

CREDANT Solutions for SOX Compliance

Financial data needs to be protected across the enterprise – and beyond.



CREDANT SOLUTION

CREDANT Mobile Guardian (CMG) ensures that SOX encryption and security mandates are consistently and efficiently enforced – regardless of where the data resides.

Only CMG enables organizations to:

- › Encrypt and secure data across multiple, diverse platforms from a single console.
- › Create automatic audit trails that offer proof of end-to-end data security.
- › Provide a transparent end-user interface that supports user productivity while keeping data safe.

CMG's Intelligent Encryption provides centrally-managed, highly scalable and architecturally flexible security to manage all data endpoints. With CREDANT, organizations can:

- › Ensure data security without the risk of users placing data in areas that are not encrypted.
- › Provide confidentiality, privacy and auditing of data residing on any endpoint.
- › Protect sensitive data from unwarranted access, thus reducing risk of internal breaches.

Regulatory overview

The Sarbanes-Oxley (SOX) Act is a United States federal securities law designed to protect shareholders and the general public from accounting errors and fraudulent practices by publically held companies. Signed into law in 2002, SOX establishes a large number of mandates involving records retention requirements for audit papers, auditor independence, transparency for accounting and criminal penalties relating to fraud, conspiracy and interfering with investigations.

The compliance challenge

Perhaps no other government regulation has had a greater impact on U.S. businesses over the past decade than SOX. Although the law is focused primarily on the accuracy of financial reporting and accounting controls, it also affects IT security through the need to ensure the reliability and integrity of financial data.

For example, Section 103 of SOX requires maintenance of all audit-related records (including electronic data) for seven years. Section 802 regulates the retention and protection of audit and related documents, with criminal penalties for altering documents. Especially important is Section 404 which mandates effective internal control structures and reporting procedures for financial information. These structures include a framework for controlling and auditing who accesses financial information and a framework for controlling and auditing what financial information is accessed.

To demonstrate compliance efforts, organizations must also establish specific security policies regarding mobile devices. This includes defining what kinds of mobile devices can be used, what information can be stored on them such as customer information or intellectual property, who can use them, and where they can be used – whether at home, at the office or on the road.

CREDANT

More than 700 enterprises and government agencies – including 50 of the Global 500 – rely on CREDANT to ensure security compliance, protect their brand and enhance IT and end-user productivity.