Deloitte.

# Internal controls and risk assessments: What every private company should know

## A matter of business risk management

Any business can benefit from having transparent financial and operational information available for decision-making and reporting to stakeholders. In fact, strategic business decisions increasingly rely on timely, accurate, and reliable information. Anything less can present a business risk for any organization, whether it's undertaking an important transaction, introducing a new product or service, or fulfilling a regulatory obligation.

As the owner, executive, or investor of a private company, what can you do to increase your certainty about the information coming to you from across the enterprise? Whether your company is venture-backed, funded by private equity investors, or a family business, internal controls are an important part of the answer as you grow.

In this point of view—the first of three—we'll explore what internal controls are, the role of a risk assessment, and how to apply the results of the assessment. The other two points of view in this series will address internal control design and how to sustain, monitor, and rationalize controls over time.

## What internal controls are and why they are important

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), in its 2013 Internal Control – Integrated Framework report, defines internal control as:

"A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives related to operations, reporting, and compliance."

No definitive requirement exists for private companies to establish a system of internal controls. As a result, there may be misconceptions that controls 1) are seen to slow the business down; 2) are not aligned with business objectives, resulting in duplication and gaps; 3) provide a false sense of compliance; 4) waste significant time and resources on manual interventions and activities; 5) do not leverage technological or digital capabilities to increase efficiency and effectiveness; and 6) do not consider changes in the business over time.

Contrary to those misconceptions, a system of internal controls should be viewed as an integral part of operations that can help mitigate risks and add business value. Simply stated, a well-designed risk management program that incorporates a system of strategic internal controls can help executives and investors effectively manage the organization.

Internal controls can be preventive or detective in nature; that is, designed to prevent something from going wrong or to detect if something did go wrong. Internal controls can also be manual or automated. Manual controls are typically performed by people in the company, while automated controls are usually built into software applications. As with any activity performed by humans, manual controls may add a layer of variability or inconsistency in performance.

Automated controls, once developed, should work consistently as programmed unless there is a change to the system.

Automated preventative controls might seem the logical choice for companies to implement, but there may be incremental costs associated with them, such as those related to the purchase, development, or implementation of software applications. For this and other reasons, many companies opt for a balanced combination of preventive and detective controls, some automated and others manual.

While no two organizations are alike, most businesses may already have internal processes in place that are not being leveraged as effectively as possible as internal controls and may include:

- Segregation of duties
- Authorization controls
- Reconciliation controls
- Physical inventory counts (if applicable)
- Periodic review of organizational performance, such as analysis of budget to actual
- IT general controls, including system access security, change management, and network operations

It's important to note that effective internal controls don't need to be complicated. They should be designed to address the particular risks the company may face and the specific information needs of management. Their performance should be consistent and repeatable. When they are a natural part of the process, they are likely to operate more effectively if they have been designed with the related risk in mind. This brings up two questions: What risks does your company face, and what controls will help mitigate them? A thoughtful risk assessment can help you find answers.

## The role of a risk assessment

A risk assessment can help you identify which critical processes might be susceptible to errors and create quantitatively and qualitatively significant risks for your company. It can help you determine what impacts the company might sustain if such errors occurred and help you focus on the ones that matter most to your business strategy and operations. Essentially, a risk assessment helps you critically think about and answer questions such as:

- Who are my stakeholders?
- What are our key business risks?
- What information can help us manage identified risks?
- How susceptible to error is the information we currently have, and how can that affect strategic decisions and governance obligations?
- What resources do we need to address these risks?

There are many factors to consider when performing a risk assessment, including:

- The industry in which your company operates
- General economic conditions
- The size and complexity of your organization
- Regulatory changes
- Your company's operational strategies and objectives
- A potential exit strategy—i.e., if your company plans to go public (whether traditionally through an initial public offering (IPO) or through a special-purpose acquisition company (SPAC)) or merge with or be acquired by another company

Other factors might also come into play. For example, what activities across the enterprise do you currently monitor? What questions do you regularly hear from your board of directors and other stakeholders? If your business has debt, what are the debt covenants based on? Bottom line: if the results matter to you or your stakeholders, they should be assessed.

Next, determine the level of risk that each operational metric, reported balance, or disclosure represents by considering:

- *Estimates and judgments* – Are there estimates, assumptions, or judgments in the amounts you are reporting? If so, how predictable are they? Are they the same period over period such that there is little judgment being applied, or do they vary? If they vary, on what is that variance based?
- *Quantitative materiality* – How large is the amount? The size of the account balance overall may increase the level of risk and focus. How is the amount accumulated? Is it made up of a high volume of low-dollar items, or does it consist of several larger items?
- *History of errors* – Is there a history of errors that have been found? If there is a history of processing errors or errors in the computation of an amount, that could lead to greater risk.
- *Complexity* – Is the calculation itself complex? Or is there complexity in the underlying inputs into the calculation? Do the inputs come from multiple data sources that require aggregation? Are each of those data sources reliable?
- *Related parties* – Are there transactions or considerations included that are with parties under common ownership or control that may not be indicative of arm's-length results? How should these be considered?

Answering questions like these can help you identify metrics, balances, and disclosures that have a degree of risk and importance associated with them. By categorizing and ranking these risks, you can begin to focus on what matters most and where opportunities exist to apply internal controls.

## Using the output of the risk assessment

Once you've identified and prioritized potential risks, it's important to understand the nature and extent of your company's exposure. That means analyzing related processes and identifying gaps or weaknesses that can lead to potential problems.

From there, you may want to refine the processes and implement controls where required. This might be accomplished through process standardization, implementation of new processes, or a combination of the two. Standardizing processes can help streamline tasks so they can be performed more consistently and efficiently or so they can be performed by other people if the need should arise.

Once the specific processes have been reviewed and refined, the next step is to examine any existing controls that may be in place, enhance those controls if needed, and design new ones if appropriate.

## Summing it up

A common misstep that organizations make during internal control design is to jump into the details without adequate preparation using a one-size-fits-all approach. It is important to start with a risk assessment and let its results guide the development of your internal controls framework as a whole and the controls tailored to your organization. Although the goal is to design effective controls, the risk assessment allows for a risk-based decision-making approach to be applied to that process.

Understanding the most important risks to your organization and designing relevant internal controls to mitigate those risks can be key differentiators as your private company grows and evolves. Although internal controls have inherent limitations, when they are designed and operating properly, they can help your company manage and mitigate risks, as well as potentially provide valuable business insights. They can provide reasonable assurance around the timely, accurate, and reliable accumulation of data used to develop financial reports that support strategic decision-making. They are also integral to providing investor assurance in situations such as an IPO, SPAC, or acquisition.

[i] https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf.

# 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.