Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act

Dimitris Karagiannis*, John Mylopoulos, Margit Schwab***

*Universität Wien
Faculty of Computer Science
Department Knowledge Engineering
Bruenner Strasse 72
A-1210 Vienna
{dk / margit.schwab@dke.univie.ac.at}

** University of Toronto
Department of Computer Science
40 St. George Street
Toronto, Ontario M5S 2E4
{jm@cs.toronto.edu}

Appeard In:
Proceedings of the Requirements Engineering Conference, 2007,
RE '07. 15th IEEE International
October 2007, pp. 315-321

Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act

Dimitris Karagiannis
University of Vienna
Dept. of Knowledge and Business Engineering
dk@dke.univie.ac.at

John Mylopoulos
University of Toronto
Dept. of Computer Science
jm@cs.toronto.edu

Margit Schwab
BOC Information Technologies Consulting Ltd.
Margit.Schwab@boc-ie.com

Abstract

Balance Sheets and Annual Financial Reports play a major role in determining the public worth of any company. In the wake of corporate scandals such as Enron and WorldCom, the US and other countries passed legislation governing reporting processes. The Sarbanes Oxley Act of 2002 (hereafter SOX) requires US national securities exchange and US national security associations not to list any securities of any issuer that is not in compliance with the act. In this paper, we present a business process-based solution to the SOX compliance problem and offer evidence that such a solution is feasible through an industrial case study. The proposed solution aims to support SOX reporting requirements based on core business processes and a continuous improvement of the company's adopted business processes. This means that the solution integrates SOX-related tasks into the "daily work" of a company, rather than achieve compliance on a project basis.

1. Introduction

In an ever-more complex and fluid world, there has been a steady increase in government laws and regulations, industrial standards, and company policies that need to be taken into account during the development of a socio-technical system. These laws, regulations and policies constitute rich sources of requirements, and need to be analysed and accommodated, somehow, during design. The problem of compliance to regulations is even more difficult for an existing organisation who has to restructure and reengineer its operation to achieve compliance. This paper presents a business process-based solution to a particular governance regulation, the Sarbanes-Oxley Act of 2002 (hereafter SOX) and offers evidence through an industrial case study that such a solution is feasible and has advantages.

Balance sheets and annual financial reports play a major role in the evaluation of any company by the public. Analysts determine their ratings for a given company on the basis of such published statements and reports. Companies with strong reported results do well in stock markets and are highly sought-after business partners. SOX introduced new, stricter financial regulations and stronger governance rules in order to ensure that public statements about a company's record are, in fact, accurate.

SOX was passed in the U.S. in the wake of the Enron, WorldCom and other corporate scandals. Most public companies listed on U.S. stock exchange, who issue securities in the U.S., must comply with this law. Other countries' securities regulators, such as the Ontario Securities Commission (Canada) have also adopted similar (but less restrictive) measures. The intent behind SOX has been to increase trust in public reports on a company's record. A "SOX-compliant" company follows particular reporting procedures and has a higher awareness of how its business is conducted.

Not surprisingly, there has been a tremendous effort in the U.S. and around the world to change company practices and make them SOX-compliant. Requirements derived from SOX have an extensive impact on existing reporting procedures, in safeguarding management responsibilities and in setting up new procedures. Consequently, a sound preparation is essential in reengineering an enterprise to make it SOX-compliant.

In considering possible solutions, there are obvious competing types. For instance, one may want to consider technology-based solutions where existing technology is extended or new technologies are introduced to ensure compliance with a new regulation. This is, in fact, the approach adopted with Hippocratic databases [10] for compliance to privacy legislation.

The same is true for security-related regulations where compliance is highly dependent on technology. A different type of solution may be business process-based in the sense that business processes are revised for compliance but no technology is extended/ introduced.

The main objective of this paper it to present evidence that a business process-oriented framework for making a company SOX-complaint is feasible and has several merits. The evidence is provided through an industrial case study where the proposed framework has been applied.

The rest of the paper is structured as follows. Section 2 presents background material on risk and control management requirements as well the concept of continuous improvement processes. Section 3 presents the ADONIS® platform for modelling, analyzing and managing business processes. In section 4 we present the basic elements of an ADONIS® implementation for SOX-compliance. Section 5 evaluates the proposed solution and provides other details of an industrial case study. Section 6 concludes and suggests possible research directions.

2. Background

2.1 The Sarbanes Oxley Act - SOX

The Act consists of eleven Titles and a number of underlying Sections, which altogether regulate the structure of enhanced financial disclosures, liabilities and auditor practices. The sections that affect companies most are sections 302 "Corporate Responsibility for Financial Reports" and 404 "Management Assessment of Internal Controls". The former outlines the responsibilities of the signing officers which are:

- "(A)… establishing and maintaining internal controls;
- (B) to have designed such internal controls to ensure that material information relating to issuer and its consolidated subsidiaries is made known to such officers ….
- (C) to have evaluated the effectiveness of the issuer's internal controls …
- (D) to have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation …."

To comply with the above, a company must first identify necessary internal controls in its service provision processes. Through knowledge of these processes, many of the requirements derived from SOX can be addressed. The steps involved would be:

- Model business processes in sufficient detail to be able to identify "hidden" risks and set-up appropriate internal controls;
- Collect identified controls and the risks they are intended to mitigate into a central catalogue or library;
- Distribute disseminated information to relevant parties.

Regarding (C), the evaluation of the effectiveness of the established controls cannot be accomplished by just analysing existing business processes. In order to ensure that established controls are effective and appropriate, they need to be "tested". This involves:

- Setting-up a test environment with test plans, a test scope, test descriptions, testers, responsible persons within the company for the test environment or only for single tests etc. including the analysis of the test results,
- Depending on the results, it may be necessary to define remediation measures for cases where controls failed,
- After receiving an overview of the entire internal control framework, an assessment of the effectiveness of the internal controls is possible,
- Finally, assessment and evaluation results need to be documented.

Section 404 (second section) of the SOX Act is new and work-intensive. It requires "… each annual report ... 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 of the issuer for financial reporting.
(2) Contain an assessment, …, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting[1]."

According to this, management is required to state that they are aware of the risks, and are satisfied that assigned controls work. This section also implies a testing concept for existing or newly introduced internal controls. The required assessment is intended to ensure that management is aware of business details and therefore liable in case these details violate the act. Generally speaking, Section 404 requires awareness of a company's risk situation at the highest levels.

2.2 Risk and control management

There have been several proposals for approaches and solutions that help an organisation deal with risk management, governance, control and assurance. One such proposal by the Committee of Sponsoring Organisations (COSO) elaborates a framework called Enterprise Risk Management (ERM) that can assist

companies that have to comply with government regulations [2]. In order to achieve an enterprise's mission (be it a profit or non-profit one) the board of directors has to select strategies, derive concrete operations out of these strategies, has to report on the operations and finally has to check whether their actions are compliant to applicable laws and regulations [3]. This structuring of tasks needs also to be coordinated according to enterprise risk management components, as applicable laws may require detailed reports on various aspects of an enterprise's operations.

The ERM is a procedure-oriented model, which describes three dimensions that together build a comprehensive organisational framework for effective management in terms of limitations, internal controls, roles and responsibilities [4]. SOX and COSO framework requirements can clearly only be met if all relevant departments of a company are integrated in the assessment. This means that compliance is a global problem that is only solvable by looking at the operations of a whole organisation.

Additionally, evaluating the effectiveness of a company's internal control structure needs to be documented in any financial reporting. This implies an ongoing process, rather than a static, one-time-only statement. The concept of "continuous improvement" takes into account that fact and the dynamics in a company's business processes, the risk situation and general development influenced by market trends and constraints.

2.3 Continuous improvement

The concept of continuous improvement is an adaptable framework that supports organisations with the aim of achieving compliance with legal, IT-based, and organisational requirements on an on-going basis [4]. The Continuous Improvement Approach serves as a procedural model for the implementation of steps that are necessary to find a path to compliance. The approach is method-independent in its structure, which means that it can be used for a great number of regulations.

The first step of the approach is an analysis of both the specific set of regulations (e.g. COBIT, SOX, or similar) and the current status of the business processes within an enterprise. This analysis step should be completed by a development of a compliance vision, which determines the goal that should be achieved as well as a first draft of the path that has to be undertaken to reach the stated goal. This part is crucial as it forms the fundamentals for later stages and decisions.

After having analysed the current situation, a detailed plan of affected business units has to be elaborated. Together with the relevant parties, the business processes in affected units have to be analysed and potential changes have to be discussed in detail. These changes may be necessary as the identification of risks within the business processes represents an integral step of the whole approach. After evaluating alternatives, a plan for operational measures -- i.e. changes that have to be undertaken to reach compliance – is elaborated in cooperation with affected parties and possibly external experts. Finally, the last step focuses on the realisation of the planned measures that have to be executed for achieving compliance.

3. The ADONIS® platform

The proposed solution is supported by the ADONIS® platform. ADONIS® is the Business Process Management tool of the BOC Group. Its components support information acquisition, modelling, analysis, simulation, evaluation, costing, documentation, and import/export for business process and other organisational models. The ADONIS® platform supports meta-modelling, as well as method engineering. This means that new business modelling tools can be generated to meet new requirements for modelling and analysis [5].

In order to apply this platform to the SOX compliance problem, there had to be two extensions to what was already available. Firstly, the ADONIS® meta-model had to be extended to support the modelling of SOX-specific concepts, such as those of risk and control.

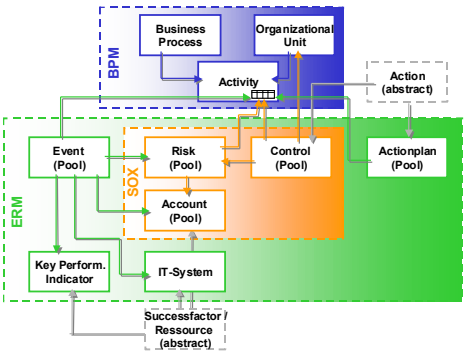

Figure 1. ADONIS® extensions to support ERM

Figure 1 represents through colours different application scenarios of the ADONIS® tool in the context of risk assessment or compliance solutions. The blue part represents the meta-model of the ADONIS® standard modelling language. The orange part encompasses the extensions needed to elaborate

requirements specified in the SOX Act. The green part shows extensions that support the design and realisation of risk management in an enterprise-wide context according to the COSO approach.

The SOX extension introduces meta-classes for Event/Risk, Control and Account.

The ERM Extension comprises the following classes: Event/Risk, IT-System, Key Performance Indicator, Initiative/Remediation Measure, Derived Action, Derived Success Factor. These classes have specific attributes and links through which their instances can be related to instances of other classes.

The second required extension in applying ADONIS® to the SOX compliance problem was managerial. At a very early stage in the discussions on how to address SOX compliance within the company, it became apparent that it would be difficult to identify authoritative models of business processes and business data. SOX documentation is voluminous and complex, as it affects many different divisions within a company. For these reasons, an integrated SOX portal was implemented in order to offer an integrated front end for decentralised data acquisition, planning and administration of the testing procedure, and the creation/generation of different SOX reports.

The SOX portal is populated through the ADONIS® Documentation Component with approved versions of business processes, to be included in official SOX reports; as well, versions of these processes to be tested against. Additional data is entered manually when collecting data for the SOX reports or in case of setting up and performing the testing procedure for the internal controls. Depending on the type of data different menus are offered in the portal.

4. A business process-based approach to SOX

Knowing the requirements of the SOX Act – in brief, the implementation of internal controls and assessment of the management of these controls – we now present a process-based solution that addresses these requirements. The solution was intended to not only ensure SOX compliant at the end of the annual reporting year, but also to create a basis for ongoing SOX compliance. The solution depends heavily on the availability of business process, risk and internal control models, as well as the SOX portal for documents, reports and other data.

The proposed solution consists of five steps supported by the models and portal offered through the ADONIS® platform. A final sixth step shown in the solution concerns a final quality check and approval from the company's auditor who must approve the company's SOX compliance. The six steps are portrayed in Figure 2.

It should be noted that after the initial set-up and in the absence of any updates to process models, only steps 4-6 are required to ensure SOX compliance.

Figure 2. Six-step framework for SOX compliance

The first step, Business Process Acquisition, involves the acquisition of detailed business processes. After all, it is through these that one can get an accurate and realistic view of existing risks and possible controls. This step results in well-elaborated and approved business process models that serve as basis for following tasks.

The insurance company that served as case study for the proposed solution needed about eight months for this step alone. The step was about eighty percent completed before starting work on the implementation of the presented solution.

The second step, Risk Assessment and Scoping, SOX rules for financial reporting are comprehensive and imply, among other things, the following:

- Some accounts affect financial reporting and therefore also need to be controlled; these are labelled significant accounts;
- Internal controls, along with an internal control framework, need to be set-up; including activities or processes that influence financial reporting;
- In order to evaluate controls, relevant risks need to be identified and assessed.

Significant accounts are accounts relevant to the balance sheet of a company that have a major impact on reported results. Such accounts need to be identified as they hold a major portion of the content of financial reports. Examples of such accounts are ones for "Investments", "Gross Premiums Written", "Unearned Premiums" etc. During the 'Risk Assessment and Scoping' step, these accounts may be associated with the business processes that affect their balance.

Significant accounts are identified, recorded and documented in a "Significant Account Model", along with account-related data. This task is carried out by the Chief Financial Officer and the Chief Internal

Auditor, or their surrogates. The determination of significant accounts needs to be signed-off.

SOX-related risks are identified and modelled next. This means the collection of risks, negative events, in a risk catalogue and the assignment of these to the activities of business process models susceptible to the identified risk. The risks may involve failed/incorrect processing of an invoice, missing data when creating a customer profile, or even insufficient skills for persons who are responsible for critical steps within a business process. SOX is not concerned with business-related risks, e.g., the risk associated with a particular insurance contract.

During this assignment, risks are assessed with respect to their likelihood and impact. Figure 3 gives an example of a table and the display of an activity object where risk assignment and assessment may be performed. The traffic-light-coding gives immediate feedback about the risk situation in terms of likelihood and impact.

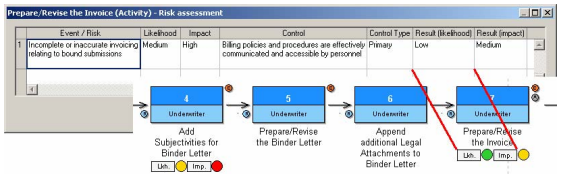

Figure 3. Table and display for the assignment of risks and controls

For the identification and assignment of risks to activities, subject matter experts from financial and business units and the designated expert for SOX-related matters are required. Moreover the process owner contributes to this assessment and is responsible for signing-off the results together with the Chief Internal Auditor. By analyzing risks within its business processes, the company now has a detailed overview of its risk situation. This is the starting point for determining appropriate controls in order to reduce the likelihood that risks will occur, or reduce their impact when they cannot be avoided.

Controls such as "have a senior-level employee check particular agreements", "consistency checks within an IT-system", "middleware auto-emails alerts on processing failures", "simulation of account entries" are recorded and documented in a control catalogue or Control Model, along with information such as: Classification (primary, secondary or other), Anti-fraud relevant, Classification if preventive or detective, Executed automatic, semi-automatic or manual, Assertions, Control Owner, Frequency of Execution. The assignment of controls to risks is a many-to-many relation. For each control, there may be "control processes" and "control activities". Control activities are part of the checking procedure of the entire control and are usually of a different business process than the activity incorporating the risk. Control processes are separate processes which produce as a result the defined control for a risk in a different business process.

The definition and documentation of controls is also performed by subject matter experts from financial and business units, process owners, the Chief Financial Officer, the Chief Internal Auditor and the SOX Expert.

A difficulty we encountered while carrying out this step for our industrial case study was risk synonymy: the same risk name may have different meanings in the context of different business processes. This was also the case for controls. To overcome this problem, some business process models had to be revised to improve accuracy.

The third step, Design Effectiveness, deals with the revision of internal controls, intended to balance risks and control costs is called "Design Effectiveness". This means that internal controls have not been over-/ under-engineered (by leaving in the system so-called "control free zones") [6].

The "gap analysis" considers situations where a company is unable to implement all necessary controls in one shot. Some controls require the set-up of separate IT projects, which means that design effectiveness is not addressed immediately. The SOX portal supports this step with functionality to perform the "testing" and the various tasks to test the set-up of the internal control framework. These functions/tasks are:

- Documentation: This task lists business processes and additional information belonging to a test cycle.
- Scope: Scoping concerns the determination of controls that should be tested. This task reduces the number of controls to be tested and the frequency of testing.
- Plan: After scoping, test plans are created with parameters including: Test Plan Status, Test Plan Type, Tester, Test Period, Test Plan Description, Test Evidence, Sample Size and "traffic light code" to show the degree of completion. Each test plan automatically receives a "Test ID" in order to be able to reference at any time to a particular entry related to the test as this makes the test traceable for audit purposes.
- Execution: This step consists of the actual execution of the test. The execution has to be conducted according to the description and guide entered in the test plan. Test results from the execution are documented.

- Gaps/Remediation: After performing a test, the results have to be evaluated in order to assess the company's situation. If a test was not passed, or passed with exceptions, it is necessary to improve on the situation. For this, remediation measures need to be defined. A final statement about the test results and the sign-off of these results will be required by the above mentioned roles. The External Auditor receives this report about the situation of the design effectiveness, so the condition of the control framework of a company as information. A "notice of acceptance" of the External Auditor is an indicator that the initial scoping for the design effectiveness and the set-up procedure was in accordance with the External Auditors assessment.
- Re-Design: Depending on the outcome of the tests and the final assessment of the internal management, some of the process models or controls might require improvement. In this case, tests need to be repeated for these parts.

For our industrial case study, we made sure that during this step we documented initiatives that were already running in order to finalise the set-up of the company's internal control system. This documentation is essential as planned but not yet fully implemented internal controls need to be taken into account during the evaluation of the Operating Effectiveness. If such documentation is missing, it may lead to failed tests, and therefore repeat of the testing process.

This fourth step, Operating Effectiveness, is intended to determine whether internal controls are effective during actual operation. To answer this, the company either needs to conduct self-assessments, internal audit reviews or testing procedures of its controls. The actual steps are the same as the ones carried out for testing Design Effectiveness.

The main difference between this phase and Design Effectiveness is that the test results of this phase are integrated with the financial reporting of the company. As before, and depending on the test results, appropriate remediation measures may have to be defined. If the test results are generally poor, it may be necessary to repeat the whole testing procedure. The External Auditor decides if repetition is necessary.

For our case study, the main challenge of this step was to define appropriate volume and scope of the tests. In addition, we had trouble determining how to actually perform tests such as checking log files.

In the fifth step, Internal Management Review, predefined strategic and operational goals are assessed against test results to determine if the company is SOX-compliant. Management needs to sign-off the report to be filed as an official document to the External Auditor. This report together with other financial reports constitutes the basis for assessing if the company is SOX-compliant.

In the sixth step, Auditor's Final Review, the External Auditor receives financial reports along with the internal management review report. Independently of these, the External Auditor retains a continuous insight of the company's financial and accounting situation.

5. Evaluation and lessons learned

5.1 Evaluation

The solution presented herein constitutes an approach to integrate SOX reporting requirements in the "every-day-life" of a company. After the initial set-up of the solution, compliance to SOX amounts to revised business processes, along with new infrastructure consisting of the SOX portal. Moreover, the proposed solution is both generic in that it applies to any company that operates on the basis of business processes, and non-intrusive in that it only affects SOX-related aspects of a company.

The solution has been adopted by an U.S. insurance and re-insurance company to revise its SOX-specific financial reporting operations. In total, the compliance project involved:

- 180 business processes including sub-processes for three different subsidiaries;
- 203 identified risks;
- 192 identified controls, including 50 IT controls; that required an appropriate test environment.

The overall project duration was 9 months and involved 18 person-months for developing the solution. These figures are comparable with figures from other SOX projects [7].

5.2 Lessons learned

Though the proposed solution worked well at the end, there were particular areas where the initial conception needed to be reworked.

The first area involved the determination of Design Effectiveness. We initially assumed that design gap analysis would be performed in the ADONIS® platform. This turned out to be difficult as it was necessary to provide very distinct access rights for different entry fields and attributes for a single activity. This proved quite difficult and complex to realise. Instead, the evaluation of Design Effectiveness was realised in the SOX portal.

The other area of difficulty was the entire topic of testing, i.e. Operating Effectiveness. Again, dealing

with requirement of very detailed access rights for many different roles who enter information proved tricky. Some roles should only have access to very specific information. Moreover, access may range from "not at all" through "read-only" to "write" on attributes of activities, significant accounts, risks and controls. This could only be realised through the portal.

The initial version of our solution turned out to be rather complex and was not immediately picked up by our customer. Consequently, we developed the "six-step framework" in order to give our solution a structure and a procedure model. Within this structure, wizards were added to support different dialogues. These structures made the compliance procedure transparent to the actual user. This proved essential for the acceptance of our solution.

Once users started implementing our procedure, they commended that the use of MS Word and Excel documents could make SOX reporting much easier. This change made it possible to tracks who did what, when and generate an overview changes, e.g., for a test cycle.

Having said all this, it should not be inferred that our proposed solution is "ready to be installed". The introduction of ADONIS® and the SOX portal is certainly possible for any company. However, every company has its informational and reporting idiosyncrasies that need to be taken into account in tailoring a solution.

6. Conclusions

The requirements a company has to fulfil in order to gain SOX compliant are comprehensive and affect the whole company. In coping with these requirements, one has to keep in mind that SOX compliance is not a one-off project but a continuous process that needs to be integrated into existing processes and reporting cycles. Consequently, continuous improvement solutions should be preferred because they may be updated and improved on an on-going basis. The case study provides concrete evidence that continuous improvements solutions to SOX compliance that are business process- rather than technology-based are feasibility and quite attractive from a customer perspective. Moreover, such solutions lead to higher formalization and standardization of business processes thereby improving synergies between different business units [8].

The solution presented here can be enhanced along several directions. Firstly, it would be useful to have more precise rules about compliance to regulations, so that a solution can be evaluated objectively. In addition, the project would have benefited tremendously by tools that support different risk analysis techniques, also testing techniques for proposed solutions.

Acknowledgements

The authors thank all the colleagues from the University of Vienna and BOC for helpful discussions and comments during the "development phase" of this paper.

References

[1] One Hundred Seventh Congress of the United States of America. 2002. Sarbanes-Oxley Act., http://www.law.uc.edu/CCL/SOact/soact.pdf, [Last access, May 11th, 2006]

[2] The Institute of Auditors. 2004. Enterprise Risk Management – Integrated Framework. http://www.coso.org/Publi-cations/ERM/COSO_ERM.ppt, [Last access, May 11th, 2006]

[3] Committee of Sponsoring Organizations of the Treadway Commission. 2004. Enterprise Risk Management: Executive Summary. http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf, [Last access, May 11th, 2006]

[4] Karagiannis, D., Nemetz, M., Schwab, M. 2006: Dashboards for Achieving Compliance to Regulations – A SOX-based Best Practice Scenario.

[5] Junginger, S. et al. 2000: Ein Geschäftsprozess-management-Werkzeug der nächsten Generation-ADONIS: Konzeption und Anwendungen. In Wirtschaftsinformatik 42, no. 5: 392-401.

[6] Price Waterhouse Coopers 2004. Sarbanes-Oxley Act: Section 404, Practical Guidance for Management.

[7] Ritschel, A., Hochstein, A. Josi, M., Brenner, W.: SOX-IT-Compliance bei Novartis. In Fröschle, H.-P., Strahinger, S. (Eds.): Praxis der Wirtschaftsinformatik, HMD Verlag, Number 250, Heidelberg, August 2006.

[8] Breaux, T., Vail, M., Antón, A.: Toward Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations. Proceedings IEEE International Conference on Requirements Engineering. Paris, September 2005.

[9] U.S. Securities and Exchange Commission http://www.sec.gov/spotlight/sarbanes-oxley.htm, [Last access, May 11th, 2006]

[10] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic Databases. In Proceedings of the 28th International Conference on Very Large Data Bases, 143–154. Morgan Kaufmann, 2002.