The Self-Assessment Process: Management’s Tool for Reinforcing Process Owner Accountability

In Issue 12 of Volume 1 of The Bulletin, we discussed the organizational structure needed to facilitate ongoing compliance with Sections 404 and 302 of The Sarbanes-Oxley Act of 2002 (SOA). As discussed in that publication, one of the cornerstones of this structure is an effective self-assessment program. This inaugural issue of Volume 2 of The Bulletin discusses the self-assessment process and how you can implement one to reinforce process owner accountability or, if you already have a process in place, how you can improve it and make it more effective.

What is self-assessment?

Self-assessment is a recognized best practice and has been applied to risks and controls for many years. Systematically applied across the organization at the entity and process levels, self-assessment is a pre-determined approach whereby individuals self-review or self-audit the controls for which they are responsible AND communicate the results to appropriate management. In response to the upward reporting of process owner assessments, follow-up is taken where necessary. Used in combination with an effective entity-level monitoring process and periodic controls testing, self-assessment is a powerful and flexible element of an ongoing Section 404 compliance program because it enables certifying officers to receive, from people who should know, a comprehensive statement that key controls are in place and operating effectively. Just as the internal control report provides assertions from certifying officers to investors, a self-assessment process reports upward relevant assertions from managers and process owners. These assertions provide clear points of focus for internal auditors as they plan controls testing.

Self-assessment is not a novelty. The Public Company Accounting Oversight Board (PCAOB) has pointed out that company-level controls include “controls to monitor other controls, including ... self-assessment programs.” Many companies have used risk and control self-assessments for a long time. While self-assessment may be limited to financial controls to support SOA compliance, the process is flexible enough to apply to other risk areas, such as compliance with other laws and regulations, and operational effectiveness and efficiency.

Why perform a self-assessment?

Self-assessment is a management tool that drives the “tone at the top” down to process owners by reinforcing their responsibility and accountability for internal control over financial reporting and other risk areas. Self-assessment sets expectations about policies and procedures. Companies embracing self-assessment often view it as a cost-effective technique for establishing “touch points” with the right people, enabling management to communicate as well as educate. An effective self-assessment program reports process-based assertions from process owners upward in the organization and identifies matters requiring follow-up and possible disclosure. Self-assessment supports the certifying officer assertions in the internal control report. It is an integral part of the transition from the intense project mode of first-year Section 404 compliance to an ongoing process in Year Two and beyond at costs that are reasonable and sustainable on an ongoing basis. These are important benefits to certifying officers and their companies.

Who performs a self-assessment?

Because process owners are the men and women closest to the critical control points within the organization, they are the ones who know what’s working and what isn’t, when process changes are occurring, and whether changes in procedures, systems and the workforce are impacting process performance. Process owners “own” the processes within which the controls are embedded. Control owners “own” the responsibility to execute the controls. Process owners both execute controls (as a control owner) AND supervise and monitor the execution of controls (by designated control owners). Process owners are ultimately responsible for assessing the design and the performance of controls. Self-assessment reinforces this accountability.

Clarify the process ownership issues

It is important to define roles, responsibilities, authorities and accountabilities over key financial reporting risks and the management of those risks. Generally, this task starts with the Section 404 documentation of the key controls and the owners of those controls. While the task
is not always easy to do, it is vital to identifying a process owner. To be effective, process owners must be authorized to do at least three things – they must be empowered to make decisions with respect to a process, they must be responsible for the adequacy of process design and they must monitor execution of the process.

The question of “ownership” is oftentimes obscured by the “command and control” structure of most organizations because that structure has always placed strong emphasis on managing silos. This leads to the need to control the critical interfaces or “touch points” among various functions that make the process work. There must be owners of the controls over these interfaces who are accountable for their effective operation. Thus many companies face situations in which process ownership must be clarified, particularly at the interface points within processes. These situations present a significant change management issue. The mere exercise of assigning responsibility can result in redrawing the scope of control responsibilities that previously existed for specific individuals. This can present challenges when deploying a self-assessment process because, to make self-assessment happen, every key control must have a name by it.

What controls are self-assessed?

Self-assessments are often completed for all of the company’s primary controls, i.e., those controls that are especially critical to the mitigation of financial reporting risk and the ultimate achievement of one or more financial reporting assertions. The Section 404 documentation lays the baseline for ongoing self-assessment. That documentation addresses such questions as:

- What are the key controls at the entity and process levels?
- What risks do they address?
- Who owns them?
- How are they rated as to design effectiveness? Are they adequate in mitigating the risks they are intended to address?
- How are they rated in relation to operational effectiveness? When tested, do they work and operate as intended?

The primary controls selected as most critical and significant for purposes of Section 404 compliance should be the focus of an ongoing self-assessment program.

How is self-assessment accomplished?

As discussed above, it is necessary to identify the key controls and the owners of those controls to begin a self-assessment process. In addition, self-assessment involves several key components:

- Predetermined questions approved by management – When process owners are required to respond to relevant questions regarding specific controls for which they are responsible, accountability is reinforced and transparency in the “chain of accountability” is created for internal control over financial reporting. The most effective way to develop relevant self-assessment questions is to base them on the documented key controls supporting management’s Section 404 assessment and the financial reporting assertion risks those controls address.
- Criteria for supporting responses to the self-assessment questions – Management must define the extent to which process owners are required to support their assessments. For example, process and control owners often use inquiry, observation and inspection techniques as they supervise and monitor the activities for which they are responsible to assess whether the controls are functioning properly. They may also use reports to evaluate the effectiveness of the process, e.g., suspense reports, aging of items in suspense and other substantive data analysis techniques provide an indication as to the effectiveness of internal control over processing transactions. These activities provide the basis for periodic self-assessments, as they are an integral part of day-to-day business activities. These activities may also be augmented by additional audit tests, administered by the process owners or by others assisting process owners (such as risk control specialists), to address selected controls. If audit tests are required, management should provide guidance regarding the scopes process owners should use in the organization’s testing plan.
- Rigorous deployment throughout the organization – A rigorous self-assessment process provides a powerful fact base, which enables certifying officers to sustain high confidence in the ongoing operating effectiveness of critical internal controls. Although the self-assessment process may be deployed in many ways, larger companies are using web-enabled assessment tools to implement it. Some of these tools include e-mail notification during different phases of the assessment process (e.g., scoring, management review, signoff, etc.) targeted at specific individuals. Others provide for control workflow (e.g., setup of action, monitoring and test plans) in a dynamic fashion by determining the answers that create workflow (e.g., actions and/or tests). These and other features make the process more intuitive, user-friendly and flexible. The process should also be documented. For example, an illustrative summary of the steps involved in the self-assessment process is provided on the following chart.
• Communication of results to management – Self-assessment results are a vital part of the written record supporting management’s assertions in the annual internal control report as well as the representations included in the quarterly executive certification. These results provide evidence, direct from responsible personnel, that the key controls are in place and are operating effectively. Results may be communicated through simple aggregation techniques used when compiling surveys. More sophisticated techniques such as “dashboard reporting” visually indicate aggregated assessment information (status, due date, action plan and test plans, for example) and provide for “drill downs” to the appropriate level.

• Timely follow-up when issues arise, including resolution of exceptions and open matters – Once potentially significant deficiencies are identified, they should be evaluated on a timely basis. Keep the following in mind:
  – If unresolved control deficiencies “stack up,” there is a risk the external auditor could conclude the deficiencies, in the aggregate, comprise one or more material weaknesses in internal control over financial reporting. If there is uncertainty over a multitude of unresolved deficiencies, legal counsel may also advise public disclosure to protect management.
  – Respondents may add “gratuitous comments” that create risk for the company unless the company deals with them adequately. Comments left unaddressed are discoverable and could create risk of embarrassment later unless the appropriate people review them and follow-up.
  – If a process owner surfaces a potentially significant deficiency, then typically he or she should be involved in the subsequent resolution of the matter. However, if upon investigation management concludes that the matter is not a significant deficiency, the reporting process owner should be informed of management’s assessment and how the matter was resolved – particularly if the process owner did not participate in the decision-making process.

• Frequent internal audit testing – The effectiveness of self-assessment is evaluated in terms of the quality and reliability of the assurances the process provides to certifying officers. Therefore, internal audit should test selected controls to evaluate the quality of the assertions reported through the self-assessment program. In such instances, internal audit’s testing work product should be documented “outside” of the self-assessment program used by process owners.

These six components are integral to an effectively functioning self-assessment process. When scoping the level of effort required to initiate and sustain the assessment program, management must first consider the extent to which process owners are required to support their assessments and set appropriate metrics around execution.

How often are self-assessments conducted?

Self-assessment is so versatile and flexible in application, management can conduct the process as often as desired. Technology-based solutions are designed to provide the flexibility to conduct the self-assessment process continuously or as of the end of any period, including year-end and quarter-end. This form of validation enables management to confirm controls operating effectiveness at any time. Self-assessments can also be conducted all at once, or staggered over a period of time. Conducting these assessments on a regular and recur-
ring basis allows the organization to reinforce the importance of the internal control structure, which is a priority once the initial internal control report is filed.

**What is done with self-assessment results?**

Self-assessment results provide a body of evidence supporting management's assertions in the annual internal control report. While self-assessments should be performed for the primary and critical controls, they cannot be relied upon as the sole source of evidence supporting management's conclusions regarding internal control over financial reporting. For primary controls, for example, other forms of validation are needed through entity-level monitoring and tests of controls to support management's assertion as to controls effectiveness in the annual internal control report. Therefore, self-assessment complements other sources of evidence to provide certifying officers assurance that the primary controls are operating as of a point in time, e.g., at year-end or quarter-end.

There are three relevant questions that define the reporting protocol for a self-assessment process:

- **How are self-assessment results reported?** – This question is about defining how results are aggregated, whether by process, by location, by unit, by group or by geography. Dashboard reporting and flexible tools facilitate customization of reporting according to the organization's needs. Exceptions and negative responses warrant attention to understand and evaluate the impact and remediation plans. Positive responses (i.e., controls are working) require periodic validation over time to assess their reliability.

- **From whom are self-assessment results reported?** – This question deals with who reports the results. Is it the control owners, the process owners, or the unit or functional managers? Judgment is often required to evaluate the focal point for self-assessment. For example, it may be desirable, although somewhat unwieldy, to require each control owner to report his or her self-assessments. Alternatively, it may be appropriate for process owners (to whom multiple control owners report) to communicate their self-assessments. Finally, reporting could come from each manager to whom multiple process owners report – a reporting model that could be elevated as high as unit and functional managers.

- **To whom are self-assessment results reported?** – This question deals with who receives the results. Management should consider such alternatives as the certifying officers, the disclosure committee and/or the Section 404 compliance committee. The audit committee may want to receive a summarized version of the self-assessment results. In addition, applicable operating unit and functional managers should be privy to self-assessment results involving their respective process owners, and their participation should be requested when follow-up is necessary for matters requiring remediation.

On the matter of reporting, process owners, control owners and internal audit must be provided with a process for escalating potentially significant deficiencies and other internal control issues outside the formal reporting process to highlight them for resolution as soon as practicable. Parties responsible for all significant aspects of financial reporting should be requested to surface internal control issues in a timely manner for evaluation, particularly during the quarterly reporting season.

**Instill the appropriate discipline**

However management chooses to design the self-assessment program, appropriate discipline should be instilled into the process so that (a) control deficiencies identified by process owner self-assessments (as well as by risk control specialists, by internal audit and by external audit) are reported by source, and (b) progress from evaluation of the deficiency to completion of remediation is carefully tracked. In addition, everyone who is expected to complete a self-assessment should be monitored to ensure that they do so. An SOA program management organization (PMO) or internal audit may administer the program to instill discipline.

**Some best practices to consider**

Following are specific practices we recommend each organization consider, whether they are implementing a self-assessment program or evaluating an existing program:

- **Link the self-assessment process to what matters.** Make the process more robust by linking it to the priority business processes, specific risks and critical controls that have been identified by the Section 404 compliance process and that support management's assertions in the internal control report. In addition, make it an integral part of the disclosure process and continuous monitoring required by Section 302 reporting.

- **Consider the organization's culture when implementing a self-assessment program.** Whether implementing a new program or modifying an existing program, there may be change management issues. For example, is there an open culture in the organization that facilitates upward communication of assessments, good as well as bad? Is there sufficient clarity as to process ownership, such that process owners consider controls over the interfaces among functions that make their processes work? Some change management issues may surface when assigning ownership over specific controls.

- **Make sure the self-assessment process has substance.** Provide guidance to your process owners as to what is expected of them in supporting the assessments they submit. Let your process owners know internal audit will periodically review the basis for their assessments. Make sure the internal audit plan is aligned with the self-assessment program. Most importantly, make sure the self-assessment process is well-defined, informative, value-added and efficient enough to warrant manage-
ment’s insistence on process owner participation and time investment.

- **Get management involved.** Engage the operating unit managers by making them privy to self-assessment results and request their participation when follow-up on matters requiring remediation is necessary.

- **Coordinate the self-assessment activity with the company’s periodic reporting.** Complete the self-assessment process in adequate time to compile the results for use during the interim Section 302 certifications and the annual Section 404 assessment.

- **Follow-up timely on changes, deficiencies and exceptions arising from self-assessments.** Update controls documentation timely for changes in business processes and systems, fix control deficiencies timely, and document satisfactory resolution of gratuitous comments and control exceptions timely.

- **Begin preparations for Year Two implementation sooner rather than later.** Implement a full self-assessment program only after first piloting the program on a limited basis.

**Summary**

If your organization doesn’t have a self-assessment process, it should implement one. If your organization has a self-assessment process already in place, it should improve it. Self-assessment is a flexible management tool that drives the “tone at the top” down to the process owners by reinforcing their responsibility and accountability for internal control over financial reporting. An effective self-assessment program supports the quarterly Section 302 executive certification process and the annual Section 404 internal control reporting with process-based assertions and identifies matters requiring follow-up. It should be an integral part of the transition from the first year Section 404 compliance to an ongoing process in Year Two and beyond.

**Key Questions to Ask**

**Key questions for board members:**

- Have you inquired of management as to whether there is a self-assessment process in place that engages the organization’s managers and process owners responsible for internal control over financial reporting and reinforces their contribution to reliable reporting? If there isn’t such a program, how does management reinforce accountability for financial reporting within the organization going forward?

- Is the audit committee receiving candid and unvarnished information from management as to self-assessment program results or is it otherwise privy to the program results?

- If there is a self-assessment process in place, are you satisfied that management has instilled an open culture in the organization that facilitates upward communication of assessments, good as well as bad? Do you understand how management will consider exceptions and control deficiencies reported through the self-assessment program? Are you satisfied a “shoot the messenger” mentality does not exist?

- For private companies and not-for-profit organizations, have you inquired as to whether management has considered implementing a self-assessment program?

**Key questions for management:**

- If you have a self-assessment process:
  - How do you know it is working effectively?
  - Is the program linked to the priority business processes, specific risks and critical controls identified by your Section 404 compliance process?
  - Does the program consider the controls over critical interfaces or “touch points” among various functions that make your processes work?
  - Have you provided guidance to your process owners as to what is expected of them in supporting the assessments they submit?

- If you don’t have a self-assessment process:
  - Have you considered implementing one?
  - Are your process owners accountable for the design and operating effectiveness of internal control over financial reporting? Do they understand they are accountable?

- Is your self-assessment program an integral part of the disclosure process and continuous monitoring required by Section 302 reporting?

- Are your process owners vested with the responsibility to make decisions, ensure adequacy of design, and monitor the process and its controls? If not, are there gaps and overlaps in process ownership that could contribute to misunderstanding and control failures?
Protiviti continues to be recognized worldwide for its informative resource guides, helping directors and executives address key governance and other issues impacting today’s companies. Recently we released Guide to Internal Audit, a comprehensive publication containing more than 65 frequently asked questions about internal audit and the related New York Stock Exchange listing requirements. Public and private organizations alike have turned to this guide for the latest insights and information regarding their internal audit functions.

And now, those who rely on Protiviti’s highly regarded Sarbanes-Oxley FAQ guides will be pleased to hear we’ve issued the 3rd edition of Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements. The updated publication contains 90 new questions and well over 100 pages of new or substantially revised material. Those seeking expertise in all phases of Section 404 compliance, as well as related issues with respect to Section 302 compliance, will find this publication to be an invaluable resource.

Get the facts and learn what you need to know from the industry thought leader. Call 888.556.7420 to request a complimentary copy of Protiviti’s Guide to Internal Audit: Frequently Asked Questions about the NYSE Requirements and Developing an Effective Internal Audit Function, or Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements.