Addressing Information Security Mandates of Sarbanes-Oxley
Keys to Safeguarding Critical Data and Achieving Data Privacy inside the Enterprise

Passed in 2002, the Sarbanes-Oxley Act was enacted in response to the widespread incidence of accounting scandals and high-level corporate fraud that were garnering national attention. The implications of this act are profound, necessitating a fundamental change in the way business is conducted in the U.S. Sarbanes-Oxley features comprehensive guidelines on the establishment of accounting oversight boards, corporate responsibility and accountability, enhanced financial disclosures, and more.

Sarbanes-Oxley, and privacy legislation and security mandates that are being enacted across a range of industries and geographies, are serving to place an even greater premium on the ability of organizations to safeguard data. As companies look to contend with the myriad implications of this act, they are increasingly compelled to address the way sensitive data is being managed inside the organization.

Although most companies have a strong perimeter security defense in place, today most damaging cyber attacks tend to occur on sensitive business information within the enterprise, often after it is stored on unsecured back-end servers and databases. While perimeter security technologies remain critical, the reality is that the perimeter will never be 100% foolproof, and the threats from inside the organization need to be mitigated. Thus, there’s a growing momentum behind data privacy. Data privacy is the process of securing critical data assets—such as credit cards, social security numbers, passwords, and addresses—as they are being stored, transmitted, and used within the enterprise.

Ingrian enables organizations to encrypt and secure critical data inside the enterprise, and so ensure data privacy. By managing all cryptographic services and keys on this specialized security platform, Ingrian can interface with each server and process hundreds or thousands of encryption requests in a way that is faster, simpler, and far more secure than any other commercially available alternative. With its granular encryption capabilities and centralized key management, Ingrian enables organizations to more effectively control what financial data can be accessed, and by whom. Further, it offers detailed logging capabilities so that organizations can both understand and thus knowledgeably report on the way sensitive financial data is used and managed.

This document will review some of the specific guidelines of Sarbanes-Oxley and how Ingrian’s data privacy solutions help address some of the key mandates for information security.
Access Control

Section 103 of Sarbanes-Oxley states that organizations must undertake “an evaluation of whether such internal control structure and procedures... include maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer... [and] provide reasonable assurance that transactions are recorded as necessary.”

As administrators look to evaluate their internal controls, they often realize that sensitive financial data inside their organizations is accessible to far more people than it needs to be.

Further, section 302 of the Sarbanes-Oxley Act mandates that “the signing officers have disclosed... all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer’s ability to record, process, summarize, and report financial data and have identified for the issuer’s auditors any material weaknesses in internal controls; and any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer’s internal controls.”

Ingrian’s field-level encryption capabilities offer a way to secure critical data inside organizations, and protect that data from both internal and external threats. By implementing this solution, organizations significantly enhance internal controls, gain more sophisticated visibility of how and when sensitive data is accessed, and mitigate the threat of internal fraud.

DataSecure’s robust authentication and authorization capabilities allow the enterprise to restrict which applications and business processes can access sensitive data in the clear. With DataSecure, organizations gain a strong layer of security with granular access controls for both data and the keys used to unlock that data.

These capabilities are critical to Sarbanes-Oxley compliance: If administrators can’t ensure that only authorized staff can access sensitive data, and record how and when that data is accessed and by whom, they can’t authoritatively attest to the accuracy of the reports that are based on that data.

Audit Trails

Sarbanes-Oxley stipulates “each annual report... contain an internal control report, which shall... contain an assessment... of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.” (Section 404)

Clearly, Sarbanes-Oxley mandates greater disclosure of internal controls. By augmenting internal controls over how critical data is accessed and managed, financial institutions can benefit by communicating these sophisticated safeguards—and the enhanced control of data—to auditors and shareholders.

A fundamental aspect to achieving data privacy in an organization is the task of monitoring and logging all attempts to access or manipulate sensitive data. Largely, this is the only way administrators can be sure that critical data is in fact secured. Being able to log and monitor this activity is also a fundamental requirement for compliance.

When encrypting data within an enterprise, one has to consider the fact that data, keys, and logs will be accessed, encrypted, managed, and generated on multiple devices and in multiple locations. With DataSecure, administrators can centrally log and audit access to data and keys, and so gain a range of benefits:

- By leveraging a single and centralized interface, the cost of management is reduced.
- Security is enhanced because administrators gain a centralized mechanism with which to view information as attempted attacks occur.
- Organizations can more effectively ensure compliance with Sarbanes-Oxley logging and auditing requirements as well as other governmental and industry legislation.

About Ingrian Networks

Ingrian Networks brings complete data privacy to the enterprise. Ingrian DataSecure Platforms ensure that sensitive information is impervious to attacks, whether data is at rest, in transit, or in use. Ingrian DataSecure Platforms offer intelligent, granular control over what data is protected, they adhere to open standards and are cost effective to deploy, and they deliver comprehensive security capabilities. For all these reasons, Ingrian is the smart choice for addressing one of today’s most critical security threats—data left unprotected within the enterprise. For more information, visit www.ingrian.com.

© Copyright 2004 Ingrian Networks. The Ingrian Logo, Ingrian, and DataSecure are trademarks of Ingrian Networks. All other brand names are trademarks of their respective holders.