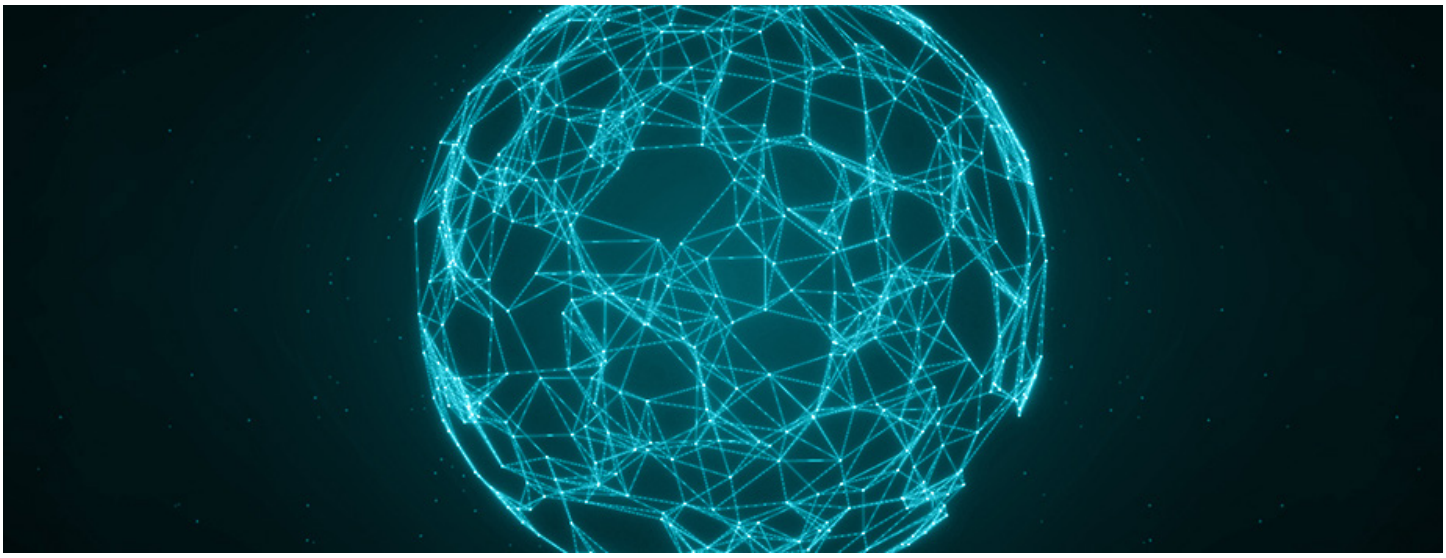
Deloitte.



Deploying internal controls: What private companies can learn from public entities

Leverage the lessons learned from public companies

When the Sarbanes-Oxley Act of 2002 (SOX) was first enacted, many publicly held companies viewed its financial reporting requirements to be a complicated and costly compliance exercise. A significant part of that was establishing and maintaining an effective internal controls environment.

Yet during the years since SOX's enactment, it has become clear to many public companies that the benefits of an effective internal controls framework can balance some of the investment and effort required. In fact, many companies now view internal controls as an integral part of operations that can help mitigate risks and add business value, which supports the company in achieving its operational and financial objectives.

If public companies believe internal controls are beneficial—perhaps even a competitive advantage—shouldn't private company owners, executives, and investors give them another look? In a previous point of view, we explained what internal controls are, why they are important, the role of a risk assessment, and how to apply the results of the assessment in a private company.

Here, in the second of three points of view, we offer insights on internal control design and implementation. In our final point of view, we'll explain how to sustain, monitor, and rationalize your controls over time.

Start by digging deeper into identified risks

Designing and implementing controls to manage business risk is a multistep process. A risk assessment (the subject of our first point of view) can help you identify which processes might be susceptible to errors and create quantitatively and qualitatively significant risks for your company. With the results of the risk assessment in hand, it's time to develop a clear picture of "what could go wrong" in each area—a prerequisite to designing effective internal controls. Some questions to consider include:

- Who is involved in the process?
- Do those individuals involved have conflicting responsibilities?
- What information is used in the process, and what could cause that information to be incomplete or inaccurate?
- How frequently or infrequently do these processes occur?
- What would be considered a deviation in the process?

When designing controls to mitigate the "what could go wrong," several general questions can help guide you, including:

- Who should perform the control?
- What is the control activity that should be performed?
- When should the control be performed?

- How often should the control be performed, and are there triggers for control performance?
- What information is used in, and/or is necessary for, the proper execution of the control process?
- What is considered to be a deviation in control performance, and what requires further investigation?
- Is there a level of aggregation or predictability to the information?

As a more specific example, consider the risk of error or potential fraud in the reconciliation of an account balance to a bank statement. You might ask the following more detailed questions to understand where and how an error or fraud might occur:

- What items are being reconciled?
- Who performs the bank reconciliation?
- Who reviews the reconciliation?
- What information is needed to execute the reconciliation?
- When and how often is the reconciliation performed?
- What factors trigger reconciliation?
- What items in the reconciliation require investigation?
- Is there a level of aggregation or predictability to the information?

The answers to these questions can be used as inputs to design controls for almost any transaction or area of risk that your company identifies.

Then it's important to consider the approach, nature, and type of control you want to apply. This can vary as follows:

- *Approach* – Is the control preventive or detective?
- *Nature* – How will the control be executed: manually or through automation?
- *Type* – What type of control activity will be performed—i.e., verification, reconciliation, authorization or approval, physical controls and counts, controls over data or information, or controls with a review element (including management review controls)?

The assessed level of risk, whether higher, normal, or lower, should drive the answers to these questions, including the nature, approach, and type of control; how frequently the control will be performed; and the competence or seniority level of the "control owner"—i.e., the person who performs the control activity.

Such factors influence the level of complexity of the control. Typically, the higher the risk, the greater the level of scrutiny placed on the control, such as requiring multiple levels of reviews and/or more senior-level individuals being control owners.

When determining the nature of the control to implement, it's generally preferable to leverage automation as much as possible. When designed appropriately, automated controls are inherently more reliable than manual controls due to a lack of judgment involved and a lower opportunity for human error once the control is implemented.

Cost is another potential deciding factor between automated and manual controls. It should be no surprise that there may be a cost to implementing automated solutions, most likely software-related, but once they are implemented, the return on investment can be quick and sustainable.

Controls can also be designed to either prevent or to detect an error. For example, you could implement a preventive control requiring review of invoices and requests for cash disbursements prior to issuing payments. Alternatively, you could implement a detective control that matches all payments to invoices at the end of a period.

The level of personnel executing each aspect of the control can also vary depending on delegation of authority levels, which can be broken down by dollar thresholds. For example, higher dollar values might require a higher level of approval.

The variability, or lack thereof, may also drive the frequency with which the control operates. For example, if your company has fixed assets and is in a mature, built-out office where additions and improvements are infrequent, you may want to perform a quarterly reconciliation of fixed assets. On the other hand, if your company is building out a new manufacturing complex and production lines, you may want to reconcile the fixed assets account monthly.

Other considerations

Almost all companies have some controls that are integral to their business operations, such as:

- A budget- or forecast-to-actual control
- A control to identify inappropriate or unauthorized uses of cash
- A control to prevent or detect misappropriation of physical assets (inventory, property, etc.)
- Account reconciliation controls
- If not already included in the above, a control designed to prevent or detect fraudulent or erroneous material entries into the accounting system
- IT general controls, including system access security and change management

If such controls are already in place in your company, you'll want to decide whether to stay the course with them as they are currently designed or consider whether they should be enhanced or replaced with new controls.

One area that companies may struggle with is segregation of duties. That's a key element of internal controls where multiple people are involved in a process to ensure that no one individual is performing contradictory activities. For example, if you are evaluating the design of controls over your company's cash reconciliation process, you can assess how separation of duties is carried out. You might want to make sure that there are controls in place to receive bank statements directly, limit the number of people who have access to online banking, and be confident that the person completing the reconciliation is not the one who disburses the funds.

It's also important to know whether existing controls or those being designed are dependent on other controls or on information that should be considered. If the information being used in the control is not complete or accurate, the overall reliability of the control itself could be compromised from the start.

Finally, there is no magic number of internal controls. The size, scale, and complexity of your organization and its associated risks should determine the nature and extent of the controls required to effectively manage the business. There is no one-size-fits-all approach, regardless of the industry your company operates in. And, while there may be some "standard" controls for common accounts and processes such as cash and accounts payable, your company's internal control framework, just like its risk profile, is going to be unique.

Implementation: Where the rubber meets the road

As you deploy your controls, it's important to document them step by step. This may seem basic, but the control owner should clearly understand:

- The key pieces of information they are using in the control
- Where this information comes from
- Any procedures they must perform to validate the information
- How each step in the process works to execute the control
- Who to contact if they have any questions related to the process or if any they find any deviations
- The expected output of the control

Documenting this information and making sure the control owner understands and executes it appropriately should increase the reliability of the control. Yet it's not unusual for a small finance department to take an ad hoc approach to the documentation process—for example, pulling up information about account fluctuations and reasons for variances from budgets and relying on "knowledge in the room" for answers to questions. Without adequate documentation, it's hard to replicate a consistent, thorough review as the company grows and other people perform the control activity.

Proper documentation and training can also help with the consistency of data sources when performing a control, another area from which errors can arise. For example, if in one accounting period a control owner uses information from Report A to explain a difference and then uses Report B in the next period, and the two reports have different data sources, the control may not identify what it was designed to find.

A thoughtfully designed, consistent, and scalable control process is key. Documentation is important because it's your record of how the process should work and how the related controls should operate. This will help as you evaluate how the controls perform in the future to make sure they are operating as designed and continue to mitigate the risks you have identified.

Summing it up

As public companies have discovered over the nearly 20 years since SOX was enacted, effective internal controls can serve a higher purpose than compliance alone. It can also provide vital information to a management team about company performance, operational efficiency, and risk management. Through thoughtful internal control design, which takes into consideration the factors discussed in this point of view and which meets the specific needs of your private company, you can derive similar benefits going forward.

After designing and implementing the controls, it's time to step back and let them to operate. But it's also important to remain vigilant. In the final installment of this series, we'll highlight ways to sustain, monitor, and rationalize controls over time.

Contact us

Jessica Ackerman
Audit & Assurance, managing director
Deloitte & Touche LLP
+1 617 585 4762
jtackerman@deloitte.com

Theresa Koursaris
Audit & Assurance, senior manager
Deloitte & Touche LLP
+1 212 492 3666
tkoursaris@deloitte.com

Jim Traeger
Audit & Assurance, partner
Deloitte & Touche LLP
+1 713 264 2418
jtraeger@deloitte.com

Reshma Shah
Audit & Assurance, senior manager
Deloitte & Touche LLP
+1 312 486 2596
reshah@deloitte.com

Special thanks to Stuart Rubin for his contributions.

www.deloitte.com/us/accounting-advisory-transformation

Deloitte.