As organizations look toward year two of Sarbanes-Oxley, there are several steps they can take to ensure a more effective and efficient documentation process.

In the wake of first-year filings for Section 404 of the U.S. Sarbanes-Oxley Act of 2002, best practices in project management have begun to emerge that can save companies time and money. For the 20 percent of public companies that are nonaccelerated filers and U.S. companies with a foreign parent that have not yet completed their Section 404 work, now
is a great time to learn from the larger companies who have already filed and exceeded their budgets. For the companies that have already filed, there are lessons to be learned that can help save money in year two and beyond.

A typical Section 404 project incurs six major costs:
1. Business process documentation labor — mostly the flowcharting of processes that directly impact financial statements and the development of risk and control matrices.
2. Business process testing labor — testing and remediation to ensure controls are in place and functioning.
3. Information technology (IT) general controls documentation and testing labor — describing and testing general controls around IT systems, namely data centers, computer networks, hardware, and operating systems.
4. The review and edit of resulting documents — a quality control process to ensure appropriate review of documentation before completion.
5. Documentation and testing tools — either Web-based or application software used to gather and store results of documentation and testing.
6. Audit fees — costs incurred for the review of documentation produced during the project and the subsequent tests conducted by auditors.

Within this article are several strategies for managing an effective and efficient documentation project for Section 404 of Sarbanes-Oxley. The article should not, however, be considered all-inclusive of appropriate procedures and tests to comply with the act. In determining the propriety of any specific procedure or test, Section 404 project managers should apply their own professional judgment and should obtain the judgment of the company’s external auditors as to the specific control circumstances presented by the particular environment.

SELL THE PROJECT INTERNALLY

Without visible support from the top, it is unlikely that employees further down in the organization will participate in the project as actively as needed. One of the best ways to elicit participation throughout the organization is to conduct kickoff meetings. After educating the chief executive officer (CEO) and chief financial officer (CFO) about the requirements of Sarbanes-Oxley, the next step is to speak directly to the CEO’s staff. During these presentations, it is important to emphasize that Sarbanes-Oxley is a law, and the consequences of noncompliance could harm relationships with customers and vendors and adversely affect the share price of the company’s stock.

Further down the organization, the project team should educate employees on Sarbanes-Oxley and give them an estimate of how much time they will spend participating in the Section 404 project. Often, it will be less time than they expect. For example, if there is a separate documentation team, employees will only be interviewed regarding processes in which they are involved. These meetings may only take an hour each, and it may require only two or three of these meetings to document an entire process.

STRATEGIZE DOCUMENTATION LABOR

If outsourced, documentation labor will be one of the most expensive components of a Section 404 project. Therefore, it is important to correctly identify the roles of everyone involved. Suggested team roles include:

- Project manager. Among the project manager’s many responsibilities are coordinating project efforts and hiring for other roles. The project manager should have project and people management experience, audit experience, and presentation and communication skills, as well as knowledge of generally accepted accounting principles (GAAP).
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) frameworks, and Public Company Accounting Oversight Board (PCAOB) standards.
- Documenters/testers. Documenters interview the process owners, knowledge experts, operations owners, and IT applications administrators and recommend operational process improvements. Documenters must understand the business processes relevant to the company and should have communication and flowcharting skills, as well as internal audit experience.
- Librarians. By offloading routine tasks from busy employees, documenters, and outside contractors, librarians can save much time in the project. Skills required of librarians include clerical and computer experience.
- Review committee. The review committee evaluates the importance of control gaps and decides the extent of remediation required. The committee must have knowledge of GAAP, the COSO frameworks, and PCAOB standards. Committee members also should have public company U.S. Securities and Exchange Commission reporting experience.
- Steering committee. This committee approves the scope, schedule, and resources dedicated to the project and monitors the project’s progress as reported by the project managers. Some steering committee members may overlap the review committee. Members of the committee should have executive-level decision-making, leadership, influence, and communication skills.

Well-trained documenters will save a lot of time on Section 404 projects. Before preparing any documentation, the project managers should meet with the documenters to ensure they understand the project’s scope and know how much detail to document, and to determine if existing resources are available that can speed the documentation phase. Additionally, documenters should follow a series of steps — predetermined by the project manager — to document each process.
**DEFINE THE SCOPE**

The company will save unnecessary work by clearly defining the scope of the Section 404 project. The project team should begin by deciding a materiality threshold for including processes in the project scope by consulting with the company’s external auditors. Typically, auditors recommend materiality based on factors such as revenue, earnings, working capital, and the like. The steering committee should approve overall materiality before the project begins.

Next, the team should identify relevant locations for performing documentation. Rather than documenting each of the company’s locations, it is more efficient to group locations that have similar procedures. Testing procedures, however, cannot be performed in a single location on behalf of multiple locations. External auditors likely will require at least a sampling of all locations tested, even if their procedures are the same.

The next step in determining scope is to develop a list of processes. There are several ways of ensuring a complete list:

- Obtain process lists from other companies in similar businesses.
- Review predefined lists that may be available in some Sarbanes-Oxley documentation tools.
- Review the aforementioned lists with process owners and others during kick-off meetings.
- Review the list of relevant processes with the company’s external auditors.

After obtaining a comprehensive list of processes, the list should be grouped into five or 10 supersets, or “business cycles.” An example of a business cycle is the “purchasing/expense cycle,” which would include all processes starting with a requisition and ending with vendor payment.

The relationship between each process should be determined. One way of identifying relationships is to flowchart each cycle on a single page using flowcharting software. “Simplified Expenditures Cycle (EXP)” on this page, represents each process with a single box. Arrows illustrate the relationship and flow between processes. Users can slide the boxes around the flowchart until the relationship between processes is correct. This method ensures that there are no overlaps or gaps from one process to another.

The project manager should mark those processes on the flowchart that contain transactions (e.g., create entries in subledgers or the general ledgers). These processes are most likely to have many risks and controls associated with them. The project manager should identify the information in these processes that is used to create transactions. The project team can follow these threads of information upstream (backwards) on the flowchart to predecessor processes that create the information. This enables the company to document only the portions of the predecessor processes that actually supply information to the transaction. It also spares the company unnecessary time in documenting entire predecessor processes.

Another method for identifying relevant processes is to score the processes numerically. Processes can be ranked based on:

1. The dollar amount of materiality flowing through the process. (Note: This is not the dollar amount of materiality in balance sheet accounts affected by the process. It is more likely the income statement amount.) Evaluators should keep in mind that aggregation can be applied to processes. It is not appropriate to describe processes so narrowly that individually they are immaterial, whereas collectively they would have been material.

2. The subjective amount of risk inherent in the process. Generally, there is more risk if there is less monitoring done of the process. Factors that may decrease the amount of risk in a process include:
   - There is simplicity to the process.
   - There is good existing documentation for the process.
   - The process is stable and unchanging.
   - There have been no audit deficiencies in the process.
   - Spreadsheets or databases are not used.
   - People involved are experienced, and their turnover is low.
   - There is good employee supervision.
   - No employees in the process access both assets and records.
   - Reports originating within IT systems are checked for accuracy.
   - Financial data in the process is compared to operating data.
   - Financial data is signed off at low levels in the organization.
   - Financial records are reconciled with physical assets.
   - Internal audits are performed and are effective.
   - Employees perform internal self-testing.

After ranking the processes, it is helpful to multiply the materiality and subjective scores, reaching a composite prioritization score.

The prioritization scores should be posted to the cycle-level flowchart. The end-result should be a complete picture of the process flow and the importance of individual processes in the cycle. The project team should discuss this picture with the steering committee and consult external auditors when deciding which processes to document for Section 404 and to what level. Processes that the company may want to exclude are those that have no effect on financial statement groupings (even though the transactions may affect individual accounts.

---

**Simplified Expenditures Cycle**

```
<table>
<thead>
<tr>
<th></th>
<th>EXP1</th>
<th>EXP2</th>
<th>EXP3</th>
<th>ETC.</th>
<th>EXP6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prepare a requisition</td>
<td>Issue a purchase order</td>
<td>Receive goods (transaction)</td>
<td>Pay vendor (transaction)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(1-5 SCALE)</td>
<td>(1-5 SCALE)</td>
<td>(1-5 SCALE)</td>
<td>(1-5 SCALE)</td>
<td></td>
</tr>
<tr>
<td>MATERIALITY</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>SUBJECTIVE RISK</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>PRIORITY SCORE</td>
<td>15</td>
<td>15</td>
<td>20</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>
```
within the grouping), processes that will no longer be performed as of the compliance deadline, and processes too far upstream — where the stronger controls are further downstream and closer to the transaction.

Once the final list of processes is completed, the team should number the processes chronologically within the cycle. For example, the expenditures cycle may contain process EXP-1 for preparing a requisition, EXP-2 for generating a purchase order, etc. This numbering system will assist in tracking the progress of documentation and review, particularly if a software tool is used.

The scope exercise should be performed for all of the cycles in the company before any process documentation work begins. The standard number of hours required to document a single process should be multiplied by the number of processes within each cycle to estimate the total documentation hours required per cycle.

**ESTABLISH PROCESS TEAMS**

At this point in the project, it is important to identify the people to interview for preparing the documentation. For most processes, four people should be identified:

- **Process owner** — the financial person who has managerial responsibility for the process.
- **Knowledge expert** — the financial person who works with the process on a daily basis.
- **Operations owner** — a participant who is familiar with the nonfinancial aspects of the process.
- **IT applications administrator** — the person who is most familiar with IT applications used in the process.

After identifying the process teams, the project manager can estimate the hours required of each team member. Each member can expect to spend three to four hours in meetings for each process as documenters gather and review their information. The total hours required from each employee can be based on the number of process teams to which they are assigned, multiplied by three or four.

Each documenter should work on only one cycle at a time. Documentation for each cycle should be planned based on the number of documenters, the number of processes within each cycle, the schedules of individual employee team members, and the hours required of them. Also, consider employee vacations, accounting closing and reporting schedules, and other non–Sarbanes–Oxley projects when scheduling the timing of documentation.

**STRUCTURE DOCUMENTATION AND ASSESSMENT TECHNIQUES**

Scheduling the documentation of processes within a cycle should begin with processes that cause financial transactions to occur. This helps identify the information used and avoid unnecessary documentation of information not used in the transaction.

The best documentation consists of four elements:

1. **A flowchart illustrating the process.** Flowcharts should illustrate each process. They should be drawn in a “swim lane” format, reserving a horizontal row for each person involved in the process. Any activities performed by a person should be shown on his or her row. Swim lanes help identify the segregation of duties, and help identify information and communication — one of the COSO requirements. The top lane should identify predecessor processes, which are feeding into the current process. The bottom lane should identify dependent processes — processes fed by the current process (see “Receiving Goods,” this page.)

2. **A risk and controls matrix.** A risk and controls matrix should be entered into the company’s software tool. The team must be sure to capture COSO and PCAOB elements as it identifies risks and controls.

The team can start with the assertions that management makes about the correctness of its financial statements and, by implication, the transactions comprising the accounts that go into controls. The team should identify whether each control:

- Is a key control. The definition of key control is still an item under discussion in accounting literature. Some audit firms have agreed that key controls are those that stop the most obvious and likely risks. For instance, the most obvious risk for a sales process would cause an overstated. Therefore, the key controls in the sales process would be those that prevent sales overstatement.

- Performs a monitoring function.
- Prevents fraud.
- Safeguards assets.
- Is a manual activity, an IT activity, or both. If the control relies upon an IT activity, then identify the relevant IT application. (Do not confuse IT application controls with IT general controls).
■ Prevents a risk from happening or detects a risk once it has already happened.
■ Is designed in such a way that it mitigates the risk.

Also, the project team should determine the frequency with which the control is performed and who performs the control, which will be important in identifying segregation of duties issues.

Documenters should suggest tests to verify that the control is effective and is operating. If there are no controls in place for a given risk, it may help the company if the documenter suggests what controls should be in place.

3. A segregation of duties matrix. Segregation of duties issues exist when a single individual performs more than one of the following functions: authorizing a transaction, entering data for a transaction, having custody of the underlying assets, or performing a control. For each transaction, team members should capture the names of the people — not the job titles — who perform each of these tasks. If any person does more than one of these tasks, segregation of duties issues should be researched further. The company’s software tool should be used to identify segregation of duties issues. A single segregation of duties matrix for an entire cycle is a good approach for capturing segregation issues occurring across related processes.

4. A handoff list. Handoffs of data occur when one process feeds another process. When documenting a single process within a cycle, it is important to remember the data passes from predecessor processes. Therefore, when documenting the predecessor process, evaluators should examine that data for risks and controls as well. Sometimes, a risk in one process is mitigated further downstream in a subsequent process. Evaluators should use a handoff list as a reminder to describe these downstream controls when eventually documenting the downstream process. A handoff list is a good way of tracking process interdependencies (see “Handoff List,” this page).

**CONDUCT PROCESS TEAM MEETINGS**

To minimize the number of necessary meetings, it is important that the documenter come prepared for the session with the information listed previously — assertions, possible risks, handoffs, etc. — and that each member of the documentation team (process owner, knowledge expert, operations owner, and IT applications administrator) be present in a single meeting. If several people are involved in related processes, it may be useful to hold a single session to discuss several processes at once and minimize the effort to gather the right people for multiple meetings.

The project team should use a large white board or projector to draft the documentation flowchart. The swim lane flowchart should show where in the process the control is performed. These controls should be identified with a symbol on the flowchart. The symbol should cross-reference to the matrix where the control is described further.

In addition to the flowchart, risk and controls matrix, segregation of duties matrix, and handoff list, information that should be collected during these meetings includes:

■ General ledger accounts affected by the process. The company’s software tool or an Excel spreadsheet should be used to cross-reference each process to each general ledger account. This will save the external auditors time later, because they will want assurance that each significant general ledger account has been documented in one or more processes.

■ Document samples and screen prints. These should be stored with the process documentation and used when performing a walkthrough and determining testing procedures.

■ Names of third-party outsourced vendors who perform crucial activities in the process. These include vendors such as an outside payroll processing service, or a third-party warehouse to receive and ship goods and store inventory.

**EVALUATE CONTROLS AT THIRD-PARTY VENDORS**

If critical controls occur at a third-party vendor, it is important to document and test those controls as well as underlying IT systems that may be used. Often, third-party vendors have an audit report prepared so each of their customers will not have to sponsor an audit of their own. The audit report acceptable for Sarbanes-Oxley Section 404 is a SAS 70 type II report.

To use the SAS 70 type II report, the timing of the report must be close enough to the company’s year-end so the controls described can reasonably be expected to remain in place within the last six months of the fiscal year. Additionally, the report must cover controls the company is relying on, and those controls must be sensitive enough to detect an error that is material to the company. This dollar amount may be significantly less than what is considered material by the third-party outsourced vendor.

Small vendors may also strive to pass along the costs of an SAS 70 report to their customers. Due to these conditions and the inherent risk in trusting a vendor, the company may find that it is best not to rely upon the controls at the third party, and instead build controls around the third party, within its own operations. This may be particularly true for small third-party vendors.

**IMPLEMENT QUALITY CONTROL**

One of the best ways to avoid errors and to ensure the Sarbanes-Oxley project will work well is to document just one process — not an entire cycle — from start to finish as a pilot. The pilot process selected should involve transaction posting where key

---

<table>
<thead>
<tr>
<th>Handoff List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SENDING (PREDECESSOR) PROCESS</strong></td>
</tr>
<tr>
<td>Issuing a purchase order — EXP2</td>
</tr>
<tr>
<td>Receiving goods — EXP3</td>
</tr>
</tbody>
</table>
controls and gaps may be found. Additionally, the company’s review team, external auditors, and senior management can review the pilot to understand the company’s approach.

After documenting all processes within a cycle, the documenters should select one or two records as far upstream as possible — for example, the first process in the cycle — and trace these records through to the last process in the cycle. This will ensure that flowcharts and other documentation are correct. This is an important step, because the external auditors will perform a similar walkthrough and base their opinion on it.

A review team, consisting of the company controller, project manager, a documenter, overall cycle process owner, and a high-level IT manager, should decide which gaps could create material misstatements in the financial statements, and which gaps are not significant. The group will also determine which gaps need remediation and may propose various remediation ideas.

Establishing a quality control process for the documentation produced as part of the project will save time for all parties concerned (see “Quality Control Review Process,” this page).

PERFORM TESTING
Both COSO and the PCAOB require that testing be performed to validate controls are in place. For the first year of compliance, testing should be performed close enough to the reporting deadline so the company can be reasonably sure that tested controls will remain in place through the fiscal year-end. Also, tests should be performed early enough so that if operational deficiencies are encountered, there will be time to make corrections.

Tests should be designed so that a single test covers as many controls as possible. It is best to select sample sizes from processes that are far upstream in the business cycle. For instance, if process A feeds process C, which feeds process D, then samples could be selected from process A and traced through processes C and D. Process B, however, would need separate samples selected. Required sample sizes for testing are still under discussion among large accounting firms, so it is important that the company consult with its external audit firm before beginning testing.

Some accounting firms are willing to use tests performed by the company to satisfy part of their own testing requirements. If this is workable with the firm, it will save the company audit fees. While this area is also under discussion between the large accounting firms and their clients, some general guidelines are emerging:

- The more independent the tester is from the process, the better. Ideally, an internal auditor would perform the testing. A second choice may be to have the company’s operations staff perform tests (for example, having the accounts payable manager test the accounts receivable processes and vice versa).
- The tester must be competent. This is another reason to use internal auditors for testing. If internal auditors are not used, then people who have experience in auditing or hold a certified public accountant certificate are a good second choice.
- In all cases, external auditors must perform most of the testing work in each process. In some areas, external auditors will want to perform all of the testing. In other areas, such as routine processes like accounts payable and accounts receivable processing, they may be willing to use a larger percentage of internal testing as a substitute for their own work.
Although it may be possible to document similar locations centrally, testing must be performed at a sample or at all locations. The purpose is to provide assurance that the required procedures are actually followed from one location to another.

External auditors may place more reliance on processes that have lower priority scores.

Again, before beginning work on testing, the company’s external auditor should review and agree to all of these requirements.

**Document The Control Environment**

Chapter 2 of COSO’s internal control framework requires that companies have an ethical workplace and that management and the board of directors place appropriate emphasis on controls. Application of the COSO framework requires that companies document the control environment. The American Institute of Certified Public Accountants sells a COSO Control Environment checklist on its Web site for US $35. This is a good tool to start with in gathering control environment documentation. However, the sections on Control Environment dealing with nonfinancial issues may be omitted from Sarbanes-Oxley documentation if the company’s external auditors agree.

In addition, wherever IT applications provide controls to business processes, there is a need to document and test controls for data centers, networks, operating systems, and client-server and Web-server databases supporting those applications. *Control Objectives for Information and Related Technology (COBIT)*, developed by the IT Governance Institute (ITGI), is sometimes used as an operational and compliance guideline for IT managers. In 2003, the ITGI published the document, *IT Control Objectives for Sarbanes-Oxley*, which addresses the financial reporting aspects of COBIT. The ITGI document is a cross-reference between COSO and COBIT. While COBIT has 34 IT processes and 318 detailed control objectives, the *IT Control Objectives for Sarbanes-Oxley* has just 27 IT processes and 136 detailed control objectives. This is an excellent starting point for examining IT general controls required for Section 404.

The company should review this document with its external auditors to see which sections specifically apply to the company and IT environment. Some areas that the external auditors may waive are strategic planning, human resources, system acquisition, service levels, performance and capacity, and disaster recovery.

**Make Improvements**

Section 404 documentation and testing present unique opportunities for improving operations. There are significant advantages in having dedicated resources review every financial process in the company. Documenters with creativity and experience will find many opportunities for process improvement— not necessarily improvements in internal controls, but rather improvements in the processes themselves.

There should be a repository for accumulating these ideas for follow-up later as part of another process improvement project (see “Documentation Software Tools,” this page). Some documentation software tools include a place to enter and track these process improvement ideas. If the company’s tool does not provide such a feature, a document on a shared network drive will suffice. Many companies used Excel to document their first-year projects and now will need to collect their work into a software tool.

Although complying with Section 404 of the Sarbanes-Oxley act is expensive, with top management endorsement and good project management strategies, the cost can be reduced significantly. In addition, efficiencies gained through process improvement opportunities may even pay for much of the effort.

*To comment on this article, e-mail the author at bdouglas@theia.org.*

---

### Documentation Software Tools

<table>
<thead>
<tr>
<th>CAPABILITIES</th>
<th>SPREADSHEET</th>
<th>DATABASE</th>
<th>WEB-BASED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share controls and tests between documenters</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Ensure pre-defined and uniform data capture</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Run consolidated reports for all documenters</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Easy to set up</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Customize screens</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Customize reports</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Responsive (no latency)</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Low cost</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>E-mail notification</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Number of simultaneous users</td>
<td>1</td>
<td>about 5</td>
<td>dozens</td>
</tr>
</tbody>
</table>

This article was reprinted with permission from the June 2005 issue of *Internal Auditor*, published by The Institute of Internal Auditors, Inc., www.theia.org.