

WHITEPAPER

SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?





SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?

Executive Summary	3
Sarbanes-Oxley	5
Control Environment	5
Risk Assessment	5
Control Activities	5
Information and Communication	6
Monitoring	6
California Senate Bill SB 1386	7
Gramm-Leach-Bliley Act	8
The Regulations and Mobile Devices	8
How CREDANT Mobile Guardian Enterprise Edition Helps You Meet Your Compliance Objectives	9
Sources	10
Other Useful Resources	10

SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?



Executive Summary

Mobile computing, as the next wave in the evolution of computing, is bringing substantial benefits to many organizations. Having access to critical business information anytime and anywhere helps make employees more productive and the organization itself more competitive.

However, mobile devices present well-known risks for the organization. Laptops are easily lost or stolen, and the information on them is easily compromised unless encryption is utilized to protect sensitive data. In fact, in the 2009 CSI Computer Crime and Security Survey, 42% of all respondents reported experiencing laptop theft or loss. Smartphones can also contain enormous amounts of information and may have no enterprise-enforced security capabilities unless additional mobile security software is used. Many of these devices may be employee-owned, increasing the risk to unprotected data even more unless new policies, processes and technology are put into place.

The security of mobile devices MUST be considered when developing compliance strategies for regulations such as Sarbanes-Oxley, California SB 1386 (in addition to SB 1186) and Gramm-Leach-Bliley.

Sarbanes-Oxley mandates that an organization's officers attest to having effective internal controls, which must include controls over mobile devices and how they need to be secured to ensure adequate protection of corporate assets.

California SB 1386 recognizes the benefits of encrypting stored data, including data on mobile devices, by not requiring organizations to disclose a breach if personal data is encrypted.

Gramm-Leach-Bliley requires that organizations protect customer information stored on mobile devices, requiring organizations to take control and enforce appropriate security on all kinds of mobile devices.

SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?



This whitepaper will:

- › Summarize how mobile devices relate to Sarbanes-Oxley, California SB 1386 and Gramm-Leah-Bliley,
- › Detail why compliance strategies MUST include control and protection of mobile devices, and
- › Describe how CREDANT encryption management solutions are uniquely capable of addressing mobile security compliance issues for organizations such as yours.

SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?



SARBANES-OXLEY

The Sarbanes-Oxley (SOX) Act of 2002 significantly impacts the processes and accountability for financial reporting in publicly-traded US companies and makes executives responsible for establishing, evaluating, and monitoring the effectiveness of internal controls over financial and operational processes. In fact, senior executives must sign an attestation that they are responsible and that the internal controls meet the requirements of SOX.

In particular, Section 404: Management Assessment of Internal Controls requires that each annual report contain an “internal control report” which shall:

1. State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
2. Contain an assessment, as of the end of the issuer’s fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting

The Committee of Sponsoring Organizations (COSO) Internal Control - Integrated Framework (Control Framework) has been widely accepted as the internal control standard for organizations implementing and evaluating internal control in compliance with the Sarbanes-Oxley Act. COSO requires five interrelated components: the control environment, risk assessment, control activities, information and communication, and monitoring.

From a mobile device security perspective, the existence of mobile devices within an organization has an impact on all of these components.

CONTROL ENVIRONMENT

The control environment sets the tone of an organization. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity’s people, management’s philosophy and operating style, the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.

Mobile devices are a critical part of the control environment. The existence of company-owned notebooks and employee-owned smartphones and PDAs must be acknowledged by the organization as being a part of the control framework.

RISK ASSESSMENT

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is the establishment of business objectives, and that they be linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achieve specific business objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

CONTROL ACTIVITIES

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address the risks to achieve the entity’s objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?



Given the risks associated with the use of mobile devices, control activities need to be put into place to manage the risks. One key differentiator for mobile devices is that they are not always connected to the organization's network, but must be protected even when they are not connected. Enforcing that all business information stored on notebooks is encrypted to protect it from the risk of loss, theft or attack is required, as is the ability to detect and enforce appropriate security on all smartphones and PDAs used throughout the organization, whether they are owned by the organization or the employee. Equally important is the ability to deny access to organization resources which don't meet corporate policy, and a method to remediate those devices by pushing policies to them to bring them into compliance and allow them to have access.

INFORMATION AND COMMUNICATION

Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that makes it possible to run and control the business. They deal not only with internally-generated data, but also information about external events, and activities and conditions necessary for informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that the control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

Security policies must be in place to cover the use of mobile devices, and these policies must be communicated to employees throughout the organization. Communications regarding the current state of the usage and compliance of mobile devices to senior management is necessary to ensure adequate control is in place.

MONITORING

Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

Monitoring mobile device usage and ensuring that it complies with the control systems that are in place needs to be an ongoing activity. The usage of employee-owned devices needs to be covered in the policy, but must also be monitored on an ongoing basis to ensure that there is effective control over input and output of information from these devices to the organization.

In summary, the key requirements to ensure SOX compliance with respect to the use of mobile devices are to ensure that policies, procedures and controls cover:

- › What kinds of mobile devices can be used (type and ownership – organization or employee)
- › Who can use them (employees, contractors, others)
- › What information can be stored on them (customer information, sensitive, internal, public)
- › What applications can be used on them

SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?



- › What security protection is required (access control, encryption, other)
- › Where they can be used (workplace, home, while traveling)
- › What networks can they be used with (internal, public, home...)

Once the policies are in place, security software and systems can be used to enforce the policy, and provide ongoing monitoring and control of the use of mobile devices throughout the organization.

CALIFORNIA SENATE BILL SB 1386

Passed July 1, 2003, California Civil Code Section 1798.8 is the law formerly known as SB 1386. It applies to any entity doing business in California or that handles the personal information of California citizens.

It provides for a mandatory notification obligation in the event of unauthorized acquisition of Californians' "personal information" that is stored in electronic form.

Personal information includes name and either:

- › Social security number,
- › Driver's license number, or
- › Account number, credit or debit card number, along with any required security code, password, or access code that would allow access to an individual's account.

An organization must disclose a breach in data security to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The notification must occur "in the most expedient time possible and without unreasonable delay."

The notification can be written or electronic. If the cost of providing the notification exceeds \$250,000 or

if the number of affected persons exceeds 500,000, then an organization may satisfy the notice requirement by taking three steps:

- › Emailing all individuals for whom it has an email address,
- › "Conspicuous" posting of notice on the company web site, and
- › Notification of major statewide media

From a mobile device perspective, the legislation is explicit in noting that notification is not required if the information is encrypted. This is a significant, because if encryption is used to protect personal information that is stored, accessed or even displayed on a mobile device, then there is no notification requirement if the device is lost, stolen or attacked, as the information is protected by the encryption.

Best practices to deal with SB 1386 and mobile devices is to ensure that ALL sensitive information stored on the device—whether that device is a notebook, tablet, smartphone or PDA—is protected by encryption, ensuring that no notification will be required in the event of a lost or stolen device. The benefits of using stored-data encryption are the cost savings with NOT having to notify, and the reputation/brand protection that comes from NOT having to make a public notification of potential harm to end users.

Even though SB 1386 is only for a Californian's personal information, some organizations such as GMAC have notified over 200,000 customers outside of California when a notebook was stolen that contained their personal information. The possible addition of the provisions within SB 1186 further clarify what is required by way of notification in SB 1386, again, raising the bar on the workload and cost associated with a breach of unencrypted data. Ensuring that information is encrypted is a best practice for protecting that data, and will help an organization comply with SB 1386 and other legislation such as Gramm-Leach-Bliley.

SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?



GRAMM-LEACH-BLILEY ACT

The Financial Modernization Act of 1999, also known as the “Gramm-Leach-Bliley Act” or GLB, includes provisions to protect consumers’ personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Pretexting Provisions and the Safeguards Rule.

The GLB Act applies to “financial institutions,” including not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are:

- › Lending
- › Brokering or servicing any type of consumer loan
- › Transferring and safeguarding money
- › Preparing individual tax returns
- › Providing financial advice and credit counseling
- › Providing residential real estate settlement services
- › Collecting consumer debts
- › An array of other activities

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to companies – such as credit reporting agencies – that receive customer information from other financial institutions.

Mobile devices are important to consider for compliance with the Safeguards Rule. As with California SB 1386, it is clear that the usage of mobile devices must take into consideration the storage of any sensitive information. Again, best practices to meet GLB are to ensure that usage of mobile devices is controlled throughout the organization and that all information on

the devices is protected by adequate access control mechanisms and stored data encryption. GLB also requires the ability to deny access to organization resources to those devices which don’t meet corporate policy, and a method to remediate the devices by pushing policies to the devices to bring them into compliance and allow them to have access.

THE REGULATIONS AND MOBILE DEVICES

All three regulations require organizations to take control of mobile devices, such as laptops and smartphones. These devices may contain sensitive information, such as customer personal information, financial information contained in an email or other types of information, which is subject to the regulations.

In the case of Sarbanes-Oxley, the requirement to have effective internal controls dictates that organizations should have a written policy about the use of mobile devices. Ensuring adequate internal controls would dictate that the usage of mobile devices be controlled, and the sensitive information stored on them protected by access control and stored data encryption. An employee-owned smartphone containing an email detailing financial results not yet released to the public could cause substantial damage to an organization’s reputation if it was made public, but would also be a good example of ineffective internal controls – unless the device was protected by mandatory access control and stored data encryption. Continuous detection, inventory and enforced protection of mobile devices is required to ensure that the written policy is complied with, and is considered best practice for controlling mobile devices. This is necessary to ensure that organizations can control what is connecting to their networks, and apply policies to allow access if the device is not in compliance.

For SB 1386 and Gramm-Leach-Bliley, the requirement to protect customer information means that organizations must ensure that customer information is

SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?



secure at all times, including when stored on a mobile device. SB 1386 in particular notes that encrypting the information eliminates the notice requirement in the event of a breach. If the information contained in emails or a contact database was encrypted on a mobile device—which can be easily lost or stolen, no notice would have to be given, saving the organization from making a potentially expensive and embarrassing public disclosure.

Independent of the regulations, the potential for damage to an organization's reputation should a mobile device fall into the wrong hands has meant that many organizations have followed best practices for controlling mobile devices, including applying appropriate levels of access control and security to the devices themselves.

Overall, these regulations provide organizations with yet another reason to effectively secure mobile devices.

HOW CREDANT ENCRYPTION MANAGEMENT SOLUTIONS HELPS YOU MEET YOUR COMPLIANCE OBJECTIVES

CREDANT encryption management solutions allow you to put your paper security policies for mobile devices into action at the enterprise level, giving you control over mobile devices accessing your sensitive data. It can detect and report on devices that synchronize within your network. It can also automatically install identity- and role-based security software on devices and:

- › Requires mobile device users to authenticate by entering a PIN or password, or by answering a question, protecting sensitive data from unauthorized users, ensuring compliance with SOX, GLB and SB 1386 requirements for mandatory access control.
- › Can automatically encrypt all vital information stored on mobile devices, including information stored on removable media such as CompactFlash cards and

USB flash drives, specifically meeting the encryption requirements of SB 1386 and ensuring adequate protection of information for SOX and GLB.

- › Can track and maintain mobile device inventories to support internal controls for the use of mobile devices. This capability enables an organization to control and know what types of devices are actually connecting to their networks. In addition, CREDANT provides you the ability to log and track administrative activity such as changes in security policies to ensure traceability and accountability.

Working with CREDANT also reduces your cost of compliance by implementing solutions that:

- › Inheriting roles (groups) and users from your existing LDAP directory, eliminating the need to re-enter and separately maintain this information
- › Providing self-service PIN/password reset, minimizing the number of calls to your help desk and maximizing end user productivity
- › Automatically installing security software on mobile devices and updating the users' policies during synchronization, eliminating the need for manual provisioning

For more information on how CREDANT can help you secure mobile devices and meet the demands of mandates such as GLBA, SOX and state breach notification laws, please visit www.credant.com.

SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance?



OTHER USEFUL RESOURCES

1. CREDANT Mobile Guardian Enterprise Edition Technical Whitepaper - for additional technical detail about how CREDANT Mobile Guardian Enterprise Edition works and can help you, click [here](#) or go to the Resource Center of the CREDANT Web site, register (if you're not already a member) and look under Whitepapers.
2. For healthcare institutions, CREDANT has a whitepaper specifically addressing HIPAA, the Health Insurance Portability and Accountability Act. Click [here](#), or go to the Resource Center at www.credant.com, register and look under Whitepapers.