WHITE PAPER

SOX Security Compliance for Salesforce

The Security Audit Solution

Table of Contents

Introduction

The Sarbanes-Oxley (SOX) Act of 2002 represents a significant change to federal securities law, and was passed due to accounting scandals at Enron, WorldCom, Global Crossing, Tyco and Arthur Andersen, that resulted in billions of dollars in corporate and investor losses. These huge losses negatively impacted both financial markets and general investor trust.

SOX is about corporate governance and financial disclosure. It requires all financial reports to include an Internal Controls Report to show that a company's financial data is accurate and adequate controls are in place to safeguard financial data. Effective in 2006, all publicly-traded companies are required to implement and report internal accounting controls to the SEC for compliance. [i]

Sarbanes Oxley Auditing Requirements

SOX auditing requires that internal controls and procedures can be audited using a control framework like COBIT (a framework for developing, implementing, monitoring and improving information technology (IT) governance and management practices). SOX compliance dictates that log collection and monitoring systems must provide an audit trail of all access and activity to sensitive business information. Specifically, SOX sections 302, 404 and 409 (details in reference below) require the following parameters and conditions must be monitored, logged and audited, and require a SOX auditor:

- ✓ Internal controls
- ✓ Network activity
- ✓ Database activity
- ✓ Login activity (success and failures)
- ✓ Account activity
- ✓ User activity
- ✓ Information Access

Section 404 is the most complicated, most contested, and most expensive to implement of all the Sarbanes Oxley Act sections for compliance. It specifies that all annual financial reports must include an Internal Control Report stating that management is responsible for an "adequate" internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these controls must also be reported. In addition, registered external auditors must attest to the accuracy of the company management assertion that internal accounting controls are in place, operational and effective.[ii]

What does Sarbanes-Oxley compliance require?

All applicable companies must establish a financial accounting framework that can generate financial reports that are readily verifiable with traceable source data. This source data must remain intact and cannot undergo undocumented revisions. In addition, any revisions to financial or accounting software must be fully documented as to what was changed, why, by whom and when. [iii]

This is where corporations using Salesforce typically run into trouble, as there is no virus scanning built into Salesforce. Malicious programs can easily compromise the security of end users in Salesforce and on desktop and laptop computers. This is especially true with regard to attachments, and the use of Salesforce communities (public and internal) since there is no inherent virus scanning mechanism built into Salesforce. Without the connection of a third-party virus scanner to Salesforce environments, the data is not secure, nor is the network.

Currently, there are two third-party software's available which provide virus scanning for large enterprises using Salesforce – EZProtect® by Adaptus, and Cloud Protection for Salesforce by F-Secure. Both products do the job well, but EZProtect is the only solution designed by certified Salesforce architects who understand the vulnerabilities of Salesforce and supports scanning of multiple Salesforce environments under one license, on both commercial and FedRAMP approved hosting. The company, Adaptus, is also domestically based which is important to both state and federal government agencies and employs active development on the product to expand to other cloud-based tools such as box.com and others in 2018.

What is the Sarbanes-Oxley Act comprised of?

The Sarbanes-Oxley Act itself is organized into eleven sections, but sections 302, 404, 401, 409, 802 and 906 are the most important in terms of compliance. Section 404 seems to cause the most difficulties for compliance. More specifically, Sarbanes-Oxley established new accountability standards for corporate boards and auditors, established a Public Company Accounting Oversight Board (PCAOB) under the Security and Exchange Commission (SEC), and specified civil and criminal penalties for noncompliance.[iv]

What are the penalties for noncompliance with Sarbanes-Oxley?

Besides lawsuits and negative publicity, a corporate officer who does not comply or submits an inaccurate certification is subject to a fine up to $1 million and ten years in prison, even if done mistakenly. If a wrong certification was submitted purposely, the fine can be up to $5 million and twenty years in prison.[v]

Relevant Sections to Security Compliance

Section 302: Corporate Responsibility for Financial Reports

The essence of Section 302 of the Sarbanes-Oxley Act states that the CEO and CFO are directly responsible for the accuracy, documentation and submission of all financial reports as well as the internal control structure to the SEC. Here is the direct excerpt from the Sarbanes-Oxley Act of 2002 report:

a. Regulations Required. The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934, that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—

1. the signing officer has reviewed the report;
2. based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;
3. based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;
4. the signing officers--
   A. are responsible for establishing and maintaining internal controls;
   B. have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;
   C. have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and
   D. have presented in the report their conclusions about the effectiveness of their internal 5 controls based on their evaluation as of that date;
5. the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function) —
   A. 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
   B. any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and
6. the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

b. Foreign Re-incorporations Have No Effect. Nothing in this section 302 shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302, by an issuer having reincorporated or having engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States.[vi]

Section 404: Management Assessment of Internal Controls

Section 404 is the most complicated, most contested, and most expensive to implement of all the Sarbanes Oxley Act sections for compliance.

All annual financial reports must include an Internal Control Report stating that management is responsible for an "adequate" internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these controls must also be reported. In addition, registered external auditors must attest to the accuracy of the company management assertion that internal accounting controls are in place, operational and effective.

A direct excerpt from the Sarbanes-Oxley Act of 2002 report for section 404:

(a) Rules Required. The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 to 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; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) Internal Control Evaluation and Reporting. With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.[vii]

Section 409: Real Time Issuer Disclosures

The essence of Section 302 of the Sarbanes-Oxley Act states that companies are required to disclose on an almost real-time basis information concerning material changes in its financial condition or operations. Here is a direct excerpt from the Sarbanes-Oxley Act of 2002 report for section 409: Section 13 of the Securities Exchange Act of 1934, as amended by this Act, is amended by adding at the end the following:

(l) Real Time Issuer Disclosures. Each issuer reporting under section 13(a) or 15(d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest.[viii]

Conclusion

All publicly-traded companies in the United States, including all wholly-owned subsidiaries, all publicly-traded non-US companies doing in business in the US, and any private companies that are preparing for their initial public offering (IPO) need to comply with certain provisions of Sarbanes-Oxley. Corporations using Salesforce without the addition of a third-party virus scanner such as EZProtect will not meet SOX compliance standards, and will therefore fail upcoming security audits. Failure to meet SOX compliance will also jeopardize the corporations' SEC filing status, as well as threaten legal action against the CEO and other senior executives.

About Adaptus

Adaptus, LLC is an application development and Salesforce architecture consulting firm based in Austin, TX. Founded in 2012 on the premises of collaborating with customers to solve real problems, Adaptus products are used by large, Fortune-500 companies with thousands of users. Adaptus provides reliable, high-quality and cost-effective information technology solutions and custom cloud-based computing applications designed to integrate with Salesforce.com. Our applications and architectural consulting services help businesses optimize their operations by working smarter, while increasing productivity and profitability. Led by certified Salesforce architects, Adaptus specializes in customer-driven product solutions to provide highly relevant, efficient and cost-effective solutions for large-enterprise users around the globe. For more information about our products, or to request consulting services, please visit www.adaptus.com.

End Notes

[i] http://www.complianceguidelines.com/sox-compliance.htm
[ii] http://www.complianceguidelines.com/sox-compliance.htm
[iii] http://www.complianceguidelines.com/sox-compliance.htm
[iv] http://www.complianceguidelines.com/sox-compliance.htm
[v] http://www.complianceguidelines.com/sox-compliance.htm
[vi] http://www.complianceguidelines.com/sox-compliance.htm
[vii] http://www.complianceguidelines.com/sox-compliance.htm
[viii] http://www.complianceguidelines.com/sox-compliance.htm