Fine tuning your internal controls with COSO
The CPA's role in maintaining security and promoting data privacy

Overview

COSO Internal Controls framework

Updated

Contents

Summary of key updates

Impact of COSO to business

Q&A
Let us know, which among the words comes into your mind first when you think about **internal controls**?
Internal control is a process, effected by an entity’s board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

Definition under the 2013 COSO Internal Control – Integrated Framework

- Geared to the achievement of objectives
- A process
- Effected by people
- Provide reasonable assurance
- Adaptable to the entity structure
In 1992, COSO published the original IC Framework (authored by PwC), which allows the management of an organization to
• establish,
• monitor,
• evaluate, and
• report on internal control.

The original IC Framework has gained widespread acceptance and use worldwide.

In 2013, COSO published the updated IC Framework (also authored by PwC) to ease use and application,

• considering changes in business and operating environments,
• articulating principles and clarifying requirements for effective internal control, and
• encouraging users to apply internal control to additional objectives.
COSO’s Internal Control and Enterprise Risk Frameworks

- Both framework adopt principles driven approach thus are suitable to most entities
- Geared towards seeking greater transparency and accountability
- Consider the increasing complexity and technological advancements of business environment
### Updated IC Framework Eases Use and Application

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

#### Risk Assessment
- **Specifies suitable objectives**
- **Assess fraud risk**
- **Identifies and analyzes risks**
- **Identifies and assesses significant changes**

#### Control Activities
- **Selects and develops control activities**
- **Selects and develops general controls over technology**
- **Deploys controls through policies and procedures**

#### Information and Communication
- **Generates/obtains and uses information**
- **Communicates internally**
- **Communicates externally**

#### Monitoring Activities
- **Performs ongoing and/or separate control evaluations**
- **Evaluates and communicates control deficiencies**

---

Fine tuning your internal controls with COSO
PwC
Summary of key updates

What is NOT fundamentally changing?

• Core definition of internal control
• Three categories of objectives and five components of internal control
• Each of the five components of internal control are required for effective internal control
• Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness
Summary of key updates

Update articulates principles as important characteristics of the components of internal control

- Principles are suitable and presumed relevant for all entities
- Principles can support achievement of a single, multiple, or overlapping objectives
- When principles are present and functioning, objectives are specified with sufficient clarity to assess risk and deploy controls to mitigate risk to acceptable level
- Applying principles provides a basis for checking what’s covered and what’s missing across the business—including dispersed and outsourced operations
Summary of key updates – what IS changing?

Control Environment

- Governance- Management’s philosophy and operating style
- Linkages between various components of internal control
- Organizational structure
- Integrity and ethical values
- Linking risk and performance
- Organizational complexities
- Roles and responsibilities alignment
Summary of key updates – what IS changing?

Risk Assessment

- Risk assessment process
- Risk severity
- Risk tolerances
- Impact of internal and external factors
- Fraud risk
Summary of key updates – what IS changing?

Control Activities

- Evolution of technology
- Automated controls vs. general controls over technology
- Control techniques
- General technology controls
- Policies and procedures vs. control activities
Summary of key updates – what IS changing?

Information and Communication

- Information quality
- External reporting information
- Information protection and reliability
- Information volumes and sources
- Impact of technology
- Communication with third parties
Summary of key updates – what IS changing?

Monitoring

- Monitoring activities terminology
- Establishing evaluations
- Technology and service providers use
What are driving the focus on internal controls?

Impact of COSO to your business, stakeholders, and users

Consequences of control failure—financial, reputational, regulatory
Accelerating pace of business change
Complex, interconnected businesses and systems
Complexity of “extended enterprise”

These factors are pushing us to rethink about controls

Desire for common standards (and efficiencies)
Increased regulatory scrutiny and stakeholder demand
Governance effectiveness requirements (Board requirement)
Digitisation/technological advancements
Design principles of a target operating model for internal controls

01. Structure and Governance
02. Communication, culture and training
03. Roles and responsibilities
04. Processes
05. Tools, technology and reporting
06. Working groups and integration
07. Accountability and performance management
01. Structure and governance

• Clear responsibility for oversight and assurance of business controls.

• Divorcing control operation and control review providing reliable and quantifiable independent assurance that is suitable for audit leverage.

• A simplified structure that reduces the risk created through multiple hand-offs.
• A behaviour and cultural shift in line with the seven critical behaviours.

• Business sees value in controls through greater understanding.

• Clear understanding of process and control principles (e.g. detective/preventative and good control design).
Design principles of a target operating model for internal controls

03. Roles and responsibilities

- Risk owners have clear understanding of the risk and how this is mitigated through controls.
- Clear roles and responsibilities for controls going through business change.
- SMART objectives set, and agreed, for each Risk and Control resource
Design principles of a target operating model for internal controls

04. Processes

- Consistent approach and focus to the management of risks and controls across the business.
- Documentation standards and guidelines.
- Fundamental processes captured and operational (e.g. Business change, reporting, incident management, training etc...).
05. Tools, technology and reporting

- Effective use of an appropriate tool(s).
- Leveraging existing sources of best practice.
- Company technology resources and future system landscape.
- Automation of control.
- Effective dashboard reporting.

Design principles of a target operating model for internal controls
Design principles of a target operating model for internal controls

06. Working groups and integration

- An awareness and clarity of the risk and response managed by the 1st line.

- Transparency in process and reporting so there is one view of the truth that is appropriate at all levels.

- Strong relationships and engagement within the business.
07. Accountability and performance management

- Clear accountability for controls and control failures within 1st line

- Clear accountability for risks (understanding of risk appetite and risk impact to the business).

- Incremental steps to embedding accountability and changing the culture. Progress mapped against these steps.

- Consistent reporting of leading indicators in control design and effectiveness.

- Internal control objectives within Business Unit plans and Director objectives as appropriate
These are the potential lead indicators for control failures:

- Accounting and reporting changes
- Usually prolonged success
- Autonomy and override
- Over reliance on 3rd line of defense
- Reliance on self-assessment
- Reliance on management integrity
- Wide scope for local interpretation
- Dominant management style
- Governance
- Inadequate resourcing

Fine tuning your internal controls with COSO
PwC
Identifying controls

Objective  Risk  Control  Alignment
In practice, stakeholder engagement and control design are key in achieving control effectiveness.

1. Context and stakeholder engagement
   - Understand the current state, engage with stakeholders, agree the process objectives and risk appetite

2. Process, risk and controls review
   - Walkthrough end-to-end process and identify risk sources. Understand key controls currently in place at the process level

3. Interpret, feedback and validation
   - Determine the right controls, using risk assessment, appetite and control objectives. Identify potential improvements, gaps or incomplete controls

4. Update and report
   - A process for updating, iterating and improving the control environment
A strategic perspective on internal control

- Internal control empowers employees
- Internal control helps in achieving important objectives
- Internal control is dynamic and changes with the business
Questions?