

Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology

Rakesh Agrawal, Christopher Johnson,
Jerry Kiernan
IBM Almaden Research Center
650 Harry Road, San Jose, CA 95120
{rAgrawal, johnsocm, jkiernan}@us.ibm.com

Frank Leymann
University of Stuttgart
Universitätsstraße 38
70569 Stuttgart, Germany
frank.leymann@informatik.uni-stuttgart.de

Abstract

The Sarbanes-Oxley Act instituted a series of corporate reforms to improve the accuracy and reliability of financial reporting. Sections 302 and 404 of the Act require SEC-reporting companies to implement internal controls over financial reporting, periodically assess the effectiveness of these internal controls, and certify the accuracy of their financial statements. We suggest that database technology can play an important role in assisting compliance with the internal control provisions of the Act. The core components of our solution include: (i) modeling of required workflows, (ii) active enforcement of control activities, (iii) auditing of actual workflows to verify compliance with internal controls, and (iv) discovery-driven OLAP to identify irregularities in financial data. We illustrate how the features of our solution fulfill Sarbanes-Oxley requirements using several real-life scenarios. In the process, we identify opportunities for new database research.

1. Introduction

The United States Congress enacted the Sarbanes-Oxley Act (“Act”) [1] in June 2002 in the wake of several highly-publicized corporate scandals. The Act imposed sweeping reforms designed to increase the transparency of financial reporting under federal securities laws. Most notably, Sections 302 and 404 of the Act require companies reporting under sections 13(a) or 15(d) of the Securities Exchange Act of 1934 to implement systems of internal control over financial reporting. Management of each company is responsible to maintain these controls and ensure the propriety of financial and accounting processes.

Over the past three years, reporting companies have spent considerable time and effort designing and implementing internal control systems. Enforcement and monitoring of internal controls consume numerous

employee hours and impose a significant financial burden on these companies. Surveys of large public companies indicate that Sarbanes-Oxley compliance costs exceeded \$4 million per company in the fiscal year 2004 [2] [3].

As a result of these high compliance costs, reporting companies are looking for technological solutions to automate internal control processes. Most Sarbanes-Oxley software products currently on the market offer controls over the access and manipulation of data and assist in documenting compliance efforts, but require manual implementation of financial reporting controls. To address this gap, we propose using workflow modeling, compliance auditing, and online analytic tools to automate many internal control functions.

The remainder of this paper is structured as follows. Section 2 summarizes the basic internal control requirements of the Act. Section 3 describes the current level of automation in Sarbanes-Oxley compliance. Section 4 outlines our proposed solution design. In Section 5, we offer scenarios to demonstrate the utility of the solution. In section 6, we identify challenges and propose topics for future database research. We conclude in section 7.

2. Internal Control Requirements

2.1. Sections 302 and 404 of the Act

Section 302 of the Sarbanes Oxley Act requires executive officers of reporting companies to certify the accuracy of the company’s financial statements and verify that they have designed internal controls over financial reporting. Section 404 requires each company’s annual report to contain an internal control report, which must include: (i) management’s framework for evaluating internal controls; (ii) its assessment of the effectiveness of internal controls at the end of the fiscal year; and (iii) an outside auditor’s attestation of the internal control system.

2.2. Definition of Internal Controls

The Securities and Exchange Commission (“SEC”) adopted a Final Rule under Section 404 [4] that defines internal control over financial reporting as a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with generally accepted accounting principals (“GAAP”).

The Rule states that internal controls must include policies and procedures pertaining to the maintenance of records that: (i) accurately and fairly reflect the company’s transactions and dispositions of assets; (ii) assure that transactions are recorded as necessary to prepare financial statements in accordance with GAAP; (iii) assure that receipts and expenditures are made only pursuant to authorizations of management and directors; and (iv) reasonably assure prevention or timely detection of unauthorized acquisition, use, or disposition of the company’s assets that could have a material effect on the financial statements.

2.3. Contents of the Internal Control Report

2.3.1. Internal Control Framework. The SEC Rule requires companies to adopt a suitable framework to implement their internal controls. The most widely used framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission (“COSO”) in 1992 [5]. The COSO framework outlines the following five elements of internal control over financial reporting, which have been ratified by the accounting standards of the Public Company Accounting Oversight Board [6].

Control Environment is the “tone at the top” of an organization. Establishing a suitable control environment involves designing management policies and control structures that encourage integrity and responsibility and foster competent and ethical behavior within the organization.

Risk Assessment involves an in-depth analysis of a company’s business, operations, and financial reporting processes to identify internal and external risks inherent in achieving the company’s objectives.

Control Activities are designed to mitigate company-specific risks and ensure that management’s policies and directives are implemented. Examples of control activities include approvals, authorizations, verifications, reconciliations, performance reviews, and segregation of duty constraints.

The **Information and Communication** element is intended to assure that material information is disseminated within and outside of the organization. This

ensures that managers are able to make the proper decisions, investors have access to sufficient information to evaluate the company, and regulators have a basis to determine whether the company has complied with applicable laws.

Finally, the **Monitoring** element of the internal control framework requires the company to assess its internal control system, on an ongoing and periodic basis, to identify and correct any material weaknesses.

2.3.2. Management’s Assessment of Controls. After the internal control system has been designed and implemented, management must periodically determine which controls need to be tested, evaluate the likelihood that failure of a control could result in a material misstatement or omission in the financial statements, and identify any deficiencies or material weaknesses in the control system [7]. Results of this assessment must be documented for auditor review.

2.3.3. Auditor’s Evaluation of Controls. Lastly, the internal control report must contain an outside auditor’s attestation of the internal control system. Auditors are required to evaluate management’s assessment and documentation and perform their own independent review and testing of controls.

3. Current State of Technology

In view of the substantial compliance obligations imposed by Sarbanes-Oxley, reporting companies are interested in deploying sophisticated systems to enforce internal controls and assist management in evaluating their effectiveness. Unfortunately, technology has not kept pace with these market needs.

3.1. Degree of Automation

Compliance with the internal control requirements of the Act remains a predominantly manual process. Companies typically assign each control to an “owner” who is responsible to implement the control and an “assessor” who is responsible to assess the control. Additional time and labor is then required to document and report on the effectiveness of the internal controls. Automating some of these manual tasks would substantially reduce the overall cost of compliance.

3.2. Current Software Products

Most Sarbanes-Oxley software products on the market address the information and communication element of the control framework, but rely on manual implementation of control activities and monitoring requirements. For instance, IBM’s Workplace for Business Controls and Microsoft’s Solution Accelerator

for Sarbanes-Oxley provide central content repositories with controlled access to company financial data. They assist managers in organizing written risk assessments and control policies and assigning implementation and monitoring responsibilities to employees. But owners within the company must manually verify whether each control has been implemented and assessors must likewise indicate whether each control has been effective.

Other products, such as Oracle's Internal Controls Manager, offer conventional workflow modeling capabilities, in addition to the foregoing features. Virsa's Continuous Compliance suite also provides some application-level authorization and separation of duty controls. However, a considerable opportunity exists to develop new technologies that further automate the most labor-intensive internal control processes.

3.3. Continuous Assurance Technology

For the last decade, accounting research has advocated moving toward "continuous assurance" [8] [9], defined as "technology-enabled auditing which produces audit results simultaneously with, or a short period of time after, the occurrence of relevant events" [10]. Continuous assurance relies on capturing information about transactions and processes and monitoring flows of transaction data to identify discrepancies between actual and expected results. Significant discrepancies trigger alarms that require investigation by managers and auditors [11] [12] [13].

Many in the accounting community expect Section 404 financial reporting controls to be integrated with continuance assurance, reporting, and monitoring as soon as technology permits. Some suggest that "tools for automatic control mapping, evaluating online real-time control functioning, and selecting alarms for auditor review will greatly facilitate 404 compliance" [14]. Our proposed system of active enforcement of controls, workflow auditing, and anomaly detection analytics operationalizes this notion of continuous assurance.

3.4. Database-Level Enforcement

Computer science research has begun address database-level enforcement of legal regulations. Hippocratic databases have been proposed to actively enforce data disclosure policies [15] and audit compliance with privacy laws [16], such as the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act. Methods for maintaining tamper-resistant audit logs for legal compliance purposes are discussed in [17]. Although these technologies relate to privacy laws rather than Sarbanes-Oxley, they show the benefits of managing compliance at the database level. In the

sections that follow, we identify database technologies that can be applied Sarbanes-Oxley compliance.

4. Solution Architecture

The architecture for our Sarbanes-Oxley solution consists of four main components: (i) workflow modeling, (ii) active enforcement, (iii) workflow auditing, and (iv) anomaly detection. Figure 1 illustrates how these components interoperate.

The following definitions are relevant to understanding our solution architecture.

Transaction: A transaction is a set of activities comprising a business operation that generates an entry in the company's financial statements.

Activity: An activity is a self-contained task in the execution of a transaction.

Workflow: A workflow consists of an ordered set of activities and is the means of executing a transaction. Workflows are enactments of business processes performed within an IT environment.

Routine vs. Non-Routine: A routine transaction is executed with sufficient regularity within a company that it has a defined workflow. Conversely, a non-routine transaction is not executed on a regular basis.

Material: Information is material if there is a substantial likelihood that a reasonable investor would consider it important in deciding whether to buy, hold or sell a security. For instance, a financial reporting inaccuracy that would have a *de minimis* effect on a company's reported income may nevertheless be material if it suggests fraudulent reporting practices.

Financial Statements: Financial statements include a company's balance sheet, income statement, cash flow statement, and other financial information filed with the SEC.

4.1. Workflow Modeling

The first component in our solution architecture is workflow ("WF") modeling. We view internal control processes as sets of workflows, each containing required control activities. To model these required workflows, we suggest an inductive bottom-up approach, using logs of past activity executions. This method is preferable to normative top-down modeling techniques, which may not comport with existing company culture and modes of doing business [18].

4.1.1. Activity Logging. Initially, we record certain transaction activities in logs that are stored in database tables. These activities include controls over initiating,

authorizing, recording, processing, and reporting significant accounts, disclosures and related assertions in the financial statements [19]. Logs include information about the activity, the identity of the person who performed the activity, the time of execution, and other contextual information.

Upon invocation of an activity in a workflow, the system records the fact that it has been invoked and generates a log record. For activities performed outside of a workflow system, a WF Step Interceptor extends existing middleware to intercept activity invocations and pass corresponding information to the Log Record Generator.

In application server environments, containers hosting executable activities may observe invocations of each activity and pass corresponding information to the Log Record Generator. Special deployment descriptor extensions prescribe such behavior for corresponding executables. Systems management environments may also be extended to intercept activity invocations based on new types of management events. In web service environments, policy annotations may declare services as activities to be monitored. Such policy annotations may direct attendant SOAP headers to the Log Record Generator.

4.1.2. Modeling Required Workflows. Next, we mine the activity logs to construct past transaction workflows.

We then use these as a baseline to model required workflows for routine company transactions. Managers can use the WF Modeling GUI to refine the workflows and ensure that they incorporate appropriate internal controls. Research concerning construction of workflow models from logs of past activities includes [20], [21], and [22]. A survey of workflow mining approaches is offered in [23].

Each required workflow should include controls over initiating, authorizing, documenting, processing, and reporting the transaction. Graphs of these workflows are compiled and stored in Executable WF database tables maintained for active enforcement and auditing purposes. Required workflows can be updated at any time and resubmitted for compilation.

4.2. Active Enforcement

The second component of our Sarbanes-Oxley solution, active enforcement, imposes policy-based constraints on workflows at the time of execution. This component is intended to ensure that routine transactions comply with prescribed workflows. Other components of our solution are intended to handle non-routine transactions and detect fraud perpetrated outside of the internal control system.

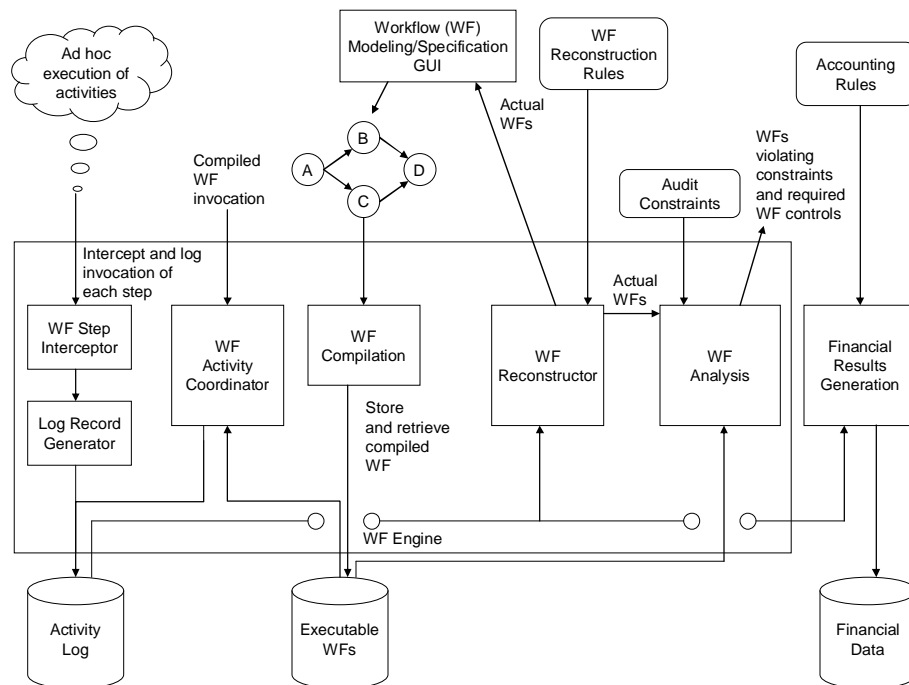


Figure 1. Workflow execution and analysis infrastructure

One method of active enforcement is to apply process constraints that do not allow completion of non-compliant transactions. Examples of this type of active enforcement include workflow authorization constraints [24] [25], secure co-processors to verify contract authorizations [26], and temporal database constraints [27]. Another method is to allow non-compliant transactions to proceed, but log all exceptions to the required workflows [28].

Figure 2 depicts the organization of the active enforcement system. The workflow engine manages and coordinates the execution of individual activities in the workflow. The WF Coordinator passes the activities onto the WF Exception Detector, which determines whether each activity complies with the required workflow. If an activity is in violation, the workflow engine can block execution of further activities in the transaction. Alternatively, the engine can allow the non-compliant transaction to proceed, but record the violation in an activity log to be maintained for audit purposes. This alternative avoids problems associated with enforcement errors and immaterial process deviations. Auditors can use exception data gained from periodic audits to investigate violations and refine workflow models.

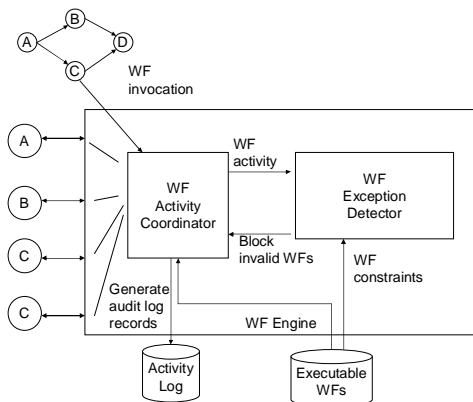


Figure 2. Active enforcement of controls

4.3. Workflow Auditing

The third component of our proposed solution provides two types of workflow auditing – compliance verification and query-based auditing. This component can be used by internal or external auditors to assess the effectiveness of internal controls.

4.3.1. Compliance Verification. The compliance verification system reconstructs actual workflows and compares them with required workflows to identify control violations.

Reconstruction of Actual Workflows: The WF Reconstructor uses correlation rules to reconstruct actual workflows from the activity logs. Correlation rules assign individual activities to workflows. For example, these rules can associate activities into a workflow based upon a unique identifier assigned to all activities in an individual workflow instance. The rules may be supported in an environment-specific manner. Application servers may support deployment descriptors identifying elements of the signature of the executable invoked. In web service environments, correlation properties and aliasing mechanisms defined in [29] may be used to support association of individual activity invocations to workflow instances. Other rules can reconstruct workflows by joining all activities performed on behalf of a certain user during a specified timeframe.

Comparison to Required Workflows: After the actual workflows have been reconstructed by the WF Reconstructor, they are compared with the required workflows to determine whether transactions are compliant with internal controls. Methods of comparing directed graphs are discussed in [30]. This comparison process presents non-trivial problems, as it requires more than a simple matching of graphs. The system should be able to distinguish between immaterial process deviations and actual breakdowns in the internal controls scheme. For instance, in many compliant transactions, activities and controls may be completed in different orders. Often, substitute controls may also be acceptable. In addition, many actual workflows may be compared to determine whether process deviations are systemic problems or isolated instances. Approaches such as those proposed in [20], [21], and [22] can be used for this purpose.

4.3.2. Query-Based Auditing. Query-based auditing enables companies to audit the activity logs to investigate suspicious transactions and periodically assess the effectiveness of the internal control system. Audits are expressed as constraints against workflow instances. An audit returns as its result instances of workflows that violate these constraints.

Auditors can analyze actual workflows, using the WF Analysis component to uncover workflows that violate audit constraints specified by an auditor. For example, in the course of assessing internal controls, an auditor might want to investigate a suspicious manager by requesting an audit of all transactions approved by that particular manager. Or perhaps she would like to audit all transactions executed within a certain time period. She could also request an audit of all routine transactions executed within a specified timeframe that are non-compliant with the company’s system of internal controls. As depicted in Figure 1, the stored workflows are input to the WF Analysis module for this purpose.

4.4. Financial Analytics for Anomaly Detection

The final component of our proposed solution involves the use of OLAP analytics [31] [32] to uncover potential anomalies in financial data that may suggest accounting errors or improprieties. External auditors often uncover such anomalies in periodic audits, leading them to investigate significant reporting inaccuracies. This requires in-depth review of journals, records, and other underlying accounting data and evidentiary matter, as analysis of top-line financial statements is generally insufficient to find meaningful anomalies. Internal and external auditors could more efficiently analyze this data and gain much further insight using OLAP techniques.

OLAP cubes provide data operations such as drill-down, roll-up, and selection to uncover material data anomalies. However, standard OLAP methods rely on analysts to choose the proper search dimensions and data operations. This hypothesis-driven OLAP analysis is difficult given the large number of potential paths through the cube and often does not yield fruitful results due to the large volumes of data, multiple search dimensions, and cancellation effects that may obscure anomalies in lower-level data. Accordingly, we suggest using a discovery-driven approach to OLAP analysis, as described in [32].

Instead of relying on analysts to select appropriate cube views, discovery-driven OLAP searches for indicators of anomalies in various levels of the data to guide further exploration. The method of identifying such indicators should accurately reflect relevant business and financial metrics. The system should also be able to explain the relevance of the indicators in sufficient detail for an analyst to determine what additional cube views and data operations are necessary [33]. Such discovery-driven analysis should isolate meaningful anomalies in the financial data.

Figure 3 presents the system organization for the automated detection of anomalies in financial results.

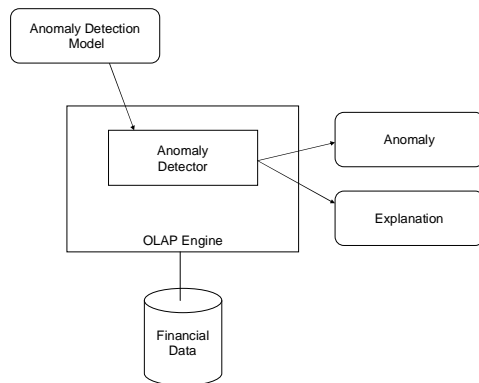


Figure 3. OLAP anomaly detector

5. Solution in Action – Rhone Auto Parts

The following scenarios illustrate the application of our solution to various financial transactions. In the scenarios, Rhone is a fictitious publicly-traded manufacturer and wholesaler of automotive parts. Its CEO has established an earnings growth target of 10% per year and tied management compensation to this target.

5.1. Routine Sales Transaction Scenario

In a typical Rhone sales transaction, a sales manager solicits orders from auto parts distributors. For each order, the sales manager prepares an electronic invoice, which is then forwarded to the shipping and accounts receivable departments. Upon receiving the invoice, the shipping department checks Rhone’s inventory for the requested parts. If they are in stock, the invoice is forwarded to a shipping manager for approval. Upon receiving an approved invoice, the shipping desk fills the order and ships the parts. The accounts receivable department then mails a bill to the distributor. On the other hand, if the parts are not in stock, the shipping desk advises the distributor how long the order will take to fill. The distributor can elect to proceed, modify, or cancel the transaction. As soon as the parts leave the loading dock to be shipped to the distributors, an accountant records the total price of the order as revenue. Per accounting rules, the cost of goods sold is recognized on a per unit basis in the same period each unit is sold.

Workflow Auditing: Rhone would like to audit a particular sales transaction for which a distributor was billed, but never received delivery of the parts. To begin, a Rhone auditor specifies the transaction by invoice number and requests a workflow audit. Upon receipt of the audit request, Rhone’s compliance verification system uses activity logs to reconstruct the actual workflow for that transaction. Comparing it to the required controls, the system determines that a critical activity is missing. Although the transaction has been recorded as complete, the shipping clerk never confirmed shipment. Either the goods were never shipped or the clerk did not verify the shipment. Auditors can use this information to investigate whether the transaction was improperly recorded.

The auditor can also use the query-based auditing feature to determine whether there are similar transactions for which revenue was improperly recognized, but the shipment was not confirmed. This information will help the auditor determine whether this is a one-time occurrence or a systemic problem.

Active Enforcement: In the future, Rhone could implement active enforcement controls that would not allow routine transactions to proceed in the absence of a required activity. For example, the accountant would be

prevented from recording the sale in the accounting ledgers until there was a confirmation of the shipment. As an alternative, the system could allow the transaction to proceed, but log the exception for later review by internal auditors.

Financial Analytics: Discovery-driven OLAP may assist in detecting systemic problems in large numbers of routine transactions. For instance, a proactive OLAP audit may reveal anomalies such as: (i) a period-to-period change in the ratio of recognized sales to confirmed shipments for a particular region; (ii) a significant increase in accounts receivable for sales generated by a particular sales manager; or (iii) a change in the ratio between orders and shipments for certain accounts. Hypothesis-driven OLAP methods would identify these anomalies only if the auditor had reason to search the proper dimensions of the financial data. On the other hand, discovery-driven methods would be more effective in uncovering unsuspected anomalies in large volumes data with numerous search dimensions.

5.2. Prevention and Detection of Fraud

The following two scenarios discuss the use of our solution to detect fraudulent accounting methods that are used to inflate earnings.

5.2.1. Revenue Manipulation Scenario. Susan is Vice-President of Sales for Rhone. Upon learning that Rhone is unlikely to meet its 10% earnings growth target for the first quarter, Susan encourages her sales managers to engage in aggressive tactics to increase revenues before the quarter end. Several managers enter into unwritten agreements with their distributors, wherein they will ship an extra 20% worth of parts. However, the account manager will not require payment for the extra parts unless and until the distributors are able to unload them to retailers. Using this scheme, the sales staff increases revenues and ensures that earnings targets are met for the quarter.

Workflow Auditing: A workflow audit would reveal that the sales managers submit orders directly to the shipping desk without verification or approval from a shipping manager. Although Rhone recognizes the sales as revenue upon shipment of the goods, it does not receive payment for the goods unless and until they are sold to retailers. This causes misleading earnings inflation by swelling accounts receivable.

Active Enforcement: Rhone could prevent these non-compliant transactions from proceeding by not allowing the shipment until the system receives invoice verification and shipping manager approval. Alternatively, the system could log records of these non-compliant transactions, which could be revealed and investigated in quarterly

compliance audits. In either case, Rhone could automatically detect this type of revenue manipulation early in the process.

Financial Analytics: In some situations, active enforcement and auditing would not reveal this revenue manipulation. For instance, the sales manager could produce fraudulent invoices for the additional orders and collude with a shipping manager to verify and approve these invoices. In this case, the analytics component would assist Rhone's internal auditors in uncovering the fraud. In comparing period-to-period financial data, it would uncover anomalous increases in the ratios of accounts receivable to revenue and earnings. Further drill-down would allow internal auditors to isolate sales and shipping managers with lower collection ratios associated with their invoices.

5.2.2. Cost Manipulation Scenario. During the second quarter, Susan again fears that Rhone will not meet its earnings target. This time, Susan approaches Carlos, the assistant controller, and asks him whether there is any slack in the company's accounting figures keeping earnings growth down for the quarter. Carlos suggests that Rhone is incurring significant expense in a promotional campaign to ship free product samples to retailers and repair shops. Since this campaign is creating demand pull for new products, Carlos decides to categorize it as a long-term customer acquisition cost rather than a period cost. As such, he capitalizes these expenses over the next ten years, rather than fully recognizing them in the current year. This reduces period costs, allowing Rhone to meet its earnings target without any further increase in sales.

Workflow Auditing: Rhone's internal controls require its controller and assistant controller to review and approve the draft financial statements at the end of each period before they are certified by the executive officers and filed with the SEC. In this case, Carlos unilaterally changes the accounting treatment for the sample parts. If senior management does not approve the statements, a quarterly workflow would reveal this process violation. But if the statements are approved without comment, a subsequent OLAP audit would reveal this violation.

Financial Analytics: Discovery-driven OLAP analysis would reveal a significant decrease in per-unit cost in the second quarter and a large increase in capital expenses. It would also show that changes in contribution to profit from the new parts are disproportionate to the increase in sales for those products. These anomalies could be uncovered by specific SQL queries or existing hypothesis-driven OLAP techniques only if the auditor had an idea of where to search for the anomalies. On the other hand, if there are nearly infinite potential cube views, discovery-driven methods are more proficient.

5.3. Compliance in Non-Routine Transactions

The final scenario describes how our solution assists in handling non-routine transactions, for which required processes may not be specified ahead of time.

5.3.1. Hidden Debt Transaction. Fred is Rhone’s Chief Financial Officer. During the third quarter of Rhone’s fiscal year, Fred is approached by Ziske Auto Racing Company with a proposal to develop a series of high-end auto racing parts. Fred assigns a finance department team to perform due diligence on the transaction. The team determines that the proposed venture is very risky, but will yield high returns if it can establish a foothold in this niche market.

Fred is interested in this venture, but does not want Rhone to lose its high debt rating by incurring additional debt on its balance sheet. Thus, he structures a joint venture, called Fastlane, in which Rhone and Ziske each invest \$5 million in company stock in exchange for a limited partnership interest. The general partner is FS Partners, LLC, which lists Adam, Rhone’s Assistant CFO, as its sole director. Adam invests \$200,000 in Fastlane in exchange for a 4% general partnership interest. Fastlane borrows \$10 million from Carnegie Bank, secured by the Rhone and Ziske stock. The structure of this transaction is depicted in Figure 4.

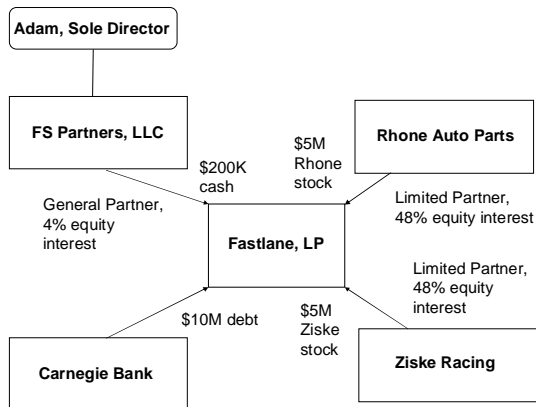


Figure 4: Rhone hidden debt transaction

Using this transaction structure, Rhone invests in a high-risk, high-return venture without expending any cash or reflecting any additional debt on its balance sheet. This structure is unlawful because it hides debt that should be aggregated with Rhone’s financial statements. To qualify for non-aggregation and keep this debt off the balance sheet, accounting rules require that the venture be an arms-length transaction, in which a non-related general partner invests at least 3% of the funds. Neither is the case here.

Because this is a non-routine transaction, Rhone has not prescribed its required workflow. However, Rhone should have sufficient separation of duty and authorization constraints in place to ensure that all transactions of a certain magnitude are thoroughly reviewed before being executed. For instance, Rhone could require that all transactions exceeding \$1 million in value must have (i) comfort letters from outside counsel and auditors; (ii) informed consent of the CEO and Board after reviewing transaction documentation and attorney and auditor letters; (iii) approval of an executive from a different department before funding the deal; and (iv) electronically signed verifications.

Workflow Auditing: An audit of the workflows in this transaction would reveal that it was initiated by Fred, approved by the Board and CEO without any indication of document review, and funded by the signatures of Fred and the Assistant CFO, Adam. Comparing the actual workflow to the required general workflow for transactions exceeding \$1 million would reveal the reasons this transaction is non-compliant.

If the Board independently became suspicious of Fred, it could use query-based auditing to request an audit trail of all transactions above \$100,000 that were initiated by Fred within a certain time period. If the Board suspects collusion between Fred and Adam, the auditor could request an audit of all transactions containing approvals of Fred and Adam. Because all activity logs are kept in the database, various audit queries can help investigate suspected improprieties and evaluate the effectiveness of internal controls.

Active Enforcement: Rhone could also have active enforcement controls in place to prevent the transfer of the \$5 million investment from its treasury stock pending recognition of both comfort letters and the required electronic signatures of the CEO, the secretary of the Board, and another executive officer.

6. Opportunities for Future Research

6.1. Process Discovery

The greatest challenge to designing a Sarbanes-Oxley compliance solution is the volume and diversity of transactions that are handled by each internal control system. The needs of individual companies vary considerably based upon size, location, industry, culture, management structure, and operational needs. Solutions require a great degree of specialization and must accommodate large numbers of transactions.

We have suggested a bottom-up approach to discovering and modeling these processes, using activity logs to uncover and model actual workflows, which can

then be modified to include required internal controls. Initial approaches to such workflow modeling techniques have been proposed in [20], [21], and [22], but further research is required to capture the complex conditional relationships that may exist between the individual steps in a workflow.

6.2. Modeling Non-Routine Transactions

In addition to routine transactions, effective workflow models must also capture and document complex, non-routine transactions, for which there is no precedent to guide process development. A polymorphic process model has been proposed in [34] to model abstract workflows without immediately requiring the implementation details of each activity. BPEL [29] enables abstract description of observable behavior in executable processes. These descriptions may represent constraints imposed on executable processes. It would be interesting to explore extensions needed to model and audit non-routine transactions.

In addition, complex workflows often share common sub-processes or control activities that are critical to their execution. For example, non-routine transactions often involve the transfer of money or assets, such as company stock. Critical activities, such as dual authorization requirements, constrain such non-routine transactions even though there may not be formal processes prescribed for other elements of the transaction. There is a research challenge in the selection and modeling of such critical activities in a way that large classes of non-routine transactions can be controlled and audited in terms of these controls.

6.3. Methods for Handling Exceptions

Exceptions to required workflows are often permissible. For instance, activities may be completed in different orders, substitute authorizations may be acceptable, and activity schedules may be modified. Systems that impose overly-rigid execution rules are impractical because they do not accommodate exceptions that are common in practical situations [18]. Many workflow systems explicitly model such exceptions, but do not account for unanticipated exceptions. Methods for handling exceptions in the course of enforcement and auditing are necessary to build effective solutions. Thus, further research is needed to develop process modeling tools that update workflows by migrating exceptions into accepted business practices [35].

6.4. Storage and Retrieval of Executions

We observe the need for database systems to view workflows as first class objects and provide facilities for

storing and querying past executions. Although they consist of atomic activities, workflows have rich dependency structures. The value of workflow data is significantly reduced if this structure is lost. There is an important research challenge in developing storage models that represent the complex relationships between business activities in a workflow.

Further, traditional query languages such as SQL are inadequate to query a workflow repository due to the variety of stored business transactions and the possible alternatives and exceptions for each transaction. While XQuery's notion of ordered elements is helpful, XML queries over such transaction data are likely to become overly verbose and error-prone. Accordingly, workflow repositories warrant a new and powerful query language to uncover exceptions and deficiencies in business processes.

6.5. New Sources of Activity Data

RFID technology will provide large volumes of highly detailed information about business activities that have been infeasible to record in the past [36]. RFID readers can track the flow of products across manufacturing and distribution channels. They can also track other details of business activity, such as grouping of individual RFID tagged items involved in activities along with temporal signatures of events. Although privacy issues will have to be addressed [37], RFID data will be invaluable in analyzing the details of individual workflows. Managing the rate and volume of information generated by RFID readers will present scalability challenges [38]. Also, workflow reconstruction and auditing systems must be able to handle uncertainty introduced by incorrect aggregation of simultaneous but unrelated events.

7. Closing Remarks

Sarbanes-Oxley Act compliance is a multi-billion dollar problem for SEC-reporting companies. As the need for automated compliance solutions has outpaced the development of technology, there are significant opportunities for innovation. In this paper, we have presented a solution designed to address the complex internal control requirements of the Act. We demonstrated the utility of this solution using several real-life scenarios. We have also outlined important technical challenges and suggested topics for database research. We hope this work provides the basis for innovations that revolutionize internal control systems.

References

- [1] Pub. L. 107-204, 116 Stat. 745 (2002).
- [2] T. Hartman, Foley & Lardner LLP, "The Cost of Being Public in the Era of Sarbanes-Oxley," June 2005.
- [3] Financial Executives International (FEI), "Sarbanes-Oxley Compliance Costs Exceed Estimates," March 2005.
- [4] 17 CFR Parts 210, 228, 229, 240, 249, 270, and 274.
- [5] Committee of Sponsoring Organizations of the Treadway Commission, Internal Control - Integrated Framework, 1992.
- [6] PCAOB Accounting Standard No. 2, paragraph 49.
- [7] "Material weakness" and "deficiency" are defined in PCAOB Accounting Standard No. 2, paragraphs 8-10.
- [8] D. Kneer, "Continuous Assurance: We are Way Overdue," *Information Systems Control Journal*, vol. 1, 2003.
- [9] Canadian Institute of Chartered Accountants, *Continuous Auditing Research Report*, Toronto, Canada, 1999.
- [10] M. Alles, A. Kogan, and M. Vasarhelyi, "Black Box Logging and Tertiary Monitoring of Continuous Assurance Systems" *Information Systems Control Journal*, vol. 1, 2003.
- [11] M. Alles, A. Kogan, and M. Vasarhelyi, "Would Continuous Auditing Have Prevented the Enron Mess?" *CPA Journal* 72, no. 7, Jul 2002, p. 80.
- [12] R. Jamieson and S. Loh, "Continuous Assurance of E-Business Transactions for Fraud Detection," University of New South Wales, Sydney, Australia.
- [13] R. Weber, *Information Systems Control and Audit*, Upper Saddle River: Prentice Hall, 1999.
- [14] M. Alles, A. Kogan, and M. Vasarhelyi, "The Law of Unintended Consequences? Assessing Costs, Benefits and Outcomes of the Sarbanes-Oxley Act," *Information Systems Control Journal*, vol. 1, 2004, ISACA.
- [15] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, "Hippocratic Databases," *Proc. of the 28th Int'l Conf. on Very Large Databases*, Hong Kong, China, August 2002.
- [16] R. Agrawal, R. Bayardo, C. Faloutsos, J. Kiernan, R. Rantzaou, and R. Srikant, "Auditing Compliance with a Hippocratic Database," *Proc. of the 30th Int'l Conf. on Very Large Databases*, Toronto, Canada, August 2004.
- [17] R. Snodgrass, S. Yao, and C. Collberg, "Tamper Detection in Audit Logs," *Proc. of the 30th Int'l Conf. on Very Large Databases*, Toronto, Canada, August 2004.
- [18] G. Button, "Changing Ways of Working?" Almaden Institute on Work in the Area of the Global, Extensible Enterprise. IBM Almaden Research Center, 2004.
- [19] PCAOB Accounting Standard No. 2, paragraph 40.
- [20] R. Agrawal, D. Gunopulos, and F. Leymann, "Mining Process Models from Workflow Logs," *Proc. of the Sixth Int'l Conf. on Extending Database Technology (EDBT)*, Valencia, Spain, 1998.
- [21] F. Casati, U. Dayal, M. Sayal, and M. Chan, "Business Process Intelligence," Software Technology Laboratory, HP Laboratories, Palo Alto, California, April 2002.
- [22] W. van der Aalst, A. Weijters, and L. Maruster, "Workflow Mining: Discovering Process Models from Event Logs," *IEEE Transactions on Knowledge and Data Engineering*, 16(9):1128-1142, 2004.
- [23] W. van der Aalst, B. van Dongen, J. Herbst, L. Maruster, G. Schimm, and A. Weijters, "Workflow Mining: A Survey of Issues and Approaches," *Data & Knowledge Engineering*, Vol. 47, No. 2, November 2003, pp.237-267.
- [24] E. Bertino, E. Ferrari, and V. Atluri, "Specification and Enforcement of Authorization Constraints in Workflow Management Systems," *ACM Transactions on Information and System Security*, Vol. 2, No. 1, Feb. 1999, pp. 65-104.
- [25] F. Casati, S. Castano, and M. Fugini, "Managing Workflow Authorization Constraints through Active Database Technology," *Information Systems Frontiers*, vol. 3, No. 3, September 2001, pp. 319-338.
- [26] K. Goldman and E. Valdez, "Matchbox: Secure Data Sharing," *IEEE Internet Computing*, November 2004.
- [27] J. Chomicki and D. Toman, "Implementing Temporal Integrity Constraints Using an Active DBMS," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 7, No. 4, August 1995.
- [28] F. Casati, S. Ceri, S. Paraboschi, and G. Pozzi, "Specification and Implementation of Exceptions in Workflow Management Systems," *ACM Transactions on Database Systems*, Vol. 24, No. 3, Sept. 1999, pp. 405-451.
- [29] F. Curbera, Y. Golland, J. Klein, F. Leymann, D. Roller, S. Thatte, and S. Weerawarana, "Business Process Execution Language for Web Services (BPEL4WS)," July 2002.
- [30] J. Bang-Jensen and G. Gutin, *Digraphs: Theory, Algorithms and Applications*, 2001.
- [31] J. Gray, A. Bosworth, A. Layman, and H. Pirahesh, "Data Cube: A Relational Operator Generalizing Group-By, Cross-Tab and Sub-Totals," *Proc. Of the 12th Int. Conf. on Data Engineering*, pp. 152-159, 1996.
- [32] R. Agrawal, N. Megiddo, and S. Sarawagi, "Discovery-driven Exploration of OLAP Data Cubes," *Proc. of the Sixth Int'l Conference on Extending Database Technology (EDBT)*, Valencia, Spain, March 1998.
- [33] R. Agrawal and S. Sarawagi, "System and Method for Explaining Exceptions in Data," United States Patent No. 6,691,098, Issued February 10, 2004.
- [34] H. Schuster, D. Georgakopoulos, A. Cichoki, and D. Baker, "Modeling and Composing Service-based and Reference Process-based Multi-enterprise Processes," *Proc. of the Int'l Conf. on Advanced Information Systems Engineering*, Stockholm, Sweden, 2000.
- [35] M. Reichert and P. Dadam, "ADEPTflex - Supporting Dynamic Changes of Workflows Without Losing Control," *Journal of Intelligent Information Systems*, 10(2) (1998).
- [36] M. Greenstein and M. Vasarhelyi, "The Electronization of Business," *Electronic Commerce*, McGraw-Hill, 2001.
- [37] Electronic Privacy Information Center, Guidelines on Commercial Use of RFID Technology, July 9, 2004.
- [38] S. Madria, M. Tubaishat, "Sensor Networks: An Overview," *IEEE Potentials*, April/May 2003, pp. 20-23.