

Private companies:
are your internal controls supporting your business strategy?*

private companies and internal controls



Benefits for private companies // 3

Internal controls today // 4

An internal controls framework // 6

Identifying controls at the
activity level // 11

IT controls // 12

Where are the greatest risks to
a private company? // 14



In years past, the words “internal controls” were rarely mentioned in the business section of newspapers or in business magazines. Today, however, thanks to recent headlined scandals, frauds, and business failures, you’re almost as likely to see internal controls mentioned on the front page of the newspaper as in the business section.

More often than not, the names *Sarbanes-Oxley* will appear in the same story. This, of course, refers to the 2002 federal legislation requiring public companies to meet strict requirements for implementing, documenting, and testing internal controls. Its enactment was a response to widely-publicized control failures and their sometimes catastrophic consequences. By compelling transparency in financial statements and holding management more accountable for its actions, Sarbanes-Oxley seeks to restore rigor to financial reporting and confidence to investors.

The law was enacted as a corrective measure. What has emerged as companies work to bring themselves into compliance, however, is the significant *business benefits* that flow from the strengthened internal controls it mandates. Although the law and its supporting regulations apply only to public companies, putting aside the compliance factor, private companies usually derive the same benefits from enhanced controls as public companies. And the benefits can be very significant.

Benefits for private companies

Appropriate, properly functioning internal controls offer powerful benefits to private companies in a number of key areas. As an example, if a company is contemplating an initial public offering, readiness to comply with Sarbanes-Oxley is essential. If the owners of a private company are considering the sale of all or part of the entity, or are seeking private equity financing, effective controls can increase prospective buyers' willingness to pay a premium for the acquisition. Controls enhancements can also lower borrowing costs and help attract new business partners.

Many potential private-equity investors and venture-backed companies are also seeking to invest in companies with strong and well-documented internal controls. Should these companies eventually go public, the road to compliance will be an easier process.

Conversely, if a private company's internal control environment has *not* been adequately designed and documented, potential acquirers, business partners, and lenders may look elsewhere to invest. Today, investors, credit grantors, and business people in general are keenly aware that the lack of strong internal controls increases investment and operational risk.

Therefore, private companies are now actively seeking to enhance their internal controls, ensure the credibility of financial information, and receive the operating benefits that a strong system of internal controls can provide.

Let's take a closer look at some of those benefits.

- Financial reporting benefits
 - Heightened credibility provided to all stakeholders, whether they be owners, employees, customers, lenders, or vendors
 - Better information to manage the business
 - Reduced risk of errors or irregularities
- Operational benefits
 - Clarity on the roles and responsibilities of both management and employees
 - Greater controls over the management of business growth
 - Reduced costs obtained from greater operating efficiency
 - Maximized operating performance
- Regulatory benefits
 - Decreased risk of litigation or business disruption, thanks to the focus on compliance
 - Lowered risk of employee or customer litigation
 - Increased credibility with the IRS, FDA, FTC, and other regulators
 - More credibility in contractual relationships with vendors and customers

The bottom line for business owners: *increased focus on internal controls maximizes the value of a business.*

Internal controls today

In many if not most private companies, controls are informal. As a consequence, controls may not be known or adhered to, or may not be accomplishing their objectives. While management may believe controls are in place, they may not be functioning as intended, may not be fully implemented, or may not have been initially implemented at all. Lack of segregation of duties can exacerbate control problems. In short, companies with inadequate internal controls remain unprotected against risks they thought were being mitigated.

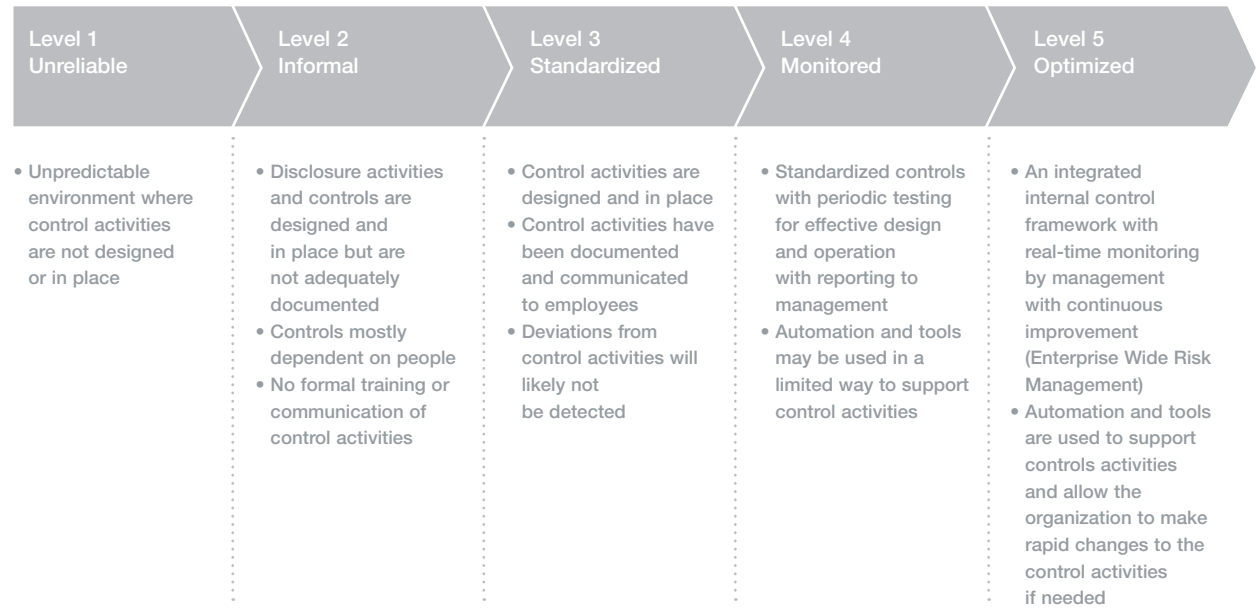
Even when controls exist, they're often *detective* rather than *preventive*—designed to uncover problems after they occur, rather than prevent them from occurring. Such controls are often manual and lack formality or discipline. Employees usually want to do the right thing, but may not understand exactly what they are expected to do to ensure that controls are being followed. In addition, even if there are controls in place, they may not be regularly evaluated for compliance and effectiveness.

Control errors and failures can also arise from poor communication among departments and operating functions. In addition, since many companies now use spreadsheet programs such as Excel as part of their key accounting records, there may be no controls over the accuracy of such spreadsheets. Multiple changes may be made to such spreadsheets over time, which can cause errors in the underlying accounting information—and can materially impact a company's financial reporting.

All these issues will have a negative impact not just on financial or regulatory controls, but also on the business itself.

The following illustration identifies the stages of maturity in private companies' control programs.

Where is your company on the internal controls maturity framework?

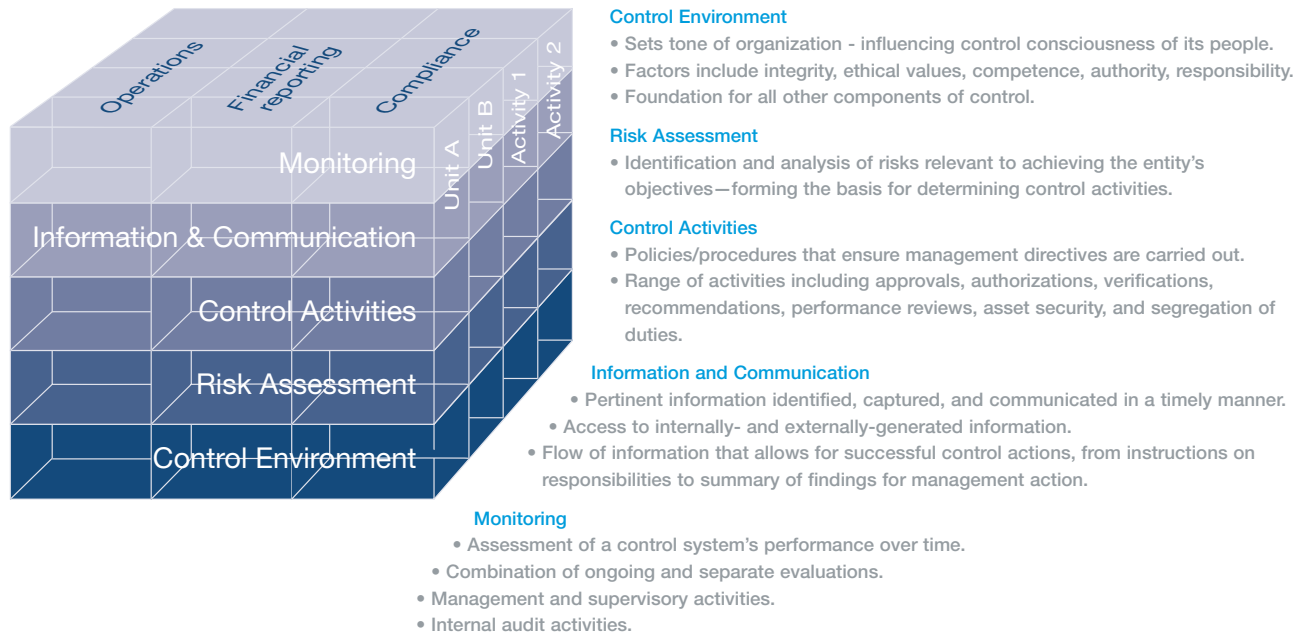


An internal controls framework

The standards for internal controls were initially established in 1992 by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. COSO was a blue-ribbon body chartered by leading accounting organizations to articulate the purpose and elements of internal controls. The group's work is widely acknowledged today as definitive. It identified five components that must be in place at the entity level for controls to be effective: (1) the control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. They are illustrated here.

COSO components: five components of internal controls

All five entity-level components must be in place for controls to be effective.



All the components are indispensable, but an effective internal controls structure starts with the **control environment**. Ingredients in setting the critical “tone at the top” should include a clear mission statement and a written, reinforced, broadly communicated code of conduct.

Compliance with the code should be periodically confirmed. Companies may also want to establish an “ethics hotline” as a reprisal-free medium for reporting ethical breaches. Investigation and enforcement must be a visible reality, fostered and strengthened by the ethical behavior of senior management and the owners. An independent advisory board can help monitor and adjudicate control issues. Organization-wide training programs will further ensure compliance with policies, codes, and control activities.

The goal of risk assessment, as it relates to the objective of reliable financial reporting, involves the identification and analysis of risk of material misstatement in financial reporting and mitigation of such risk.

Control activities include top-level performance reviews against budget, forecasts, prior periods, and competitors. Duties must be segregated among different staff to forestall error or malfeasance. Equipment, inventories, cash, and other assets must be physically secured and regularly compared with control records. Access to them should be restricted to designated personnel.

The consistent communication of a company’s code of conduct and business ethics is one example of **information and communication**. In addition, management should encourage department heads to solicit and consider suggestions from their staff. Employees need to understand why they are performing an activity and how that activity contributes to overall objectives. In addition, two-way communication between senior management and operational personnel should allow for clear working channels to make recommendations for improvement.

Regular reviews of control processes and procedures are a basic element of **monitoring**. The only way to evaluate whether controls are working as intended is to ensure that appropriate monitoring, by a level above the person performing the control, is taking place. In addition, recommendations by the external auditors to enhance controls should be fully considered and promptly addressed.

Documents such as communications from vendors and monthly accounts payable statements can serve as further control-monitoring tools. And—another basic—management must ensure that inventories are counted on a formal, periodic basis, and that variances from recorded inventory amounts are fully investigated.

Finally, companies should require everyone in the organization to confirm compliance with the company’s code of conduct.



Initial questions in evaluating internal controls

The following questions have been provided as guidance in evaluating the basic principles representing the fundamental concepts associated with the five components of internal control.

Control Environment

- Has management developed and clearly articulated a **statement of integrity and ethical values** that is understood by all employees? Are processes in place to monitor adherence to and remedy deviations from these values?
- Does the company have a **board of directors/advisors**, consisting primarily of individuals outside of management, with defined roles and authority, to evaluate the risk of management override of internal controls? Do its members meet with the auditors, oversee the quality of financial reporting, and evaluate business decisions?
- Do **management's philosophy and operating style** set the tone for the organization with both internal staff and external parties?
- Is the company's **organizational structure formalized** and documented with an organization chart that sets forth roles, job descriptions, authority, and reporting line responsibilities for all employees? Are key employee roles aligned with operating and financial reporting processes?
- Does the company have **competent individuals in financial reporting** and oversight roles?
- Do the company's human resource practices demonstrate its **commitment to integrity, ethical behavior, and competency** in the recruiting, training, development, and evaluation of employees?

Risk Assessment

- Does management specify financial reporting objectives with sufficient clarity to enable the identification of risks that might affect the reliability of such information? Such risk assessment should include business processes, information technology and both internal and external factors.
- Does management consider the potential for fraud in its financial reporting risk assessment—including incentives and pressures to commit fraud, the likelihood of fraud, and the impact of fraud on financial reporting? Does the company implement antifraud programs and controls?

Control Activities

- Does the company **design control activities to mitigate financial reporting risks**, considering all points of entry into the company's general ledger? Do the control activities, where appropriate, use information technology tools to identify and manage fraud risk?
- Do the **designed control activities encompass a full range of activities**, including approvals, authorizations, reconciliations, verification, reviews of operating performance, security of assets and segregation of duties? Do these activities balance preventive and detective controls?
- Have **policies and procedures** been established, documented and communicated throughout the company? Are they performed on a timely basis and built into the company's regular business processes, enabling management's directives to be carried out?
- Have **information technology controls** been designed to ensure the completeness and accuracy of valid and authorized transactions? Are critical general computer controls in place to ensure the integrity of the system and of the data processed?

Information and Communication

- Is the **pertinent information captured** being provided on a current and accurate basis and used to help achieve financial reporting objectives?
- Is such **information being distributed** and used to execute the appropriate control components of financial reporting, permitting prompt resolution of exceptions and maintaining the quality of the information produced?
- Does the company's **communication enable all personnel to understand** internal control objectives and processes, their responsibilities in achieving internal control objectives, and the importance attached to those responsibilities?
- Are **communication channels** available to outside parties to facilitate their input on information affecting the achievement of financial reporting objectives?

Monitoring

- Does the company continuously monitor its internal controls over financial reporting, use knowledgeable personnel to evaluate the results of such monitoring, and adjust the scope and frequency of evaluations to **determine whether controls are functioning as designed**?
- Are **internal control deficiencies identified and communicated** in a timely manner to parties responsible for taking corrective action, and to management and the board/advisors as appropriate? Is timely corrective action in fact taken?

Identifying controls at the activity level

Whether preventive or detective, manual or automated, control activities support the control objectives of Completeness, Accuracy, Validity and Restricted access (CAVR). The five main steps below will help private companies begin the process of evaluating and strengthening internal controls at the activity level.

- Step 1 Assess areas and cycles where lack of a control could cause asset impairment, financial-statement errors, operational problems, or noncompliance with regulatory requirements.
- Step 2 Start with one cycle and identify key processes and sub-processes (see Exhibit, below).
- Step 3 For each sub-process, document controls in a narrative or flowchart. Interview department personnel, walk through each process, and identify controls that meet the CAVR objectives noted above.
- Step 4 Identify controls that are now in place and those that need to be modified, implemented, or enhanced, and implement such enhancements.
- Step 5 Test controls in place to determine if they are working as designed; evaluate results.

Exhibit: Most common processes

Payroll/HR	Revenue & receivables	Information systems
Asset management	Taxes	Customer allowances
Equity & stock administration	Legal	G/L accounting
Treasury	Financial reporting	Fraud policies
Purchasing & payables	Excel spreadsheets	Entity-level controls
Manufacturing & inventory		

As an example, the evaluation of sub-processes in Payroll/HR might include:

- New employee
- Compensation
- Payroll disbursement
- Benefits administration
- Change in status
- Payroll calculation
- Payroll accounting

Post-evaluation, management should communicate control processes to the departments affected to ensure that employees understand the design of each control and their related responsibilities. A policies and procedures manual that codifies the control architecture should be the keystone of this communication. Business process narratives compiled in the evaluation process noted above can serve as the manual's base source.

Companies should review and test documentation periodically to ensure that controls remain in place and are functioning as designed. It is essential to understand that as the business changes, controls will also need to change.

IT controls

Four areas of a company's information technology activities require specific control attention.

Management's first task is to ensure that effective controls on **systems development and implementation** are operational. Before introducing any new system, management must ensure the *initial* accuracy and proper operation of accounting calculations such as payroll, depreciation, and overhead allocations; automated controls (e.g., edit checks, automated approvals, document matching, control total balancing, and configurable security controls); and reports that support manual controls (e.g., exception reports, audit trails, and management reporting).

Managing the development and implementation of new IT systems will then encompass controls over project initiation and related approvals; requirements definition; package selection; testing and quality assurance; data conversion from old to new systems; launch or "go-live"; documentation; and training.

Systems maintenance and change management controls ensure the continued accuracy and proper operation of calculations, automated controls, and reports (e.g., management of maintenance activities; specification, approval, and tracking of change requests; construction; testing and quality assurance; authorization of transfers to production, including emergency changes; restricted access to production; documentation; and training).

Security controls protect the continued accuracy of data, deny unauthorized individuals access to accounting functions, and block unauthorized changes. They include controls over the company's security organization, management, policies, and procedures; application security administration; data files and databases; operating system security; internal and perimeter network security; and physical security.

Computer operations controls also target the continuing accuracy and proper operation of calculations, automated controls, and reports, but with a focus on daily systems operations management; scheduling and batch processing; backup and recovery procedures; network management; capacity planning; performance management; the help desk function; and management of outsourced relationships.

Companies should review and test documentation periodically to ensure controls remain in place and are functioning as designed.

Where are the greatest risks to a private company?

First, there's the control environment. If the critical "tone at the top" is unclear, poorly communicated, or never enunciated to begin with, there may be no real focus on promoting ethical behavior, no written code of conduct, no ethics hot line, and no advisory board in an oversight role. Controls may be detective rather than preventive—focused after the fact rather than before. The company may not even have a process for reviewing significant non-routine transactions involving management.

Or, a company may simply **lack controls** to prevent such occurrences as:

- Inappropriate revenue recording
- Unauthorized revenue transactions (pricing changes, credit limit authorizations, weak customer acceptance policies)
- Excess inventory purchases
- Purchases of products and services at higher-than-expected costs
- Unapproved payroll changes, risking unauthorized salary increases, employee salaries in excess of authorized levels, and the potential for fictitious or "no-show" employees
- Unauthorized wire transfers
- Inappropriate investment of excess funds
- Unnecessary fixed-asset purchases
- Theft

Smaller companies often struggle to **segregate duties** effectively without hiring significantly more administrative personnel. However, appropriate segregation of duties can be achieved, even in smaller companies, by the involvement of senior management in the review and approval process.

Another risk is that the **information used to monitor operations** may be flawed or inappropriate. Shortcomings may include a lack of sufficient detail, inattention to the details provided, or over-reliance on reports whose source data is not periodically checked.

In some cases, employees **do not understand the reasons** they are performing certain procedures or what procedures should be performed to ensure their compliance with the internal controls process. Staff turnover, a significant issue in today's business environment, exacerbates this problem, as does failure to document policies and procedures. Documentation is critical because as people change roles and responsibilities, there needs to be a process to ensure that controls assumed to be in place and operating as planned are in fact continuing as a new employee takes on that responsibility. This safeguard will prevent the control process from going away with the former employee.

Inadequate security is a serious control risk. Financial and physical assets need to be secured, as does access to information technology assets, both hardware and software. Securing intellectual property, such as formulas and customer information, is equally important.

Finally, **regulatory noncompliance** is a significant control risk that demands the focused attention of private companies. At the federal level alone, agencies such as the IRS, FDA, FTC, and EPA issue and enforce regulations that apply to both private and public companies. If employees do not follow the relevant company policies and procedures, or do not know what they are, problems are likely to ensue.

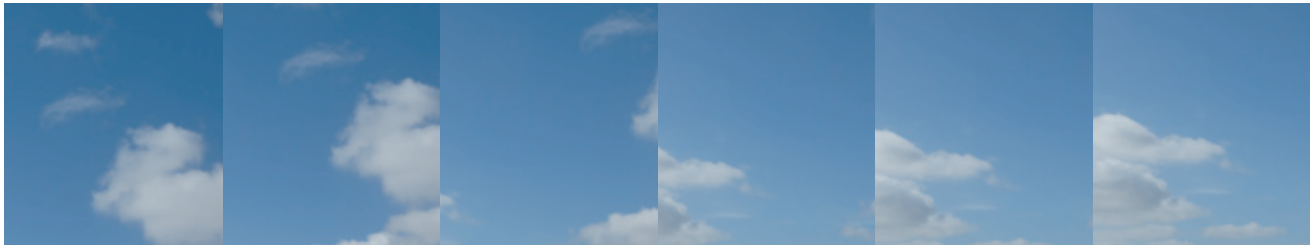
The time to act is now

It is clear that businesses will be held accountable by their stakeholders for being in control of the actions of their company, its management, and its employees. For public and private companies alike, the emphasis on, and need for, effective internal controls will increase as business becomes more complex.

The Sarbanes-Oxley control provisions may become the "gold standard" for controls in all companies, both public and private—defining the level of excellence that leading businesses will strive to reach.

Business is personal. We treat it that way.

PricewaterhouseCoopers' Private Company Services practice is an integrated team of audit, tax and advisory professionals who focus on the unique needs of private companies and their owners. Within the practice, our professionals concentrate on the needs of manufacturing, retail, wholesale and distribution, construction, and food and beverage companies, as well as on the needs of law firms and other professional service organizations. They are committed to delivering cost-effective, practical solutions and proactive services with the quality clients expect from PricewaterhouseCoopers. For more information about PricewaterhouseCoopers' Private Company Services practice, visit www.pwc.com/pcs.



This document is provided by PricewaterhouseCoopers LLP for general guidance only, and does not constitute the provision of legal advice, accounting services, investment advice, or professional consulting of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisors. Before making any decision or taking any action, you should consult a professional advisor who has been provided with all pertinent facts relevant to your particular situation.

The information is provided as is, with no assurance or guarantee of completeness, accuracy, or timeliness of the information and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability, and fitness for a particular purpose.

© 2006 PricewaterhouseCoopers LLP. All rights reserved. 'PricewaterhouseCoopers' refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, other member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. *connectedthinking is a trademark of PricewaterhouseCoopers LLP (US).