BUSINESS OBJECTS AND **SOX:** **9 STEPS** TO COMPLIANCE

Executive Summary

The Sarbanes-Oxley Act (SOX) demands that companies establish internal controls to protect financial data. To comply with SOX, companies must be able to locate and safeguard financial data. Business intelligence applications expose data and therefore must be used in a manner that supports the goals and upholds the requirements of SOX. GB&SMITH, creator of 360Suite solutions to enhance Business Objects, developed a 9-step process to help organizations think through the challenges of SOX compliance and take appropriate action.

What is SOX?

SOX is shorthand for the Sarbanes-Oxley Act, which is a U.S. law that outlines auditing and financial regulations for publicly-traded companies. (Note: Some provisions apply to *all* enterprises, including private companies and not-for-profit organizations.) The Act was named for its sponsors -- U.S. Sen. Paul Sarbanes (D-MD) and U.S. Rep. Michael Oxley (R-OH). It was signed into law on January 30, 2002 by President George W. Bush.

SOX was enacted in response to corporate scandals in the late 1990s and early 2000s (e.g., Enron, WorldCom, Tyco, etc.). It closed loopholes in accounting practices in an effort to improve the reliability of financial reporting and restore investor confidence. The goal of SOX is to protect shareholders, employees, and the public from accounting errors and fraudulent financial practices.

SOX requires companies to establish internal controls to prevent tampering with financial data. It adds a section to the United States Code stating that “any person who attempts or conspires to commit any offense . . . shall be subject to the same penalties as those prescribed for the offense.” It also establishes harsh criminal penalties for anyone who is found guilty of *certifying* misleading or fraudulent reports. Finally, it requires external auditors to express an opinion on a company’s internal control structure.

Many other countries have regulations similar to SOX, including:

- Australia (Corporate Law Economic Reform Program Act aka CLERP 9)
- Canada (Keeping the Promise for a Strong Economy Act aka Bill 198 or Canadian Sarbanes-Oxley Act or C-SOX)
- France (Financial Instruments and Exchange Act aka Loi de sécurité financière or LSF)
- Germany (Deutsche Corporate Governance Kodex and Mindestanforderungen an das Risikomanagement)
- India (Clause 49 of the Listing Agreement to the Indian stock exchange)
- Italy (Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari)
- Japan (Financial Instruments and Exchange Act aka J-SOX)
- Netherlands (code-Tabaksblat, code-Frijns, and code-Van Manen)
- South Africa (King Report on Corporate Governance)
- UK (Companies (Audit, Investigations and Community Enterprise) Act 2004)

How does SOX impact BI?

Forrester defines Business intelligence (BI) as "a set of methodologies, processes, architectures, and technologies that transform raw data into meaningful and useful information used to enable more effective strategic, tactical, and operational insights and decision-making" (Evelson, 2008). Business intelligence applications (e.g, Business Objects, Tableau, Power BI, etc.) support this process by retrieving, analyzing, transforming, and reporting on data. It is safe to assume that all information technology, including CRM platforms, ERP systems, and BI applications contain financial data obtained from databases. SOX comes into play when BI applications are used to prepare, share, and publish financial data.

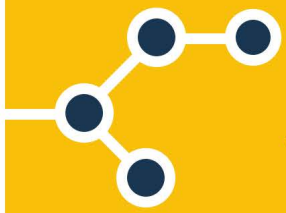
Business Objects and SOX: 9 Steps to Compliance

1
Back Up

2
Manage Security Rights

3
Find and Tag Sox information

4
Monitor and Document Sox Info



5
Implement Version Control

6
Find and Fix Discrepancies

7
Check for Deleted Content

8
Control Ungoverned Content

9
Archive Sox info

360 Suite
Business Objects Solutions
www.360suite.io

SAP® Certified
Integration with SAP BusinessObjects

SAP Partner

STEP 1: BACK UP

One way for companies to ensure the reliability of financial data is to back them up regularly. A typical Business Objects recovery strategy involves backing up the entire Business Objects server and CMS database. This makes it possible to restore the full system, but not to perform selective rollbacks or restore individual deleted objects. Backing up the entire Business Objects server also doesn't address the problem of corrupted environments (i.e., if an environment is corrupted, so too is the mirrored backup) and won't restore personal folders and security settings if users are accidentally deleted.

In contrast, 360Suite incremental backups allow organizations to perform full backups as well as restore previous versions of any object in any folder at any time. Incremental backups are particularly important in the context of financial data for the following reasons:

1. Every time IT modifies something, it opens the door to the possibility of technical issues, human error, or fraudulent behavior.
2. Information that was not originally identified as relevant to SOX may later become important due to tagging or segregation of duties (SOD).
3. Incremental backups allow for business continuity in the event of a non-technical crisis, including a natural or man-made disaster.

SOX outlines rules for maintaining (aka archiving) information. Whereas archiving ensures that prior year information is accessible, backups ensure that current year information is accurate and complete. Both are important components of a robust internal control policy.

STEP 2: MANAGE SECURITY RIGHTS

To safeguard data impacted by SOX, companies must control access to them. 360Suite makes it possible to identify, monitor, and control who has access to what information by:

- Taking snapshots to track, document, and compare security over time;
- Providing user-centric and resource-centric views of security;
- Providing a patented comprehensive view of inherited rights, double-inherited rights, and broken inheritances, to protect against a cascade effect when security is modified;
- Simplifying the process of auditing, recertifying, and modifying security rights;
- Automating the process of administering and managing security to reduce human error; and
- Making it possible to enforce the segregation of duties (SOD) by finding, flagging, viewing, and tracking potential conflicts of interest.

STEP 3: FIND AND TAG SOX INFORMATION

Companies must identify data impacted by SOX so they can take the necessary steps to safeguard them. 360Suite facilitates this process by making is possible to export Business Objects document properties and Universe object properties (e.g., name, description, SQL statement, etc.) to Excel spreadsheets that can be shared with data owners. Data owners can then tag SOX-related information (i.e., #SENSITIVE DATA_SOX) and document it in a data catalogue, taking into account that some information is impacted by SOX only when used in combination. Tagging can also include information about data sensitivity, life cycle, SOD, etc. Once tagging is complete, 360Suite can import tags back into Business Objects to update documents and Universe object descriptions.

STEP 4: ANALYZE AND DOCUMENT SOX INFO

Tags make it easy to monitor actions on SOX data and spot unusual behavior. Companies should analyze and document the following in order to answer the questions: What? Why? When? By whom?

- Security changes
- Type of action/inaction on SOX data
- Number of actions on SOX data
- Number and format of exports and schedules of SOX data
- Data report sources
- Creation of new content based on SOX data

Business Objects has powerful auditing capabilities, but can be subject to performance degradation over time. For example, Business Objects systems with a high rate of utilization can become bloated if they track every possible auditable event, write events to text files before they are loaded into the audit database, and retain audit data for long periods of time. This is why many organizations opt to purge Business Objects data after one year.

Another problem is that Business Objects can audit actions, but not *inactions*. Sometimes what *wasn't* done to SOX data is just as significant as what *was* done to them. Also, when organizations migrate Business Objects (e.g., from 4.1 to 4.2), the schema changes so they start a new Audit database. Since most companies migrate Business Objects every three or four years, their audit history is rarely longer than that.

In contrast, 360Suite captures regular snapshots of metadata extracted from the CMS database, the Audit database, and the Input and Output Filestores. This makes is possible to display the activity of specific users on specific objects. And because the information is stored in an offline data mart specifically designed for BI-on-BI reporting, it doesn't put a load on Business Objects during peak times.

STEP 5: IMPLEMENT VERSION CONTROL

Version control refers to a system that records changes to a file or set of files over time, and makes it possible to recall specific versions. In the context of SOX, version control ensures the transparency and traceability of financial data and is an important part of an adequate internal control structure.

360Suite makes it possible to understand who made changes -- when, why, and how -- and who approved the changes. 360Suite features that contribute to version control include:

- A check-out/check-in process for documents, Universes, and connections;
- "Secured check-out," which ensures that only the user who checked out an object can edit it (except the Administrator), until the object is checked back in;
- The ability to require users to include a comment explaining changes at check-in;
- A workflow approval process that requires changes to be approved before publication;
- The ability to compare document versions and record changes over time; and
- The ability to compare Universes and record changes over time.

STEP 6: FIND AND FIX DISCREPANCIES

Because the intent of SOX is to improve the accuracy and reliability of corporate disclosures, and because SOX grants issuers the opportunity to cure any defects, companies must devise a strategy to find and fix discrepancies in SOX data. Discrepancies can appear in documents, metadata, variables, and/or security.

One way to identify discrepancies is through regression testing, which is an important quality assurance practice following upgrades, changes, and migrations. Regression testing is often performed only at the database level, but this approach has the potential to overlook regressions in documents published by business intelligence applications. 360Suite can perform regression testing at the document level. It can also search for

regressions in images (e.g., graphs, charts) at the pixel level, which is particularly useful for highly formatted documents. 360Suite can even identify regressions in metadata from the CMS and FileStore. And it can test for variable discrepancies caused by calculation engine changes, determine if the variables are used in other documents, and push bulk fixes.

Another important quality assurance practice is regular user account recertification to reflect changes to staff and job functions. 360Suite facilitates this practice by tracking and documenting security over time, and identifying security discrepancies. This is an extension of Step 2 (Manage Security Rights), because controlling who has access to SOX data is not a one-off activity.

360Suite automates manual processes, like regression testing, that are time consuming and prone to human error. By scheduling regression testing using the latest values and highlighting differences, 360Suite helps companies find and fix discrepancies in SOX data before they cause lasting damage.

STEP 7: CHECK FOR DELETED CONTENT

SOX makes it a crime to knowingly alter, destroy, mutilate, conceal, cover up, or falsify documents. That's why companies should keep track of all "delete" actions.

Sometimes content is intentionally deleted for valid reasons. For example, employees may duplicate documents, customize them, and then delete one or more versions. Other times, content is accidentally deleted as a result of IT issues, human error, or fraudulent behavior.

Business intelligence applications, like Business Objects, treat deletions as auditable events and record them. 360Suite accesses these audit records and combines them with information from the CMS and FileStore to generate a list of all actions (e.g., delete, copy, save to, etc.) linked to specific users. Because 360Suite back ups are incremental (see

Step 1), companies have the ability to restore suspiciously deleted content (e.g., users, inboxes, access control levels, etc.) at the object level. 360Suite also goes beyond the Business Objects recycle bin by making it possible to restore inboxes, including personal folders and security settings, if users are accidentally deleted.

STEP 8: CONTROL UNGOVERNED CONTENT

Despite their popularity, business intelligence applications haven't entirely replaced ungoverned end-user computing (EUC) applications (e.g., Excel). It's not uncommon to see data from business intelligence reporting (e.g., Webi) exported to Excel and then used as the basis for SOX reporting.

Ungoverned content is problematic because:

- Data sources can't be controlled;
- The information is easy to share;
- The information is easy to alter, including for fraudulent purposes;
- The information is hard to track; and
- The information is subject to regressions when converted from the original format.

Ideally, companies should take steps to prevent ungoverned content. At a minimum, they should take steps to control it. 360Suite makes it possible to password-protect .pdf, .xls and .zip instances from Business Objects. This limits unwanted sharing and minimizes security issues, but doesn't necessarily prevent fraudulent behavior. 360Suite can also watermark .pdf and .xls documents. Finally, 360Suite can perform regression testing on Webi report sources before data are exported to Excel to ensure consistency.

STEP 9: ARCHIVE SOX INFO

SOX requires companies to establish internal control structures and procedures that include maintaining records. In addition, SOX requires registered public accounting firms to maintain audit-related information for at least seven years. When archiving information, companies need to consider whether or not a particular format is likely to be retrievable seven or more years into the future.

360Suite supports automatically archiving and pseudo-archiving SOX content based on predetermined values (e.g., fiscal year) in common format standards. For the purposes of this paper, archiving refers to storing information outside of Business Objects, and pseudo-archiving refers to storing information within a Business Objects environment. In both cases, it's important to consider restoration scenarios and security aspects.

There are six ways to archive/pseudo-archive with 360Suite:

1. Take Webi (.wid) .pdf, .xls, .txt, and .csv instances of Business Objects documents and save them to a file system outside of Business Objects. (Note: Archiving a .wid requires access to the Web Intelligence Rich Client in order to open it.)
2. Flag unused content with #TOARCHIVE and automatically promote it to a folder on the current or another BIP environment.
3. Back up all content and delete unused content from the BI Platform, with the option to restore individual items, if required.
4. Pseudo-archive dynamically when triggered by Business Objects events, and burst instances to an external network location for record-keeping.
5. Pseudo-archive via security, so content remains within Business Objects, but is hidden from users via custom access level rights.
6. Pseudo-archive via security, so content remains within Business Objects but is stored in restricted folders. (Note: Only the Administrator can restore content to its original folder.)

If desired as part of internal control procedures, 360Suite can archive information to a "Write Once, Read Many" (WORM) device, from which information can be retrieved, but neither modified nor deleted.

CONCLUSION

Complying with SOX has a lot in common with complying with other regulatory requirements (e.g., GDPR, HIPAA, FISMA, etc.). But there are also important distinctions. For example, GDPR requires organizations to *delete* personal data in many situations, while SOX regulations require organizations to *save* financial data and be able to substantiate all deletions.

- GDPR: Governs the processing and free movement of personal data
- HIPAA: Regulates access to health information
- FISMA: Requires federal agencies to implement an information security program
- SOX: Requires companies to establish internal controls to prevent tampering with financial data

In every case, organizations must understand what information is subject to regulations, be able to find and monitor that information, and safeguard the information by controlling access to it, ensuring accuracy, and creating backups. 360Suite achieves all these goals with unique and powerful solutions that run behind the scenes to help companies comply with SOX and other regulations in the context of business intelligence applications.

REFERENCES

Sarbanes-Oxley Act of 2002. Retrieved from https://www.congress.gov/bill/107th-congress/house-bill/3763/text

Evelson, B. (2008). Topic Overview: Business Intelligence. Retrieved from https://www.forrester.com/report/Topic+Overview+Business+Intelligence/-/E-RES39218

Authors: Kristen Champagne Gray - Bruno Masek

BE SOX COMPLIANT WITH 360SUITE

GET STARTED!

360 Suite

Visit https://360suite.io