The Bulletin

protiviti®
Independent Risk Consulting

VOLUME 2 ISSUE 3

Achieve Sustainability by Integrating the Section 404 and Section 302 Compliance Processes

For most companies, the administrative burden encountered during the first year of Section 404 compliance warrants a fresh look at the overall compliance process. This issue of *The Bulletin* will focus on strategies for integrating compliance activities around Sections 404 and 302 of The Sarbanes-Oxley Act of 2002 ("SOA") with the objective of achieving sustainability of the internal control structure.

What is sustainability?

From a compliance standpoint, "sustainability" refers to the continuing effectiveness of two interrelated management imperatives:

(1) The repeatability and effectiveness of the internal control structure

(2) The cost-effectiveness of the organization's capabilities to comply with SOA, and Sections 404 and 302 in particular, over time

Why is sustainability important?

Sustainability is critical because of the dynamic environment in which organizations operate. When managers evaluate sustainability, they consider how effectively the internal control structure will continue to perform as change occurs, i.e., new systems are implemented, processes are changed, the workforce is reduced, new entities are acquired, and complex new accounting and reporting requirements emerge. An important aspect of sustainability is whether the organization's compliance approach will withstand scrutiny over time. When managers are focused on sustainability, they ask tough questions about whether the right structure is in place and whether that structure is conducive to ensuring the effectiveness of internal control over financial reporting and the adequacy of disclosures in public reports over time.

Integration of Section 404 and Section 302 compliance impacts sustainability

Going forward, management should think of compliance with SOA Sections 302 and 404 as a SINGLE requirement of continuous reporting. There are several reasons why this integration positively affects the sustainability of the compliance process:

- After the first internal control report is issued, the company's 302 executive certification will incorporate more explicit recognition of management's responsibility for internal control over financial reporting.

  To illustrate, the Securities and Exchange Commission (SEC) inserted the following new language in the amended Section 302 executive certification:

  > [The certifying officers] are responsible for establishing and maintaining… "internal control over financial reporting" and have… designed internal control over financial reporting, or caused such internal control over financial reporting to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.

  Going forward, this representation will be incorporated in each quarterly certification.

- There is significant overlap between "disclosure controls and procedures" and "internal control over financial reporting." Each quarter, the certifying officers must represent that they evaluated the effectiveness of the entity's disclosure controls and procedures. These controls and procedures include internal controls that provide reasonable assurance that transactions are properly recorded and disclosed in the financial statements. Thus, for the most part, internal control over financial reporting is a subset of disclosure controls and procedures.

- There are important interrelationships between Sections 302 and 404 with respect to timely reporting of significant deficiencies in internal control over financial reporting to auditors and audit committees. The quarterly executive certification states:

  > [The certifying officers] have disclosed, based on their most recent evaluation of internal control over financial reporting, to the auditors and to the audit committee all significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the company's ability to record, process, summarize and report financial information…

  Therefore, when company personnel identify deficiencies relating to internal control over financial reporting, they must escalate these matters in a timely manner, through a systematic process, to enable management to consider them for appropriate action and disclosure.

- The current quarterly executive certification already addresses the implications of change on internal control over financial reporting. The specific language in the certification is as follows:

  [The certifying officers]…have…disclosed in the report any change in the issuer's internal control over financial reporting that occurred during the issuer's most recent fiscal quarter (the fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the issuer's internal control over financial reporting.

  This representation is not only in play right now, it is a major reason why hundreds of companies have disclosed internal control related issues over the last 12 months.

- Quarterly reporting is as important as annual reporting because material weaknesses in internal control over financial reporting can arise from risks of misstatement to both. The Public Company Accounting Oversight Board defines a material weakness as "a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement in the annual or interim financial statements would not be prevented or detected." No certifying officer relishes the prospect of discovering control failures in the fourth quarter after issuing "clean" certifications during the first three quarters.

We present ideas for integrating Section 302 and Section 404 compliance using the four themes below.

Four integration themes leading to sustainability

First-year Section 404 compliance is just the beginning. Because annual Section 404 compliance, like quarterly Section 302 reporting, is an ongoing activity, management should strongly consider the following integration themes as they seek a cost-effective and sustainable internal control structure and compliance process:

(1) Implement an organizational infrastructure facilitating ongoing compliance with Sections 302 and 404 – This integration theme is discussed in depth in Volume 1, Issue 12 of *The Bulletin*, which is available at **www.protiviti.com**. That publication introduces three alternative structures for ongoing compliance: traditional internal audit, independent risk control group and embedded risk control specialists. These structures address the transition from a first-year project mentality to an ongoing process mentality. Management should "institutionalize" the compliance process by:

– Defining, resourcing and budgeting the necessary program infrastructure support to sustain the required controls documentation and testing

– Achieving unit management buy-in and acceptance, including the absorption of program costs into unit budgets

– Strengthening continuously the organization's entity-level controls, including its anti-fraud program

– Remediating unresolved significant control deficiencies as soon as possible so that company personnel can focus on change versus repairing prior year issues

– Coordinating controls validation activities throughout the year with interim reporting

The Section 404 compliance process can provide a "wake- up call" on sustainability. Note that the external auditor may conclude a material weakness in the control environment exists if significant deficiencies, previously communicated to management and the audit committee, remain uncorrected after a reasonable period of time. Therefore, if management is successful in keeping the list of control deficiencies a manageable "short list" over time, the internal control structure and the compliance process will be more sustainable.

(2) Establish accountability of process owners and others for internal control – Section 404 compliance should be process-owner driven, not project-team driven as it is for most companies during Year One. Now that the rules are on the table, management should work with the audit committee and external auditors to manage the audit process and ensure that controls evaluation activities are an integral part of ongoing business routines, are less intrusive and optimize the auditor's reliance on the work of others. As accountability for internal control and financial reporting is established throughout the organization, management should drive desired behaviors by:

– Requiring process owners and others, in accordance with their state of readiness, to understand, accept and own responsibility for all critical financial reporting controls, including controls around the vital "touch points" across business functions and traditional boundaries

– Developing effective control evaluation methodologies and delivering appropriate process owner guidance, training and support to facilitate the expected execution

– Articulating effective protocols with respect to (a) escalation policies, with emphasis on timely action and disclosure, and (b) remediation and retesting, with emphasis on strengthening internal controls and supporting ongoing compliance

– Appropriate and timely consultation with the disclosure committee when evaluating the disclosure implications of Section 404 assessment results

The challenge of creating accountability for processes crossing functional boundaries and traditional organizational hierarchies should not be underestimated. **A self-assessment process, linked to the Section 404 controls documentation, can be a useful tool to reinforce process owner and unit manager accountability for internal controls.**

(3) Implement an effective change recognition process – To comply with Section 302 reporting requirements, certifying officers need a change-recognition process that surfaces

new developments and events in a timely manner for subsequent follow-up and possible disclosure. An important aspect of change recognition is to ensure that the impact of changes in policies, procedures, people and systems on internal control over financial reporting is accurately reflected in the underlying controls documentation so that updates can be made to management's evaluation of controls design effectiveness and to management's testing plan for evaluating controls operating effectiveness. Steps management should take include (a) articulating and communicating responsibilities for identifying and reporting change in a timely manner, (b) establishing protocols for updating controls documentation for change and (c) examining disclosure committee performance versus charter.

(4) Identify and capitalize on additional improvement opportunities – For most companies, the first-year compliance process will identify opportunities to achieve (a) an appropriate emphasis on automated controls and preventive controls, (b) more targeted controls testing through better "filtering" of controls, (c) more mature business processes and (d) more predictable compliance costs going forward. Management should, among other things:

- Understand the interdependencies between IT general and application controls, and incorporate that understanding into the organization's controls documentation
- Leverage programmed controls embedded within ERP systems to (a) address deficiencies in controls relating to segregation of duties and key applications and (b) facilitate increased reliance on automated controls
- Align the cycle for new systems conversions and upgrades with the Section 404 compliance process, with emphasis on avoiding lengthy blackout periods for systems changes that slow down business innovation
- Optimize testing plans by confirming controls selection; assessing testing scope and timing; revisiting remediation, retesting and refresh testing methodologies; and integrating self-assessment techniques and entity-level monitoring into the organization's overall controls validation model
- Understand and select the appropriate technology solution to update and archive controls documentation going forward
- Formalize the process to assess, classify and dispose of deficiencies in a timely manner
- Identify and prioritize opportunities to improve efficiency, compress transaction processing cycle times, eliminate nonessential activities, and simplify, focus and automate manual processes, as discussed in Volume 2, Issue 2 of *The Bulletin*, available at **www.protiviti.com**

In summary, the message is that companies need to "institutionalize" their compliance process. As they do so, they should (1) budget and build the infrastructure required to sustain controls documentation and testing, (2) create process owner accountability for controls, (3) implement a change-recognition process and (4) "clean up" Year One issues with particular attention to technology issues.

How is sustainability evaluated?

First-year Section 404 compliance is not necessarily a reliable measure of sustainability. An audited, unqualified management assertion that internal control over financial reporting is designed and operating effectively may provide an *output measure* that confirms "the controls are in place." However, it does not provide the information boards and management need to understand the maturity of the entity's processes and how effective they are vis-à-vis its risk profile. Because continued acceptance of control deficiencies can lead to significant deficiencies over time and continued tolerance of significant deficiencies can lead to material weaknesses over time, boards and management need more than a simple "pass/fail" report to evaluate the effectiveness of the control structure. One possible measure, equivalent to a *process measure*, is the capability maturity model, which is a scale boards and management may find useful when evaluating the maturity of an organization's processes.

Adapted from the Carnegie Mellon Institute, the model provides five states for rating the maturity or capability of any process ranging from "initial" to "optimizing." The higher the state of maturity, the more sustainable the process. The more sustainable a given process, the more effective the entity's internal controls within that process in reducing risk. Following is a brief description of each state:

- At the *Initial State*, internal control is fragmented and ad hoc. The organization manages individual risks and controls in silos and is generally reactive. Policies and formal processes are lacking, so the organization is dependent on people acting on their own initiative to "get things done." The Initial State is rarely sustainable because the significant inefficiencies that characterize this state drive high costs, many of which may be unknown to management, as well as high potential for error.
- Moving to the *Repeatable State*, the organization's capabilities are improved with a basic policy structure, basic processes and controls, and increased clarity as to defined roles, responsibilities and authorities. The "repetition" that is taking place is a result of increased process discipline and established guidelines. There is still reliance on people at this state; therefore, accountability

is an issue. However, this state is also characterized by high costs, and process and controls documentation is still lacking.

- As companies progress to the *Defined State,* policies are further developed and processes further refined as controls awareness takes hold. Process documentation is kept current using appropriate point technology solutions. Risks of errors are sourced within the processes, and key controls that mitigate these risks are identified; however, there isn't reasonable assurance that all significant gaps are identified. Process owners do not self-assess processes against established control standards linked to the controls documentation supporting management's internal control report.
- The *Managed State* of capability is more quantitative, with entity-level analytics and monitoring. Performance measures provide the basis for management to determine whether mitigating controls are functioning as intended. The operating effectiveness of the most critical control activities is evaluated periodically. Process owners self-assess the controls for which they are responsible and report the results to management, establishing a "chain of accountability" linked to the Section 404 controls documentation. Internal audit plans focus on evaluating the quality of process owner self-assessments.
- At the *Optimizing State,* the organization continuously improves the process capabilities developed during the prior states. Organized efforts are made to remove inefficiencies with formal cost/benefit analysis applied to process activities and controls. Entity-level monitoring and "dashboard" analytics are fully operational, with real-time reporting and early warning systems driving timely, informed decisions. Process owners use appropriate platform technology solutions to keep the controls documentation current and facilitate identification and sharing of best practices across the organization. This state achieves the greatest ongoing efficiencies in the design and operation of the entity's processes.

The capability maturity model is a powerful process-oriented tool for evaluating sustainability. Using this model, management rates the enterprise's processes in key areas affecting financial reporting, identifies gaps based on the level of capability desired in specific areas and shifts the dialogue on operating metrics to incorporate appropriate emphasis on process maturity. The model provides a valuable framework for facilitating substantive, fact-based dialogue among audit committees, certifying officers, Section 404 project committees, internal auditors and others regarding the capability of the organization's processes as compared to the higher risk areas identified in their risk assessments. Armed with this tool, boards and certifying officers can assure themselves that process improvements are focused on the areas of greatest concern and exposure.

Summary

Certifying officers should focus on achieving sustainability through a repeatable and cost-effective compliance process. The more sustainable the control environment, the more capable the organization's processes and controls in dealing with change. Sections 302 and 404 of SOA provide the "launching pad" to improve the sustainability of the internal control structure and, in turn, enhance the reliability of the financial reporting process over time.

Key Questions to Ask

Key questions for board members:

- Has management reviewed with the board its plan for implementing an organizational infrastructure facilitating continued compliance with Section 404? Does that plan include establishing accountability of process owners and others for internal control over financial reporting and implementing an effective change recognition process?
- Do you and management understand the interrelationships between Section 302 compliance and Section 404 compliance? Have you considered the implications of those interrelationships to the organization's compliance process?
- If there are unresolved significant deficiencies, does management have a plan to remediate them? If management does not have a remediation plan, have you and management considered the company's exposure to a material weakness determination by the external auditor if the significant deficiencies are not corrected within a reasonable period of time?

Key questions for management:

- Are you developing a more efficient and effective compliance process to ensure sustainability of the internal control structure and proactively address the implications of change in people, processes and technology? Have you reviewed your implementation plans with the audit committee?
- Are you improving your processes and controls to ensure sustainability and to seamlessly embed your compliance activities into your business processes?
- Have you defined, resourced and budgeted the necessary program infrastructure support for Year Two and beyond?
- Have you achieved operating unit management buy-in and acceptance, including an agreement to absorb program costs into unit budgets? Have you considered the change readiness of your organization's operating units and process owners for implementing your compliance process?