Law and Best Practices for a Sarbanes-Oxley Systems Review

Any organization would like to have an optimal approach to a Sarbanes-Oxley Act review, whether it is the process used or the Sarbanes-Oxley review team’s composition. What is the recommended best process to review the internal controls in the core enterprise resource planning (ERP) business application? And what about the team composition? Drawn from a varied background, the team should be able to implement an internal control system commensurate with the size and nature of the organization. But who indeed should constitute this team and what should be their associated skill sets? This is a conundrum that many organizations face as they expand around the globe.

A LEGAL BACKGROUND ON SARBANES-OXLEY

“In the turn of the twenty-first century, several high-profile corporate scandals shook public trust. Insider trading, fraudulent financial records, and other deceitful incidents caused investors to question the integrity of the stock markets and their listed companies. Investors began to move toward more conservative investments and abandon the stock market. Publicly listed companies swiftly began to lose their market value.

The issues at stake were highlighted by Alan Greenspan in his autobiographical The Age of Turbulence, in which he further mentions that the “ultimate control of American corporations by their shareholders is essential to our market capitalist system.” Corporate leaders had become a Platonic “wise elite” with “absolute power.”

It is, therefore, to reassert the control on corporations that the act, authored by US Senator Paul Sarbanes and US Congressman Michael Oxley, “to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes” was enacted on 30 July 2002. Sections 103, 302 and 404 govern the legal dimensions under which the information systems (IS) audit is conducted for Sarbanes-Oxley, as internal control in the modern corporation is implemented through information systems.

Section 404 (a) (1) notes, “the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.” And, section 404 (a) (2) requires “an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.”

In recent years, several amendments have been made to the legislation. These amendments attempt to ensure that the legislation is in step with the needs of economic activity and the fact that some companies may be unable to afford Sarbanes-Oxley provisions in exceptional circumstances (figure 1).

The US Housing and Economic Recovery Act of 2008 has no effect on section 404 of Sarbanes-Oxley; the Dodd-Frank Act of 2010 includes exemption to nonaccelerated filers from section 404 (b); and the JOBS Act of 2012 exempts emerging growth companies from section 404 (b).

A QUEST FOR AN EFFECTIVE PROCESS AND TEAM COMPOSITION

The recommended process (in summary) for the annual Sarbanes-Oxley analytic review is (where not expressly indicated, the tasks are expected to be done by the audit manager in association with the ERP specialist):
1. Initiate the review process:
   - Get the charter from the head of finance or head of organization in regard to the annual Sarbanes-Oxley review commencement for the fiscal year.
   - Identify stakeholders affected by the Sarbanes-Oxley annual review.

2. Plan the review process:
   - Create a Sarbanes-Oxley review plan, scope and schedule.
   - Make a list of the stakeholders involved in the review.
   - Make a Responsible, Accountable, Consulted and Informed (RACI) chart of the stakeholders involved in the review.
   - Plan risk management:
     - Make a risk management plan.
     - Identify risk and create a risk register.
     - Perform qualitative risk analysis, as applicable, using risk probability and impact assessment, probability and impact matrix, risk data quality assessment, risk categorization, risk urgency assessment, and expert judgment.
     - Perform quantitative risk analysis, as applicable—data gathering and representation techniques, quantitative risk analysis and modeling techniques, and expert judgment.
     - Plan risk responses—strategies for negative risk or threats, strategies for positive risk or opportunities, contingent response strategies, and expert judgment.

3. Execute the review process:
   - Generate (completed by the security officer) the spreadsheet with the current user population using the ERP system(s), with the associated environments, menu masking, programs, business unit and function key securities to which the users have access. The human resources (HR) specialist provides the review team with the job descriptions currently on file.
   - Perform an analytical programmatic review (figure 2) (performed by the review team), and send the spreadsheet draft for discussion.
   - Complete iterative deliberations between the review team and the security officer.
   - Generate the pre-final spreadsheet (generated by the review team).
   - Implement pre-final recommendations (completed by the security officer).

4. Monitor and control the review process:
   - Control the review schedule.
   - Manage rollbacks:
     - Receive requests for rollbacks.
     - Review rollbacks for risk.
     - Perform discussions on rollbacks with user teams.
     - Approve rollbacks, if found justified.
     - Implement (by the security officer) approved rollbacks.
   - Control risk—risk reassessment, risk audits, variance and trend analysis, technical performance measurement, reserve analysis and meetings.

5. Close the Sarbanes-Oxley annual review project:
   - Complete reporting and attestation of the Sarbanes-Oxley annual review for the fiscal year. File the final spreadsheet.
   - Note and file the lessons learned in the review.
   - Update job descriptions of users (completed by the HR specialist).
   - Update the risk register.

THE ANALYTICAL PROGRAMMATIC REVIEW

At first a risk assessment may be done identifying program areas as high, medium or low risk. If there is a stiff time deadline, the focus is on high- and medium-risk areas. High-risk areas are those relating to revenue and cost. Medium-risk areas are those relating to selling, general and administrative overheads. Other income and deductions are low risk. For risk management, the processes recommended by the Project Management Institute (PMI) could be adopted.

First, the environments being used by the ERP application need to be identified and the methods of promoting configurations from one environment to another need to be checked. Especially of concern are the interfaces to the production or live environment. Second, the list of menu masking (“a method of securing entire menus or individual selections on a menu by a user”) is examined on a need-to-have basis. Third, the programmatic (action code—concerned with Add, Change and Delete to a table) accesses are subject to scrutiny on a need-to-have or need-to-know basis. Fourth, business unit security (legal entities or business units being accessed) needs to be scrutinized once again on a need-to-have or need-to-know basis. Business unit security is a “passive security mechanism. If you do nothing, there will be no business unit security.” With regard to business unit and legal entity security, the need-to-have or need-to-know element should be considered as the user may or may not need to know what is being done by another legal entity. Sometimes this would also mean that new user groups or responsibilities (always ensure that users are linked to a user group/responsibility with the
requisite security) would be spawned as the user’s roles and responsibilities may be exclusive enough to warrant this. At times, therefore, inquiry-only access may be granted and may be enough for the user to perform day-to-day tasks. Fifth, function-key security (“allows one to set up security on function keys and/or options by forms or user”\textsuperscript{12} and can be used for reports and programmatic security) is examined—once again, on a need-to-have basis. Sixth, a list of unattended night operations (sleeper) jobs and people with access must be examined on a need-to-have basis. Also, the sleeper jobs for the entity need to be checked thoroughly. Finally, a list of functional users who have performed transactions and system adjustments (system specialist) should be corroborated with the user list from the security officer and placed under the microscope especially for material transactions.

Some examples of appropriate role-based security are to ensure separation of manufacturing users involved in work orders and sales order administrators involved in invoicing; separate accounts receivable users handling sales invoices from those handling cash applications; and separate accounts payable users entering vendor invoices from those processing payments. A risk-based focus is always an imperative so that one does not get lost in the woods with trivialities. A laser-shape focus, especially while analyzing high-risk areas (such as programs relating to revenue and costs), helps the perspective a great deal. Those requiring compensating controls could be, for example, when revenue-side programmatic accesses overlap with expense or cost-side accesses—such as in the case of drop ship orders (when the vendor ships directly to the customer) when a sales order administrator generates a purchase order back to back. Always bear in mind that section 404 of Sarbanes-Oxley ultimately drives all this with its objective of having an adequate internal control system structure in place (figure 3).

Then the most important thing to consider for section 404 is to examine the trial balance generated by the ERP system and reconcile it to the numbers in the financial reporting software. Usually these are separate software in large corporations. Besides, given that the financial reporting software ultimately provides the numbers in the annual report and is available in the public domain, this is a key area. The controls associated with this are critical and need to be a mandatory target for access controls and internal controls to ensure accuracy of...
the numbers. Besides, people responsible for the financial reporting should not have access to do manual journal entries (figure 2). Users doing cash or bank reconciliation should not be involved in the operational aspects, doing cash or bank receipt applications and cash or bank payments. And the payroll administrator should not have access to make payroll payments in the ERP’s HR suite.

**THE PRIMARY SARBANES-OXLEY REVIEW TEAM AND THE ANALYTICAL REVIEW**

The primary review team needs an internal audit manager, an HR specialist, a finance specialist, an ERP specialist and an ERP security officer. For the purpose of explanation, call this team Team Composition A. The internal audit manager serves as the facilitator for the discussions. The HR specialist brings the job descriptions as of that fiscal year. The security spreadsheet from the ERP security officer details the security roles each person has on the ERP application. The ERP specialist contributes what each program does and its functionality. The team then works through this and the output is a color-coded spreadsheet following the stop-light approach (figure 3). Red indicates access that needs to be removed. Amber indicates items that need further thought and iterative discussions with the ERP security officers (they have an in-depth knowledge of the ERP security system). Green indicates those users who can maintain status quo. Next on the agenda is a preimplementation review meeting. The output of this meeting is that the recommendations become dual color as red means that accesses needed removal and green means that status quo could be maintained until the next review.

There is a need to budget for business down time during the period in which the security officer implements the recommendations. Strong requests to roll back some of the recommendations may be the order of the day. Users may, for example, voice strong arguments for access that the review team thought unnecessary.

Over the years, the team members achieve a rhythm in their work; go through the “forming, storming, norming, performing phases”, and actively challenge each other, if required, without conflict. But specialization does not easily keep in step with business growth. While suitable for an organization of fewer than 1,000 employees, growth beyond that would need a different team composition, much like Team Composition B (figure 4).

**THE FINAL FRONTIER SARBANES-OXLEY REVIEW TEAM**

The team members involved in Team Composition A would not know the shifting sands of time in terms of the users’ current roles and responsibilities as the business roared ahead. This is where the business leaders (executive-level management) bring in their expertise in terms of the needs of the business and how that translates in terms of roles and responsibilities for various users of the ERP systems. Moreover, the business leaders are

---

**Figure 3—The Applications Programs Associated With the ERP in Use**

![Figure 3](source: Frederick G. Mackaden. Reprinted with permission.)
the data owners for operational areas of the business. They are responsible for the sales-order processing, purchase-order processing and work-order processing. For finance, the relevant business unit finance controller or director becomes the data owner. This is how the futuristic Team Composition B (Figure 5) evolves when business unit leaders or their knowledgeable delegates join the review team.

Multiple points of view may coalesce as shown in Figure 5. The security team would also engage in training business unit leaders and acting as the final sounding board and implementers of the annual review—this time, hopefully, without any rollbacks. Team Composition B may run into problems, especially as decentralization brings delays and with the difficulty of educating business leaders (for more strengths and weaknesses, refer to Figure 6). But the central Team Composition A would also need to help educate and develop the new business-savvy team members. This also conforms to the idea that such “knowledge is not only valuable in itself but can contribute to the wise government (of the corporation) and reform.” Rollback requests would be extremely minimal as the business takes responsibility for annual reviews. Another future area for consideration would be the possible automation of the process, where possible.

**Other Basic Areas to Be Reviewed**

The other areas that also need to be considered, in addition to application access and associated controls, are physical access and its associated controls and network access and its associated controls. With regard to physical access, the best access is through dead-man doors because of their inherent ability to prevent tailgating. As applications are hosted on a server, the access to the server would be only for people authorized through swipe cards and passwords. If wireless is used, the unauthorized access is checked through a firewall so that war driving is prevented. For applications, basic login is through a user ID and password. The password needs to have an expiry date not greater than 90 days, and unused user identities would need to be disabled after a period of 30 working days (assuming some users may take long holidays). When a user leaves the organization, network access must be disabled prior to departure and the physical entry access card must be returned to the organization.
CONCLUSION
A Sarbanes-Oxley review is not a simple task, and over time the complexity may increase exponentially in proportion to the length, breadth and depth of the business. It involves multiple departments and leads to revisions to job descriptions for the users concerned.

Following the initial analysis of the business, it is imperative to create a roles and user profiles matrix (figure 2) to identify the conflicting roles that need to be a focus for the Sarbanes-Oxley audit. Areas supporting the application also need to be checked for appropriateness for supporting the internal control structure. In this spirit lies the need to have “adequate internal control structure and procedures.”

A methodical approach, especially one with a project management approach, helps enhance the credibility and efficacy of the review. Furthermore, an approach with experienced team members ensures that the Sarbanes-Oxley audit is not “asking the ignorant to use the incomprehensible to decide the unknowable.” It evolves over time and the team can make recommendations that may involve a few rollbacks. Users and their managers understand that the process for rollbacks is not always simple. But the flip side is inaction. “Inaction….in the present means deep trouble in the future. Here…lies the threat to capitalism. It is what causes men who know that that things are going quite wrong to say that things are fundamentally sound.”

ENDNOTES
4. Ibid, p. 31
6. Ibid.
7. Howe, J. S.; The Sarbanes-Oxley Act at 10, Ernst and Young LLP, 2012
9. Ibid.
11. Ibid.
12. Ibid.
13. Op cit, Project Management Institute
14. Op cit, Stevenson, p. 34
15. Op cit, Sarbanes-Oxley