond simply logging security information, and instead speed threat identification and provide an accurate picture of risk. These technologies are architected to handle the massive volume of security information from network-related sources as well as server logs, applications, and databases and identify attacks from the inside and beyond based on a thorough understanding of network and user activity. The correlation technologies process large volumes of data from the perimeter down to the core to identify real-time threats and historical patterns. Organizations can leverage their broad security knowledge base and correlate the information to uncover threats that would otherwise go undetected, facilitating proactive security management.

- **Incident detection through visualization and reporting –** With the BlackStratus solution, organizations can visualize threats as well as the security information underlying the threats. Security teams can assimilate information faster and then focus on the real security threats, mitigating vulnerabilities before threats proliferate. Through in-depth reporting, key stakeholders and auditors have ready access to actionable information on all security related issues such as viruses, worms, and other malicious code; all system status and configuration changes; and privilege and authorization changes.

- **A highly scalable and redundant security architecture –** The extensive scalability of BlackStratus architecture cost effectively supports growth and ensures that as your organization grows and changes, your SIM solution can grow and evolve with it. These robust SIM architectures incorporate high volumes of data from across the organization, regardless of the number of devices, applications and databases. BlackStratus offers the only multitier SIM architecture with full failover to ensure SOX compliance.

SECURITY AND COMPLIANCE MANAGEMENT SOLUTIONS

With BlackStratus Security information and Log Management platform capabilities, BlackStratus delivers the most well-engineered security compliance management solutions available today: powerful, scalable and flexible. From real-time threat identification and mitigation to log management and audit readiness, BlackStratus is renowned for providing solutions that help organizations take control of security, operations and compliance. Our patented, award-winning technologies tie together silos of data to obtain a complete, understandable picture of network security and compliance posture. By centralizing huge volumes of data - from the perimeter to the core of the network - and delivering the right security information into the right hands at the right time, BlackStratus solution dramatically improve your organization's ability to identify and rapidly respond to threats. Companies can finally gain an effective, proactive approach to protecting critical data and ensuring compliance with regulatory mandates and corporate policies. The BlackStratus platform delivers a whole new breadth and depth of security intelligence, regardless of organizational

size, type, or budget. Unlike other SIM or Log Management vendors, BlackStratus will not force an overly expensive SIM with more horsepower than you need, or try to ineffectively scale a basic log management solution to fit the needs of a complex, distributed environment. We are the only SIM vendor that has a complete line of solutions to effectively address your specific needs, from both a performance and cost perspective. We believe that no matter how large or small your network, you should not have to make a choice between being secure and being compliant.

BlackStratus – Enterprise-class Security and Compliance Platform

The BlackStratus security and compliance platform, the industry's most robust Security Information Management software solution, transforms huge volumes of disparate, security-related data into understandable, actionable intelligence. Built on a highly-scalable n-tier architecture, it enables large organizations with complex networks to centrally gather, analyze, and accurately report on security events and risk posture. By identifying and enabling a rapid response to threats and providing an auditable compliance framework, it helps protect valuable data and address a myriad of regulatory challenges.

BlackStratus offers an all-in-one or combined SIM and Log Management appliances that are fast, effective and exceptionally affordable. Easy to deploy and use, BlackStratus features advanced correlation technologies and real-time monitoring for rapidly identifying and prioritizing threats. Add to that comprehensive log collection, documentation and storage - and organizations can now cost-effectively meet compliance demands while enhancing their overall security posture. BlackStratus offers flexible deployment options to accommodate any size networking environment.

CONCLUSIONS

With concerns regarding ongoing costs associated with addressing a SOX audit, many affected organizations lose sight of the positive effect on corporate governance gained by improving the accuracy and reliability of financial data. SOX compliance can assist organizations in improving operational efficiencies, and provide assurance of good business practice to consumers and investors. Section 404 mandates that management take an active role in operational oversight. Additionally, many organizations have a new appreciation for the role of IT in the internal control structure and a renewed appreciation for effective information security controls. Management needs to work closely with IT organizations on risk assessment and the implementation of security policies and operations. Overall, a security program that integrates people, policies, process, and technology is the best approach to managing Section 404 compliance. Fully implemented, holistic SIM solutions like BlackStratus, along with alignment of human, process, and information controls, enables organizations to meet SOX objectives. By leveraging existing technology and tools, organizations can identify, assess, and report on the status and security of financial-related processes and information, and can provide tangible evidence of their information security initiatives.

ADDITIONAL RESOURCES

Further information about Sarbanes-Oxley is available at the following websites:

- **The Securities and Exchange Commission:** www.sec.gov – the official source of government information on regulation, documentation, interpretation, and updates
- **The Public Company Accounting Oversight Board:** www.pcaob.org – the official source of Sarbanes-Oxley for auditors
- **The IT Governance Institute:** www.itgi.org – an industry consortia that has produced interpretation documentation and guidance for filers and implementers
- **SOX Financial Frameworks:** http://www.soxonline.com/coso_cobit_coso_framework.html – information on Sarbanes-Oxley and supporting working documents, with daily news updates
- **Sarbanes-Oxley.com:** www.sarbanes-oxley.com – a private information website, portions of which are available only to subscribers

ABOUT BLACKSTRATUS

BlackStratus is a pioneer of security and compliance solutions deployed and operated on premise, in the cloud or "as a Service" by providers of all sizes, government agencies and individual enterprises. Through our patented multitenant security information and event management (SIEM) technology, BlackStratus delivers unparalleled security visibility, prevents costly downtime, and achieves and maintains compliant operations at a lower cost to operate.

BLACKSTRATUS™

BlackStratus, Inc. | 1551 South Washington Avenue Suite 401 | Piscataway, NJ 08854 | T. 732.393.6000 | F. 732.393.6090 | www.blackstratus.com