Risk Insights

COSO 2013
Implementation

Reflecting today's business environment by implementing COSO 2013 internal control-integrated framework

TODAY'S BUSINESS ENVIRONMENT is highly automated and globally connected. Remote workforces are common and businesses face ever increasing expectations for transparency. The 2013 COSO Internal Control-Integrated Framework acknowledges those changes. The 2013 COSO Framework retains the principles-based internal control components found in the 1992 COSO Internal Control Framework while re-codifying 17 concepts associated with those components. The changes enable organizations to more effectively address internal control concerns.

The Committee of the Sponsoring Organizations of the Treadway Commission (COSO) released its updated Integrated-Internal Control Framework in May 2013. The updated framework serves as an enhancement of the 1992 COSO Integrated-Internal Control Framework and is recommended for use by December 15, 2014, for companies that must comply with Security and Exchange Commission (SEC) regulations. The Institute of Internal Auditors (IIA) also recommends prompt implementation of the 2013 framework. Regardless of the particular compliance requirements an organization faces, implementing the 2013 framework as soon as possible can bring value to an organization.

The Need for an Updated Framework

INTERNAL ORGANIZATIONAL ENVIRONMENTS and specific control needs for today are very different than they were 1992. Technology drives virtually all business activities. Organizations face stronger overall governance expectations, along with increasing expectations to prevent and detect fraud. Outsourcing and other contractual relationships are more common. Global commerce is more prevalent. Now compliance measures enacted during the past two decades require specific control measures, and organizations face stakeholder expectations for greater accountability and transparency.

Organizations have always needed to consider the likelihood of an adverse event occurring and its potential impact. The revised framework now specifies risk ***velocity*** and risk ***persistence*** as crucial factors to be evaluated as part of the risk assessment process.

weaver
Assurance • Tax • Advisory

COSO 2013 INTERNAL CONTROL FRAMEWORK

Internal control is defined as a process effected by an entity's board of directors, management and other personnel and designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

The COSO 2013 framework identifies five components of control that need to be in place and integrated to ensure the achievement of each of the above objectives.

Evaluate the control environment to ensure it adheres to the following key principles, as defined by COSO:

- Demonstrates commitment to integrity and ethical values
- Exercises oversight responsibility
- Establishes structure, authority and responsibility
- Demonstrates commitment to competence
- Enforces accountability

Discovery of a data security breach, for example, represents a high velocity risk. There are sudden losses in stakeholder confidence and trust following disclosure. There are immediate costs in mitigating potential damage. Liability exposure dramatically increases. Such a risk can strike quickly and with great impact.

But, data security breach may also be viewed as a persistent risk, an always-present risk, a risk requiring continual monitoring of information technology (IT) networks, a risk requiring security patches and other mitigation efforts whenever a new vulnerability emerges.

Recognition of how different internal control needs manifest in today's business environment illustrates the benefits gained from applying the 2013 framework.

The Enhanced Benefits Associated with the 2013 Framework

THE 2013 FRAMEWORK RETAINS the principles-based approach of the 1992 framework as well as the role of management judgment in implementing and sustaining internal control. That flexibility enables companies across all industries to scale and adapt the framework to fit unique organizational characteristics. The 2013 framework also retains the 1992 framework's focus on control environment, risk assessment, control activities, information and communication, and monitoring.

Table 1 lists the 17 principles and their relationship to the five internal control components of the 2013 framework. That combination of principles and components provides structure and direction for incorporating effective, integrated internal controls while also affording flexibility and scalability to address specific organizational characteristics.

The control environment component addresses how internal control is designed and sustained throughout an organization. A vital element of an organization's control environment is senior leadership's "tone at the top." That element is encompassed in Principle 1. The other four related principles address how that commitment to integrity and values is defined, implemented, evaluated and enforced throughout the organization.

> "Recognition of how different **internal controls needs** manifest in today's business environment illustrates the **benefits gained** from applying the 2013 framework."

Every organization faces risks, and the risk assessment component provides a means for identifying and evaluating those risks. Principle 6 emphasizes a top-down approach in which the most crucial risks receive the most attention. Direction for applying that top-down approach is defined in Principles 7, 8 and 9, with additional emphasis on examining scenarios that present fraud exposure.

The control activities component provides direction for establishing practices that mitigate risks. As stated in Principle 10, an organization needs control activities designed to mitigate risk. Principle 11 acknowledges the pervasive importance of general IT controls to all operations, reporting or compliance controls. Principle 12 codifies the importance of defining and documenting how internal controls are deployed with the expectation of consistent execution.

The information and communication component (Principles 10, 11 and 12) emphasizes the importance of obtaining and sharing relevant information for internal control purposes. Recognizing that data tells a story but must be managed and turned into information for management's use, and Principle 13 emphasizes the importance of culling crucial information from that data. That information needs to be communicated to internal and external stakeholders, as emphasized in Principle 14 and Principle 15, respectively.

The monitoring activities component illustrates the need to regularly evaluate internal control functions and effectiveness. Principle 16 addresses the need for regular examinations to ensure consistent execution and performance of the control activities, while Principle 17 emphasizes the importance of addressing and communicating deficiencies.

Table **1**

2013 COSO Internal Control-Integrated Framework Components and Principles

Internal Control Component 1: Control Environment

Principle 1: Demonstrates commitment to integrity and values
Principle 2: Exercises oversight responsibility
Principle 3: Establishes structure, authority and responsibility
Principle 4: Demonstrates commitment to competence
Principle 5: Enforces accountability

Internal Control Component 2: Risk Assessment

Principle 6: Specifies suitable objectives
Principle 7: Identifies and analyzes risks
Principle 8: Assesses fraud risk
Principle 9: Identifies and analyzes significant change

Internal Control Component 3: Control Activities

Principle 10: Selects and develops control activities
Principle 11: Selects and develops general controls over technology
Principle 12: Deploys thorough policies and procedures

Internal Control Component 4: Information and Communication

Principle 13: Uses relevant information
Principle 14: Communicates internally
Principle 15: Communicates externally

Internal Control Component 5: Monitoring

Principle 16: Conducts ongoing and/or separate evaluations
Principle 17: Evaluates and communicates deficiencies

COSO 2013 Implementation

Each supporting principle is supplemented with points of focus offering additional direction. The 2013 framework also recognizes the integration among an organization's operations, reporting and compliance objectives. A further enhancement is the recognition of an organization's entity, division, operating unit and functional layers components.

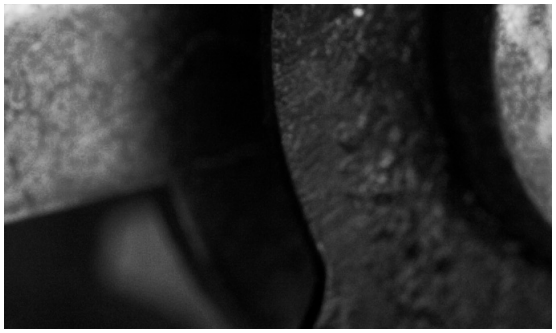
> "Organizations should evaluate **current** internal control structures against the **new framework.**"

The 2013 framework acknowledges that critical business transactions, such as sales and supply chain activities, span risk and influence concerns across various business objectives and functions. Greater internal control integration is needed to address such concerns. For example, inventory practices are a vital operations concern, as well as a crucial financial reporting concern. Likewise, safety issues relate to multiple organizational objectives. Such recognition helps organizations move beyond siloed internal control responses, identify control gaps and eliminate instances where redundant controls may exist for a single vulnerability.

Initial Planning for 2013 Internal Control Framework Implementation

INITIAL PLANNING FOR IMPLEMENTING the 2013 framework should include senior leaders, operational managers and others with internal control responsibilities. Those individuals have the greatest impact for establishing a positive internal control environment. They are also responsible for overseeing the implementation of more specific controls related to operations, reporting and compliance objectives.

Organizations function in dynamic environments. Individuals take different leadership roles. New IT components replace older hardware and software. Proposed compliance requirements become law. Given how much change occurs, organizations should evaluate current internal control structures against the new framework.



The 2013 framework specifies that a control be present (in place) and functioning (working as anticipated). Operational processes evolve in response, but existing controls might not recognize such change. That may result in control gaps. Long-standing controls may not incorporate the most effective design. In some cases, redundant controls may have been implemented by various organizational functions. Evaluating the existing internal control structure to ensure the coverage of each principle and the relative design effectiveness is a healthy exercise for any organization.

Within various organizations, internal control structures sit along a spectrum that ranges from informal actions that focus on just trying to record transactions to highly intentional, effectively controlled and mature controls. Upon examination, a business might conclude its control structure is near the mature, effectively controlled end of the spectrum. Such a business is likely already adhering to 2013 framework specifications. On the other hand, ad-hoc organizations that are not strongly controlled, are stale and/or highly dependent upon manual controls need to implement more material changes.

Table 2 lists four levels in internal control maturity, and the characteristics associated with each level. The table provides guidance for evaluating existing controls and any needs for improvement.

Table **2**

Four Maturity Levels for Internal Control

Level 1: Informal or Ad-hoc

- Control activities fragmented
- Control activities may be managed in “silo” situations
- Control activities dependent upon individual heroics
- Inadequate documentation and reporting methods
- Inadequate monitoring methods

Level 2: Standard

- Control awareness exists
- Control activities designed
- Control activities in place
- Some documentation and reporting methodology exists
- Automated tools and other control measures may exist, but are not necessarily integrated within all functions
- Accountability and performance monitoring requires improvement

Level 3: Managed and Monitored

- Key Performance Indicators (KPI) are defined for monitoring effectiveness
- Well-understood chains of accountability exist
- A formal controls framework exists
- Automated tools and other control measures are used to generate more standardized assessments

Level 4: Optimized

- Highly-automated control infrastructure
- Benchmarking, best practices and continuous improvement elements incorporated into monitoring efforts
- Real-time monitoring

COSO 2013 Implementation

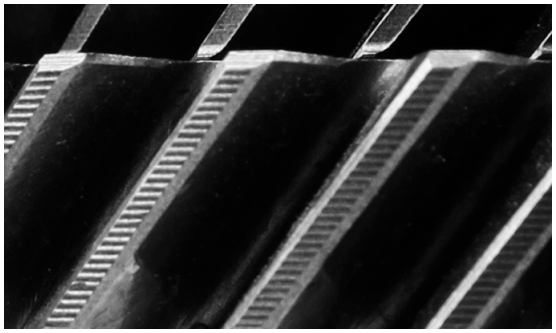
Numerous factors need to be considered when assessing the completeness of coverage and current maturity level of the organization's internal control structure across the significant processes. Internal changes require adapting existing controls or implementing new controls. The desired outcome of the COSO 2013 evaluation is to establish a layered control environment that incorporates all of the internal control principles and has a balance of automated and preventive controls that accompany management review and manual procedures. Various risk assessment factors —likelihood, impact, velocity and persistence—need to be considered in determining the appropriate maturity level for each control. Change in prioritizing resources is likely to occur based on the risk assessment under the new framework. In addition, more mature environments align the control activities with the relevant risk and operations key performance indicators.

> "Automated controls **reduce risks** associated with **human error or neglect.**"

As part of the evaluation, an organization should also consider how its internal control efforts align with the specific compliance requirements it faces. For some public corporations, the primary compliance requirement might be Sarbanes-Oxley. A health care organization may need to address Health Insurance Portability and Accountability Act (HIPAA) requirements, while a retailer may need to meet Payment Card Industry (PCI) requirements. The compliance standards relevant to the organization should be used as benchmarks for evaluating internal control effectiveness.

Organizations vary immensely in staffing resources, financial resources and other factors. Automating controls whenever possible and embedding control functions within routine processes represent improvement opportunities for virtually any organization.

Automated controls reduce risks associated with human error or neglect. IT access restrictions or application files that close following brief periods of inactivity are examples of automated controls. Higher level automated controls may include dashboard reporting tools that provide real-time updates or data mining tools that extract transaction anomalies from vast data sets.



Making control functions part of everyday activities mitigates the possibility that a deficiency could go unnoticed for a considerable span of time. Such embedding may include prompt reconciliations for financial transactions or brief worksite safety inspections each day.

Once internal controls have been designed, the organization can review, identify and remediate any unforeseen difficulties.

Long-term Benefits of Applying the 2013 COSO Internal Control-Integrated Framework

MEETING APPLICABLE COMPLIANCE MEASURES may provide impetus for implementing the 2013 framework, but the benefits extend far beyond satisfying regulatory requirements. Introduction of the revised framework presents a great opportunity to take a fresh look and determine if the way business is transacted could be more effective, efficient or automated to benefit the company.

Are processes scalable if the company experiences growth? Is automation being deployed to prevent adverse events, while also lowering labor costs? Are such automated controls standardized, so they can be transferred to a new location? Every business can benefit from asking such questions and having internal controls that are intentional and prevention-focused.

The paradigm used in examining internal control issues has a direct relationship to the outcome as well. That is why consultative assistance is so beneficial. Experts help attain that extra value, rather than approaching an internal control examination as an academic exercise that involves checking the right boxes. The updated framework provides direction for more effectively addressing various exposures that were not present or as prevalent in 1992, thereby more effectively mitigating the risks associated with adverse events. Migrating to the 2013 framework prompts an organization to engage in self-assessment, self-assessment that leads to identification of controls gaps, ineffective controls, redundant controls and potential improvements.

By ensuring that an effective internal controls framework is in place, an organization is better equipped to mitigate risks and respond to opportunities. Efficiency, trust and confidence follow, thereby enabling the organization to more effectively pursue its business strategies.

Weaver Services: A Closer Look

INTERNAL AUDIT. Weaver's customized internal audit process provides you with complete insight into your business operation so that you can make mission-critical decisions with confidence. Our risk advisory services team begins by implementing internal audit strategy designed to cover the critical risks that are significant across your key business functions. Our procedures are designed to gain an understanding and create confidence in your company's internal controls and related business risk mitigation efforts. We are vigilant and cognizant of changes in your business, environment and industry. Information on emerging trends, industry benchmarks and best practices adds value; we provide the qualitative, comparative financial performance analysis that can help you recognize the strengths, weaknesses and opportunities in your organization.

INTERNAL CONTROL EVALUATION. Whether your organization is in the early stages of development or a mature operation, Weaver's internal control evaluation services can build a foundation for long-term, strategic, entity-wide risk management and compliance monitoring. In this capacity, our role is to determine whether management's internal control is well designed, implemented and operating effectively.

Taking an independent, objective and disciplined approach, our team evaluates specific, relevant risks and the operating effectiveness of existing controls to mitigate those risks. While the responsibility for establishing and maintaining effective internal control belongs to management, we can make recommendations to more efficiently improve internal controls.

BUSINESS PROCESS IMPROVEMENT. Through Weaver's business process improvement (BPI) services, we improve your performance by streamlining systems, operational processes and performance measurement techniques that provide the basis for continuous improvement. We focus on leveraging existing investments and designing improvement efforts that meet the longer-term growth and profitability goals of a business.

The principal goal in business process analysis and improvement is to increase both efficiency and effectiveness of current processes. We strive to reduce organizational risks, integrate business processes with technology, prepare for successful implementation and create an aligned and streamlined set of business processes across the organization.

CONTACT US

Alyssa G. Martin, CPA, MBA
Partner-in-Charge
Risk Advisory Services
alyssa.martin@weaver.com

Weaver's risk advisory services are strategic, executable and measurable–and our nimble process is designed to help companies remain optimally functional as they identify and manage risk. We work closely with our clients to customize services that fit their existing staff structure and operations. Integral to this sensitive work, we believe our communication skills are as valuable as our technical knowledge and professional insight. You will experience thoughtful, purposeful communication throughout the process. Specific services we provide include:

- Business continuity planning
- Business process improvement
- Contract monitoring and compliance
- Enterprise risk management
- Internal audit
- Internal control evaluation
- Integrated financial and IT audit
- Performance audit and measurement
- Regulatory compliance
- Risk assessment
- Sarbanes-Oxley compliance

weaver
Assurance • Tax • Advisory