Addressing SOX compliance with XaitPorter

Version 1.0 Sept. 2014

Xait

Table of Contents

1 Addressing Compliance

XaitPorter ensures confidentiality and integrity while enabling companies to stay compliant with different regulations and corporate policies throughout the corporate document creation process and information life cycle. Compliance is achieved through XaitPorter's innovative database driven document creation engine, review process, versioning, and logging framework. Created from a security management perspective, XaitPorter enforces compliance requirements, and mitigates legal, financial and reputation risks associated with document creation, distribution and enterprise content management (ECM). At the same time, XaitPorter securely facilitates real time online collaboration, global access, optimal performance and optimized quality, which are all critical to business success.

According to Checkpoint's security report of 2013, file sharing is considered a high risk application in industrial, government, telecommunications, finance and consulting. The root of the problem to enable efficient and secure document collaboration is the fact that "collaborative" systems today are based on files. This poses a risk as the file format was never designed to address today's compliance requirements or security standards.

2 SOX Compliance

The **Sarbanes-Oxley Act of 2002** or **SOX**, is a United States federal law that sets new or enhanced standards for all U.S. public company boards, management and public accounting firms and requires top management to individually certify the accuracy of financial information. In addition, penalties for fraudulent financial activity are much more severe. Also, SOX increased the independence of the outside auditors who review the accuracy of corporate financial statements, and increased the oversight role of boards of directors. *(From Wikipedia)*

Sarbanes-Oxley Section 302: Disclosure controls
Section 302 of the Act mandates a set of internal procedures designed to ensure accurate financial disclosure. The signing officers must certify that they are "responsible for establishing and maintaining internal controls" and "have designed such internal controls to ensure that material information relating to the company 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." 15 U.S.C. § 7241(a)(4). The officers must "have evaluated the effectiveness of the company's internal controls as of a date within 90 days prior to the report" and "have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date."

Sarbanes-Oxley Section 401: Disclosures in periodic reports (Off-balance sheet items)
The bankruptcy of Enron drew attention to off-balance sheet instruments that were used fraudulently. During 2010, the court examiner's review of the Lehman Brothers bankruptcy also brought these instruments back into focus, as Lehman had used an instrument called "Repo 105" to allegedly move assets and debt off-balance sheet to make its financial position look more favorable to investors. Sarbanes-Oxley required the disclosure of all material off-balance sheet items. It also required an SEC study and report to better understand the extent of usage of such instruments and whether accounting principles adequately addressed these instruments; the SEC report was issued June 15, 2005. Interim guidance was issued in May 2006, which was later finalized. Critics argued the SEC did not take adequate steps to regulate and monitor this activity.

Sarbanes-Oxley Section 404: Assessment of internal control
The most contentious aspect of SOX is Section 404, which requires management and the external auditor to report on the adequacy of the company's internal control on financial reporting (ICFR). This is the most costly aspect of the legislation for companies to implement, as documenting and testing important financial manual and automated controls requires enormous effort.

Under Section 404 of the Act, management is required to produce an "internal control report" as part of each annual Exchange Act report. The report must affirm "the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting." The report must also "contain an assessment, as of the end of the most recent fiscal year of the Company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." To do this, managers are generally adopting an internal control framework, such as COSO or DAMA.

Both management and the external auditor are responsible for performing their assessment in the context of a top-down risk assessment, which requires management to base both the scope of its assessment and evidence gathered on risk. This gives management wider discretion in its assessment approach and they are required to:

- Assess both the design and operating effectiveness of selected internal controls related to significant accounts and relevant assertions, in the context of material misstatement risks
- Understand the flow of transactions, including IT aspects, in sufficient detail to identify points at which a misstatement could arise

- Evaluate company-level (entity-level) controls, which correspond to the components of the COSO or DAMA framework
- Perform a fraud risk assessment
- Evaluate controls designed to prevent or detect fraud, including management override of controls
- Evaluate controls over the period-end financial reporting process
- Scale the assessment based on the size and complexity of the company
- Rely on management's work based on factors such as competency, objectivity, and risk
- Conclude on the adequacy of internal control over financial reporting

Sarbanes–Oxley 404 and smaller public companies
The cost of complying with SOX 404 impacts smaller companies disproportionately, as there is a significant fixed cost involved in completing the assessment. For example, during 2004 U.S. companies with revenues exceeding $5 billion spent 0.06% of revenue on SOX compliance, while companies with less than $100 million in revenue spent 2.55%.

Sarbanes–Oxley Section 802: Criminal penalties for influencing US Agency investigation/ proper administration
Section 802(a) of the SOX, 18 U.S.C. § 1519 states:

```
Whoever knowingly alters, destroys, mutilates, conceals, covers up,
falsifies, or makes a false entry in any record, document, or tangible
object with the intent to impede, obstruct, or influence the investigation
or proper administration of any matter within the jurisdiction of any
department or agency of the United States or any case filed under title 11,
or in relation to or contemplation of any such matter or case, shall be
fined under this title, imprisoned not more than 20 years, or both.
```

Sarbanes–Oxley Section 906: Criminal Penalties for CEO/CFO financial statement certification
§ 1350. Section 906 states: Failure of corporate officers to certify financial reports

(a) Certification of Periodic Financial Reports.– Each periodic report containing financial statements filed by an issuer with the Securities Exchange Commission pursuant to section 13 (a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m (a) or 78o (d)) shall be accompanied by Section 802(a) of the SOX a written statement by the chief executive officer and chief financial officer (or equivalent thereof) of the issuer.

(b) Content.– The statement required under subsection (a) shall certify that the periodic report containing the financial statements fully complies with the requirements of section 13 (a) or 15(d) of the Securities Exchange Act of [1] 1934 (15 U.S.C. 78m or 78o (d)) and that information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer.

(c) Criminal Penalties.– Whoever– (1) certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than $1,000,000 or imprisoned not more than 10 years, or both; or

(2) willfully certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than $5,000,000, or imprisoned not more than 20 years, or both.

SOX requires the CEO and CFO certify that controls have been in effect for the entire quarter.

In order to do so, you may want to consider some or all of the practices below:

- Develop a process to audit changes to content, users, responsibilities.
- Enable audit tracking of all processes relating to Segregation Of Duties (SoD) so that an audit trail can be maintained.
- Develop a process to report the audit trail or alerts key users to SoD violations.
- Develop audit plan for Internal Audit to test and monitor that these controls are in place.
- Test controls to ascertain that they have been in effect all quarter.
- Provide proper audit trail for changes in your documentation.

Challenge

- How can you be sure your key controls and involvement have been working effectively throughout the quarter?
- Is that documentation being maintained as you add new modules or roll out your system to additional business units?
- Are changes to your setups properly documented?
- Are your testing plans and results well documented?
- Is access to key figures limited to only those that have proper authorization to view or make changes?

How can XaitPorter help you stay compliant?

XaitPorter will help you implement security management as a strategic business initiative with your document creation process for financial reports while mitigating the associated legal and financial risks.

- Ease involvement of CEO and CFO
- Ensure Confidentiality
- Ensure Effectivity
- Ensure Integrity (Fine grained access on object level, access-integrated workflow, Audit log, Metadata) (Section 802)
- Segregation of Duties (SoD) (access-integrated workflow)
- Disclosure Control (Fine grained access on object level, Audit log) (Section 302)

3 Key Benefits

Minimize Financial, Legal and Reputation Risk
XaitPorter enables your business to stay compliant and thus reduces both financial, legal and reputation risks associated with non-compliance. XaitPorter provides access control, access-integrated workflow, version control, revision control, audit trail and action logs for any content in your document to protect against litigation.

Enhance Security
XaitPorter provides fine grained access within the document to protect the data from unauthorized access, enabling restrictions to sensitive information such as tables, sections and attachments.

Increase Productivity and Quality
By using XaitPorter you focus on the content only - to increase both productivity and quality. The system takes care of security and compliance, and enables users to quickly find and reuse data.

Ensure Integrity
XaitPorter eliminates outdated or irrelevant information, and ensures your mission critical data is up to date and preserves integrity within and across different documents.

Reduce Costs
XaitPorter enables corporations to lower administrative overhead associated with compliance.

4 Contact Information

Xait Headquarter
Luramyrveien 42
4313 Sandnes
Norway
Phone: +47 51 95 02 00
E-mail: post@xait.com, support@xait.com

Xait US – Austin
Sales and support office
11940 Jollyville Rd, Suite 105N
Austin, Texas 78759
Phone: +1 512 266 1676
Toll free: +1 855 886 1666
E-mail: support.usa@xait.com

Xait UK
Sales office
81 Rivington Street, London EC2A 3AY
Phone: +44 (0)203 170 5673
E-mail: post@xait.co.uk

www.xait.com