

Identity Management and Sarbanes-Oxley Compliance

September 2005



Think IDentity

Table of Contents

INTRODUCTION.....	3
THE SARBANES-OXLEY ACT OF 2002.....	3
HOW SARBANES-OXLEY AFFECTS IT PROCESSES.....	6
IDENTITY MANAGEMENT FOCUS UNDER SARBANES-OXLEY.....	7
A10 NETWORKS' SMART IDENTITY MANAGEMENT SOLUTION.....	10
IDSENTRIE COBIT COMPLIANCE MATRIX.....	11
SUMMARY.....	15

Disclaimer

Although A10 Networks has attempted to provide accurate information in these materials, A10 Networks assumes no legal responsibility for the accuracy or completeness of the information. More specific information is available on request from A10 Networks. Please note that A10 Networks' product information does not constitute or contain any guarantee, warranty or legally binding representation, unless expressly identified as such in a duly signed writing. A10 Networks and IDSentrie are registered trademarks of A10 Networks, Inc.

Obtaining More Information

For more information on A10 Networks' Smart IDentity Management solution and its IDSentrie product family, please visit A10's web site at www.a10networks.com.

Corporate Headquarters

A10 Networks, Inc.
2125 Oakland Road
San Jose, CA 95131-1578
USA

+1 (408) 325-8668 (main)
+1 (408) 325-8666 (fax)

Introduction

The U.S. Federal Government introduced the Sarbanes-Oxley Act (SOX) in 2002 to restore confidence in the equity markets and strengthen integrity of financial reporting produced by publicly traded companies after allegations of questionable accounting practices and major corporate scandals. Compliance with SOX and other new corporate reporting requirements have proven costly and challenging for many US companies to implement, as the SOX act covers many different areas of business practices for internal controls and financial reporting.

The need to comply with Sarbanes-Oxley has exposed many weaknesses in corporate financial and information system processes over the last few years and has highlighted the need for publicly traded companies to improve. For many companies, accelerating their Section 404 filings to meet the initial November 2004 deadline meant implementation of manual temporary workaround and “quick fix” solutions to patch systems, applications, and processes.

This whitepaper discusses the impact of Sarbanes-Oxley on information technology and illustrates how A10 Networks’ Smart IDentity Management solutions simplifies the SOX Section 404 compliance process.

The Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002, also known as the Public Company Reform and Investor Protection Act, is the largest corporate reform of business practices in modern times. SOX directly affects U.S. public companies with revenues over \$75 million and includes not-for-profit organizations. Sarbanes-Oxley created a new level of accountability by imposing severe penalties for corporate wrongdoing. The Sarbanes-Oxley Act includes 11 titles which cover a broad spectrum of business practices for financial record keeping, auditing, reporting, and securities fraud. Two of the most visible sections of the act are Title III, Section 302 and Title IV, Section 404.

Section 302 of the Act holds the CEO and CFO of a company responsible for properly certifying the accuracy of quarterly and annual reports under the penalty of law. Under Section 302, executive management is also responsible for implementing and maintaining the necessary internal controls, ensuring the effectiveness of those controls, reporting all significant deficiencies in the design or operation of the internal controls, reporting fraud committed by management or employees that have a major role with internal controls, and reporting all changes in internal controls.

***Over 50% of US
multinational companies
polled by PriceWater-
houseCoopers are
considering new tech-
nologies to improve
reporting infrastructures
to satisfy Sarbanes-
Oxley’s corporate
reporting compliance
laws***

First year SOX compliance costs range from \$1.9 million to over \$4.7 million with internal labor hours totals ranging from 12,000 to more than 35,000 hours

For Information Technology (IT) professions, Section 404 is the most critical. Section 404 of the Act focuses heavily on the effectiveness of the internal controls used to govern the accuracy of information reported in financial reports and emphasizes the importance of ethical conduct and reliable information. In the annual filing, management must provide its assessment of internal control over the financial reporting – including a statement on maintaining adequate internal controls, identification of the framework used in accessing the effectiveness of controls, an assessment of the effectiveness of the internal controls over the last fiscal reporting year, and verification that auditors have attested to management’s assessment of the internal controls over financial reporting.

To ensure a standard method of reporting, auditing, and measuring compliance, the Committee of Sponsoring Organizations (COSO) framework of the Treadway Commission and the US auditing standards are recommended under Section 404. Under SOX, management must comply with:

- The effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Many companies rushed to meet their first-year SOX compliance in 2004 and experienced firsthand the tremendous cost and complexity of SOX adherence. According to a study by Finance Executives International (FEI), first year compliance costs for Section 404 averaged \$1.9 million, including an additional \$509,000 in auditing expenses and \$700,000 in IT consulting and software. Companies polled reported an average of 12,000 hours of internal time required to complete first year compliance. For companies with revenues over \$5 billion, FEI found higher first year costs of \$4.7 million and 35,000 hours of internal time to meet compliance.

Even with costs in the millions to achieve compliance, many companies still implemented manual procedures and temporary workarounds to meet their first SOX deadline. Going forward, these companies will need to invest in additional work to replace “quick fixes” with solid, scalable and sustainable solutions to meet future compliance more efficiently. According to Ventana Research, some auditors predict that 10-20% of companies covered by the Act will fail to comply fully in their first year and companies that rushed to achieve compliance with short-cuts will end up spending more to redesign their controls and effectiveness tests – making SOX Section 404 compliance even more complicated and time consuming.

Despite the heavy burden and costs on publicly traded companies, many businesses are reporting the benefits of SOX compliance and how working through the process has helped strengthen many aspects of their financial and information security processes that were not tracked previously. The benefits experienced by companies included:

- Accountability of individuals involved in financial reports and operations
- Reduced errors in financial operations
- Reduced risk of financial fraud
- Improved accuracy of financial reports
- Improved decision making through better information
- Improved investor confidence and shareholder value

But there is still a lot of work to be done to make the processes more efficient. PriceWaterhouseCoopers' Management Barometer Survey on Compliance Costs for US based companies shows that an overwhelming number CFO's and Managing Directors polled are planning improvements for subsequent years following their initial year compliance.

Despite the heavy workload and cost of Sarbanes-Oxley compliance, many companies are reporting the benefits of going through compliance

Planned Improvements*	
Strengthening Programs to Reduce Compliance Issues	82%
Improving Risk Management	79%
Streamlining for Cost Efficiency	72%
Centralizing People, Processes	52%
Increased Use of Technology	50%
Other	3%

*Multiple answers

Figure 1: PWC Planned Improvements Poll

Figure 1 demonstrates that the majority of companies polled will be spending a lot more effort to strengthen programs to reduce compliance issues, improve risk management and streamline cost efficiency – with 50% planning to increase the use of technology to improve compliance efficiency.

From the same PWC survey, Figure 2 shows that less than one-third of all companies polled are reporting “very efficient” compliance methodologies and practices – leaving the majority saying that their compliance programs can be improved.

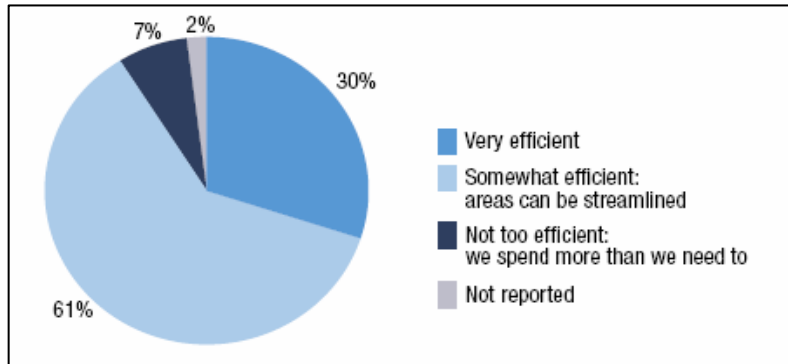


Figure 2: PWC Sarbanes-Oxley Compliance Efficiency Poll

How Sarbanes-Oxley Affects IT Processes

For Information Technology and Information Security (InfoSec) departments, Section 404 of the Sarbanes-Oxley Act is the most important. With the role computers play in the day-to-day activities of all publicly traded companies, there is no doubt that the success of a company’s SOX compliance program will depend heavily on its IT and InfoSec groups – as most business systems such as Enterprise Resource Planning (ERP) and financial reporting is controlled and run on systems IT manages. Under SOX, IT and InfoSec roles are expanded to include:

- Understanding the company’s internal control program and financial reporting
- Mapping IT systems for internal control & financial reporting to financial statements
- Identifying and understanding the risks related to these IT systems
- Providing the security and monitoring systems necessary to protect these IT systems
- Documenting and testing IT controls
- Ensuring IT controls are updated with changes in internal control or financial reporting processes
- Ensuring data confidentiality and integrity as well as availability of both real-time and historic data
- Architecting solutions to increase efficiency and lower costs of SOX compliance

In addition, for all audit related information, reports, and paperwork, SOX Section 103 requires that they be maintained for a period of 7 years – meaning IT and management must provide robust and secure systems with good logging, reporting and archiving capabilities.

Section 404 of the Sarbanes-Oxley Act affects IT and InfoSec professionals the most, and incorporating them throughout the compliance process will be critical to the success of SOX

Although Sarbanes-Oxley and COSO do not specifically provide insight into how internal controls are to be established with IT security, there have been separate references created to help guide IT and InfoSec professionals for SOX compliance. Two of these references are the Control Objectives for IT (COBIT) 3rd Edition and the ISO 17799: Code of Practice for Information Security Management. COBIT also provides a document created by the IT Governance Institute and the Information Systems Audit and Control Association called the "IT Control Objectives for Sarbanes Oxley" that maps the IT requirements to each of the Act's compliance components. This document can help IT and InfoSec professionals come up to speed on Sarbanes-Oxley requirements as they relate to IT.

More information on each of these references can be found at the following Web sites.

COBIT: <http://www.isaca.org>
 ISO 17799: <http://www.iso.org>

Although Sarbanes-Oxley doesn't specify the IT and Data Security requirements, COBIT and ISO 17799 can provide the accepted guidelines on how IT resources can be used to attain SOX Section 404 compliance

Identity Management Focus Under Sarbanes-Oxley

The complexity and effort required to meet SOX's financial compliance and internal control requirements will vary for each company and IT should analyze their infrastructure and controls to meet their company's specific objectives. Figure 3 highlights the Control Objectives as stated by COBIT and the US Public Company Accounting Oversight Board (PCAOB) and how they relate between each other.

COBIT Control Objective Heading	PCAOB IT General Control Heading			
	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire or develop application software.	●	●	●	●
2. Acquire technology infrastructure.	●	●	●	
3. Develop and maintain policies and procedures.	●	●	●	●
4. Install and test application software and technology infrastructure.	●	●	●	●
5. Manage changes.		●		●
6. Define and manage service levels.	●	●	●	●
7. Manage third-party services.	●	●	●	●
8. Ensure systems security.			●	●
9. Manage the configuration.			●	●
10. Manage problems and incidents.			●	
11. Manage data.			●	●
12. Manage operations.			●	●

Figure 3: PCAOB and COBIT Control Objectives Matrix

By keeping account information across separate and dissimilar data stores, management complexities and overhead are created that can make SOX compliance much more difficult

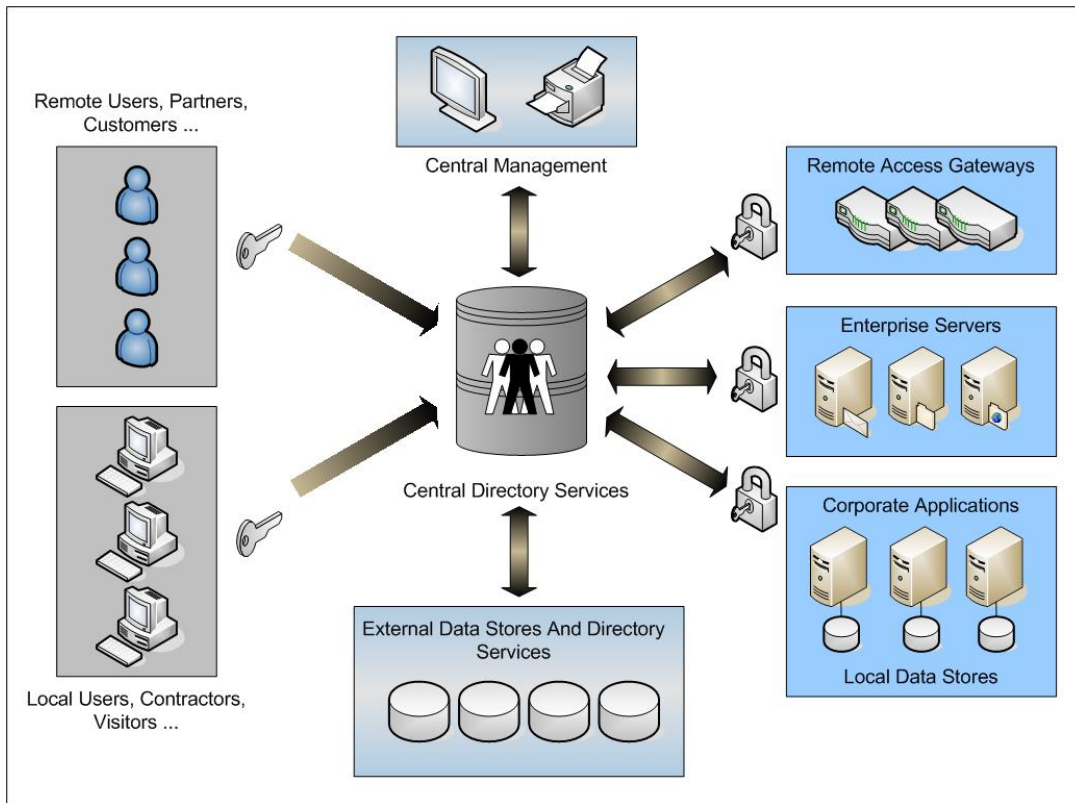
A key control category as outlined by both COBIT and PCAOB is “Access to Programs and Data” and states that access controls over programs and data must assume greater importance as internal and external connectivity to entity networks grows. To meet this need, IT must implement strong and accountable controls to provide assurance against unauthorized and inappropriate access to systems. Protection must be provided to safeguard against both external and internal threats. In addition to authentication control, SOX compliance requires a “separation of duties” for employees using SOX related systems. Access to applications and their functions must be restricted to authorized users only – users that must have them to perform their jobs.

Security Monitoring also becomes a high priority under SOX compliance. Proper monitoring helps reduce the risk of unauthorized access, risk of processing unauthorized transactions, generating erroneous reports, and reduces access to key systems in the event of application or infrastructure compromises. To safeguard critical resources, the first line of defense is authentication and authorization – making sure access to the systems and resources are granted to the right individuals.

As straightforward as this sounds, most enterprises are still using multiple data stores to house their user account and access policy information – LDAP, Active Directory, Novell eDirectory, Unix NIX and so forth. By keeping account information across separate and dissimilar systems, management complexities and overhead are created that can make SOX compliance much more difficult.

- Authentication credentials stored on different data stores across the enterprise causes user access issues, management overhead, account & policy inconsistencies, and increases the likelihood of administrative mistakes
- Data stores housed on insecure hosts can expose critical and personal information and grant unauthorized access
- Outdated accounts left over from previous employees, contractors, partners, and vendors that are not removed immediately greatly jeopardize corporate security
- Authentication policies are not consistent across the enterprise and can grant unauthorized access
- Disparate data stores cannot provide a unified view of all account information and authentication policies, making management and access tracking difficult

To help solve the problems mentioned above, Identity Management solutions are being developed to incorporate new ways to authenticate, authorize, and account for user activity. Identity Management is a system of integrated components that enable organizations to properly provision, manage, synchronize, and track user and application activity across the enterprise – making it easier to control and track access to critical SOX systems and satisfy compliance requirements.



Identity Management solutions are being developed to incorporate new ways to authenticate, authorize, and account for user activity

Figure 4: Centralized Account Management - Identity Management Solution

Figure 4 illustrates the benefits of centrally managing identity information through an Identity Management solution. A common management platform provides consolidated access to all identity information across disparate data stores containing user information and access policies. Changes performed by the identity management console can be synchronized with all other external data stores to ensure consistent identity information and authentication policies across the enterprise.

With Identity Management, access visibility is elevated to give IT a true picture of the number and types of accounts used throughout the company and the policies which govern them. Risks of unauthorized access are reduced, errors associated with multiple data store management are eliminated, access through unknown or illegitimate accounts is minimized, and user access activities are monitored and logged to meet strict regulatory requirements.

A10 Networks' Smart IDentity Management Solution

Authentication, authorization, accountability, and monitoring of user and system access are critical roles under COBIT's DS5 process

The COBIT framework for managing risk and control of IT resources is a very comprehensive guide which covers four domains, 34 IT processes and 318 detailed control objectives as it relates to financial reporting and Sarbanes-Oxley requirements. The four COBIT domains include:

- Planning and Organization
- Acquisition and Implementation
- Delivery and Support
- Monitor

DOMAIN	PROCESS	Information Criteria							IT Resources				
		effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data
Delivery & Support	DS1 Define and manage service levels	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS2 Manage third-party services	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS3 Manage performance and capacity	P	P			S				✓	✓	✓	
	DS4 Ensure continuous service	P	S			P			✓	✓	✓	✓	✓
	DS5 Ensure systems security			P	P	S	S	S	✓	✓	✓	✓	✓
	DS6 Identify and allocate costs		P					P	✓	✓	✓	✓	✓
	DS7 Educate and train users	P	S						✓				
	DS8 Assist and advise customers	P	P						✓	✓			
	DS9 Manage the configuration	P				S		S		✓	✓	✓	
	DS10 Manage problems and incidents	P	P			S			✓	✓	✓	✓	✓
	DS11 Manage data				P			P					✓
	DS12 Manage facilities				P	P						✓	
	DS13 Manage operations	P	P		S	S			✓	✓		✓	✓

Figure 5: COBIT Delivery & Support Domain Processes and IT Relationship

Figure 5 illustrates COBIT's Delivery & Support domain, its processes, and the IT resources necessary for compliance. The Delivery and Support domain is typically the most important COBIT domain for IT and InfoSec groups as it focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results, as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training. For Identity Management purposes, a large part of compliance revolves around how well each of the Delivery & Support domain processes are adhered to - authorized access control, monitoring of identity resources, and the ability to accurately recall the information (up to seven years) for auditing purposes.

IDSentrie COBIT Compliance Matrix

A10 Networks' Smart IDentity Management solutions provide a comprehensive suite of identity management tools to meet many of COBIT's Delivery and Support domain requirements. The following IDSentrie COBIT Compliance Matrix is an example of how A10 Networks' IDSentrie product family can help attain compliance for COBIT's Delivery and Support domain. As IDSentrie is designed to provide enhanced identity management and authentication security, the matrix concentrates primarily on process 5 - the Ensure System Security (DS5.x) section. But the matrix also shows the A10 advantages, on a higher level, for each of the other sections and illustrates the role IDSentrie can play in obtaining better compliance in these areas.

Note: As each company's compliance needs are different, A10 Networks recommends that customers perform a full analysis and risk assessment using one of the recommended SOX frameworks to properly evaluate their corporate compliance and control requirements.

Domain Process	A10 Networks Smart IDentity Management Solution
Delivery and Support Processes DS1 - DS4	
DS1.x – Define and Manage Service Levels	A10's IDSentrie provides scalable and flexible authentication policies that can be controlled through realms, groups, and individual users. These policies can be tied to each service and access level defined to control and monitor access.
DS2.x – Manage Third-party Services	IDSentrie's granular group-based authentication policies can restrict authentication access to limit access and control where and when partners authenticate. IDSentrie's advanced logging and reporting features and Firewall Log Analyzer accurately track 3 rd party users as they authenticate and access critical business systems.
DS3.x – Manage Performance and Capacity	IDSentrie's performance tuned and hardened platform provides high-availability clustering functions and a performance rating of over 6000 authentications per second. Deploying multiple systems throughout the enterprise allows for rapid scaling to meet capacity requirements.
DS4.x – Ensure Continuous Service	IDSentrie is designed to ensure non-stop service. All major hardware and software components are proactively monitored for failure and High-Availability clustering provides rapid failover to the secondary unit. System backup and restore ensures that configuration and data files are safely stored and available for fast recovery.

IDSentrie COBIT Compliance Matrix – Continued

Domain Process	A10 Networks Smart IDentity Management Solution
DS5.0 - Ensure Systems Security	
<i>DS5.1 – Manage Security Measures</i>	IDSentrie's Unified IDentity Manager provides central provisioning, management, and monitoring of identity information. Flexible authentication policy enforcement reduces complexity and eliminates potentially costly mistakes and security issues.
<i>DS5.2 – Identification, Authentication, and Access</i>	IDSentrie can authenticate users with its own local AAA RADIUS server and support Authentication Proxy to any supported external data store (LDAP, Active Directory, iPlanet, eDirectory, NIS and many others). Centralizing authentication activity and access policies to critical financial systems increases visibility and security. IDSentrie supports a broad range of authentication protocols and external data stores to maximize compatibility and implementation flexibility.
<i>DS5.3 – Security of Online Access to Data</i>	IDSentrie supports the latest strong authentication technologies such as 802.1x, EAP, certificates, and secure tokens to protect user credentials as they are transmitted over the airwaves or wire. Strong authentication prevents identity hijacking and theft of identity information to gain illegitimate access to data. IDSentrie's management system also provides secure and robust access to the IDSentrie appliance itself and encrypts all critical information on its hard drives to prevent theft and misuse of information.
<i>DS5.4 – User Account Management</i>	IDSentrie's Unified Identity Manager (UIM) provides complete centralization of identity information from local and multiple external data stores to simplify provisioning and management. Centralized management quickly identifies redundant, unused, unauthorized, and outdated accounts and allows IT to remove potential security issues and standardize identity information across all data stores throughout the enterprise.
<i>DS5.5 – Management Review of User Accounts</i>	IDSentrie's Unified Identity Manager and Advanced Reporting provide a centralized view of all account and identity information throughout the enterprise. Illegitimate accounts are quickly identified and IT can proactively deactivate or remove accounts for terminated users through IDSentrie's event scheduling module – eliminating the security issues caused by "left-over" accounts.

IDSentrie COBIT Compliance Matrix – Continued

Domain Process	A10 Networks Smart IDentity Management Solution
<i>DS5.6 – User Control of User Accounts</i>	IDSentrie’s User Self-Help module provides users with controlled access to their account profiles – allowing them to make simple changes, password renewals, and recover lost passwords. Administrators govern what information can be accessed and changed to prevent unauthorized modification of identity information.
<i>DS5.7 – Security Surveillance</i>	IDSentrie’s Advanced Reporting and Logging modules incorporate a sophisticated correlation engine that allows all authentication activities to be accurately identified to the user. Central logging, reporting, and alerting provide corporate-wide audit trails and notification capabilities. To preserve logs and audit trails, IDSentrie provides secure offloading of all log information to 3 rd party network storage systems.
<i>DS5.9 – Central Identification and Access Rights Management</i>	IDSentrie’s granular policy creation and enforcement based on realms, groups and users allows centralized authentication enforcement and control. Using Authentication Proxy and Unified IDentity Manager, all user access is accurately identified and logged no matter where the user’s authentication credentials are located.
<i>DS5.10 – Violation and Security Activity Reports</i>	IDSentrie’s advanced logging, reporting, and alerting modules provide a complete picture for all authentication information. The Firewall Log Analyzer provides additional tracking of policy violations and provides an audit trail of the activity. Violation reports, escalations and alerts provide IT and management with a clear view of inappropriate use. Access to security logs are restricted to system administrators and authorized personnel only.
<i>DS5.11 – Incident Handling</i>	IDSentrie combines several technologies to provide advanced identity-based forensic capabilities. Advanced logging and alerting modules with secure administrative access enables fast and reliable responses to authentication and security incidents.
<i>DS5.12 - Reaccreditation</i>	IDSentrie’s centralized policy enforcement allows management to periodically review all access methods controlled by IDSentrie to ensure authentication policies are still valid and up-to-date for safeguarding critical systems.
<i>DS5.13 – Counterparty Trust</i>	IDSentrie supports a broad range of authentication protocols, access methods, and 3 rd party data stores to support reliable counterparty authentication - including passwords, tokens, certificates, and other authentication mechanisms.

IDSentrie COBIT Compliance Matrix – Continued

Domain Process	A10 Networks Smart IDentity Management Solution
DS5.16 – Trusted Path	IDSentrie's Authentication Proxy module can protect existing external data stores by proxying authentication requests. With Authentication Proxy enabled, only IDSentrie needs to communicate with the external data stores – allowing IT to fully restrict access from all other users and create a trusted path to the data store.
DS5.17 – Protection of Security Functions	IDSentrie provides a hardened and purpose-built platform and operating system to safeguard identity information and security functions. Limited protocol support on all user-facing interfaces limit access to only authorized authentication protocols. All critical security and user information is encrypted to prevent unauthorized use and theft of information. Configuration and user information files can be backed up and restored to protect against failure.
DS5.18 – Cryptographic Key Management	IDSentrie provides PKI management for authentication protocols requiring certificates and supports the latest authentication protocols requiring certificates.
DS5.19 – Malicious Software Prevention, Detection, and Correction	IDSentrie's hardened platform is resistant against many intrusion attempts, viruses and worms. Its Firewall Log Analyzer module also identifies popular protocol anomalies and attacks traversing the firewall and provides alerts and reports based on user identity.
DS5.20 – Firewall Architecture and Connections with Public Networks	Although IDSentrie is not a firewall, its Firewall Log Analyzer module provides a sophisticated capability of analyzing user activity as it traverses the firewall and accurately associates the activity with the true identity of the user. IDSentrie provides more than 120 activity reports to enhance visibility and forensic activities.
Delivery and Support Processes DS9 – DS13	
DS9.x – Manage the Configuration	By allowing all identity information to be centralized, IDSentrie provides a unified approach to managing identity information. This ensures a standardized approach to authentication and identity management functions that are difficult to achieve with dissimilar and separate data stores. Access to configuration information is protected and restricted to authorized personnel only.
DS10.x – Manage Problems and Incidents	IDSentrie's logging, reporting, alerting, and auditing functions can provide valuable information to help with DS10 processes.
DS11.x – Manage Data	IDSentrie's authentication capabilities ensure that only authorized personnel are allowed to gain access to critical systems. User access is logged and retained for auditing purposes.
DS13.x – Manage Operations	IDSentrie's scheduling facility allows IT to schedule the deletion of user accounts to properly terminate access for users leaving the company. Operation logs can be securely offloaded onto network storage systems to comply with compliance requirements.

Summary

The Sarbanes-Oxley Act of 2002 was implemented to regain the trust of investors and consumers after several high profile financial scandals and is considered to be one of the most rigorous pieces of legislation ever enacted. Compliance with SOX Section 302 and 404 has strengthened the position of companies and helped regain the trust of investors and consumers alike. A10 Networks' Smart IDentity Management solutions provide improved SOX Section 404 compliance based on COBIT security objectives and enhance identity reliability, accountability and integrity throughout the enterprise. IDSentrie allows IT and InfoSec professionals to regain control of their identity information no matter where it's located in the enterprise – lowering provisioning and management overhead, cost of ownership, and eliminating costly mistakes and potential security risks.

For more information on A10 Networks' Smart IDentity Management solution and its IDSentrie product family, please visit A10's web site at www.a10networks.com.