RECIPROCITY®

INTERNAL CONTROLS BEST PRACTICES

www.reciprocity.com

Strong internal controls are vital for every modern organization. Controls are the set of procedures that enable a company to safeguard assets, ensure the reliability and integrity of its financial records, and remain compliant with the relevant laws and regulations affecting its operations.

This article provides an in-depth view into internal controls, types, benefits, and best practices. If your organization is planning to revamp or implement a system of internal controls, keep reading to see how to optimize these processes.

What Are Internal Controls?

Internal controls enable organizations to maintain process efficiency, performance, and reliability within their business. These controls may take any number of forms, such as:

- Physical safeguards
- IT general controls (ITGC)
- Account reconciliations
- Independent audits of activities or balances
- Transaction authorizations
- Operating metrics reviews
- Analyses of budgets to actuals
- Separation of duties

Regardless of the type, internal controls are essential to improve operational performance, avoid adverse risk events, safeguard assets, and meet the demands of regulators, auditors, boards, and customers.trols.

What Are the Benefits of Internal Controls?

Internal controls protect your business from many operational, financial, and compliance risks that compromise asset security and increase your vulnerability to theft. These risks can also result in operational uncertainties that disrupt business continuity and weaken competitiveness, which can ultimately decrease your ability to achieve goals and objectives.

Strong internal controls provide a safeguard against such adverse events. The main objectives of internal controls are:

- Verify the reliability, accuracy, and timeliness of financial reporting
- Minimize the risk of fraud, errors, and discrepancies
- Achieve compliance with laws and regulations
- Optimize operational efficiency and financial management

With strong internal controls, you promote integrity, accountability, and transparency. Over time, you develop a reputation as a financially stable, ethical, and sustainable organization and thus earn stakeholder confidence, trust, and loyalty.

Conversely, a lack of internal controls or weak internal controls diminish the integrity of the organization's financial reporting infrastructure. It limits operational effectiveness, increases the chances of fraud, and multiplies financial costs. You may also suffer reputational damage, incur fines, and lose stakeholder trust.

Types of Internal Controls Activities

An effective internal control system comprises three different types of internal controls that work together.

Preventive Controls

Preventive controls proactively eliminate problems such as fraud or cyber-attacks before they happen. A comprehensive variety of preventive controls is a sign of a robust system of internal controls.

Common examples are:

- Segregation of duties
- Proactive verification of financial transactions
- Authorization and approvals of invoices and expenditures
- IT access controls
- Employee cybersecurity training
- Physical security

Detective Controls

Detective controls aim to find errors or problems after they have already occurred. Although not proactive, these controls are also critical because they help you catch misstatements before financials are reported. By correcting the errors, you avoid possible legal, regulatory, or reputational fallout.

They can also help you determine if preventive controls are adequate and address gaps. Detected errors should be evaluated to see if there are opportunities to improve process quality or preventative controls.

Some typical detective controls you can implement are:

- Monthly transaction reconciliations
- Organizational performance reviews
- External audits
- Internal audits
- Cash and inventory counts

Corrective Controls

Corrective controls help organizations resolve problems that could lead to fraud, financial losses, fines, or reputational damage. Any time a detective control identifies an issue, a corrective control will fix the problem at hand and determine if there is a systemic gap in the process to prevent a recurrence.

Many organizations implement corrective controls like:

- Reports
- Ledger verification
- Software patches or upgrades
- Disciplinary action
- New or updated policies and procedures

What Are Internal Control Risks?

Internal control risks affect the effectiveness and efficiency of internal controls and thus prevent the organization from achieving its stated objectives. These risks are a part of:

> **Operational Risk:** The risk of unexpected operational disruptions or failures that could be caused by personnel, technology, or processes

> **Compliance Risk:** The risk of not maintaining compliance with laws or regulations, such as SOX or FCPA

Common internal control risks you should consider are:

Management Override of Controls

Often, financial statement fraud is perpetrated by senior management, such as c-suite executives. This is usually because their compensation is directly tied to the organization's financial performance, which gives them an incentive to manipulate financial statements or accounting records to their benefit.

Moreover, managers usually create, implement, and maintain internal controls, enabling them to bypass those controls. Strong governance is essential to identify and prevent fraud at a managerial level.

Limited Segregation of Duties

Segregating duties among multiple employees means that one person is not both authorizing and recording transactions. Different people should perform these responsibilities to improve quality verification and avoid the temptation of fraud.

Some organizations fail to properly segregate duties due to limited staffing or improperly designed segregation controls. This can increase the risk of error or fraud. Oversight, supervision, and monitoring are crucial when segregation of duties is difficult to implement.

Lack of Preventative Controls

Some organizations over-emphasize detective and corrective controls while neglecting preventive controls. Solid preventive controls are essential to reduce the need for detective and corrective controls.

Trusting and Not Verifying

Everyone who handles financial transactions or reporting must be supervised, and their work should be validated and authorized – no matter how trustworthy they appear. To prevent fraud and other adverse events, adopt the "don't trust, always verify" approach promoted by cybersecurity concepts like zero-trust.

What Is an Internal Control Risk Assessment?

An internal control risk assessment evaluates both the internal and external risks that can affect your organization's ability to create reliable financial reports, protect assets, achieve regulatory compliance, and maintain effective operations. Assessment should drive the development or improvement of your internal control system.

A risk assessment comprises of:

- Identifying qualitative and quantitative risks
- Evaluating the severity and probability of these potential risks
- Prioritizing risks to ensure the most severe risks receive the most potent controls
- Establishing control measures to safeguard against those risks

What Is the Relationship Between Internal Controls and Risk Management?

Risk management and internal controls seem like similar concepts. However, there are some differences in their objectives and how the two ideas are emphasized and addressed.

Internal controls are geared toward meeting goals for operational efficiency, accurate financial reporting, and regulatory compliance. In contrast, an enterprise risk management plan addresses a broader range of risks, including supply chain, reputation, cybersecurity, third party, financial, and operational risks.

COSO Internal Control – Integrated Framework

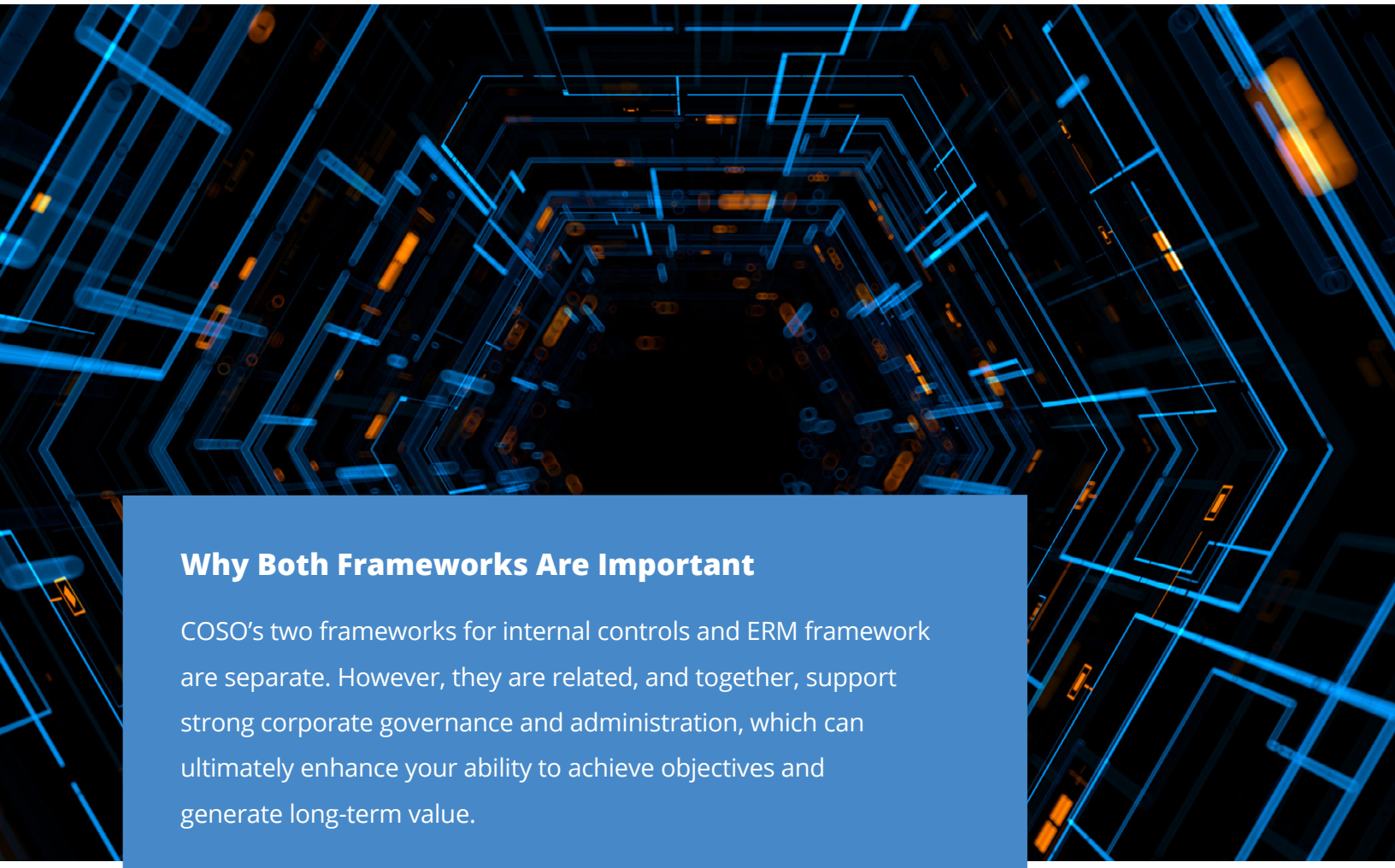
First published in 1992, the *COSO Internal Control — Integrated Framework* provides an applied risk management approach to internal controls. It is one of the most widely-used control frameworks to improve financial reporting, deter fraud or theft, and prevent reputational damage.

This framework also helps businesses demonstrate compliance with laws and regulations such as Sarbanes-Oxley Act (SOX) and the Foreign Corrupt Practices Act (FCPA).

Several high-profile business scandals and failures in the late 90s and early 2000s created a need for a robust risk management framework to help organizations identify, assess, and manage risk. The controls framework was insufficient to meet these needs, so the *COSO Enterprise Risk Management — Integrated Framework* was developed in 2004.

COSO Enterprise Risk Management – Integrated Framework

This enterprise risk management (ERM) framework defines a common ERM language and provides clear direction and guidance for ERM. It also expands on internal controls and focuses more extensively on the broader subject of ERM.



Why Both Frameworks Are Important

COSO's two frameworks for internal controls and ERM framework are separate. However, they are related, and together, support strong corporate governance and administration, which can ultimately enhance your ability to achieve objectives and generate long-term value.

Moreover, the ERM framework incorporates the internal control framework. That's why you should use these frameworks in conjunction to guide and implement your business strategy and strengthen your internal controls.

How to Assess and Implement Internal Controls

You can and should implement many kinds of internal controls in your organization. Here's how to determine which controls are most relevant and necessary.

STEP 1: Determine Control Goals

Knowing the purpose of a control – achieving operational excellence, improving financial information accuracy, achieving SOX compliance, etc. – can help you determine which control to implement. So, make sure you first determine your goals related to:

In general, you should implement controls that:

- Improve operational performance and resilience
- Help you achieve regulatory compliance
- Increase accountability
- Ensure sound business practices
- Provide accurate reports in a timely manner
- Support internal and external audits

STEP 2: Identify "Weak" Processes

Identify the business processes with control weaknesses or areas that could be the target of errors or fraud. This step will assist you with prioritizing controls and initiatives that need the most urgent attention and stringent management.

STEP 3: Establish a Common Language

By establishing a common language for risks and controls, you can:

- Improve the understanding of risk and controls throughout the organization
- Enhance risk identification, classification, and response processes
- Implement standardized controls and set the right expectations around them
- Improve reporting, gap analyses, and corrections
- Improve business decision-making
- Reduce the need for external audits

STEP 4: Set Up a Reporting Structure

Implement a reporting structure to ensure that up-to-date and reliable information about risks and controls is available to senior management, leadership, and the board of directors.

STEP 5: Leverage Technology

Use digital tools and internal controls management software to:

- Manage internal controls
- Automate many controls management activities
- Improve audit and compliance management
- Monitor controls in real-time and gauge their ongoing effectiveness
- Standardize controls

Internal Controls Best Practices

If your organization is considering implementing new internal controls or looking to improve existing controls, get started with these best practices:

Identify Internal and External Risks

Identifying risks will help you define the scope and type of controls required to manage those risks. Such risk-based scoping also ensures that controls are effective and targeted. Revise the scope periodically to accommodate the changing risk landscape.

Roll-Out Internal Controls in a Structured Manner

If you have identified multiple risks and multiple controls, the entire implementation process can be overwhelming. Break the initiatives into bite-sized pieces and roll out new controls in a phased approach.

Craft a risk/control matrix with details of the risk, control goal, and activity. Translate key activities into digestible and actionable steps. Also, consider if the costs of implementing controls outweigh the benefits and the organization's risk tolerance or appetite.

Perform a "Dry Run"

When designing controls, make sure you develop the "right" controls instead of "more" controls. Test control effectiveness before deploying in a live environment. Cumbersome controls may result in poor adoption or workarounds, negating their value.

Develop Reporting and Monitoring Mechanisms

It should not be a chore to understand and measure the progress of internal controls. That's why user-friendly reporting and monitoring tools are essential.

Encourage Org-Wide Buy-In

Internal controls are effective only when they strengthen the organization at every level. Support adoption through employee education and training. Clearly explain the purpose and value of these controls.

Create a strong tone from the top, promote a risk-aware and ethical culture, and make sure everyone is aware of all risks, responsibilities, and expectations.

Document Processes

Documenting controls processes, procedures, and policies ensure that everyone knows their role in the control environment. Clearly define each specific control, document control activities, and identify activity owners.

Leverage Technology

Use technologies like robotic process automation (RPA) to improve the efficiency, quality, and consistency of internal controls. Implement data analytics to perform internal control reviews and audits. Use software to streamline ERM and governance, risk, and compliance (GRC) processes and workflows.

Test and Monitor Controls

Monitor the effectiveness of internal controls to verify they are functioning as intended. Conduct internal control reviews, gather employee feedback, and engage external auditors to validate internal controls.

Include Reciprocity in Your Internal Control Implementation Plan

Leverage the Reciprocity® ROAR Platform to guide you as you implement internal controls within your organization. This integrated platform can help you identify risk and mitigate business exposure.

The Reciprocity ROAR Platform enables reliable risk, audit, and compliance management with complete views of control environments, easy access to information, and continuous monitoring. Consolidate policies and procedures, implement business continuity and disaster recovery plans, and protect your business with Reciprocity.

SCHEDULE A FREE DEMO TODAY

ABOUT RECIPROCITY

Reciprocity is pioneering a first-of-its-kind approach to IT risk management that ties an organization's risk directly to its business strategy.

The fully integrated and automated Reciprocity ROAR Platform, which underpins the Reciprocity ZenRisk and ZenComply applications, enables security executives to communicate the direct impact of risk on high-priority business initiatives to key stakeholders, helping them make smarter, more informed decisions.

With Reciprocity, InfoSec teams can strategically support their organization and foster company growth by optimizing resources and mitigating expensive data breaches, system failures, lost opportunities and vulnerabilities with their customers' data.

Security builds trust.

www.reciprocity.com