Entrust®

Securing Digital Identities
& Information

# The Road to Compliance: Signing Your SOX Certification with Confidence

This white paper discusses high-level requirements for complying with the Sarbanes-Oxley Act, with a specific focus on the next major section for legislated compliance, Section 404. It briefly outlines the requirements and timelines for compliance, and then provides details on how Entrust's market-leading security solutions can help organizations add accountability, privacy, and audit as a part of establishing appropriate internal controls and information security governance.

April, 2004

Entrust®

Securing Digital Identities
& Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. Lighthouse is a trademark of Waveset Technologies, Inc. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

## Table of Contents

***The Sarbanes-Oxley Act of 2002 (SOX) requires new attention to security as a part of a risk management framework to certify internal controls and attest to the accuracy of financial information (e.g., relating to fraud, accidents, or lack of discipline). Information security has moved from being a good idea to being a mandate, and companies must act now to meet these new requirements.***

*"Addressing Security Requirements in Sarbanes-Oxley",*
*Paul Proctor, METAGroup. September 22, 2003*

# Executive Summary

Information Security Governance is top-of-mind for organizations around the globe today, with legislation (such as Sarbanes-Oxley, California SB 1386, Gramm-Leach Bliley (GLBA), and Health Insurance Portability and Accountability Act (HIPAA)) and corporate scandals all playing roles in its heightened awareness. As governments move towards increased activity and legislation around information security and shareholders demand better corporate accountability from public firms, organizations are quickly being forced to look at the implications of their overall corporate governance strategy. This examination has led to an understanding that information security is not just a technical issue that can be addressed by the CIO. It is a corporate governance issue that must be addressed by CEOs and Boards of Directors, and must be then implemented and enforced at all levels of the organization. And in today's economic climate, the issue must be addressed in both a timely and cost-effective manner.

As organizations consider corporate governance issues, one of the most top of mind pieces of legislation impacting them is the Sarbanes-Oxley Act of 2002 (SOX). This US-based law is a critical piece of new legislation that affects how public organizations & accounting firms deal with corporate governance, financial disclosure and the practice of public accounting. Developed in response to realities of today's global, inter-connected business environment, the impact of SOX is far reaching, impacting organizations and individuals across internal & external boundaries. Those affected include auditors, executive management, audit committees, attorneys, and even securities analysts, providing legislated guidelines for compliance that are applicable across disciplines related to financial reporting.

Although there are many parts to the law, the next major section for legislated compliance is Section 404. Section 404 requires attestation by the CEO that his/her organization's internal controls support the validity of required financial reports. With deadlines looming for public companies from around the globe, organizations should be working today on how they will comply in a timely manner.

This white paper takes a high-level look at the legislation and the impacts it has on the various players in the industry, focusing on the fast-approaching deadline for Section 404 compliance and steps that need to be undertaken to achieve an appropriate level of internal control. With an understanding of the details and requirements for Section 404 compliance, this whitepaper delineates how Entrust's broad portfolio of security solutions are able to add accountability, privacy, and audit across the enterprise and help organizations close internal control gaps as part of SOX compliance.

# What is the Sarbanes-Oxley (SOX) Act?

The Sarbanes-Oxley Act of 2002 (SOX)[1] is a critical piece of new legislation that affects how public organizations & accounting firms deal with corporate governance, financial disclosure and the practice of public accounting. Developed in response to realities of today's global, inter-connected business environment, the impact of SOX is far reaching, impacting organizations and individuals across internal & external boundaries. Those affected include auditors, executive management, audit committees, attorneys, and even securities analysts, providing legislated guidelines for compliance that are applicable across disciplines related to financial reporting.

At a very high-level, Figure 1 below briefly outlines the impacts of SOX across various groups in the industry. For more specific information on the impact of the legislation, organizations should engage with their auditors.

| Impacted Group | High Level Summary of Impact |
|---|---|
| **Auditors** | • New system of private oversight, a revised set of independence rules and a new level of public reporting |
| **Management** | • Improved safeguards against conflicts of interest, explicit certifications of specific filings, reporting on internal controls over financial reporting and revised disclosure requirements |
| **Audit Committees** | • Continued expansion of their role in the corporate reporting framework including direct responsibility for overseeing the external audit process, pre-approval of all audit and non-audit services, revised rules regarding independence and financial expertise and monitoring, receiving and resolving complaints regarding corporate reporting and audit issues |
| **Attorneys** | • Subject to elevated levels of professional conduct |
| **Securities Analysts** | • Subject to a revised compensation and internal review structure to strengthen their independence from the investment banking side of their firms |

**Figure 1: Who is impacted by Sarbanes-Oxley & how?**

Although there are far-reaching implications to many groups, the rest of this whitepaper focuses on the impact to public companies (management and audit committees as highlighted above) as they work with their internal teams and external auditors to understand and comply with Section 404 of Sarbanes-Oxley.

# What is the timing and impact of non-compliance?

As the SOX legislation is very broad and far-reaching in its scope, it is being implemented in a phased approach, with executive management already being impacted by Section 302 of the act. As a result, most audit firms today have established practices around both auditing for SOX compliance as well as remediation of the audit findings. These audit firms are actively working with many of their customers on how to comply with the next phase of the legislation, and are typically well versed in how to achieve SOX compliance. The impacts of non-compliance ranges from monetary fines to jail terms, and includes the harsh reality that failure to comply ultimately will impact the public image of the organization itself.

The next section for legislated compliance is Section 404, which centers on the internal controls of an organization and how effective they are (in the context of how this may impact financial reporting). The chart

*[1] For more information, please refer to the Securities & Exchange Commission Web site (http://sec.gov/spotlight/sarbanes-oxley.htm), the Sarbanes-Oxley Web site (http://www.sarbanes-oxley.com) or contact your auditing firm.*

below delineates the three highest profile sections of the legislation for public companies, the dates associated with mandatory compliance, and some high-level details around each.

| Details | Section | | |
|---|---|---|---|
| | 302 | 404 | 409 |
| **What is it about?** | Certification of financial reports quarterly | • Annual certification of internal controls<br>• Independent accountant attests to report<br>• Quarterly reviews for updates/change | • Material event reporting<br>• "Real-time" implications |
| **Who signs off?** | CEO<br>CFO | • Management<br>• Independent accountant/auditor | • Management<br>• Independent accountant/auditor |
| **Effective Date?** | August 29,2002 | Fiscal year ends on/after:<br>• November 15, 2004 for accelerated filers*<br>• FY ending on/before July 15, 2005 for all others<br>**Note: For organizations on a calendar fiscal year, this means that compliance is an issue for **January, 2004*** | • Not finalized<br>• Expected in 2004 |

**Figure 2: High level details on important, time-sensitive sections of SOX for public companies**

For more detailed information, please refer to the Securities & Exchange Commission Web site (http://sec.gov/spotlight/sarbanes-oxley.htm), the Sarbanes-Oxley Web site (http://www.sarbanes-oxley.com) or contact your auditing firm.

## Assessing the path to Section 404 compliance

The reality of the Sarbanes-Oxley Act is that each public company will need to develop an individualized approach to reporting and compliance. For Section 404, it will begin with a self-assessment of the internal controls the organization has around its financial reporting process. This self-assessment will typically involve internal stakeholders as well as an external audit firm who will work through a standardized framework (such as The Committee of Sponsoring Organizations of the Treadway Commission, COSO) to identify the gaps in compliance, as well as any associated risks. This framework allows audit firms to map internal control objectives to process frameworks, like the one described in the whitepaper published by the Business Software Alliance on Information Security Governance, to address the relevant gaps for compliance. This whitepaper is available through the Entrust Web site at: http://www.entrust.com/governance/index.htm.

> *Section 404 is the largest driver of Sarbanes-Oxley compliance projects and the most significant section for IS organizations. It requires a statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company, attested to by the company's auditor.*
>
> *R. Mogull, D. Logan, L. Leskela 'How CIOs Should Prepare for Sarbanes-Oxley' Gartner, September 2003*

Once the assessment has been completed, organizations must then establish the process by which they will achieve compliance within the relevant timeframe (as described in Figure 2 ). Working with audit firms, organizations will be looking to not only remediate the gaps that have been identified within the legislated timeframe, but also do so in a cost-effective manner. In today's economically challenging times, compliance will be a balance between both time and cost, keeping in mind that this is not a one-time event and that there may be more far-reaching costs than simply implementing internal controls. Complying with the SOX legislation will be an ongoing and continual process that will typically be part of a broader corporate governance effort, forcing organizations to think strategically about how they will address the gaps in internal controls that are present today in both a cost-effective and timely manner.

## How Entrust solutions can help with Section 404 compliance

Entrust security solutions can be used to help close a number of common gaps identified on the path to Sarbanes-Oxley Section 404 compliance. The following sections briefly outline how Entrust security solutions, as a part of your overall corporate strategy, can help in remediation efforts around SOX and Section 404.

***What is COSO?***
*COSO is an integrated framework that can be used to evaluate internal controls*

- *Provides a broad, industry-accepted framework for developing internal controls*
- *Security meets the criteria of a Control Activity under COSO that has "policies, practices (e.g., ISO 17799) and procedures which ensure that management's directives are carried out "*

*More on COSO: http://www.coso.org/*

### Secure Identity Management

Organizations are receiving 24/7 demand from global users, within and external to the enterprise. Companies that are focused on remaining productive and competitive understand that customers, partners, and employees all need deeper access to the organization, giving them what they need, at the right time. Doing this effectively and in real-time means managing a multitude of user identities and interacting with a variety of systems in an environment of constant change — all while keeping quality of service high and the enterprise secure.

#### Identity Provisioning

Managing identities from inside and outside of the enterprise poses two key challenges that are directly relevant to Sarbanes-Oxley Section 404 compliance:

- ensuring accountability of transactions through audit and internal controls;
- cost-effectively managing the complete lifecycle for identities, inside and outside of the enterprise, across multiple applications and environments.

***Real-world scenario:*** *When a new employee joins a company, an account is created for them in the company's HR system (e.g., PeopleSoft). Entrust can automatically detect these changes in the HR system, assess policies to determine the user's access privileges and automate the required approvals for the user's accounts. Approvers are notified via e-mail requesting approval of the new accounts. Once approvals are received, all new accounts are automatically provisioned. This process takes place in a matter of hours — rather than weeks.*

*Consider a normal large enterprise situation:*

- *50,000 employees*
- *10,000 contractors*
- *a relatively stable turnover rate of 10% per year*

*This quickly translates into a huge identity management burden of thousands of provisioning changes per week. Without identity management, effective controls around this process can add significant cost and complexity.*

The Entrust Secure Identity Management Solution is a comprehensive, highly scalable solution that helps to address key challenges faced by commercial organizations working to comply with Section 404 of the Sarbanes-Oxley Act. In addition to helping organizations address internal control gaps for SOX compliance, the solution can quickly reduce the costs associated with managing identities across heterogeneous, complex environments. Through best-of-breed capabilities for securely deploying and managing identities, the solution maximizes the overall return on investment for organizations, providing rapid deployment, easy and secure administration, and scalability to address the largest user populations.

The Entrust Secure Identity Management Solution allows organizations to quickly and securely view, change and audit all user identities and access privileges across all users and organizations. Instead of arduous & expensive manual processes that can often take days if not weeks, companies can quickly and easily determine who has access to what information — and, within minutes, alter or end that user's access if necessary. The ability to closely track and manage user access also plays an important role in SOX compliance, as organizations will need to be able to report on who has access to what information and resources in order to comply. The Entrust Secure Identity Management Solution delivers on this requirement, providing the ability to easily audit all transactions undertaken around managed identities, as well as quickly produce customizable reports on who has access to what resources.

An effective identity management solution can also automate many of the routine yet complex IT processes associated with user administration and provisioning, reducing the time and personnel required to perform these functions. The Entrust Secure Identity Management Solution delivers automated provisioning across the heterogeneous enterprise through a unique, highly deployable architecture, allowing organizations to more quickly deploy the solution to address gaps identified through internal assessments. This solution also includes robust and flexible workflow capabilities, allowing mandatory corporate approval processes to be enforced and audited.

## Policy-based Access Control

As a part of an organization's secure identity management strategy, a Web portal can act as a window for employees, customers, and partners to access corporate applications and information. Those applications and information have varying degrees of sensitivity and importance, and need to be appropriately protected so that only authorized individuals can access them. Given that there are many different applications and points of information storage in any corporation's technology environment, it is also important to be able to centrally manage policy-based access to those applications instead of leaving this decision to individual application developers or managers. At the same time, given the volume and sensitivity of the information available, it is important to prevent unauthorized access without compromising an intuitive and personalized user experience.

The Entrust Secure Identity Management Solution delivers cost-effective policy-based access control for user access to multiple Web-based applications, providing users with single sign-on (SSO) to the applications and content they are authorized to see. It easily extends to include Web services applications via standards such as SAML, enabling organizations to confidently deploy a solution that can address gaps in internal controls today, as well as into the future. The Entrust solution also delivers the ability to centrally manage access to applications and information via policy, providing a single point of policy enforcement and audit of access for all users.

***Real-world scenario: Access Control***

*A public organization's financial results, stored in a database and accessed via a Web interface to a legacy financial system, are very sensitive and often require that access to them be limited not only by who a user is, but also by time (a general employee should not see financial results before they are made public). The Entrust Secure Identity Management Solution allows organizations to enforce policies such as: the financial data be made available to key members of the finance team, only from computers on the internal network and identified using a smart card, until the time of the earnings release. After the earnings release, access to the public information is then allowed by other employees in the organization.*

The solution enriches the traditional roles-based access control (RBAC) model with the ability to apply rules (in accordance with corporate policy) to augment internal controls for Section 404 compliance. This includes the ability to set very granular policies on information access, such as time-specific restrictions or access control based on the location of the originator, amongst other settings.

Importantly, the Web access control component of the Entrust Secure Identity Management Solution is cost-effective, using an **unlimited user**, per-processor pricing model that enables organizations to only pay for the value that they are deploying through their portal.

## Strong Authentication

As a part of managing internal controls within an organization, it is critical that individuals be appropriately authenticated before sensitive data is revealed or sensitive actions can be initiated. Authentication requirements will vary, both in strength and application, meaning that an organization will likely have to support multiple types of authentication across different applications, whether client-server, Web, or Web-services based. The Entrust Secure Identity Management Solution delivers strong authentication capabilities across all three environments. It delivers Web-based authentication using a broad range of identity types, including: usernames and passwords, SAML, Microsoft Passport, and digital certificates stored on a user's computer or on a hardware smart card, token, or biometric device. The solution has the ability to support multiple levels of authentication for a given application or information source, allowing organizations to control to a very granular level how a specific user is given access to sensitive data.

***Real World Scenario: Authentication***
*Continuing from the last example, it is important that users accessing a public organization's financial results are appropriately authenticated before allowing access to the data, regardless of how it is being accessed or from where. If it is the CFO of the organization, he or she must provide an appropriate level of authentication (for example, a smart card with a strong PIN) to access financial data. As a matter of convenience, the CFO may wish to access that data from a desktop application or via the Web. The Entrust Secure Identity Management Solution supports a broad range of authentication methods, including smart cards, for protecting access via the Web. From the CFO's desktop, the solution can enforce a range of authentication methods, including smart cards, to access and act on the financial data.*

In addition, the Entrust Secure Identity Management Solution delivers strong authentication in a client-server environment, helping to ensure that only strongly authenticated users are able to access sensitive information contained in encrypted files, folders and e-mail messages. By controlling access to confidential information that could have an impact on financial reporting activities, organizations can more confidently assert that they have effective internal controls in place.

More information on the Entrust Secure Identity Management Solution can be found online at http://www.entrust.com/identity_management/.

## Data Protection & Integrity

Internal controls around both data access and data integrity can be enforced through the use of encryption and digital signatures respectively. Data contained in files, folders, or email messages can be encrypted to prevent unauthorized access due to security breaches or weak access controls. That same data can be digitally signed to provide both transaction accountability and data integrity, supplying organizations not only with information on who signed the data, but also verification that it did not change from the time it was signed, regardless of whether it traveled across the Internet or was stored locally. Both data encryption and digital signatures may be effective methods of addressing gaps in internal controls for an organization.

Entrust offers several different solutions that can help organizations control access to data through data encryption and provide data integrity through digital signatures.

### Secure Data

The Entrust Secure Data Solution consists of a comprehensive, highly scalable suite of data security products and services that help organizations mitigate the risk of data loss, corruption and disclosure so they can confidently capitalize on new technologies that enable greater stakeholder collaboration and, ultimately, business growth. The solution also helps organizations abide by new legislative regulations that mandate stronger data security controls, without unduly burdening the people and processes that make use of this critical data. It includes the following key capabilities that can help with Section 404 compliance:

- Encryption of files and folders on employee workstations and theft-vulnerable laptop computers. Only properly-authenticated, authorized individuals can decrypt and access sensitive information.
- Digital signatures on data for integrity, including working with industry leaders, such as Adobe, to deliver secure electronic forms for both desktop and Web environments.

- End-to-end encryption and digital signing of sensitive data during Web transactions.
- Developer toolkits to enable encryption and digital signature capabilities in custom applications.

More information on the Entrust Secure Data Solution can be found online at http://www.entrust.com/data/index.htm.

### Secure Messaging

By transparently adding "end-to-end" security to e-mail applications like Microsoft® Outlook® and Lotus Notes®, the Entrust Secure Messaging Solution makes it possible to mitigate risk and help comply with Section 404. It enables e-mail messages to be encrypted and digitally signed both in transit and while at rest on e-mail servers or in end-user inboxes and outboxes. This ability to secure emails can help organizations better control access to sensitive information that often times is transmitted via email.

More information on the Entrust Secure Messaging Solution can be found online at http://www.entrust.com/messaging/index.htm.

## Sarbanes-Oxley and You: The Need to Act Now

In these difficult economic times, organizations are feeling increased pressure to lower the costs of doing business. At the same time, legislation is playing an increasing role in governing how an organization conducts business, with the Sarbanes-Oxley Act of 2002 (SOX) being top-of-mind for most public organizations. As companies leverage the Internet and enterprise networks to streamline business processes and remain competitive, they are experiencing an increased need to find new ways to service employees, partners and customers who are demanding real-time, personalized access to information. This may involve deeply integrating with partner supply chains and their associated management systems, or allowing customers to access confidential account information online. At the same time, SOX compliance demands that an organization's internal controls be held to a specific level of effectiveness in order to ensure that financial reporting requirements are met.

Entrust has a comprehensive portfolio of security solutions that are unmatched in the industry for overall cost-effectiveness, security, and scalability, making it the preferred choice for organizations that need to address internal control gaps. Deployed in concert or individually, Entrust delivers integrated solutions that include the following key capabilities that can help with internal controls and Sarbanes-Oxley Section 404 compliance:

- Secure identity management, including strong authentication, policy-based access controls, and identity provisioning
- Data protection & integrity, including encryption and digital signatures on electronic forms and email messages

The longer an organization waits to address the requirements of Sarbanes-Oxley, the greater the risk of audit failure. With real deadlines looming, some as close as November, 2004[2], companies working with auditors for compliance with Sarbanes-Oxley should consider Entrust security solutions to provide highly effective ways to add accountability, privacy, and audit, enhancing internal controls and improving information security governance.

—-

*For more information on how Entrust security solutions can help with your information security governance initiatives, please visit http://www.entrust.com/governance/.*

[2] *Refer to Figure 2 in this paper for more high-level details on timing for Section 404 compliance, or contact your audit firm*

# About Entrust

Entrust, Inc. [Nasdaq: ENTU] is a world-leading provider of Identity and Access Management solutions. Entrust software enables enterprises and governments to extend their business reach to customers, partners and employees. Entrust's solutions for secure identity management, secure messaging and secure data increase productivity and improve extended relationships by transforming the way transactions are done online. Over 1,250 organizations in more than 50 countries use Entrust's proven software and services to turn business and security challenges into secure business opportunities. Visit: http://www.entrust.com .