by Thomas A. Cronin

Corporate Compliance: Pulling It All Together (Part 2)

Feb 19, 2004

In my previous article, I focused on Sarbanes-Oxley (SOX) as an example of how to apply a flexible framework that can easily be adapted to meet other government compliance requirements, such as Basel II and the USA Patriot Act. In this article I will clarify in more detail how the framework facilitates Control Point monitoring and management, as well as other key success factors to consider.

What is a "Control Point"?

To understand how the framework facilitates Control Point monitoring and management, it's important to define what we mean by "Control Points." SOX define two types of controls: internal controls and disclosure controls.

An internal control is defined by the Committee of Sponsoring Organizations (COSO) as a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the categories of:

1. Effectiveness and efficiency of operations
2. Reliability of financial reporting
3. Compliance with applicable laws and regulations.

The first category, effectiveness and efficiency of operations, addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources. The second category, reliability of financial reporting, relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. The third category, compliance with applicable laws and regulations, deals with complying with those laws and regulations to which the entity is subject. These distinct but overlapping categories address different needs and allow a directed focus to meet the separate needs.

A disclosure control is designed to ensure required information is acquired and disclosed. Exchange Act Rule 13a-15(d) further states that disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that the information required to be disclosed by a company in the reports that it files or submits under the Exchange Act is accumulated and communicated to the company's

management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure.

Controls are established to meet their objective (reliability of financial reporting) using recognized and repeatable criteria.

Collectively, internal controls and disclosure controls are discussed in this white paper as Control Points.

Compliance with the Committee of Sponsoring Organizations Framework

The SOX Framework complies with the COSO framework in supporting five interrelated components that are derived from the way management runs a business and are integrated with the management process. They are defined as follows:

1. Control Environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The Fujitsu SOX framework provides a control environment.

2. Risk Assessment: A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. The detailed documentation built during Section 302 activities records critical processes and identifies Control Points to be monitored and tested as part of Section 404 dictates.

Associating metrics to Control Points and then establishing threshold values is a way to measure risk. Identifying appropriate threshold measurements are crucial for both real-time management and ongoing analysis of processes. Breaching a high or low threshold indicates something out of the ordinary is taking place. There may not actually be an issue, but it does deserve closer evaluation due to the implied risk that something is awry.

3. Control Activities: These constitute the policies and procedures to help ensure that management directives are carried out. They can pertain to both enterprise-wide and application-level controls for different organizational, functional, and systems activities.

Once the Control Points (identified and established in your Section 302 activities) are approved by management, you meet the initial requirements of this component. Defining the metrics to be monitored-as well as the baseline, average maximum, and average

minimum values to be measured-establishes ongoing measurements to meet control activity requirements.

4. Information and Communication Dissemination: Pertinent information must be identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across, and up the organization.

Implementation should leverage alerts and real-time dashboards, as well as reports to distribute information related to abnormal behavior and ongoing monitoring. It is important to:

    - Deliver actionable information with dashboards and/or reports. Dashboards display a set of metrics that provide an "at-a-glance" information summary. The metrics may consist of information related to a single business process or provide an aggregated view of a number of business processes.
    - Tailor information for the recipient or type of recipient.
    - Use BAM/BSM, Content Management, Business Intelligence, as well as Collaboration software to build, store, and deliver information in dashboards or reports.

5. Monitoring: Internal control systems need to be monitored-a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. The SOX framework incorporates an automated means to monitor Control Points by BAM/BSM software, content management software, and/or rules engines.

Critical Success Factors to Consider

The SOX framework ensures that critical success factors are not overlooked, such as:

- Risk management and enterprise-wide visibility
- Re-performance testing
- Use of dashboards and real-time reporting

- Use of collaboration software for verification, validation, and certification of Control Points

Each of these factors is discussed below.

Risk Management and Enterprise-Wide Visibility

Corporations typically manage risk in silos-by line of business, organizational entity, or location. The framework provides an enterprise perspective for both the technical infrastructure and critical processes. This facilitates enterprise-wide tracking of loss events, Control Point surveillance, and impact reporting on operational risk losses to management.

When every line-of-business measures and reports operational risk and control assessment differently, it can be difficult or impossible to gauge overall risk exposure and provide the disclosure required by Sarbanes-Oxley. The enterprise-wide perspective afforded by the SOX framework overcomes these traditional limitations, provides global visibility, and integrates critical processes across the organization to achieve SOX compliance for financial reporting.

Re-performance Testing

Re-performance refers to computations made to independently verify the integrity of transactions or balances. An example of this would be verifying a balance (such as number of parts, completed goods, or a bank balance.)

Re-performance testing also relates to testing the operating effectiveness of key controls. Documenting the results of tests and maintaining information as material evidence is important for your SOX efforts, as well as to meet audit requirements. Ongoing testing of the operating effectiveness of controls is necessary to meet audit committee and external auditor requests. Re-performance testing can be accomplished through synthetic transactions.

There are multiple strategies that can be employed to deliver SOX and performance information. Dashboards are the preferred approach for real-time Control Point breach notifications. Reports are the preferred delivery method for weekly, monthly, quarterly, and/or annual analysis. Tailoring information for the recipient is highly recommended and desirable.

A lot of information will be captured as part of Control Point monitoring. Process owners should be notified and afforded the opportunity to research and resolve the Control Point breach. Filtering information is therefore essential so that recipients are notified only of ongoing issues. Incorporating filtering safeguards prevents rushed problem notifications to

higher-level managers. Threshold screening, filtering and notification deferral are important for certifying officers (i.e., the executive team). They are only interested in knowing critical breaches or issues, not all incidents.

Creating an operational data store (ODS) is essential to provide long-term storage of the information (evidence). Content Management software can be utilized to enforce storage rules and to maintain your information.

BAM/BSM, Content Management, Business Intelligence as well as collaboration software can be used to build, store, and deliver information through reports and dashboards.

Use of Collaboration Software for Verification, Validation, and Certification of Control Points

The steps to perform verification and validation for Disclosure Controls and Internal Controls should be scheduled, documented (to provide evidence for auditors), and then certified. The recommended approach is shown in the illustration below.

The SOX framework outlines collaboration software that can be exploited to schedule and advance documents/approvals among all stakeholders.

In many cases, the CEO will look to his direct reports to certify their respective results. Those reports will look their management team to do the same-and so on. Collaboration software can manage the entire process and maintain an audit trail in case “evidence” is necessary at a future time.

Summary

Recent legislation, such as the Sarbanes-Oxley Act, Basel II requirements and the USA Patriot Act, have established a new approach for corporate responsibility, accountability, transparency, and behavior. As an example, SOX has ushered in a new standard for companies regarding the reporting of Control Point effectiveness.

We recommend that enterprises employ the framework outlined above or a similar approach to meet their SOX and other corporate compliance obligations. One key reason is that good Control Point management is not just a best practice. With SOX, it is required through law.