



COSO and COBIT Management using the Inferware Approach

INFERWARE CORP
<http://www.inferware.com>

Introduction

IT professionals understand the concept of frameworks. The popular J2EE software development approach, for instance, is a framework for developing enterprise Java applications. It offers a reference implementation and a set of guidelines that illustrate what can be done using repeatable software patterns. Best practice frameworks serve as excellent guides to developing enterprise requirements because they offer a validated set of processes that have been determined to be important to the domain that they serve. There are frameworks to serve most areas of the enterprise such as ITIL (The IT Infrastructure Library) used to guide IT service delivery, The Balanced Scorecard used to guide enterprise strategy alignment, and many others. These requirements are a “check list” of sorts and they can be put under management control once they are adopted by a company. Likewise, a “best practice compliance framework” is a guide to assessing and implementing internal controls. It provides objectives to help you ask the right questions, and offers guidelines for auditing and implementation.

To meet the Sarbanes-Oxley requirements for internal control systems, most Chief Compliance

Officers consider it a best practice to build processes which support two popular compliance frameworks: the financial control objectives of the Council of Sponsoring Organizations (COSO) and the Control Objectives for Information and related Technology (COBIT). Unfortunately, there is a gap between control objectives and the actual internal controls that are built into systems and programs. In the first year of Sarbanes-Oxley compliance, this gap was filled by expensive auditing companies who documented business processes and manually tested internal controls. Even smaller companies are feeling the pinch. According to a recent NASDAQ study, publicly traded companies with less than \$100 million in revenue spent an average of \$535,000 to comply with Section 404 of the law¹. *Is it possible that corporations can reduce the cost of compliance by reducing the amount of auditing required?* Can compliance be sustained without sacrificing management comfort regarding attestation? To address these questions and provide ways to align business objectives with regulatory requirements, Inferware developed an approach based on open standards and expertise-based systems architectures. Following this approach leads to an integration of IT processes

¹ Lincoln Journal Star, January 14, 2006.

with financial control objectives, resulting in a management control architecture that can be manipulated through models and assessed via dashboards.

COSO, COBIT,
and the Strategic Layer

The Council of Sponsoring Organizations for The Treadway Commission (COSO) was originally formed in 1985 as part of the National Commission on Fraudulent Financial Reporting, an independent private sector initiative. The group's mission was to study the causal factors that lead to fraudulent financial reporting. COSO developed recommendations for public companies and their independent auditors, for the Securities and Exchange Commission (SEC), other regulators, and for educational institutions.

Cobit is a best practice framework that bridges that gap between IT controls and financial controls. While COSO focuses on business level activities, **Cobit** drills down into the supporting IT activities. **Cobit** is a product of the IT Governance Institute (ITGI), which used to be called the EDP Auditors Association, and is affiliated with the Information Systems Audit and Control Association (ISACA). **Cobit** formalizes accepted international standards for best practices for IT controls in applications and in enterprise-

wide information systems. COBIT is technology independent.

When adopted by management, the objectives stipulated by COSO and **Cobit** can be considered a collection of policies. Each objective will have a different priority, depending on its value to mitigate perceived risks. The Inferware Strategic Layer™ provides semantics to express these policies in SBVR, the Semantics of Business Vocabulary and Business Rules standard from the Object Management Group. This semantic rich strategic layer is the foundation for an internal control system because it enables management to trace high level business concepts from policy statements to design models and eventually to executable code.

Drive Down to Business
Processes and Business
Rules

Models are the window into the inner workings of a business process. The use of standard notations such as UML and BPML enable business analysts to express work flows and decision rules for processes in their domain. Models provide intrinsic value by adding a visual dimension to business process management. Models have long been embraced by software development professionals because they reduce complexity,

enhance communication, and help with the discovery of requirements. The auditing community is beginning to realize that models also play a key role in the assessment and remediation of internal control systems. If you do not understand how your business process works, how can you control it?

Many companies use traditional flow chart techniques to document their processes. The most often used tool is Visio. This usually results in piles of documentation placed on the bookshelf in preparation of an audit. The audit itself adds to the paper burden because internal control tests are usually documented using desktop tools such as Word. The effort to produce this documentation, which is required to be performed by external auditors under some interpretations of Sarbanes-Oxley, is the main reason for the high cost of compliance. If you want to reduce the cost of compliance, you must integrate business process modeling into an organic repository that facilitates reuse and integrates the model with higher level abstractions and lower level design patterns.

Business processes and business rules can and should be traced back to their motivating policies which can be COSO or Cobit control objectives. The ability to

trace a control objective to the responsible business process is a key factor in proving that you have a worthy internal control system to which management will attest.

Inferware's Policy Management Framework™ product provides an environment, based on industry standards such as the Unified Modeling Language and the Meta-Object Facility, that facilitate the collaboration of the business process manager and the business analyst to define business models. The Policy Management Framework™ also provides a repository for manipulating and reusing business and technical models of all kinds.

Incorporate the System Design

Once business models are defined, the Policy Management Framework™ will generate platform specific executable code from your business rule model. Following Inferware's Policy Management Process™, the executable rule platform can then be incorporated into the overall system design using service oriented architecture standards (SOA). Various design views illustrate the actionable business processes and where the business rules kick-in. Traceability from the low level artifacts up the chain to policy is preserved. This feature is a very

strong reason why auditing expenses are reduced using the IW Approach™. This is no need to re-document the processes for the next SOX audit. Furthermore, by capturing the business rule and process execution through audit trails and alerts, proof that the internal controls work can be demonstrated.

Monitor the Execution

The design of internal control architecture must include a definition of audit trails and alerts. Audit trails register all the activity of the internal control: what transactions passed, which ones failed, and when the control was revised. Audit trails provide the raw data to feed internal control dashboards that enable managers to visually appraise the state of policy compliance in their organizations. Even more importantly, audit trails provide irrefutable evidence of how well or poorly your internal control system is working, providing a basis for future remediation efforts. The Policy Management Framework™ includes a configurable dashboard which can be used to monitor the status of your COSO and Cobit internal control objectives throughout your **business processes**.

Alerts are similar to audit trails. They are triggered when

transactions violate certain internal control thresholds. Alerts also feed dashboards, but they also may have their own workflow depending on the urgency and magnitude of the event.

Sustain the Effort

Incorporating feedback from audit trails and alerts set up on internal controls will help to improve your COSO and Cobit efforts over time; however, these frameworks are not silver bullets. An organization's internal control system improves when top management embraces the spirit of transparency and accountability in financial operations. COSO and Cobit provide well-intentioned leadership with a set of guidelines and best practices for reducing opportunities for fraud and improving the effectiveness and efficiency of operations and IT systems. Your internal control efforts will be further enhanced by using the Policy Management Process™ and the Policy Management Framework™ to build an infrastructure which will reduce the cost of auditing and Sarbanes-Oxley compliance.

Policy Example

The following example illustrates how a broadly stated business policy can be traced down to a specific internal control. The IW Approach™ offers standards-based technology to facilitate the auditing of an internal control system at every level.

Board Level: In order to fulfill their fiduciary duties, the Board adopts COSO as a framework to ensure the effectiveness and efficiency of operations and to ensure the transparency, accuracy, and truthfulness of financial reports.

C-Level: Executive management takes the following actions in order to fulfill the Board's decision to embrace COSO:

- § Issues communications from the President and CEO to set a "tone at the top" by insisting that internal control is the duty of every employee.
- § Establishes a formal and repetitive risk assessment process.
- § Dictates policies, procedures and practices to ensure that business objectives are met and risk strategies are followed.
- § Directs operational management to implement oversight of the internal controls by monitoring business processes and endorses COBIT as a framework for managing information technology resources.

Operational Management: (for instance the Director of Customer Relationships): To assess the state of internal controls, management reviews and improves the documentation of the business process and business rules in the order fulfillment cycle.

Information Technology Management: To comply with the COBIT control objective to report serious deviations in the operation of an internal control, IT develops audit and alert mechanisms which will feed a dashboard to provide the status of each internal control in the order management cycle. The following internal controls are monitored:

- § Customers who have not placed an order in more than 18 months shall have their credit re-verified.
- § A customer on credit hold is not allowed to place an order.
- § If the order amount exceeds the customer's credit balance, the order is not allowed.