Deloitte.
Private

Enhancing internal controls to improve risk management

Introduction

Private companies and family enterprises often revel in their lightly regulated status. After all, the less demanding reporting requirements and lack of outside oversight lead many to believe they can be nimbler and frees them up to focus on their highest business priorities.

But this relative freedom can cut both ways—companies that have fewer safeguards in place to manage risk can and often do have lapses. Not having effective internal controls can result in the loss of resources due to undetected inefficiencies or theft, while untimely adjustments or restatements can harm management's reputation and credibility with lenders or outside investors. A lot of the focus on enterprise risk management (ERM) programs from private companies is triggered by such events—setbacks that might have been avoided altogether if internal controls were in place.

Something that often gets lost in the discussion about internal controls is how they can empower better decision-making, in that they keep business leaders from relying on inaccurate or incomplete information. Private company and family enterprise leaders may believe that internal controls compromise agility, when, in many cases, the exact opposite is true. Almost every important decision leaders make relies on the quality of the information at their disposal. Internal controls provide added comfort that the information they have at the ready is sound, empowering them to act with speed and confidence.

In many ways, good internal controls are like an air traffic control system that moves massive airplanes in and out of crowded jetways and airspace, all day long with few exceptions. Those tracking systems are not in place to slow down air traffic or prevent planes from flying, but rather to enable the complicated movement of sophisticated aircraft in a seamless and safe manner.

Private companies and family enterprises should think about internal controls similarly. Market disruption is happening rapidly, creating the necessity for private company and family business leaders to gather accurate information quickly and act decisively. That capability, enabled by good internal controls, can spell the difference between taking off and being grounded. Plus, private companies have the flexibility to borrow leading practices in internal control design and execution from more heavily regulated businesses without having to adopt them whole cloth, so they can employ what works best for their organization and culture, ensuring the right fit.

The question then becomes: Where to begin?

Starting with a risk assessment

In our first installment in this series, we discussed the role risk assessments play in identifying which critical processes in an organization might be susceptible to errors, creating unnecessary risks for the enterprise. A well-executed risk assessment related to internal controls starts with understanding what is material to the company and which processes are the most important.

From there, it's a matter of putting pen to paper to document the current processes and controls and identifying inefficiencies in the process, as well as potential holes in controls. Once those gaps have been identified, risk leaders can estimate the time and effort it might take to address them and establish a step-by-step plan.

Most privately owned companies have a number of policies in place, as well as efficient processes intended to adhere to those policies as transactions are processed. A major mistake that many companies make is assuming that a well-designed policy or process is also a control. Process and controls are **not** the same thing.

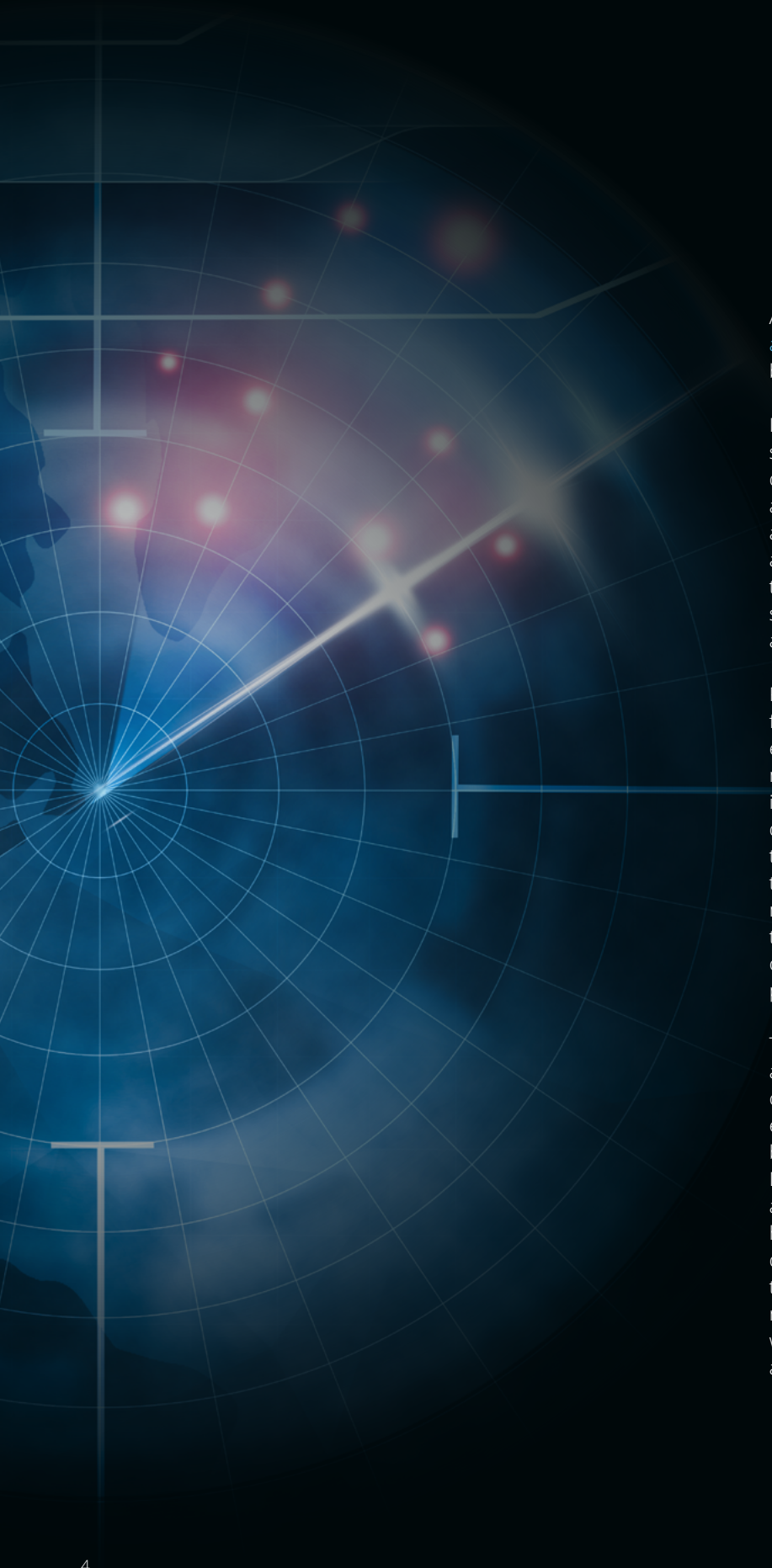
The distinction between process and controls is critical because they serve two very different purposes. A *process* relates to how a transaction is processed or how someone performs a certain task. A *control* is a mechanism that is put in place to ensure that the process is performed as it was designed.

Consider a simple example of disbursing payments to vendors. Many companies have a policy that states that before a vendor can be paid, there must be a three-way match between the quantities and pricing on (1) the approved purchase order, (2) proof that the goods were physically received, and (3) the invoice received from the vendor.

In this example, there are a number of processes in place to ensure that the entity adheres to the three-way match policy. There is a process related to approval of the purchase order. There is a process related to receipt of goods at the warehouse. There is a process where someone enters the invoice into the system. And there is a process for matching the three items together and submitting for payment.

But what control is in place to ensure that these processes are performed as intended? How does the entity know that vendors aren't being paid before these steps occur? How does the company know that the pricing and quantities match between the purchase order, receipt of goods, and the invoice? How does the company know that the amount paid to the vendor is in the right amount?

In this example, the entity might design a control whereby someone independent of the three-way match process performs a detailed review of supporting documentation for check runs prior to disbursement to ensure the three-way match has happened and everything is aligned. Another option for a control might be that the entity configures its enterprise resource planning (ERP) system to prevent a check from being written to a vendor without first matching all required fields in the system.



Distinguishing between preventive and detective controls

After the risk assessment, the work turns to designing and implementing controls. It's important to find a balance between preventive controls and detective controls.

In our experience many private companies, particularly smaller private companies, tend to lean more heavily on detective controls. As the name suggests, detective controls are designed to detect an error or an issue at some point after it has occurred but before a small problem turns into a large one. Detective controls, however, don't help prevent the problem from happening. Imagine if air traffic control systems worked this way, only sounding an alarm after an accident occurred.

Preventive controls, by contrast, help to prevent things from going awry in the first place. Let's go back to our example of disbursing payments to vendors. Logically, most companies would like to prevent unapproved, inaccurate, or fraudulent payments from ever being disbursed. But this often doesn't happen at companies that haven't invested in internal controls and instead expect to identify those issues by analyzing bank statements or monthly financial statements in search of variances. It's true that these reviews might identify unauthorized, inaccurate, or fraudulent payments, but consider if they could be prevented from being disbursed from the start?

This kind of capability can be obtained without unleashing a dizzying amount of documentation demands on an organization. We find when private companies and family enterprises are reluctant to engage in ERM initiatives, it's because they're worried about slowing things down. In a Dbriefs webcast we held on the subject, four in 10 of the attending private company executives said their company has either designed internal controls that are not clearly documented or they haven't designed any at all. In the end, though, some formalization is required to get everyone rowing in the same direction, and that means creating well-documented, explicit controls that help people at all levels make better decisions.

Don’t let perfection get in the way

It’s often said that managing risk relies on three core factors: people, process, and technology. But how each organization combines those factors for maximum effect varies widely—and resource constraints often mean the optimal mix is elusive. When talent is scarce, for example, staffing up and adding headcount might not be a viable solution for improving a control environment.

Limited resources—both talent and financial—are a common challenge for private companies and family enterprises. During that same Dbriefs webcast, nearly half of the private company executives said in response to a polling question that limited time and resources are the most significant barriers to performing a risk assessment or implementing internal controls. Many simply do not have enough back-office accounting staff with the skills required to develop and maintain a formal system of internal control.

This can lead to a sort of vicious cycle: Companies with thin back offices, lacking the resources to put together a proper system of controls, are also commonly the ones most at risk for creating, reporting, and using the inadequate financial and operational information that controls are designed to identify.

For such companies, it’s important to understand that not every control has to be leading, and the quest for perfection might hamper the introduction of solid, effective controls. When an organization can deploy [or introduce] automated controls as opposed to manual, or preventive as opposed to detective, the control’s effectiveness may be increased. However, even a manual detective control is still far better than no control at all.

Let’s revisit the payment disbursement example one more time—sure, in an ideal world with unlimited resources it would be great to implement automated controls within an ERP system to automatically perform that three-way match and initiate payment, or to reject the payment if there are discrepancies. If the people, processes, or technology are not available to make that happen, consider putting in place detective controls as a starting point. Also keep in mind that many of the workflow automation tools available in the marketplace today are relatively inexpensive and are helping a lot of private companies and family enterprises do more with less.

In short: Don’t get caught up in perfection because it rarely exists with internal controls. The important point is to start by identifying the areas with the most risk and then focus on continuous improvement. And that process can begin today by considering some questions about the current state of your internal controls:

- Which risks, if realized, could have the biggest impact on our business?
- Where are the risks that could compromise our accounting or our ability to capture, aggregate, and report data?
- How does management know what risks are being addressed?
- What are the criteria for investigating variances?
- Who reviews and approves transactions or journal entries?
- Where are we still relying on manual processes that are prone to judgments and error?

In our next installment in the series, we’ll dive into ERM implications for managing the growing threat of cyber risk.

NEXT UP IN OUR SERIES

ERM and the fight to contain cyber security threats
This article will discuss the latest cyber threat trends, including the rise of third-party vendor risks; highlight risk-probability models that private companies can use for forecasting; and provide mitigation strategies for security engineering and IT teams to keep an organization safe.

GET IN TOUCH

Kevan Flanigan
US Deloitte Private Leader, Risk & Financial Advisory
US Deloitte Private Leader, Private Equity
keflanigan@deloitte.com

Aaron Zboril
Audit & Assurance Managing Director
azboril@deloitte.com

Deloitte.